D-Link DFL-260E/860E/870/1660/2560/2560G

Network Security Firewall

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠危険	この表示を無視し、間違った使い方をすると、死亡または重傷を負うおそれがあります。
⚠警告	この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、間違った使い方をすると、傷害または物損損害が発生するおそれがあります。

記号の意味　⃠ してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠危険

⃠ 禁止
分解・改造をしない
火災、やけど、けが、感電などの原因となります。

⃠ 禁止
ぬれた手でさわらない
感電の原因となります。

⃠ 禁止
水をかけたり、ぬらしたりしない
内部に水が入ると、火災、感電、故障の原因となります。

⃠ 禁止
水などの液体（飲料水、汗、海水、ペットの尿など）でぬれた状態で触ったり、電源を入れたりしない
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止
各種端子やスロットに水などの液体（飲料水、汗、海水、ペットの尿など）をいれない。万が一、入ってしまった場合は、直ちに電源プラグをコンセントから抜く
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止
油煙、湯気、湿気、埃の多い場所、高温になる場所や熱のこもりやすい場所（火のそば、暖房器具のそば、こたつや布団の中、直射日光の当たる場所、炎天下の車内、風呂場など）、振動の激しい場所では、使用、保管、放置しない
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止
内部に金属物や燃えやすいものを入れない
火災、感電、故障の原因となります。

⃠ 禁止
砂や土、泥をかけたり、直に置いたりしない。また、砂などが付着した手で触れない
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止
電子レンジ、IH 調理器などの加熱調理機、圧力釜など高圧容器に入れたり、近くに置いたりしない
火災、やけど、けが、感電、故障の原因となります。

⚠警告

⃠ 禁止
落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない
故障の原因となります。

⃠ 禁止
発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
感電、火災の原因になります。
使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼ください。

⃠ 禁止
表示以外の電圧で使用しない
火災、感電、または故障の原因となります。

⃠ 禁止
たこ足配線禁止
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

❗
設置、移動のときは電源プラグを抜く
火災、感電、または故障の原因となります。

⃠ 禁止
雷鳴が聞こえたら、ケーブル / コード類にはさわらない
感電の原因となります。

⃠ 禁止
ケーブル / コード類や端子を破損させない
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障の原因となります。

❗
本製品付属の AC アダプタもしくは電源ケーブルを指定のコンセントに正しく接続して使用する
火災、感電、または故障の原因となります。

⃠ 禁止
各光源をのぞかない
光ファイバケーブルの断面、コネクタおよび本製品のコネクタや LED をのぞきますと強力な光源により目を損傷するおそれがあります。

⃠ 禁止
各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を接触させたり、ほこりが内部に入ったりしないようにする
火災、やけど、けが、感電または故障の原因となります。

⃠ 禁止
使用中に布団で覆ったり、包んだりしない
火災、やけどまたは故障の原因となります。

❗
ガソリンスタンドなど引火性ガスが発生する可能性のある場所や粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る
引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。

⃠ 禁止
カメラのレンズに直射日光などを長時間あてない
素子の退色、焼付きや、レンズの集光作用により、火災、やけど、けがまたは故障の原因となります。

❗
無線製品は病院内で使用する場合は、各医療機関の指示に従って使用する
電子機器や医療電気機器に悪影響を及ぼすおそれがあります。

⃠ 禁止
本製品の周辺に放熱を妨げるようなもの（フィルムやシールでの装飾を含む）を置かない
火災、または故障の原因となります。

❗
耳を本体から離してご使用ください
大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。

❗
無線製品をご使用の場合、医用電気機器などを装着している場合は、医用電気機器メーカーもしくは、販売業者に、電波による影響について確認の上使用する
医療電気機器に悪影響を及ぼすおそれがあります。

❗
高精度な制御や微弱な信号を取り扱う電子機器の近くでは使用しない
電子機器が誤作動するなど、悪影響を及ぼすおそれがあります。

❗
ディスプレイ部やカメラのレンズを破損した際は、割れたガラスや露出した端末内部に注意する
破損部や露出部に触れると、やけど、けが、感電の原因となります。

❗
ペットなどが本機に噛みつかないように注意する
火災、やけど、けがなどの原因となります。

⃠ 禁止
コンセントに AC アダプタや電源ケーブルを抜き差しするときは、金属類を接触させない
火災、やけど、感電または故障の原因となります。

⃠ 禁止
AC アダプタや電源ケーブルに海外旅行用の変圧器等を使用しない
発火、発熱、感電または故障の原因となります。

⚠警告

- ACアダプタもしくは電源プラグについたほこりは、拭き取る
  ほこりが付着した状態で使用すると、
  火災、やけど、感電または故障の原因となります。
- ACアダプタや電源ケーブルをコンセントに
  さしこむときは、確実に差し込む
  確実に差し込まないと、火災、やけど、
  感電もしくは故障の原因となります。
- 接続端子が曲がるなど変形した場合は、直ちに使用を中止する。
  また、変形をもとに戻しての使用も行わない
  端子のショートにより、火災、やけど、けが、
  感電または故障の原因となります。
- 各種接続端子を機器本体に接続する場合、斜めに差したり、
  差した状態で引っ張ったりしない
  火災、やけど、感電または故障の原因となります。
- 使用しない場合は、ACアダプタもしくは
  電源ケーブルをコンセントから抜く
  電源プラグを差したまま放置すると、火災、やけど、
  感電または故障の原因となります。
- お手入れの際は、ACアダプタもしくは
  電源ケーブルをコンセントから抜く
  抜かずに行うと、火災、やけど、感電または故障の原因となります。
- 禁止 SDやMicroSDカード、USBメモリの使用中は、
  カードやメモリを取り外したり、本製品の電源を切ったりしない
  データの消失、機器本体の故障の原因となります。
- 禁止 磁気カードや磁気を帯びたものを本製品に近づけない
  磁気カードのデータが消えてしまうおそれもしくは
  機器本体の誤作動の原因となります。
- ディーリンクジャパンが販売している無線機器は
  国内専用のため、海外で使用しない
  海外では国によって電波使用制限があるため、
  本製品を使用した場合、罰せられる場合があります。
  海外から持ち込んだディーリンク製品や並行輸入品を
  日本国内で使用する場合も同様に、罰せられる場合があります。

⚠注意

- 禁止 乳幼児の手の届く場所では使わない
  やけど、ケガまたは感電の原因となります。
- 静電気注意
  コネクタや電源プラグの金属端子に触れたり、
  帯電したものを近づけますと故障の原因となります。
- 禁止 コードを持って抜かない
  コードを無理に曲げたり、引っ張ると、
  コードや機器本体の破損の原因となります。
- 禁止 振動が発生する場所では使用しない
  故障の原因となります。
- 付属品の使用は取扱説明書に従う
  本製品の付属品は、取扱説明書に従い、
  他の製品に使用しないでください。機器の破損の原因となります。
- 禁止 破損したまま使用しない
  火災、やけどまたはけがの原因となります。
- 禁止 ぐらついた台の上や傾いた場所などの
  不安定な場所や高所には置かない
  落下して、けがなどの原因となります。
- 禁止 子供が使用する場合は、保護者が取扱いの方法を教え、
  誤った使い方をさせない
  けがや故障などの原因となります。
- 本製品を長時間連続使用する場合は、
  温度が高くなることがあるため、注意する。
  また、使用中に眠ってしまうなどして、
  意図せず長時間触れることがないようにする
  温度の高い部分に直接長時間触れると
  お客様の体質や体調によっては肌の赤みや
  かゆみ、かぶれ、低温やけどの原因となります。
- 禁止 コンセントにつないだ状態で、ACアダプタや
  電源コンセントに長時間触れない
  やけど、感電の原因となります。
- 一般の電話機やコードレス電話、テレビ、ラジオなどを
  お使いになっている近くで使用しない
  近くで使用すると、本製品が悪影響を及ぼす原因となる場合があるため、
  なるべく離れた場所で使用してください。
- 禁止 D-Linkが指定したオプション品がある場合は、
  指定オプションを使用する
  不正なオプション品を使用した場合、故障、破損の原因となります。

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。
この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- マニュアルなどに記載されている以外の方法でのご使用はやめてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。
- 本製品の開口部に物をさしこまないでください。火事や感電を引き起こすことがあります。
- 付属の AC アダプタもしくは電源ケーブルのみを使用してください。
- 感電を防止するために、本製品と周辺機器の電源ケーブルは、正しく接地された電気コンセントに接続してください。
- やむなく延長コードや電源分岐回路を使用する場合においても、延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは、電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動から本製品を保護するためには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたり躓いたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルや電源プラグを改造しないでください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いておいてください。
- 抜け防止機構のあるコンセントをご使用の場合、そのコンセントの取り扱い説明書に従ってください。
- 本製品は動作中に高温になる場合があります。本製品の移動や取り外しの際には、ご注意ください。
- 本製品は動作中に高温になる場合がありますが、手で触れることができる温度であれば故障ではありません。ただし長時間触れたまま使用しないでください。低温やけどの原因になります。
- 市販のオプション品や他社製品を使用する場合、当社では動作保証は致しませんので、予めご了承ください。
- 製品に貼られている製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

静電気障害を防止するために

静電気は、本製品内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、本製品に触れる前に、身体から静電気を逃がしてください。
さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、本製品を静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃がしてください。

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

3. 静電気に敏感な機器の取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。また、計画停電などが予定されている場合には、事前に本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

ラック搭載型製品に関する一般的な注意事項

ラックの安定性および安全性に関する以下の注意事項を遵守してください。また、システムおよびラックに付随する、ラック設置マニュアル中の注意事項や手順についてもよくお読みください。

警告 前面および側面のスタビライザを装着せずに、システムをラックに搭載すると、ラックが倒れ、人身事故を引き起こす場合があります。ラックにシステムを搭載する前には、必ずスタビライザを装着してください。

警告 接地用伝導体を壊したり、接地用伝導体を適切に取り付けないで装置を操作しないでください。適切な接地ができるかわからない場合、電気保安協会または電気工事士にお問い合わせください。

警告 システムのシャーシは、ラックキャビネットのフレームにしっかり接地される必要があります。接地ケーブルを接続してから、システムに電源を接続してください。電源および安全用接地配線が完了したら、資格を持つ電気検査技師が検査する必要があります。安全用接地ケーブルを配線しなかったり、接続されていない場合、エネルギーハザードが起こります。

- システムとは、ラックに搭載されるコンポーネントを指しています。コンポーネントはシステムや各種周辺デバイスや付属するハードウェアも含みます。
- ラックにシステム / コンポーネントを搭載した後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは 1 つのみとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。
- ラックに装置を搭載する前に、スタビライザがしっかりとラックに固定されているか、床面まで到達しているか、ラック全体の重量がすべて床にかかるようになっているかをよく確認してください。ラックに搭載する前に、シングルラックには前面および側面のスタビライザを、複数結合型のラックには前面用スタビライザを装着してください。
- ラックへの装置の搭載は、常に下から上へ、また最も重いものから行ってください。
- ラックからコンポーネントを引き出す際には、ラックが水平で、安定しているかどうか確認してから行ってください。
- コンポーネントレール解除ラッチを押して、ラックから、またはラックへコンポーネントをスライドさせる際は、指をスライドレールに挟まないよう、気をつけて行ってください。
- ラックに電源を供給する AC 電源分岐回路に過剰な負荷をかけないでください。ラックの合計負荷が、分岐回路の定格の 80 パーセントを超えないようにしてください。
- ラック内部のコンポーネントに適切な空気流があることを確認してください。
- ラック内の他のシステムを保守する際には、システムやコンポーネントを踏みつけたり、その上に立ったりしないでください。

注意 資格を持つ電気工事士が、DC 電源への接続と接地を行う必要があります。すべての電気配線が、お住まいの地域、および国の電気基準と規制に準拠していることを確認してください。

バッテリの取り扱いについて

警告 不適切なバッテリの使用により、爆発などの危険性が生じることがあります。バッテリの交換は、必ず同じものか、製造者が推奨する同等の仕様のものをご使用ください。バッテリの廃棄については、製造者の指示に従って行ってください。

安全にお使いいただくために

本書は、製品を正しくお使いいただくための取扱説明書です。
必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

製品保証規定は以下を参照ください。
https://www.dlink-jp.com/support/product-assurance-provision

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。
https://www.dlink-jp.com/support

目次

安全にお使いいただくために 2
ご使用上の注意 4
静電気障害を防止するために 4
電源の異常 4
ラック搭載型製品に関する一般的な注意事項 5
バッテリの取り扱いについて 5

まえがき 15

本マニュアルの対象者 15
表記について 15
例題 15

第 1 章 はじめに 16

1.1 D-Link NetDefendOS の機能 16
1.2 NetDefendOS アーキテクチャ 18
1.2.1 State ベースアーキテクチャ 18
1.2.2 NetDefendOS のビルディングブロック 18
1.2.3 基本的なパケットフロー 19
1.3 NetDefendOS パケットフロー 20

第 2 章 マネジメントとメンテナンス 24

2.1 NetDefendOS の管理 24
2.1.1 概要 24
2.1.2 管理アクセスの設定 25
2.1.3 管理者アカウント 29
2.1.4 Web インタフェース 30
2.1.5 CLI 接続 35
2.1.6 CLI の利用方法 38
2.1.7 CLI スクリプト 44
2.1.8 セキュアコピー 49
2.1.9 コンソールブートメニュー 51
2.1.10 RADIUS 管理認証 52
2.1.11 強化されたパスワード 55
2.1.12 詳細な管理設定 56
2.1.13 構成オブジェクトの設定 56
2.2 システムの日時設定 62
2.2.1 概要 62
2.2.2 日時の手動設定 62
2.2.3 外部タイムサーバの使用 64
2.2.4 日時設定の概要 66
2.3 イベントとログ取得 67
2.3.1 概要 67
2.3.2 ログメッセージ 67
2.3.3 ログレシーバのタイプ 68
2.3.4 Memory ログレシーバ（Memlog） 68
2.3.5 Syslog ログレシーバ 69
2.3.6 メールアラート 71
2.3.7 Severity フィルタとメッセージ例外 74
2.3.8 SNMP トラップ 74
2.3.9 詳細なログ設定 76
2.3.10 Logsnoop 76
2.4 モニタリング 79
2.4.1 リアルタイムモニタアラート 79
2.4.2 リンクモニタ 79
2.4.3 ハードウェアモニタ設定 81
2.4.4 メモリモニタ設定 82
2.5 SNMP 83
2.5.1 SNMP を使用した管理 83
2.5.2 永続する SNMP インタフェースインデックス 85
2.5.3 SNMP の詳細設定 86
2.6 診断ツール 87
2.6.1 概要 87
2.6.2 ping コマンド 87
2.6.3 stats コマンド 90
2.6.4 connections コマンド 91

2.6.5 dconsole コマンド 92
2.6.6 pcapdump コマンド 93
2.6.7 traceroute コマンド 95
2.6.8 frags コマンド 98
2.6.9 selftest コマンド 99
2.6.10 techsupport コマンド 100
2.7 メンテナンス 101
2.7.1 バージョン更新のアラート 101
2.7.2 自動更新メカニズム 102
2.7.3 コンフィグレーションのバックアップ 102
2.7.4 工場出荷時設定にリセットする 104
2.8 言語 106
2.9 診断と品質向上 107

第 3 章 基本機能 108

3.1 アドレス帳 108
3.1.1 概要 108
3.1.2 IP アドレス 108
3.1.3 イーサネットアドレス 110
3.1.4 アドレスグループ 110
3.1.5 自動生成されるアドレスオブジェクト 112
3.1.6 Address Book フォルダ 112
3.1.7 FQDN アドレスオブジェクト 113
3.1.8 FQDN グループ 117
3.2 IPv6 のサポート 118
3.3 サービス 125
3.3.1 概要 125
3.3.2 カスタムサービスの作成 127
3.3.3 ICMP サービス 129
3.3.4 カスタム IP プロトコルサービス 130
3.3.5 サービスグループ 130
3.3.6 カスタムサービスのタイムアウト 131
3.3.7 Path MTU Discovery 132
3.4 インタフェース 135
3.4.1 概要 135
3.4.2 イーサネットインタフェース 137
3.4.3 リンクアグリゲーション 144
3.4.4 VLAN 147
3.4.5 サービス VLAN 150
3.4.6 PPPoE 152
3.4.7 GRE トンネル 154
3.4.8 6in4 トンネル 156
3.4.9 ループバックインタフェース 160
3.4.10 インタフェースグループ 163
3.4.11 レイヤ 2 のパススルー 164
3.5 ARP 165
3.5.1 概要 165
3.5.2 ARP キャッシュ 165
3.5.3 ARP パブリッシュ 167
3.5.4 Neighbor キャッシュ 169
3.5.5 アドバンスド ARP 設定 170
3.6 IP ルールセット 171
3.6.1 ルールセットの概要 171
3.6.2 IP ポリシーの作成 173
3.6.3 Geolocation の使用 176
3.6.4. IP ルールセットのプロセス 178
3.6.5 複数の IP ルールセット 180
3.6.6 IP ルールセットフォルダ 184
3.6.7 構成オブジェクトグループ 184
3.6.8 ステートレスポリシー 187
3.6.9 IP ルールの作成 188
3.7 アプリケーションコントロール 190
3.8 スケジュール 199

3.9 証明書 202
3.9.1 概要 202
3.9.2 証明書のアップロードと使用 206
3.9.3 CRL 配布ポイントリスト 207
3.9.4 CA サーバアクセス 208
3.9.5 Windows CA サーバ要求の作成 210
3.10 DNS 設定 211

第 4 章 ルーティング 214

4.1 概要 214
4.2 スタティックルーティング 214
4.2.1 NetDefenOS のスタティックルーティング 215
4.2.2 スタティックルーティングの設定 219
4.2.3 ルートフェイルオーバ 224
4.2.4 ルートフェイルオーバのためのホストモニタリング 226
4.2.5 ルートフェイルオーバのアドバンスド設定 227
4.2.6 プロキシ ARP 228
4.2.7 ブロードキャストパケットの転送 229
4.3 ポリシーベースルーティング 232
4.4 ルートロードバランス 238
4.5 Active-Active セットアップ 242
4.6 仮想ルーティング 244
4.6.1 概要 244
4.6.2 簡単なシナリオ 245
4.6.3 ルーティングルールの欠点 246
4.6.4 仮想ルーティングが使用する IP ルールセット 248
4.6.5 複数の IP ルールセット 249
4.6.6 トラブルシューティング 249
4.7 OSPF 250
4.7.1 ダイナミックルーティング 250
4.7.2 OSPF 概念 252
4.7.3 OSPF コンポーネント 255
4.7.4 Dynamic Routing Rules（ダイナミックルーティングルール） 261
4.7.5 OSPF の設定 263
4.7.6 OSPF の例 266
4.7.7 OSPF トラブルシューティング 270
4.8 マルチキャストルーティング 272
4.8.1 概要 272
4.8.2 マルチキャストポリシーを使用してマルチキャストを転送する 273
4.8.3 IGMP 設定 276
4.8.4 IGMP 拡張設定 280
4.8.5 GRE を使用したマルチキャストトンネル 281
4.9 透過モード 283
4.9.1 透過モードの概要 283
4.9.2 インターネットアクセスを有効にする 287
4.9.3 透過モードの利用例 288
4.9.4 スパニングツリー BPDU のサポート 290
4.9.5 MPLS パススルー 291
4.9.6 透過モードのアドバンスド設定 291

第 5 章 DHCP サービス 292

5.1 概要 292
5.2 IPv4 DHCP クライアント 292
5.3 IPv4 DHCP サーバ 293
5.3.1 Static IPv4 DHCP Host（スタティック IPv4 DHCP ホスト） 296
5.3.2 Custom IPv4 Options（カスタム IPv4 オプション） 297
5.4 IPv4 DHCP リレー 297
5.5 IP プール 300
5.6 DHCPv6 302
5.6.1 DHCPv6 クライアント 302
5.6.2 DHCPv6 サーバ 304

第 6 章 アプリケーションレイヤのセキュリティ 308

6.1 アプリケーションレイヤゲートウェイ 308
6.1.1 概要 308
6.1.2 HTTP ALG 309
6.1.3 FTP ALG 321
6.1.4 TFTP ALG 334
6.1.5 SMTP ALG 336
6.1.6 POP3 ALG 344
6.1.7 IMAP ALG 349
6.1.8 PPTP ALG 352
6.1.9 SIP ALG 354
6.1.10 H.323 365
6.1.11 TLS ALG 390
6.1.12 DNS ALG 393
6.2 Web コンテンツフィルタリング 399
6.2.1 概要 399
6.2.2 IP ポリシーを使用した WCF の設定 400
6.2.3 IP Rule を使用した WCF セットアップの概要 402
6.2.4 WCF カテゴリ 406
6.2.5 WCF HTML ページのカスタム 411
6.2.6 WCF 性能ログ 413
6.3 メールフィルタリング 414
6.3.1 IP ポリシーベースのメールフィルタリング 414
6.3.2. DNSBL データベース 418
6.3.3 IP ルールを使用した SMTP アンチスパム 420
6.4 アンチウィルススキャン 423
6.4.1 概要 423
6.4.2 実行 424
6.4.3 アンチウイルスキャンのアクティブ化 426
6.4.4 ZoneDefense を使用したアンチウィルス 429
6.4.5 アンチウィルスキャッシュ 429
6.5 ファイルコントロール 431

第 7 章 脅威防御 434

7.1 アクセスルール 434
7.1.1 概要 434
7.1.2 IP spoofing 434
7.1.3 アクセスルール設定 435
7.2. IP レピュテーション 436
7.3 Botnet Protection 441
7.4 Denial-Of-Service Attacks（DoS）保護 442
7.4.1 概要 442
7.4.2 DoS 保護の設定 443
7.4.3 DoS 攻撃の例 444
7.5 Scanner Protection 447
7.6 侵入検知と防御 448
7.6.1 概要 448
7.6.2 IDP コンフィグレーションコンポーネント 449
7.6.3 IDP シグネチャとシグネチャグループ 450
7.6.4 Insertion/Evasion（挿入 / 回避）攻撃防止 452
7.6.5 IDP の設定 453
7.6.6 IDP イベントに対する SMTP ログレシーバ 455
7.6.7 最適な設定 456
7.7 しきい値ルール 457
7.8 ホストとネットワークのブラックリスト化 459
7.9 ZoneDefense 461

第 8 章 アドレス変換 465

8.1 概要 465
8.2 NAT（ダイナミックアドレス変換） 465
8.3 NAT プール 470
8.4 SAT（スタティックアドレス変換） 472
8.4.1 はじめに 472
8.4.2 One-to-One IP 変換 474
8.4.3 Many-to-Many IP 変換 476
8.4.4 Many-to-One IP 変換 478
8.4.5 ステートレス IP ルールセットのエントリで SAT を設定する 480
8.4.6 NAT を使用した SAT 482
8.4.7 ポート変換 484
8.4.8「SAT」が処理するプロトコル 485
8.4.9 IP ルールを使用した SAT ルールの設定 486
8.5 自動変換 491
8.5.1 NAT のみの変換 492
8.5.2 NAT/SAT 変換 493

第 9 章 ユーザ認証 495

9.1 概要 495
9.2 認証設定 496
9.2.1 設定の概要 496
9.2.2 ローカルデータベース 497
9.2.3 外部 RADIUS サーバの設定 500
9.2.4 外部 LDAP サーバ 502
9.2.5 認証ルール 507
9.2.6 HTTP 認証 508
9.2.7 MAC 認証 511
9.3 認証 HTML ページのカスタマイズ 512
9.4 認証を必要とする IP ポリシー 514
9.5 Brute Force 保護 516
9.6 User Identity Awareness 518
9.6.1 概要 518
9.6.2 Identity Awareness の設定 519
9.6.3 Identity Awareness のアクティビティをモニタする 520
9.7 多要素認証 521
9.8 RADIUS リレー 522
9.9 RADIUS アカウンティング 526
9.9.1 概要 526
9.9.2 RADIUS アカウンティングメッセージ 526
9.9.3 Interim Accounting メッセージ 528
9.9.4 RADIUS アカウンティングの設定 528
9.9.5 RADIUS アカウンティングセキュリティ 529
9.9.6 RADIUS アカウンティングと高可用性 529
9.9.7 無応答な RADIUS サーバに対処する 529
9.9.8 アカウンティングとシステムのシャットダウン 529
9.9.9 NAT での制約 529
9.9.10 詳細な RADIUS 設定 530

第 10 章 VPN 531

10.1 概要 531
10.1.1 VPN の必要性 531
10.1.2 VPN 暗号化 532
10.1.3 VPN の計画 532
10.1.4 鍵の配布 533
10.1.5 VPN の TLS 代替策 533
10.2 VPN クイックスタートガイド 533
10.2.1 事前共有鍵を使用した IPsec LAN to LAN 534
10.2.2 証明書を使用した IPsec LAN to LAN 535
10.2.3 事前共有鍵を使用した IPsec ローミングクライアント 536
10.2.4 証明書を使用した IPsec ローミングクライアント 538
10.2.5 事前共有鍵を使用した L2TP ローミングクライアント 538
10.2.6 証明書を使用した L2TP/IPsec ローミングクライアント 540
10.2.7 PPTP ローミングクライアント 540

10.3 IPsec 541
10.3.1 概要 541
10.3.2 IPsec トンネル 545
10.3.3 IPsec トンネルプロパティ 546
10.3.4 IPSec プロポーザルリスト 551
10.3.5 事前共有鍵 552
10.3.6 事前共有鍵を使用した LAN to LAN トンネル 553
10.3.7 IPSec ローミングクライアント 556
10.3.8 証明書を使用した IPSec 558
10.3.9 IPSec トンネル選択 562
10.3.10 IPsec IPv6 サポート 562
10.3.11 コンフィグモード 563
10.3.12 IKEv2 サポート 565
10.3.13 IKEv2 ローミングクライアントセットアップ 566
10.3.14 iOS ローミングクライアントの設定 571
10.3.15 IPsec プロファイルの使用 572
10.3.16 MOBIKE のサポート 576
10.3.17 IPSec トンネルモニタリング 576
10.3.18 証明書を使用した ID リスト 577
10.3.19 IPsec を使用した DiffServ 579
10.3.20 NAT トラバーサル 580
10.3.21 代替の LDAP サーバから CRL を取得する 581
10.3.22 IPSec の高度な設定 581
10.3.23 IPSec トラブルシューティング 584
10.4 PPTP/L2TP 597
10.4.1 PPTP サーバ 597
10.4.2 L2TP サーバ 598
10.4.3 L2TP/PPTP サーバアドバンスド設定 602
10.4.4 PPTP/L2TP クライアント 602
10.4.5 l2tp と pptp コマンド 604
10.5 L2TP バージョン 3 605
10.5.1 L2TPv3 サーバ 605
10.5.2 L2TPv3 クライアント 610
10.6 SSL VPN 612
10.6.1 概要 612
10.6.2 NetDefendOS に SSL VPN を設定する 613
10.6.3 SSL VPN クライアントのインストール 614
10.6.4 SSL 設定の例題 617

第 11 章 トラフィックマネジメント 619

11.1 トラフィックシェーピング 619
11.1.1 概要 619
11.1.2 NetDefendOS におけるトラフィックシェーピング 620
11.1.3 シンプルな帯域制限 622
10.1.4 双方向の帯域制限 623
11.1.5 チェーンを持つ Differentiated Limit の作成 624
11.1.6 優先度 625
11.1.7 パイプグループ 628
11.1.8 VPN とトンネルにおけるトラフィックシェーピング 630
11.1.9 トラフィックシェーピング推奨事項 630
11.1.10 トラフィックシェーピングの概要 631
11.1.11 パイプの例 631
11.2 IDP トラフィックシェーピング 634
11.2.1 概要 634
11.2.2 IDP トラフィックシェーピングの設定 634
11.2.3 プロセスフロー 635
11.2.4 Network を指定する重要性 635
11.2.5 P2P シナリオ 636
11.2.6 トラフィックシェーピングオブジェクトの参照 636
11.2.7 帯域幅制限の代わりの保証 637
11.2.8 ログへの出力 637

11.3 サーバロードバランシング 638
11.3.1 概要 638
11.3.2 SLB 分配アルゴリズム 639
11.3.3 Stickiness の選択 639
11.3.4 接続レートアルゴリズムとスティッキーな接続 640
11.3.5 サーバヘルスモニタリング 641
11.3.6 サーバ接続失敗後の動作 642
11.3.7 SLB の設定 643

第 12 章 High Availability（高可用性） 646

12.1 概要 646
12.2 High Availability（高可用性）メカニズム 648
12.3 High Availability（高可用性）設定 651
12.3.1 ハードウェアセットアップ 651
12.3.2 HA セットアップのウィザード 653
12.3.3 手動の HA セットアップ 654
12.3.4 クラスタ機能の正しい検証 655
12.3.5 ユニークな共有 MAC 655
12.4 HA（高可用性）の問題 656
12.5 HA クラスタの更新 658
12.6 リンクモニタと HA 659
12.7 High Availability（高可用性）アドバンスド設定 659

第 13 章 詳細設定 660

13.1 IP レベル設定 660
13.2 TCP レベル設定 664
13.3 ICMP レベル設定 668
13.4 ステート設定 668
13.5 接続タイムアウト設定 669
13.6 プロトコル毎のサイズ制限 670
13.7 フラグメント化の設定 671
13.8 ローカルフラグメントリアセンブリ設定 674
13.9 SSL/TLS 設定 675
13.10 その他の設定 677

付録 A セキュリティ更新サービス 678

付録 B IDP シグネチャグループ 681

付録 C アンチウィルス MIME ファイルタイプ 684

付録 D OSI 参照モデル 688

付録 E DFL-260E/860E のポートベース VLAN 689

付録 F 初期設定 691

付録 G 登録＆アクティベーション手順 693

Introduction 693
Apply for a D-Link Membership 693
D-Link NetDefend UTM Subscription 696
Activate your update service of UTM firewall 697
Extend your NetDefend UTM Update Service 699

付録 H Identity Awareness Agent (IDA) のインストールと管理 702

IDA Overview 702
IDA Installation 702
IDAManagement 703

付録 I REAT API の使用方法 707

Introduction 707
Authentication 708
Listing Currently Authenticated Users 708
Listing Information about a Single Authenticated User 709
Adding a New Authenticated User 709
Ending Authentication of a User 710

Server Load Balancing 711
Writing the Server Software 712
Error Messages from a POST Operation 712
NetDefendOS Generated Log Event Messages 712
Viewing Server Status 713
Blacklist Control 713
Adding a New Blacklist Entry 713
Deleting a Blacklist Entry 714
Listing Blacklist Entries 715
Neighbor Cache 715
Statistics Retrieval 716
About Information 717

まえがき

本マニュアルの対象者

本マニュアルは NetDefendOS が動作する D-Link ファイアウォール設定および管理を行う管理者向けに記載しています。また、本マニュアルを利用する管理者がネットワークとネットワークセキュリティの基本的な知識を持っていることを前提にしています。

表記について

本書は章およびサブセクションに分かれており、章の先頭にサブセクションの項目について記載しています。

ユーザインタフェースの項目を表すテキストは**太字**で表しています。

例題

例題は、以下のとおり先頭に例題と記載しています。例題には、CLI と Web インタフェースを使用しています。すべての CLI コマンドについては「CLI Reference Guide」を参照してください。

例題 1

例題の表記

ここには、この例題によって実現しようとしている内容を記載します。説明のために図を使用する場合があります。

CLI

コマンドラインインタフェースの例を示します。コマンドプロンプトに続いてコマンドを記載します。

```
DFL-xxxx:/> somecommand someparameter=somevalue
```

Web Interface

Web インタフェースの例を示します。メニュー項目や入力データについて、以下のように手順で記載します。

1. **Item X** > **Item Y** > **Item Z** の順にメニューをクリックします。
2. 以下の通り入力します。
   - DataItem1: datavalue1
   - DataItem2: datavalue2

第 1 章 はじめに

この章では NetDefendOS の主要な機能の概要を説明します。

- 「1.1 D-Link NetDefendOS の機能」
- 「1.2 NetDefendOS アーキテクチャ」
- 「1.3 NetDefendOS パケットフロー」

1.1 D-Link NetDefendOS の機能

D-Link NetDefendOS は、D-Link ファイアウォールハードウェア製品を実行する基本のソフトウェアエンジンです。

ネットワークセキュリティ・オペレーティングシステムとしての NetDefendOS

NetDefendOS は、ネットワークセキュリティオペレーティングシステムとして設計されており、高い信頼性に加え、非常に細やかな制御と高いスループット性能を特徴に持っています。UNIX や Microsoft Windows™ などの標準的なオペレーティングシステムで構築された製品と比較すると、NetDefendOS はすべてのサブシステムをシームレスに統合し、セキュリティ攻撃へのリスクを最小限にするためにすべての機能に徹底した管理者制御を提供します。

NetDefendOS オブジェクト

管理者の見解を反映した NetDefendOS では、論理的な構成要素やオブジェクトの設定を通じて操作をビジュアル化しています。このため制限のない多彩な方法で製品の設定を行うことができます。詳細な制御により、ネットワーク管理者のセキュリティシナリオに対して非常に多くの要件に合致することができます。

主要な機能

NetDefendOS は、広範囲にわたる多機能のネットワークオペレーティングシステムであり、最も基本的な機能として以下の項目をサポートしています。

機能	説明
IP ルーティング	マルチキャストルーティングをはじめスタティックルーティング、（OSPF を使用した）ダイナミックルーティング、仮想ルーティングを含む IP ルーティングに多くのオプションを提供しています。さらに、VLAN、経路モニタリング、プロキシ ARP、および透過機能などもサポートしています。詳しくは、「第 4 章 ルーティング」を参照してください。
ファイアウォールポリシー	NetDefendOS には、TCP、UDP、ICMP などの広範囲のプロトコルに対するステートフルインスペクションベースのファイアウォール機能があります。管理者は、送信元 / 送信先のネットワーク / インタフェース、プロトコル、ポート、ユーザ証明書、時刻などに基づいた詳しいファイアウォールポリシーを定義することが可能です。「3.6 IP ルールセット」に、NetDefendOS がどのトラフィックを許可または拒否するかを決定するポリシーの設定方法について記載しています。
アドレス変換	セキュリティの理由だけではなく機能性のために、ポリシーベースのアドレス変換をサポートしています。ダイナミックアドレス変換（NAT）はもちろん、スタティックアドレス変換（SAT）もサポートし、多くのアドレス変換のタイプに対応しています。詳しくは、「第 8 章 アドレス変換」を参照してください。
VPN（Virtual Private Network）	NetDefendOS は、仮想プライベートネットワーク（VPN）ソリューションをサポートしています。また、独立した VPN 接続のために定義可能なセキュリティポリシーを使用した SSL VPN をはじめ IPsec、L2TP、L2TPv3 および PPTP をサポートしています。詳しくは、「第 10 章 VPN」を参照してください。
TLS 終端	NetDefendOS は、TLS 終端機能をサポートしており、D-Link ファイアウォールが HTTP Web ブラウザクライアントによる接続のためのエンドポイントとして機能できます。詳しくは、「6.1.11 TLS ALG」を参照してください。
アプリケーションコントロール	NetDefendOS は、特定のアプリケーションに関連するデータ接続を識別して、ブロックまたはトラフィックシェーピングなどのデータストリーム用に定義された操作を実行できます。アプリケーションの例は、BitTorrent ピアツーピアストリーミングですが、Facebook など特定の Web サイトへのアクセスにも関連します。 詳しくは、「3.7 アプリケーションコントロール」を参照してください。
アンチウィルススキャン	NetDefendOS は、統合されたアンチウィルス機能をサポートしています。ファイアウォールを通過するトラフィックは、ウィルスを綿密にスキャンして分類し、ホストに送信したウィルスはブラックリストに追加され、ブロックされます。詳しくは、「6.4 アンチウィルススキャン」を参照してください。
侵入者検知と防御	サービスとアプリケーションの弱点へのアプリケーション層攻撃を軽減するために、強力な侵入者検知と防御（IDP：Intrusion Detection and Prevention）エンジンを提供します。IDP エンジンは、ポリシーベースで高性能のスキャンにより攻撃者を検出し、システムの保護を行い、さらに攻撃するホストをオプションでブラックリストに加えることができます。IDP 機能に関する詳しい情報は、「7.6 侵入検知と防御」を参照してください。
Web コンテンツフィルタリング	Web 利用のポリシーに従って、不適当と思われる Web コンテンツをフィルタするためのさまざまなメカニズムを提供します。Web コンテンツフィルタリング（WCF）では、URL に基づいて Web コンテンツをブロックします。Web サイトをホワイトリストまたはブラックリスト化することも。詳しくは、「6.2 Web コンテンツフィルタリング」を参照してください。
トラフィック管理	NetDefendOS は、トラフィックシェーピング、しきい値ルール（特定モデルのみ）、およびサーバロードバランシング機能を通じて広いトラフィック管理機能を提供します。トラフィックシェーピング機能は、帯域の制限と分散を可能にします。しきい値ルールは、ネットワークトラフィックに警告を送信したり、または制限を行う細かいしきい値を指定することができます。サーバロードバランシングは、NetDefendOS が動作中のデバイスが複数ホストにネットワーク負荷を分散することを可能にします。詳しくは、「第 11 章 トラフィックマネジメント」を参照してください。。

機能	説明
ユーザ認証	NetDefendOS デバイスは、保護されたリソースへのユーザアクセスを制限することができます。複数のローカルユーザベースと複数の外部 RADIUS サーバがサポートされています。異なる種類のトラフィックに対しては、それぞれ異なる認証ポリシー / 認証スキームを定義することができます。また、NetDefendOS では User Identity Awareness がサポートされています。これにより、Windows ベースのクライアントは、Windows Active Directory サーバで認証されると NetDefendOS に認証ステータスがリレーされます。詳しくは、「第 9 章 ユーザ認証」を参照してください。
マネジメントとメンテナンス	NetDefendOS デバイスの管理は、Web ベースユーザインタフェース（WebUI）またはコマンドラインインタフェース（CLI）経由で可能です。さらに、NetDefendOS は、詳細なイベントとログ取得機能に加え SNMP を経由したモニタリングもサポートしています。詳しくは、「第 2 章 マネジメントとメンテナンス」を参照してください。
高可用性	高可用性（High Availability：HA）は、セカンダリ D-Link ファイアウォールへの自動フォールトトレラントフェイルオーバーにより実現されます。2 台のシステムはクラスタとして動作し、1 台がアクティブな状態、もう 1 台がパッシブな状態となり、アクティブなシステムのミラーリングを行います。詳しくは、「第 12 章 High Availability（高可用性）」を参照してください。 注意 HA 機能は、DFL-260E および DFL-860E ではご利用になれません。
ZoneDefense	NetDefendOS は、ZoneDefense を使用している外部スイッチの制御を行います。これにより、NetDefendOS は望ましくないネットワークトラフィックの送信元であるホストを含むネットワークの一部を隔離することができます。詳しくは、「7.9 ZoneDefense」を参照してください。
仮想ルータ	2 個以上の個別の NetDefendOS ルーティングテーブルを使用して、1 つの D-Link ファイアウォールに独立した仮想ルータを作成することができます。NetDefendOS のシングルバージョンが動作していても、異なるトラフィックセットが 1 つの D-Link ファイアウォール内で完全に独立するように、個別の IP ルールまたは他の IP ポリシーのセットを作成することができます。詳しくは、「4.6 仮想ルーティング」を参照してください。
IPv6	IPv6 アドレスはインタフェースおよびルールセット内でサポートされます。本機能は、初期値では無効であり、明示的にグローバルかつイーサネットインタフェースで有効にする必要があります。本機能に関する詳しい情報は、「3.2 IPv6 のサポート」を参照してください。
REST API	NetDefendOS の一部の機能は、外部コンピュータ上で動作するプログラムによって制御可能であり、NetDefendOS REST API を利用します。API については関連セクションで説明しますが、詳細は「付録 I REAT API の使用方法」をご参照ください。

上のリストに加えて、NetDefendOS には RADIUS アカウンティング、DHCP サービス、Denial-of-Service (DoS) 攻撃に対する保護、PPPoE のサポート、GRE、ダイナミック DNS サービスなどの多くの機能があります。

NetDefendOS のドキュメント

このドキュメントを注意深くお読みになり、NetDefendOS 製品の多くの機能についてご確認ください。このドキュメントに加え、さらに別冊のドキュメントも注意して読むことをお勧めします。

- 「CLI Reference Guide」は、NetDefendOS のすべてのコンソールコマンドと NetDefendOS 設定オブジェクトについて詳しく記載しています。
- 「Log Reference Guide」は、NetDefendOS のすべてのログイベントメッセージについて詳しく記載しています。
- NetDefendOS で利用可能なすべてのアプリケーションコントロールのシグネチャの詳細は「NetDefendOS Application Control Signatures」を参照してください。

これらのドキュメントは共に NetDefendOS 操作にとって重要なドキュメントです。

注意 DFL シリーズでは下記ポートがデフォルトの管理ポートとなるため、必ず有効にしてご利用ください。無効にすると利用できなくなります。

- DFL-260E LAN ポートすべて（前面パネル 1-5）
- DFL-860E LAN ポートすべて（前面パネル 1-8）
- DFL-870 LAN1（前面パネル 4）
- DFL-1660 LAN1（前面パネル 4）
- DFL-2560 LAN1（前面パネル 7）
- DFL-2560G LAN1（前面パネル 7）

1.2 NetDefendOS アーキテクチャ

本セクションでは、NetDefendOS ソフトウェア製品の全体構造を見て、設計の背景にある重要なコンセプトの中からいくつかを説明します。

1.2.1 State ベースアーキテクチャ

NetDefendOS アーキテクチャは、ステートベースのコンセプトで作られています。従来の IP ルータやスイッチはすべてのパケットを検査し、パケットヘッダ情報に基づいて転送するかどうかを決めていましたが、これを使用すると、パケットはコンテキストのどんな意味にも関係なく転送されるため、基本的には複雑なプロトコルを検出して、それを分析し、対応するセキュリティポリシーを実行することはできません。

ステートフルインスペクション

一方、NetDefendOS デバイスは、接続単位をベースにトラフィックを検証して転送する、ステートフルインスペクションと呼ばれる技術を搭載しています。つまり、NetDefendOS は、新しい接続が確立されると情報やステートを検出し、その接続の寿命まではステートテーブルにそれらを保持します。NetDefendOS は、これを使用することでネットワークトラフィックのコンテキストを理解できるため、デバイスの詳細なトラフィックスキャン、帯域管理などの多くの機能を可能にします。

さらに、スケーラブルで先進的な設計を使用して、高スループット性能を提供します。ステートフルインスペクションを実装する NetDefendOS サブシステムを、ドキュメンテーションの中で NetDefendOS ステートエンジンと呼ぶことがあります。

1.2.2 NetDefendOS のビルディングブロック

NetDefendOS 内のビルディングブロックの基本は、インタフェース、論理オブジェクトおよび各ルールタイプ（またはルールセット）です。

インタフェース

インタフェースは、ファイアウォールを通過するネットワークトラフィックの出入り口です。インタフェースなしでは NetDefendOS システムはトラフィックを送受信する手段はありません。NetDefendOS では、いくつかのインタフェースタイプをサポートしています。NetDefendOS は、インタフェースタイプとして物理インタフェース、物理サブインタフェースおよびトンネルインタフェースをサポートしています。

- 物理インタフェース - 実際の物理イーサネットインタフェースに対応しています。
- サブインタフェース - VLAN と PPPoE インタフェースがあります。
- トンネルインタフェース - VPN トンネルを経由したトラフィックの送受信に使用されます。

インタフェースシンメトリ

NetDefendOS は Symmetric（対称的）に設計されています。これはデバイスのインタフェースがネットワークトポロジにおいて「安全な内側」/「危険な外側」に固定されないということを意味します。「内側」/「外側」の定義については管理者によって設定が可能です。

論理的オブジェクト

論理オブジェクトは、ルールセットによって使用をあらかじめ定義されているビルディングブロックとして見なされます。例えば、アドレス帳はホストとネットワークアドレスを表す名前を持つオブジェクトを持っています。論理オブジェクトの別の例としてはサービス、特定のプロトコルの表示およびポートの組み合わせがあります。また、重要なオブジェクトは、アプリケーションレイヤゲートウェイ（ALG）オブジェクトで、HTTP、FTP、SMTP および H.323 などの特定のプロトコルに追加パラメータを定義するために使用されます。

NetDefendOS ルールセット

最後に、各ルールセット内に定義したルールは、NetDefendOS セキュリティポリシーを実際に実行するために使用されます。多くの基本的なルールは IP ルールセットで、アドレス変換やサーバロードバランシングの実行をはじめ、レイヤ 3 フィルタリングポリシーを定義するために使用されます。トラフィックシェーピングルールセットは、帯域管理のポリシーを定義し、IDP ルールセットは、IDP エンジンなどの動作を制御します。

1.2.3 基本的なパケットフロー

このセクションでは、NetDefendOS デバイスによって送受信されるパケットに対するステートエンジン内のフローの基本を記述します。以下の記述は単純化されており、すべてのシナリオに完全には適用できませんが、基本的な考え方は、全ての NetDefendOS システムに有効です。

1. イーサネットフレームは、システム内のイーサネットインタフェースのいずれかで受信します。基本的なイーサネットフレーム検証が実行され、フレームが不正である場合、パケットは廃棄されます。

2. パケットは送信元インタフェースに関連づけされます。送信元インタフェースは、以下の通り決定されます。

- イーサネットフレームに VLAN ID（Virtual LAN identifier）が含まれる場合、システムは VLAN ID を持つ VLAN インタフェースをチェックします。一致するインタフェースが見つかると、その VLAN インタフェースがパケットの送信元インタフェースになります。一致したインタフェースが見つからない場合、パケットは廃棄され、イベントがログに出力されます。

- イーサネットフレームが PPP ペイロードを含む場合、システムは一致する PPPoE インタフェースをチェックします。一致するインタフェースが見つかると、そのインタフェースがパケットの送信元インタフェースになります。一致したインタフェースが見つからない場合、パケットは廃棄され、イベントがログに出力されます。

- 上のいずれにも当てはまらない場合、受信イーサネットインタフェースがパケットの送信元インタフェースになります。

3. パケット内の IP データは、NetDefendOS Consistency チェッカーに送られます。Consistency チェッカーはパケット上でチェックサム、プロトコルフラグ、パケット長などの検証を含む多くの健全性のチェックを行います。Consistency チェックに失敗すると、パケットは廃棄され、イベントがログに出力されます。

4. 到着するパケットのパラメータが照合され、既存の通信が検索されます。これには多くのパラメータが使用され、送信元インタフェース、送信元 / 送信先 IP アドレス、IP プロトコルなどが含まれます。

一致するエントリが見つからない場合、本手順から手順 9 を含む接続確立の処理が開始されます。一致するエントリが見つかった場合、手順 10 の送信処理を継続します。

5. 新しい接続の送信元アドレスが受信インタフェースで許可されるかどうかを確認するために、アクセスルールが検証されます。アクセスルールが一致すると、リバース経路検索が行われます。つまり、デフォルトでは、その受信インタフェース上への経路を定義されているネットワークに所属する送信元アドレスだけが許可されます。リバース検索では、ルーティングテーブルを参照し、該当ネットワークがインタフェース上の宛先ネットワークとして存在することを確認します。アクセスルールまたはリバース経路検索において送信元 IP が不正であると検出された場合、パケットは廃棄され、イベントがログに出力されます。

6. 適切なルーティングテーブルを使用して経路検索が行われます。これにより、接続に使用される送信先インタフェースが決定します。

7. IP ルールセットを照合して、パケットに一致するエントリが検索されます。照合処理で使用されるパラメータの一部は、以下の通りです。
- 送信元と送信先インタフェース
- 送信元と送信先ネットワーク
- IP プロトコル（例 : TCP、UDP および ICMP）
- TCP/UDP ポート
- ICMP タイプ
- 定義済みスケジュールを参照する時間

一致するエントリが見つからない場合、パケットは廃棄されます。

新しい接続に対して一致するルールが検出されると、ルール内のアクションパラメータにより実行される処理が決定されます。Action が「Drop」の場合、パケットは廃棄され、そのルールのログ設定に従ってイベントがログに出力されます。

Action が「Allow」の場合、パケットはシステムの通過を許可されます。同じ接続に属するサブシーケンスのパケットを照合するための接続テーブルに、対応するステートが追加されます。また、IP プロトコルとポートが合致した「Service」オブジェクトには「ALG」（アプリケーションレイヤゲートウェイ）オブジェクトへの参照情報が含まれている場合があります。この情報はステート内に記録され、NetDefendOS は接続中のアプリケーションレイヤ処理が必要であることを認識します。

最後に、新しい接続のオープンは、ルール内のログ設定に従ってログに出力されます。

参照 **追加のアクション**

実際にはアドレス変換、サーバロードバランシングなどの有効な追加アクションが多くあります。トラフィックの廃棄と許可の基本的な概念は、同じです。

8. IDP ルールセットは、IP ルールセットと同じ方法で検査が行われます。一致するデータが検出されると、IDP データはステートに記録されます。これにより、この接続に属するすべてのパケットに対して IDP スキャンが行われることが認識されます。

9. トラフィックシェーピングとしきい値制限のルールセットが検索されます。一致するデータが見つかると、対応する情報はステートに記録されます。これにより、接続における適切なトラフィック管理が可能となります。

10. ステート内の情報により、NetDefendOS において到着パケットに対する処理が決定されます。
- ALG 情報が存在するか、IDP スキャンが実行される場合、パケットのペイロードは TCP Pseudo-Reassembly サブシステムによって処理され、そのトラフィックをさらに解析または変換するために、異なるアプリケーションレイヤゲートウェイとレイヤ 7 スキャンエンジンが使用されます。
- パケットのコンテンツがカプセル化（IPsec、L2TP/PPTP または他のタイプのトンネルされたトラフィック）されている場合、インタフェースの照合のためにインタフェースリストがチェックされます。エントリの一致が見つかると、パケットは非カプセル化され、ペイロード（プレーンテキスト）は、トンネルインタフェースと一致する送信元インタフェースにて、再び送信されます。つまり、この処理は上の手順 3 より続いています。
- トラフィック管理情報が存在する場合、パケットはキューにセットされるか、トラフィック管理に紐づくアクションに従います。

11. 最後に、パケットはステートに従って送信先インタフェースに送信されます。送信先インタフェースがトンネルインタフェースまたは物理サブインタフェースである場合、暗号化やカプセル化のような追加処理が行われます。

以下のセクションでは、NetDefendOS を経由したパケットの流れを示した図で説明しています。

1.3 NetDefendOS パケットフロー

本セクションで示す図は、NetDefendOS ステートエンジンを経由するパケットフローのサマリです。3 つの図は連続したフローとなっています。これらの図を理解する必要はありませんが、NetDefendOS を設定する場合に参考になる場合があります。

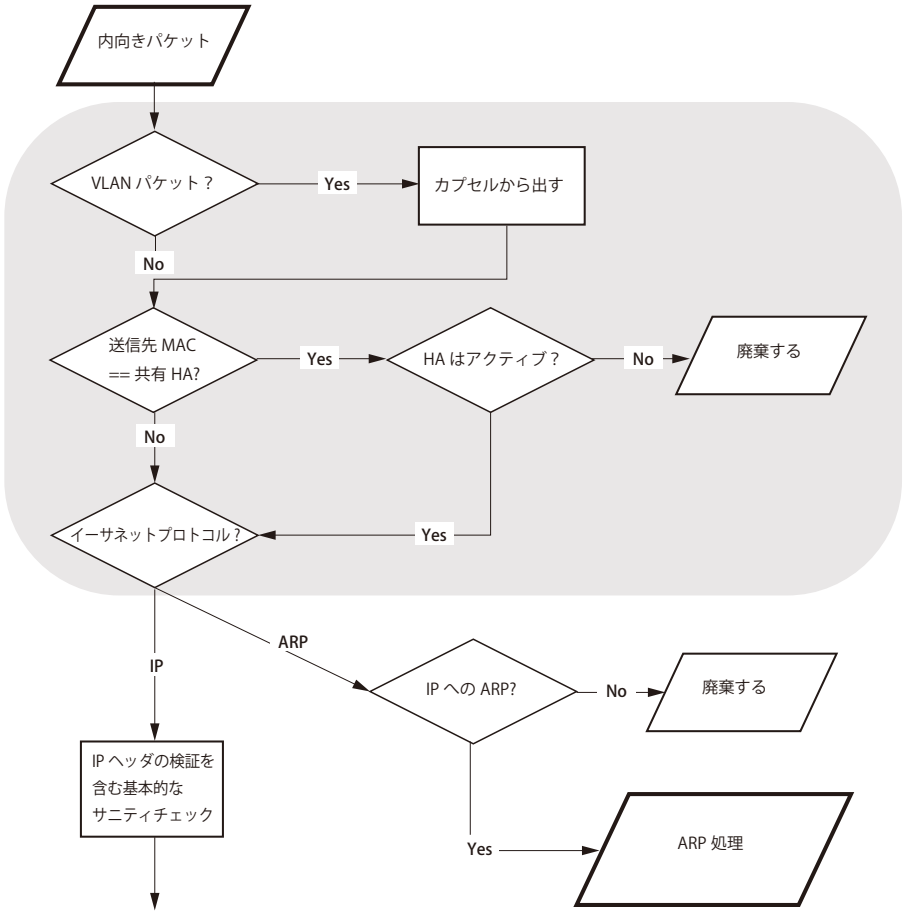


図 1-1　パケットフロー図 1

パケットフローは、次のページに続きます。

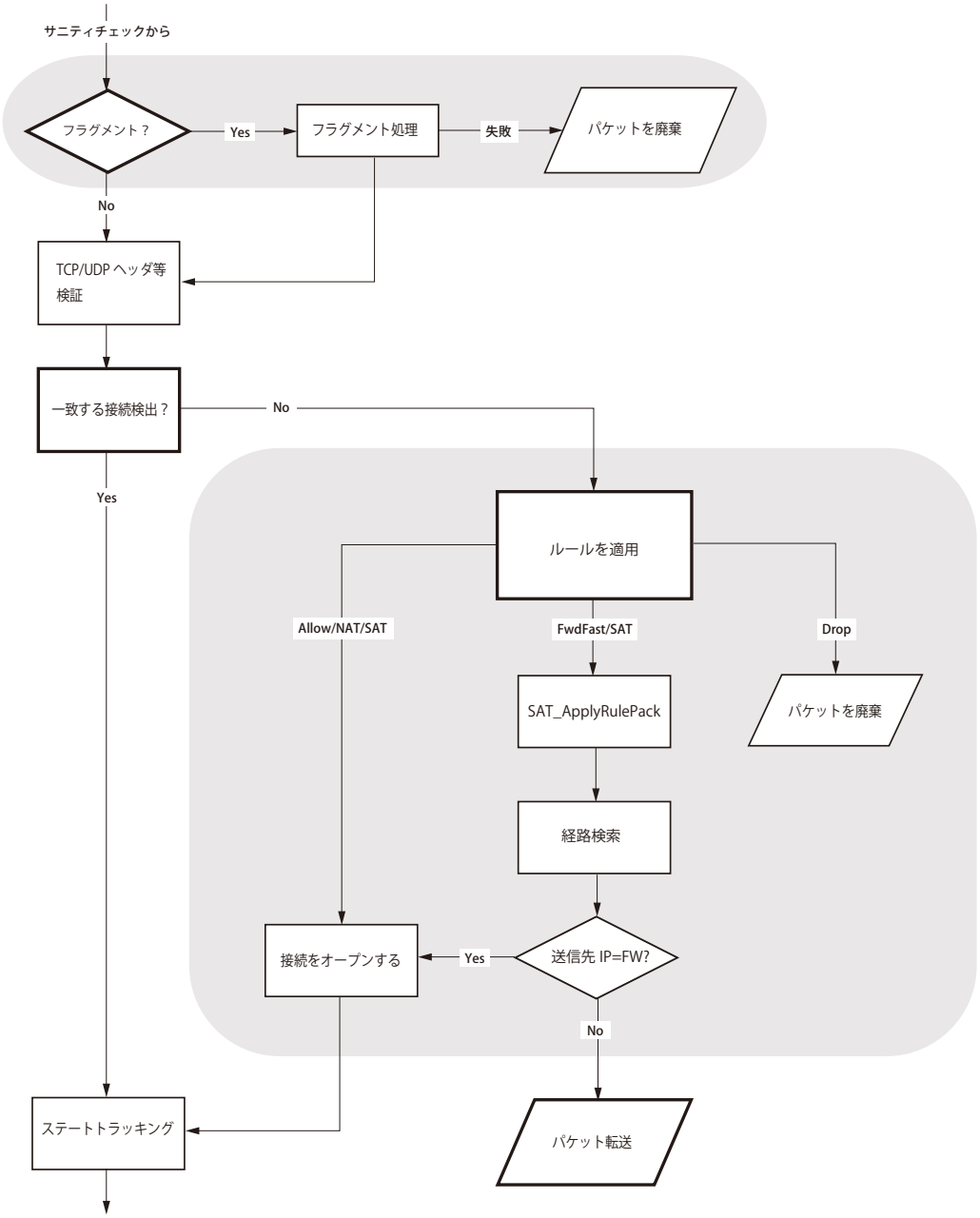


図 1-2　パケットフロー図 2

パケットフローは、次のページに続きます。

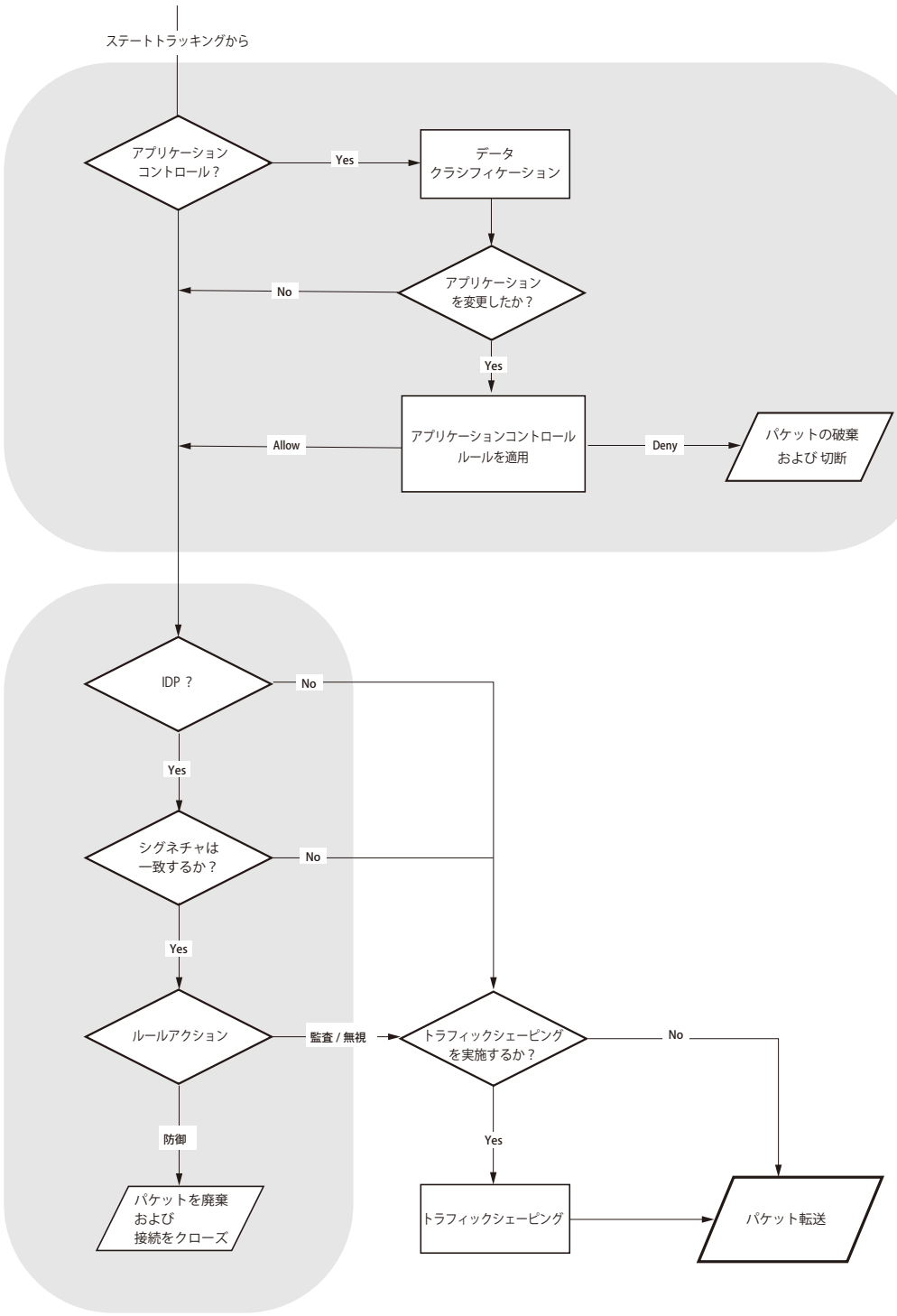


図 1-3　パケットフロー図 3

ルールの適用

以下の図では、前述の「図 1-2 パケットフロー図 2」における「ルールの適用」機能の詳しいロジックについて表しています。

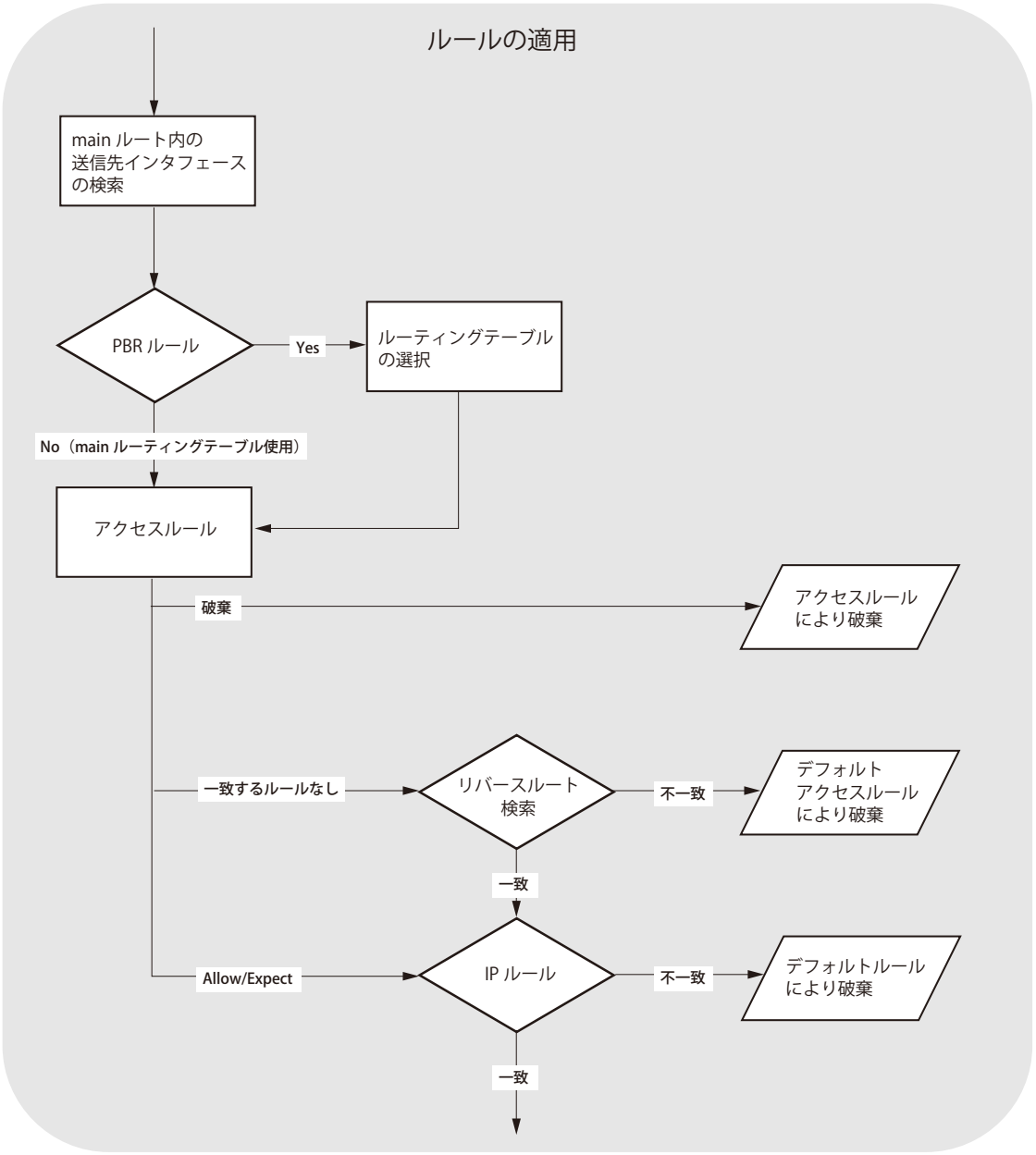


図 1-4　「ルールの適用」に関するロジックの詳細

第 2 章 マネジメントとメンテナンス

この章では、NetDefendOS のステータスに関係した操作とメンテナンスについて記述します。

- 「2.1 NetDefendOS の管理」
- 「2.2 システムの日時設定」
- 「2.3 イベントとログ取得」
- 「2.4 モニタリング」
- 「2.5 SNMP」
- 「2.6 診断ツール」
- 「2.7 メンテナンス」
- 「2.8 言語」
- 「2.9 診断と品質向上」

2.1 NetDefendOS の管理

2.1.1 概要

NetDefendOS は、高いパフォーマンスと信頼性を提供します。広範囲にわたり多彩な機能を提供するほか、管理者によるシステムの細かな制御が可能であるため、あらゆる環境に設置することができます。

システムを適切に使用するには、NetDefendOS の設定がどのように実行されるかを理解することが必要です。本セクションでは、多様な管理インタフェースにおける動作と、コンフィグレーションサブシステムについて、詳しい説明を行います。

管理ユーザインタフェース

NetDefendOS は以下の管理インタフェースを提供します。

- Web インタフェース

  Web インタフェースは、NetDefendOS に実装されており、標準的な Web ブラウザからアクセス可能な操作性がよく直感的に使用可能なグラフィカル管理インタフェースです。ブラウザは、HTTP または HTTPS（初期値では HTTPS のみ有効）を使用してハードウェアのイーサネットインタフェースの 1 つに接続し、NetDefendOS は Web サーバのように応答することで Web ページを管理インタフェースとして使用することができます。

  NetDefendOS の初期状態では、Web ユーザインタフェースアクセスは、D-Link のファイアウォールの LAN インタフェース経由で接続するネットワーク上のユーザにのみ有効とされています。（1 つ以上の LAN インタフェースが有効である製品では、LAN1 がインタフェースの初期値です。）詳しくは、「2.1.4 Web インタフェース」を参照してください。

- コマンドラインインタフェース（CLI）

  コマンドラインインタフェースは、ローカルコンソールポート経由でローカルに、または Secure Shell（SSH）プロトコルを使用してリモートからアクセスが可能です。このインタフェースでは NetDefendOS のすべてのパラメータを制御することができます。詳しくは、「2.1.5 CLI 接続」及び「2.1.6 CLI の利用方法」を参照してください。

- セキュアコピー

  セキュアコピー（SCP）は、ファイル転送のために広く使用されている通信プロトコルです。NetDefendOS の機能では SCP クライアントを提供していませんが、ほぼすべてのワークステーションで利用可能な SCP クライアントの幅広い選択が可能です。SCP は CLI を利用する際に補助的な役割を行い、管理者のワークステーションとファイアウォール間の安全なファイル転送を実現します。NetDefendOS が使用する様々なファイルは、SCP を使用してアップロードとダウンロードの両方を行うことができます。詳しくは「2.1.8 セキュアコピー」を参照してください。

- コンソールブートメニュー

  NetDefendOS を稼動させる前に、D-Link ファイアウォールのローカルコンソールポートに直接接続したコンソールを使用して、ブートメニューから基本的な設定を行うことができます。システムの電源を入れた後、NetDefendOS が起動するまでの間に、いずれかのコンソールキーを押下することでコンソールの利用を開始することができます。ブートメニューで D-Link ファームウェアローダに接続します。詳しくは「2.1.9 コンソールブートメニュー」を参照してください。

Web インタフェースへのアクセスは、特定のネットワーク上の管理ユーザに許可され、CLI アクセスは特定の IPsec トンネルを経由して接続するリモート管理ユーザに許可されます。

すべての管理アクセスには、アクセスを許可する Remote Management オブジェクトが必要です。定義済みの Remote Management オブジェクトと新規に作成する方法を次のセクションで説明します。

2.1.2 管理アクセスの設定

管理者による NetDefendOS への管理アクセスは以下の 2 つの要素に依存します。

- デフォルトの管理イーサネットに割り当てられた IP アドレス。このアドレスは変更することができます。（Remote Management オブジェクトで許可されるネットワークに所属する IP アドレスであること）
- Remote Management オブジェクトのコンフィグレーションのセットが許可するアクセスの種類。これらのオブジェクトでは、許可される管理アクセス、インタフェースで許可されるアクセスの種類、送信元 IP アドレスについて決定します。

管理アクセスのためのデフォルトインタフェースと IP

NetDefendOS で選択されるデフォルト管理インタフェースは、ハードウェアによって異なりますが、通常、最初のスタートアップ時のスキャンで検出された、利用可能なインタフェースとなります。

NetDefendOS はデフォルト IPv4 アドレス 192.168.10.1 をこの管理インタフェースに割り当てます。また、HTTPS アクセスは 192.168.10.0/24 ネットワークから許可されます。インタフェースおよび IP アドレスの割り当ては、以下の表の通りです。

ハードウェア	管理インタフェース	デフォルト IP アドレス
DFL-260E	LAN（全ポート）	192.168.10.1
DFL-860E	LAN（全ポート）	192.168.10.1
DFL-870	LAN1（ポート 4）	192.168.10.1
DFL-1660	LAN1（ポート 4）	192.168.10.1
DFL-2560	LAN1（ポート 7）	192.168.10.1
DFL-2560G	LAN1（ポート 7）	192.168.10.1

Remote Management オブジェクト

ネットワークを通じた NetDefendOS へのリモートアクセスは、一組の Remote Management オブジェクトによって制御されます。これらのオブジェクトは、以下のいずれかのタイプに分類されます。

- HTTP/HTTPS 管理
  rmgmt_http と呼ばれるこのタイプの定義済みオブジェクトは、IPv4 アクセス用の NetDefendOS 初期設定として既に存在しています。IPv6 用の HTTP/HTTPS 管理アクセスを許可するには、新しい Remote Management オブジェクトを作成する必要があります。詳細は後述します。

- SSH 管理
  このオブジェクトタイプは SSH クライアント経由のアクセスを制御します。

- SNMP 管理
  このオブジェクトタイプは SNMP クライアント経由のアクセスを制御します。このタイプのオブジェクトは、NetDefendOS のコンフィグレーションの初期設定には存在していないため、この種類のアクセスを許可するためには新しく作成する必要があります。

  SNMP アクセスについては、「2.5 SNMP」でより詳しく説明されています。

上記のとおり、以下の Remote Management オブジェクトは NetDefendOS に事前に定義されています。

- rmgmt_http
  Web インタフェース経由で HTTP と HTTPS アクセスを制御する RemoteMgmtHTTP オブジェクトです。初期値では、HTTPS だけがデフォルト管理インタフェースの 192.168.1.0/24 ネットワークから許可されています。

- rmgmt_ssh
  CLI を通して SSH アクセスを制御する RemoteMgmtSSH オブジェクトです。これは初期値で有効で、SSH アクセスは、デフォルト管理インタフェースの 192.168.1.0/24 ネットワークから許可されています。

SNMP アクセスなど他のタイプのアクセスでは、追加の Remote Management オブジェクトを作成しなければなりません。

IPv6 管理アクセスの設定

IPv6 プロトコルを使用した、HTTP/HTTPS 経由での管理者アクセスを設定することが可能です。以下の手順を実施してください。

- Network フィルターに対して、IPv6 アドレスオブジェクトセットを含む新規の Remote Management オブジェクトを作成する
- Remote Management オブジェクトで指定されたインタフェースに対して、IPv6 を有効化し、IPv6 アドレスを割り当てる

管理アクセスの損失を防止する

管理インタフェースの IP アドレスまたはリモート管理ルールを変更すると、その後の管理アクセスができなくなるリスクがあります。NetDefendOS では、以下の方法でこの問題を回避します。

- Web インタフェースを通じて行われた変更

  Web インタフェースに対するコンフィグレーションの変更では、Save and Activate の実行後に一定時間の遅延（初期値は 30 秒）が設定されています。この時間が経過した後に、Web ブラウザと NetDefendOS における接続性の自動チェックが行われ、接続が失われている場合は元のコンフィグレーションに復元されます。

  管理者が、コンフィグレーション変更により NetDefendOS と Web ブラウザ間の通信が切断されることを想定している場合（例えば管理 IP の変更）、Save and Activate を選択して、タイムアウトになる前に再度ログインします。すぐにログインを行うことにより、管理者アクセスが有効であることが認識されるため、コンフィグレーションは古いバージョンに戻りません。

- SSH の CLI を通じて変更を行う

  SSH 接続で CLI を使用するとき、管理者は、最初に以下のコマンドを発行しなければなりません。

  ```
  DFL-xxxx:/> activate
  ```

  activate コマンドは、新しいコンフィグレーションをアクティブ化しますが、以下のコマンドを発行するまで変更を恒久的なものにしません。

  ```
  DFL-xxxx:/> commit
  ```

  アクティブ化の後に commit コマンドを所定の期間（初期値は 30 秒）内に発行しないと、NetDefendOS は通信が失われたと見なし、元のコンフィグレーションに戻します。

  コンフィグレーション変更により SSH 通信が切断されると、管理者は、SSH に再びログインし、commit コマンドを発行して、変更を恒久的にする必要があります。

- ローカルコンソールの CLI を通じて変更を行う

  管理インタフェースの IP アドレス、および（または）リモート管理ルールを変更しても、SSH を使用する場合とは異なりローカルコンソールとの通信は失われません。そのため、activate コマンドの後に変更を恒久的にする commit コマンドを発行できます。しかし、commit コマンドの入力後、管理インタフェースへのアクセスが可能かどうかを手動でチェックする必要があります。

初期値の 30 秒の遅延が短すぎる場合、コンフィグレーションの高度な設定で遅延時間を変えることができます。変更する設定には Web インタフェースの Validation Timeout と CLI の NetconBiDirTimeout があり、これはグローバル設定です。

例題 2.1

Management Validation Timeout の変更

この例題では、有効期間を初期値の 30 秒から 60 秒に変更します。

CLI

```
DFL-xxxx:/> set Settings RemoteMgmtSettings NetconBiDirTimeout=60
```

Web Interface

1. **System > Device > Remote Management > Advanced Settings** の順にメニューをクリックします。

2. 以下を設定します。

< 入力例 >

- Validation Timeout: 60

3. 「OK」ボタンをクリックします。

管理インタフェースを変更する別の方法

30 秒の遅延を完全に回避する別の方法として、以下の手順を実行できます。

1. 既存のリモート管理インタフェースを使用してログインし、新しい Remote Management オブジェクトを追加して、変更を適用するためにアクティブ化とコミットを行います。

2. 現在の接続を切断後、新しい Remote Management オブジェクトによって指定されたインタフェースを使用して再接続してください。

3. 古い Remote Management オブジェクトを削除して、変更を適用するためにアクティブ化とコミットを実行します。

管理 IP アドレスの変更

以下の例題では、デフォルト管理インタフェースにアクセスするための IPv4 アドレスを変更する方法を示しています。新しいアドレスは、そのインタフェースに設定された Remote Management オブジェクトによって許可されたネットワークに所属している必要があります。そうでない場合、IP を許可するようにオブジェクトの設定を変更する必要があります。

以下の 2 つの方法で管理インタフェースを変更することができます。

- インタフェースの IP アドレスを直接変更します。CLI の実行例を以下に示します。

```
DFL-xxxx:/> set Interface Ethernet <interface> IP=<ip_address>
```

  アドレス帳のアドレスオブジェクト自体は変更されず、アドレスオブジェクトを参照する他のルールやオブジェクトもそのままとなるため、この方法は推奨されません。

- インタフェース IP 用のアドレスオブジェクトの IP アドレスを変更します。新しい管理 IP アドレスを設定する際は、こちらの方法が推奨されます。

例題 2.2

管理インタフェース IP アドレスを変更する

この例題では管理 If1 インタフェースの IPv4 アドレスを 192.168.1.1 から 192.168.1.2 に変更します。これらは同じネットワークに所属するので、ネットワークまたは管理ポリシーを変更する必要はありません。

操作を実行する 2 つの方法は以下の通りです。

CLI

```
DFL-xxxx:/> set Address IP4Address InterfaceAddresses/If1_ip Address=192.168.1.2
```

Web Interface

1. **Objects>Address Book** の順にメニューをクリックします。

2. アドレスフォルダ InterfaceAddresses を選択します。

3. アドレス帳オブジェクト If1 を選択します。

4. 以下を設定します。

< 入力例 >

- Address: 192.168.1.2

5. 「OK」ボタンをクリックします。

リモート管理オブジェクトを変更する

管理インタフェース用の IP アドレス及びネットワークが変更され、（または）異なるインタフェースが使用される場合、以下の例題で示すように、対応する管理アクセスルールも変更する必要があります。

例題 2.3

リモート管理オブジェクトを変更する

この例題では、If2 インタフェースおよび定義済みのアドレス帳オブジェクト management_net で設定されたネットワークからのアクセスを許可するように現在の HTTP/HTTP 管理アクセスを変更します。HTTP と HTTPS 接続の両方が許可されます。

CLI

```
DFL-xxxx:/> set RemoteManagement RemoteMgmtHTTP rmgmt_https HTTP=Yes HTTPS=Yes Network=management_net Interface=If2
```

Web Interface

1. **System > Device > Remote Management > rmgmt_https** の順にメニューをクリックします。

2. 以下を設定します。
   - HTTP を有効にします。
   - HTTPS を有効にします。
   - Interface: If2
   - Network: management_net

3. 「OK」ボタンをクリックします。

HA クラスタ管理 IP は別にする必要がある

NetDefendOS 高可用性クラスタでは、マスタとスレーブユニットにおける管理インタフェースに対しては、それぞれ異なる管理 IP を使用する必要があります。NetDefendOS 管理用に共有 IP アドレスは使用できません。

クラスタのマスタとスレーブユニット上の管理インタフェースに設定される各 IPv4 アドレスは、その管理インタフェースの IPv4 HA Address オブジェクト内に保持され、マスタとスレーブユニットの両方にコピーされます。どちらかのユニットで、このアドレスオブジェクトの管理インタフェース IP が変更されると、同期プロセスにより、もう片方のユニットに自動的にコピーされます。

例題 2.4

HA 管理 IP アドレスを変更する

この例題では、HA クラスタの LAN インタフェースのスレーブ管理 IP アドレスが 192.168.1.2 に変更されます。

CLI

```
DFL-xxxx:/> set Address IP4HAAddress lan_ha_ip Address:1=192.168.1.2
```

Web Interface

1. **Objects > Address Book** の順にメニューをクリックします。

2. アドレス帳オブジェクト lan_ha_ip を選択します。

3. 以下を設定します。
   - Slave IP Address: 192.168.1.2

4. 「OK」ボタンをクリックします。

アクティブ化とコミットが実行されると、この変更がクラスタ内の他のユニットに同期されます。

リモート管理オブジェクトの追加

付加的な管理アクセスオブジェクトをコンフィグレーションに追加することができます。例えば、次の例題で示すように、Web インタフェースを使用して、If2 インタフェースで HTTPS アクセスのみを許可するように、追加の RemoteMgmtHTTP を追加することができます。

例題 2.5

HTTPS 経由のリモート管理を追加する

この例題では、新しい RemoteMgmtHTTP オブジェクト https_access を追加します。これにより、任意のネットワークから If2 インタフェースへの HTTPS アクセスを許可し、ローカルデータベース AdminUsers を使用して、管理者のログイン証明書を認証します。

CLI

```
DFL-xxxx:/> add RemoteManagement RemoteMgmtHTTP https_access Network=all-nets Interface=If2
            LocalUserDatabase=AdminUsers HTTPS=Yes
```

Web Interface

1. **System > Device > Remote Management > Add > HTTP/HTTPS Management** の順にメニューをクリックします。
2. HTTP/HTTPS リモート管理のルール名を入力します。この例題では https_access としています。
3. HTTPS オプションを有効にします。
4. 以下を選択します。
   - Local User Database: AdminUsers
   - Interface: If2
   - Network: all-nets
5. 「OK」ボタンをクリックします。

all-nets ルートからの管理アクセスが失敗する場合

VPN トンネルが確立した状態で、管理アクセスが想定通りに動作しない場合、メインルーティングテーブルに追加されている all-nets ルートが原因で管理トラフィックがトンネルにルーティングされている可能性があります。この問題を回避するには、ファイアウォールから管理サブネットワークに送信される管理インタフェースのトラフィックに対して特別なルートを設定する必要があります。

2.1.3 管理者アカウント

初期値では、NetDefendOS には、定義済みのユーザアカウントを持つローカルユーザデータベース「AdminUsers」が定義されています。

初期値ではユーザ名は「admin」、パスワードは「admin」です。このアカウントには、管理用のすべての読み書き権限があります。

注意 安全のために、D-Link ファイアウォールに接続後、直ちにアカウントの初期パスワードを変更することを強くお勧めします。

新しいアカウントの作成

必要に応じて追加ユーザアカウントの作成ができます。アカウントは、完全な読み書き権限を持つユーザグループ「Administrators」、または読み取り権限のみを持つユーザグループ「Auditors」に所属できます。

1 人の管理者のみのログインが可能

NetDefendOS には、2 人以上の管理者アカウントが同時にログインすることはできません。1 人の管理者がログインすると、2 番目以降の管理者は異なる証明書を使用してログインできますが、「Audit」権限となります。つまり、2 番目以降にログインした管理者は、コンフィグレーションの読み取りのみが可能であり、それらを変更することはできません。

一方で、NetDefendOS では、同じ管理者アカウントで（同じ管理者資格証明書を使用して）同時にログインすることは可能です。例えば、管理者による CLI 操作と、Web インタフェース経由での管理操作の実行を同時に行うことが可能です。

2.1.4 Web インタフェース

NetDefendOS は、標準の Web ブラウザを使用してイーサネット経由でシステムを管理するために、直感的な Web ユーザインタフェースを提供しています。これにより、サードパーティのクライアントソフトウェアをインストールせずにプライベートネットワークまたはインターネット経由でリモート管理を行うことが可能になります。

注意 推奨 Web ブラウザ

Web インタフェースで使用する推奨ブラウザは以下の通りです。

- Microsoft Internet Explorer
- Firefox
- Safari
- Chrome
- Opera

デフォルト IP アドレスの指定

工場出荷時の設定を持つ新しいファイアウォールでは、NetDefendOS がハードウェアの LAN1 インタフェース（複数の LAN インタフェースを持たないモデルでは LAN インタフェース）に自動的に IPv4 アドレスの初期値を割り当てます。管理インタフェースに割り当てられる IP アドレスは、常に 192.168.10.1 です。

ファイアウォール内のインタフェース名とファイアウォール前面のポート配置の関係については、付録を参照してください。
初期値から管理インタフェース、IP アドレスを変更する方法については、「2.1.2 管理アクセスの設定」に記載しています。

管理ワークステーションの IP アドレスの設定

ファイアウォールの初期管理イーサネットインタフェースと外部コンピュータのインタフェースで通信を成功させるためには、これらが論理 IP ネットワークのメンバである必要があります。そのため、ワークステーションのインタフェースの接続には以下のようなスタティック IP アドレスを設定する必要があります。

IP アドレス	192.168.10.30
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.10.1

以下の図でスイッチを経由した管理ステーションの接続例を示します。

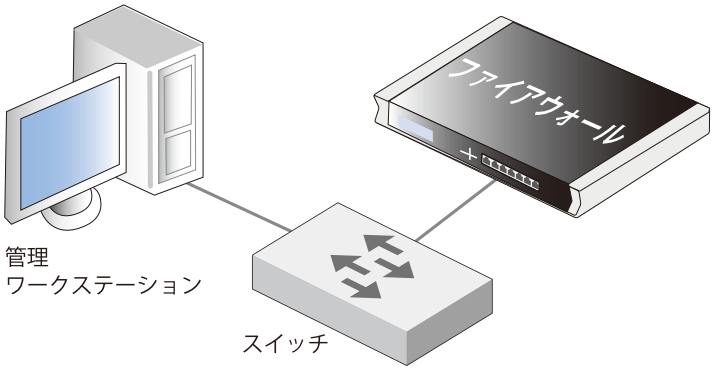


図 2-1　管理ワークステーションの接続

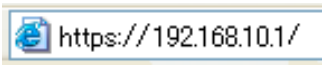
Web インタフェースにログインする

工場出荷時設定を使用して Web インタフェースにアクセスするためには、外部ワークステーションで Web ブラウザ を起動して URL に次の IPv4 アドレスを指定します。

- 192.168.10.1

NetDefendOS にはじめて接続する際、ブラウザの URL プロトコルとして必ず「https://」を使用します（例 : https://192.168.10.1）。HTTP は後で有効にすることができます。HTTPS 接続では、暗号化のために NetDefendOS の自己署名証明書が返され、ブラウザではセキュリティの例外設定が必要であることを確認するメッセージが表示されます。

以下の通りブラウザにアドレスを入力します。



セキュリティの警告画面が表示された場合は、「はい」ボタンをクリックします。

NetDefendOS との通信が成功すると、以下のようなユーザ認証ダイアログがブラウザ画面に表示されます。

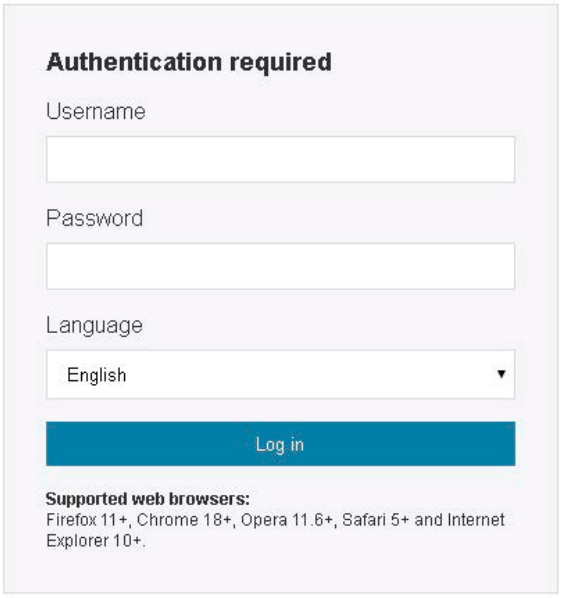


図 2-2　Web インタフェース認証

「Username」（ユーザ名）と「Password」（パスワード）を入力し、「Login」ボタンをクリックします。ユーザ名とパスワードの初期値は「admin」です。入力した内容が正しければ、メインの Web インタフェースページに遷移します。

注意 **パスワードのキャッシュは保存されません。**

Web インタフェースはログイン資格証明書からのパスワードのキャッシュを保存しません。VPN 認証のような、ブラウザ画面を通じてパスワードが要求される他の NetDefendOS 機能でも同様です。

Web インタフェースへの初めてのログインとセットアップウィザード

初めて本製品にログインする場合、ユーザ名とパスワードの初期値は「admin」です。ログインに成功すると、Web ユーザインタフェースがブラウザ画面に表示されます。ファイアウォールに対してコンフィグレーションの変更が実行されていない状態では、NetDefendOS のセットアップウィザードが自動的に起動し、NetDefendOS 設定とインターネットアクセスの確立のための必要な手順を行うように誘導します。

注意 **ポップアップブロックのオフ**

Web ブラウザおけるポップアップブロック機能は、NetDefendOS Setup Wizard を実行するために無効にする必要があります。

必要に応じて、Web インタフェースのウィザードを終了し、一連の手順を完了させることができます。CLI でセットアップを行うことも可能です。

複数言語サポート

Web インタフェースログイン画面は、インタフェース用に英語以外の言語を選択するオプションを提供しています。言語ファイルは、D-Link ホームページからダウンロード可能です。

注意 R11.10.01.06 以降のバージョンでは、日本語 GUI 言語ファイルが用意されていません。ログイン画面で English を選択してご使用ください。

Web ブラウザインタフェース

Web インタフェースの左側には、様々な NetDefendOS モジュールに接続するツリーがあります。Web インタフェースの中央のエリアはそれらのモジュールに関する情報を表示します。現在の動作情報は初期状態で表示されています。ユーザ名とパスワードの初期値に関する情報は「2.1.3 管理者アカウント」を参照してください。

参照 リモート管理アクセス

ユーザ名とパスワードの初期値は以下の通りです。

- Username : admin
- Password : admin

Web インタフェースへのアクセスは、リモート管理ポリシーによって規定されます。初期値では、NetDefendOS は内部ネットワークからの Web アクセスだけを許可しています。

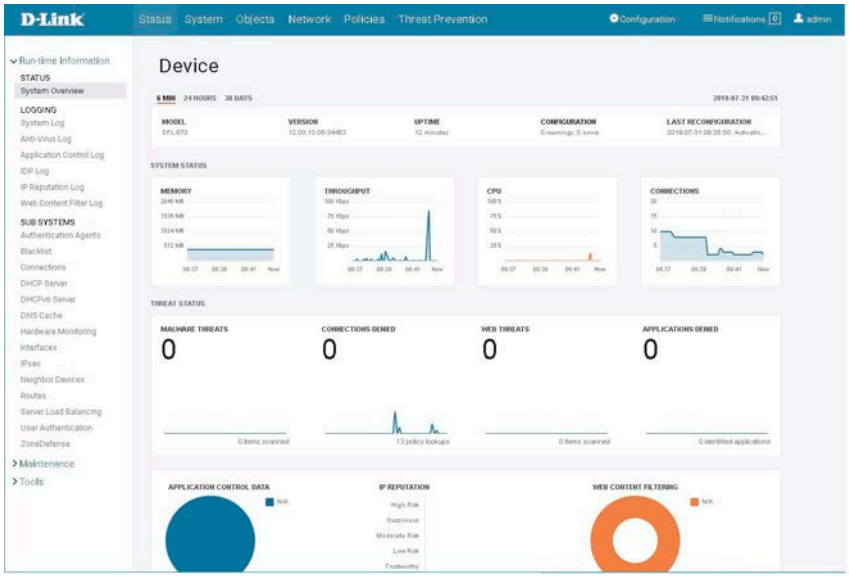


図 2-3 Web インタフェースレイアウト

インタフェースレイアウト

Web インタフェースの画面は、以下のセクションに区分されています。

メニューバー

Web インタフェースの上部に位置するメニューバーには、主要機能別にボタンが存在し、それぞれの機能にアクセスすることができます。

オブジェクトナビゲータ

Web インタフェースの左側にあるツリービューリストには、メニューバーで選択した項目の詳細セクションが表示されます。

メイン画面

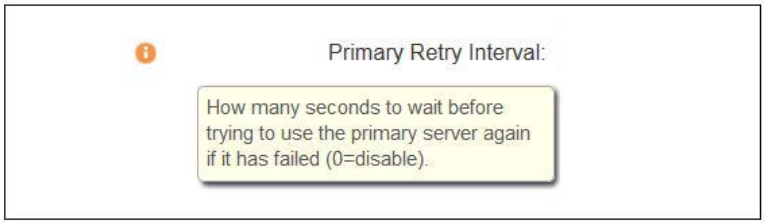
メイン画面は、メニューバーまたはオブジェクトナビゲータで選択したセクションに応じて、設定またはステータスを詳細表示します。

メイン画面で情報テーブルが表示されている場合、いずれかのエントリ（IP ポリシーなど）を右クリックすると、コンテキストメニューが表示されます。

コンテキストメニューでは、新しいオブジェクトの追加や現在のオブジェクトの削除、エントリの順番を入れ替える操作などを行うことができます。Clone 機能は、現在のオブジェクトを完全にコピーし、テーブルの最後に追加します。以下はコンテキストメニューの代表的な例です。

参照 テキスト項目の追加情報を表示する

Web インタフェースの多くのテキスト項目では、マウスポインタを項目の上に置くとアイテムに関する追加情報を表示することができます。例えば、以下の画面では、RADIUS 設定の Primary Retry Interval フィールドのテキストの上にマウスポインタをのせた時に情報が表示されることを示しています。



コンフィグレーション変更をアクティブ化する

Web インタフェースを通じてコンフィグレーション変更が行われる際、管理者がアクティブ化を実行するまで、この変更は現在動作中のコンフィグレーションには適用されません。アクティブ化を行うには、Web インタフェースメニューオプションの **Configuration > Save and Activate** を選択します。

その後、NetDefendOS は再構築の操作を実行します。これは、わずかな遅延を現在のデータトラフィックに引き起こす可能性があります。変更によって管理者がロックアウトされることを防止するため、指定遅延時間（初期値では 30 秒）後に Web ブラウザとの通信が失われると、NetDefendOS は変更前のコンフィグレーションにシステムを戻します。
「2.1.2 管理アクセスの設定」でより詳しくこの遅延について記載します。

注意 本マニュアルの例題は、アクティブ化が実行されることを想定しています。

本マニュアルの多くの例題は NetDefendOS のコンフィグレーションの編集について扱っています。基本的には、最後のアクティブ化の実行手順は明示的に記載していません。

CA 署名入りの証明書の使用
初期値では、HTTPS で Web インタフェースに接続する際、利用ブラウザに対して自己署名証明書が送信され、ユーザは証明書を明示的に許可する必要があります。これとは別に、証明書チェーンを利用することで CA 証明書を使用することも可能です。以下、例題で説明します。

例題 2.6

CA 署名証明書を使用した HTTPS 経由のリモート管理

CLI

```
DFL-xxxx:/> set Settings RemoteMgmtSettings HTTPSCertificate=HostA HTTPSRootCertificates=RootA2,RootA1,RootA3
```

Web Interface

1. **System > Device > Remote Management > Advanced Settings** の順にメニューをクリックします。
2. WEBUI セクションで HTTPS Certificate と HTTPS Root Certificates を指定します。
3. 「OK」ボタンをクリックします。

NetDefendOS SSL VPN 機能では、ユーザの初回接続時にこれと同じ CA 署名証明書が使用され、オプションのダイアログが表示されます。

警告 管理インタフェースを他の人に見せないでください。
上記の例題は、機能を説明するために記載されています。インターネット上のどのユーザに対してもすべての管理インタフェースを見せないことをお勧めします。

Web インタフェースからログアウトする
Web インタフェースでの操作終了後、システムへのアクセス権限のないユーザからの接続を避けるためにログアウトする必要があります。メニューバーの右にある「ユーザ名（admin など）」>「Logout」ボタンをクリックします。

VPN トンネルを使用した管理トラフィックのルーティング
VPN トンネル経由で通信する際、管理インタフェースで問題が発生した場合、main ルーティングテーブルをチェックし、VPN トンネルへの all-nets ルートを検索します。管理トラフィックは、このルートを使用している可能性があります。

指定ルートが管理インタフェースにない場合、NetDefendOS から到来するすべての管理トラフィックは自動的に VPN トンネルに送信されます。この場合、管理者は、管理ネットワークへ行くべき管理トラフィックを正しいインタフェースに送信するためにルートを追加する必要があります。

デバイス名の変更

D-Link ファイアウォールに設定されたデバイス名は、NetDefendOS コンフィグレーションに保存されます。このデバイス名は、Web インタフェースのステータス画面の上部に表示され、CLI プロンプトにも同様に表示されます。

初期値では「Device」ですが、Web インタフェースの **System > Device > Name** から別の名称に変更することも可能です。複数のファイアウォールを管理して、それぞれの動作デバイスを識別する場合には、デバイス名を変更することが有用です。

2.1.5 CLI 接続

このセクションでは、NetDefendOS Command Line Interface (CLI) への接続方法を説明しています。以下の方法で接続することができます。

- ローカルコンソールを使用したダイレクト接続
- SSH を使用したイーサネットインタフェース経由でのネットワークアクセス

これらの接続方法における認証についても説明します。CLI の使用方法については「2.1.6 CLI の利用方法」を参照してください。

ローカルコンソールによる CLI アクセス方法

ローカルコンソールポートは、管理ワークステーションへの直接接続を通じて NetDefendOS の CLI への管理アクセスを可能にするファイアウォールの接続ポートです。セットアップ要件の概要は以下の通りです。

- ターミナルのコンソールをエミュレートできる管理コンピュータまたはデバイス。コンソールのエミュレーション用に、適切な通信ソフトウェアをインストールする必要があります。多くのサードパーティのものが利用可能です。
- D-Link ファイアウォールをコンピュータに接続するのに適切なコネクタを持つケーブル。

以下の手順で、端末をコンソールポートに接続します。

1. 必要に応じて、適切にコンソール通信プロトコルを設定します。
2. ケーブルのコネクタの一端をファイアウォールのローカルコンソールポートに直接接続します。
3. ケーブルのもう一端を通信ソフトウェアが動作しているコンピュータに接続します。
4. ターミナルコンソールで Enter キーを押下します。NetDefendOS のログインプロンプトが表示され、CLI コマンドの入力が可能になります。

SSH（Secure Shell）

リモートホストへの CLI アクセスでは、SSH（Secure Shell）プロトコルを使用することができます。SSH は、安全が確保されていないネットワークにおいて安全な通信を行うための主要なプロトコルであり、強固な認証機能とデータ保全性を提供します。NetDefendOS では SSHv2 をサポートしています。多くのプラットフォームで SSH クライアントが利用可能です。

SSH 接続は NetDefendOS のリモート管理ポリシーによって制御され、初期値では無効化されています。以下の例題では、SSH 接続の有効化する手順を説明しています。

例題 2.7

SSH リモートアクセスを有効にする

この例題では、リモート管理ポリシーにルールを追加して、lan インタフェース経由での lannet からのリモート SSH 接続を有効化します。

CLI

```
DFL-xxxx:/> add RemoteManagement RemoteMgmtSSH ssh Network=lannet Interface=lan LocalUserDatabase=AdminUsers
```

Web Interface

1. **System > Device > Remote Management > Add > SSH Management** の順にメニューをクリックします。

2. SSH リモート管理ポリシーを以下の通り作成します。ここでは「ssh_policy」という名前のポリシーを作成します。

< 入力例 >

General
- Name : ssh_policy

Authentication
- Local User Database : AdminUsers

Access Filter
- Interface : lan
- Network : lannet

3. 「OK」ボタンをクリックします。

IPv6 を使用した SSH 接続

上記の設定例は、ファイアウォール上のイーサネットインタフェース経由で IPv4 アドレスを使用して SSH クライアントからアクセスすることを想定しています。IPv6 アドレスを使用したアクセスを設定することも可能です。NetDefendOS 設定における IPv6 管理アクセス設定は、以下の手順で行います。

- 管理接続で使用されるイーサネットインタフェース上で IPv6 を有効化し、そのインタフェースに対して IPv6 アドレスが割り当てられている必要があります。詳細は「3.2 IPv6 のサポート」を参照してください。
- 先の例題の通り、SSH 管理ルールを追加する必要があります。また、Network プロパティに接続元の IPv6 ネットワークまたはホストを設定する必要があります。

SSH キーを使用した自動認証

初期値では、SSH アクセスにはユーザ名とパスワードの入力が必要です。これ以外の方法として、SSH キーを使用することで自動的に認証を行うことも可能です。スクリプトを使用する場合、この認証方式が有用です。この方式は、公開鍵認証とも呼ばれます。

公開鍵認証では、NetDefendOS に公開鍵 / 秘密鍵のペアの公開鍵ファイルをアップロードして、関連するオブジェクトに紐付ける必要があります。公開鍵と秘密鍵ファイルの両方が接続する SSH クライアントにインストールされます。

以下の手順で SSH 鍵による認証を有効にします。

1. サードパーティのツールを使用して、適切なキーファイルのセットを作成します。キー生成は SSH クライアントによって直接行われることもあります。キーファイルは秘密鍵ファイルと公開鍵ファイルから構成されます。慣例では、これらは通常 id_rsa（秘密鍵）、id_rsa.pub（公開鍵）と呼ばれます。

2. SSH クライアントにキーファイルをインストールします。クライアントを使用してキーの生成を行った場合は、キー生成と同時にインストールまで完了している場合があります。

3. SCP を使用して、公開鍵ファイルを NetDefendOS にアップロードします。sshclientkeys と呼ばれる NetDefendOS フォルダにファイルを保存します。（SCP とこのフォルダについては「2.1.8 セキュアコピー」でより詳しく説明しています。）

   公開鍵ファイルには通常オリジナルのファイルタイプ .pub がありますが、NetDefendOS 上のファイル名は「.」（ピリオド）を持つことはできません。証明書の公開鍵ファイルのローカル上のファイル名が id_rsa.pub である場合、NetDefendOS ストレージではピリオドがないファイル名とする必要があります。例えば、以下のような SCP クライアントコマンドを使用して、新しいファイル名 my_public_ssh_key として NetDefendOS にアップロードします。

```
> scp id_rsa.pub admin@203.0.113.5:sshclientkey/my_public_ssh_key
```

4. NetDefendOS では、関連する User オブジェクトの SSH Keys プロパティに対し、アップロードされた公開鍵ファイルを設定します。例えば、ユーザ admin に対し、鍵ファイル my_public_ssh_key を割り当てることができます。このステップを以下の例題で詳細に説明します。

5. SSH を使用したキー認証で NetDefendOS に接続します。認証が自動的に行われ、資格証明書を入力するプロンプトは表示されません。

例題 2.8

SSH キーを使用した認証を有効にする

この例題では、ユーザ admin の自動 SSH 認証を有効にする方法を示しています。SCP を使用して、SSH 公開鍵ファイル my_ssh_cert が既に NetDefendOS の sshclientkeys フォルダにアップロードされているものとします。

CLI

対象ユーザを含むユーザデータベースの CLI コンテキストに移動します。

```
DFL-xxxx:/> cc LocalUserDatabase AdminUsers
```

ユーザの SSHKeys プロパティに、アップロードされた SSH キーファイルを設定します。

```
DFL-xxxx:/AdminUsers> set User admin SSHKeys=my_public_ssh_key
```

CLI コンテキストを初期値に戻します。

```
DFL-xxxx:/AdminUsers> cc
DFL-xxxx:/>
```

Web Interface

1. **System > Device > Local User Databases** の順にメニューをクリックします。

2. データベース AdminUsers を選択します。

3. Users を選択します。

4. ユーザ admin を選択します。

5. SSH Public Key タブを選択します。

6. Selected リストに my_public_ssh_key を追加します。

7. 「OK」ボタンをクリックします。

CLI へのログイン

ローカルコンソールまたは SSH クライアントを使用して NetDefendOS に対する CLI 接続が確立した際に、CLI コマンドを実行する前に、管理者がシステムにログインする必要があります。この認証を行うことにより、監査用にユーザ情報を提供し、信頼されたユーザのみがシステムに接続可能となります。

リモートから SSH 経由で接続した場合、システムはログインプロンプトを返します。ユーザ名を入力し、「Enter」を押し、続いてパスワードを入力して、「Enter」を押します。ログイン成功後、コマンドプロンプトが表示されます。

```
DFL-xxxx:/>
```

注意 安全のために、CLI Welcome メッセージを無効または匿名にすることをお勧めします。

「admin」ユーザパスワードを変更する

最初に起動した後、できるだけ早く admin アカウントの初期パスワードを「admin」から変更することを強くお勧めします。ユーザパスワードは、どんな文字列の組み合わせも可能で、長さは 256 文字以内とします。印刷可能な文字だけを使用することをお勧めします。

例えば、パスワードを「my-password」に変更するには、以下の CLI コマンドを使用します。はじめに、現在のカテゴリを LocalUserDatabase の AdminUsers（初期値で存在）に変更する必要があります。

```
DFL-xxxx:/> cc LocalUserDatabase AdminUsers
```

AdminUsers データベースを参照しています。これで、admin ユーザのパスワードを変更することができます。

```
DFL-xxxx:/AdminUsers> set User admin Password="my-password"
```

最後に、現在のカテゴリを最上位に戻します。

```
DFL-xxxx:/AdminUsers> cc
```

注意 コンソールパスワードは独立しています。

直接ローカルコンソールのアクセスを保護するために設定するパスワードは、独立したものであり、ユーザアカウントに関連するパスワードと混同しないようにご注意ください。詳しくは、「2.1.9 コンソールブートメニュー」を参照してください。

2.1.6 CLI の利用方法

NetDefendOS は、コマンドライン操作を必要とする管理者、またはシステム設定をさらに詳細に行う必要のある管理者のために、コマンドラインインタフェース（CLI: Command Line Interface）を提供しています。CLI は、ローカルコンソールに直接接続する方法と、SSH クライアントから Secure Shell（SSH）プロトコルを使用してイーサネット経由でリモート接続する方法があります。CLI の接続方法については「2.1.5 CLI 接続」で説明しています。

CLI は、設定データの編集 / 表示、システムからのランタイムデータの表示、システム管理タスクの実行などを可能とする広い範囲のコマンドを提供しています。

CLI では大文字小文字を区別しますが、CLI のタブ補完機能では、補完を実行する際に大文字小文字を区別しません。

このセクションでは、CLI の利用方法について概要のみを説明しています。すべての CLI コマンドを参照するには、「CLI Reference Guide」を参照してください。

最もよく使用される CLI コマンドは以下の通りです。
- add - IP アドレスまたはルールなどのオブジェクトを NetDefendOS コンフィグレーションに追加します。
- set - オブジェクトのプロパティに値を設定します。例えば、IP ルールに送信元インタフェースを設定するために使用されます。
- show - 現在のカテゴリを表示、または特定オブジェクトの値を表示します。
- delete - 指定オブジェクトを削除します。

CLI コマンドの構成

CLI コマンドは、通常、以下の構造となっています。

```
<command> <object_category> <object_type> <object_name>
```

例えば、以下のコマンドを使用して「my_address」という IP アドレスオブジェクトを表示します。

```
DFL-xxxx:/> show Address IP4Address my_address
```

この場合、オブジェクトカテゴリは Address で、このカテゴリ内のタイプは IP4Address です。

コマンドを入力する時、コマンドの対象が明確であるケースでは、オブジェクトカテゴリを省略することができます。例えば、前述の「show」コマンドの場合、以下のように入力します。

```
DFL-xxxx:/> show IP4Address my_address
```

ただし、Tab 補完機能では、コマンドラインにカテゴリが含まれることを想定しています。例えば、上記のコマンドにおいて、IPAddress オブジェクトタイプの途中や後にタブが押下されたとしても、コマンドの補完を実行することはできません。

同じオブジェクト名を 2 つの異なるカテゴリまたはタイプ内で使用できますが、構成を読み取る際に分かりづらくなるため、避けることをお勧めします。

注意 カテゴリとコンテキスト

CLI の説明において、「オブジェクトカテゴリ」と「オブジェクトコンテキスト」という用語は、同じ意味で使用されます。

「add」などのコマンドも、オブジェクトプロパティを持つことができます。10.49.2.1 の IP アドレスを持つ新しい IP4Address オブジェクトを追加するコマンドは以下の通りです。

```
DFL-xxxx:/> add IP4Address my_address Address=10.49.2.1
```

オブジェクトタイプは、オプションでオブジェクトカテゴリより優先することができます。カテゴリはタイプのセットを分類し、以下で説明する「Tab 補完」で主に使用されます。

参照 help に関するヘルプを参照します。

以下の通り、CLI コマンド入力します。

```
DFL-xxxx:/> help help
```

ヘルプコマンド自身の情報を参照します。

CLI コマンドヒストリ

Microsoft Windows™ の多くのバージョンのコンソールのように、上下の矢印キーにより、ユーザは CLI コマンドヒストリ内のコマンドリストを移動することができます。例えば、上矢印を一度押すことで、最後に実行したコマンドを現在の CLI プロンプトに表示します。コマンドの表示後に、オリジナルの形式で再実行することも、実行前にそれを変更して実行することもできます。

Tab 補完

すべてのコマンドとそのオプションを覚えているのは難しいことです。NetDefendOS では、「Tab」キーを押すとコマンドの現在の部分を自動的に補完する「Tab」補完と呼ばれる機能を提供します。補完ができない場合、「Tab」キーを押すことで同時に利用可能なコマンドオプションを表示します。

例えば、特定の IP ポリシーオブジェクトを作成する場合、コマンドラインは以下のように開始します。

```
DFL-xxxx:/> add IPPolicy
```

「Tab」キーを 2 回（もしくはスペースの後に「Tab」キー）を押すと、以下のように必須パラメータが表示されます。

```
A value is required for the following properties:

DestinationInterface   Name    SourceInterface
DestinationNetwork    Service  SourceNetwork
```

次のように DestinationInterface の不完全なオブジェクトを入力してみます。

```
DFL-xxxx:/> add IPPolicy DestinationI
```

ここで「Tab」が押下されると、NetDefendOS によってオブジェクト名が補完され、以下の通り表示されます。

```
DFL-xxxx:/> add IPPolicy DestinationInterface=
```

Destination のみの場合、タブ補完を適用することができません。「I」まで入力することで、文字列の始めの部分から該当のプロパティを認識することができます。このように、すべての必須プロパティを表示するために「Tab」キーを使用することができます。

```
DFL-xxxx:/>  add IPPolicy SourceInterface=If2
                          SourceNetwork=all-nets
                          DestinationInterface=If2
                          DestinationNetwork=all-nets
                          Service=all_services
                          Name=my_example_policy
```

注意 本ガイドの CLI コマンドはフォーマットが変更されています。

本ガイドでは CLI コマンドの各要素をより明確にするために、インデントを付けた個別の行で細かく分けている場合があります。
実際のコンソール画面では、それらは右端で折り返され 1 つの連続した行として現れます。

オプションパラメータの補完

Tab 補完は、すべての必須パラメータが入力されるまで、オプションパラメータに対して動作しません。必須プロパティの値がセットされた後、「Tab」キーを押下すると IP ポリシーオブジェクトの全てのオプションプロパティが表示されます。

```
Optional properties, if no value is specified the default is used:

Action      Comments                 Index           Schedule
AppControl  DestAddressTranslation   LogEnabled      SourceAddressTra
Attribute   DestinationGeoFilter     LogSeverity     SourceGeoFilter
```

初期値または現在のプロパティ値の取得

「Tab」の前の「.」文字は、まだ値が設定されていない場合、「Add」コマンドのパラメータに初期値を自動的に入力するために使用されます。例えば以下のようになります。

```
DFL-xxxx:/> add LogReceiverSyslog example IPAddress=example_ip LogSeverity=.(Tab)
```

LogSeverity に初期値が補完されます。

```
DFL-xxxx:/> add LogReceiverSyslog example IPAddress=example_ip LogSeverity=Emergenc
y,Alert,Critical,Error,Warning,Notice,Info
```

後ろ矢印と「Back space」キーにより本 LogSeverity を編集することができます。初期値がいつも利用可能というわけではありません。例えば、IP ルールの Action には初期値はありません。

Set コマンドの場合も、現在のプロパティを取得するために、同じシーケンスを使用することができます。

```
DFL-xxxx:/> set LogReceiverSyslog log_example IPAddress=.(Tab)
```

これは Address プロパティの現在値を表示します。

プロパティ値の追加

「Tab」の前の「.」文字の他の使用法は、自動的にコマンドラインのオブジェクトプロパティの現在値を書き込む機能です。既存の値のリストに新しい値を追加する必要がある場合に、非常に役に立ちます。

例えば、以下の通り未完成のコマンドを入力します。

```
DFL-xxxx:/> set Address IP4Address If1_ip Address=
```

続けて、「.」「Tab」キーの順に入力すると、NetDefendOS はアドレスパラメータとして現在の値を表示します。現在の値が IPv4 リスト 10.6.58.10、192.168.2.1 であれば、未完成のコマンド行は自動的に以下の通りに補完されます。

```
DFL-xxxx:/> set Address IPAddress If1_ip Address=10.6.58.10,192.168.2.1
```

表示された値をそのまま追加したり、コマンドを実行する前に「Back space」および「後ろ矢印キー」を使用して変更したりすることも可能です。

オブジェクトのカテゴリ

オブジェクトが IP4Address などのタイプによって分類されると説明しましたが、タイプ自体はカテゴリ別に分類されます。タイプ IP4Address はカテゴリの Address に所属します。カテゴリの主な用途は、使用する正しいオブジェクトタイプを検索する際の、タブ補完です。

「add」などのコマンドを入力してから、「Tab」キーを 2 回（もしくはスペースの後に「Tab」キー）を押すと、NetDefendOS はすべての利用可能なカテゴリを表示します。カテゴリを選択し、再度「Tab」キーを 2 回（もしくはスペースの後に「Tab」キー）を押すことによって、そのカテゴリ用のすべてのオブジェクトタイプが表示されます。カテゴリを使用することにより、簡単にオブジェクトの種類を指定することが可能であり、タブ補完後に、管理可能なオプションを表示することができます。

すべてのオブジェクトタイプがカテゴリに所属するわけではありません。オブジェクトタイプの「UserAuthRule」はカテゴリを持たないタイプであり、最初のコマンドを入力後、「Tab」キーを押下するとカテゴリのリストに表示されます。

カテゴリは、CLI コンテキストと呼ばれることもあります。コマンドにはカテゴリが必須という訳ではありませんが、タブ補完を利用する場合は常に表示されます。後述の通り、CLI スクリプトを使用して自動的にコマンドが生成される場合は NetDefendOS によってそのコマンド内のカテゴリは省略されます。

オブジェクトのカテゴリの選択

カテゴリの種類によっては、個別のオブジェクトを操作する前に、cc（change category）コマンドを使用してそのカテゴリのメンバを最初に選択する必要があります。例えば、ルートを使用した場合です。複数のルーティングテーブルが存在する可能性があるので、ルートの追加または操作する場合、対象のルーティングテーブルを特定するために「cc」コマンドを最初に使用する必要があります。

ルーティングテーブルの「main」にルートを追加します。最初のコマンドは以下の通りです。

```
DFL-xxxx:/> cc RoutingTable main
DFL-xxxx:/main>
```

コマンドプロンプトが現在のカテゴリに変更され、ルートを追加することができるようになります。

```
DFL-xxxx:/main> add Route Name=new_route1 Interface=lan Network=If1_net
```

カテゴリの選択を解除するために、「cc」コマンドを実行します。

```
DFL-xxxx:/main> cc
DFL-xxxx:/>
```

オブジェクトの操作前に「cc」コマンド実行する必要があるカテゴリは、「show」コマンドで一覧表示した際に、名前の後に「/」が付いているカテゴリです。（例：「RoutingTable/」）

複数のプロパティ値を指定する

コマンドプロパティに複数の値を必要とする場合があります。例えば、いくつかのコマンドでは、プロパティ「AccountingServers」を使用し、このプロパティに複数の値を指定することができます。複数の値を指定する場合、「,」によって区切る必要があります。例えば、3 つのサーバ「server1」、「server2」、「server3」が指定される場合のコマンドのプロパティ指定は以下の通りです。

```
AccountingServers=server1,server2,server3
```

ルールリストに挿入する

IP ルールセットなどのルールセットでは、エントリの順番が重要な意味を持ちます。CLI コマンド「add」を使用した追加の場合、初期値では新しいルールはリストの最後に追加されます。ルールの順番が重要なケースでは、「add」コマンドのオプションとして「Index= パラメータ」を含めることができます。リストの先頭位置への挿入は、「add」コマンド内で「Index=1」というパラメータを使用して指定し、2 番目の位置は、「Index=2」というパラメータというように指定します。

名前の参照

オブジェクトによっては名前を付けることも可能であり、その場合、「add」コマンドで「Name=」パラメータが使用されます。しきい値ルールなどのオブジェクトは、ルールリストにおける順番を示す「Index」値を持っていますが、オプションとして名前をを割り当てることもできます。リスト位置を示す Index、または割り当てられた名前を参照することにより、後続の処理が実行されます。

「CLI Reference Guide」では、「Name=」および「Index=」を含む各 NetDefendOS オブジェクトに利用可能なパラメータオプションをリストアップしています。

固有名称を使用する

利便性と分かりやすさのために、すべてのオブジェクトに名前を割り当てることをお勧めします。必要に応じて、割り当てた名前を参照することができます。特に、CLI スクリプトを作成する場合に、名前による参照が便利です。詳しくは「2.1.7 CLI スクリプト」を参照してください。

CLI では、オブジェクトタイプ内でそれぞれ固有の名前を割り当てる必要があります。例外として、以前の NetDefendOS との下位互換性により、IP ルールが重複名を持つ場合がありますが、こうしたケースは避けることを強くお勧めします。2 つの IP ルール名が重複している場合、後続の CLI コマンドでは「Index」値のみを使用して IP ルールの識別が可能です。重複する名前で IP ルールを参照すると、エラーとなり、エラーメッセージが表示されます。

CLI プロンプトの変更

CLI プロンプトの初期値は以下の通りです。

```
Device:/>
```

以下の CLI コマンドを使用して、「my-prompt:/>」のようにカスタマイズすることができます。

```
DFL-xxxx:/> set device name="my-prompt"
```

本マニュアルでは、コマンドプロンプト「DFL-xxxx:/>」を使用して説明します。

注意 CLI プロンプトは Web インタフェースのデバイス名です。

コマンドラインのプロンプトが新しい文字列に変更される場合、この文字列は Web インタフェースナビゲーションツリーの最上位ノードの新しいデバイス名として表示されます。

変更のアクティブ化およびコミット

CLI を通して現在の設定に何らかの変更をした場合、以下のように activate コマンドを実行しないかぎり、その変更は NetDefendOS にアップロードされません。

```
DFL-xxxx:/> activate
```

変更を正式にするために以下のように commit コマンドを発行する必要があります。

```
DFL-xxxx:/> commit
```

注意 本マニュアルの例題は、アクティブ化が実行されることを想定しています。

本マニュアルの多くの例題は NetDefendOS のコンフィグレーションの編集について記載しています。通常、最終的なアクティブ化のステップは明示的に記載していませんのでご注意ください。

「activate」コマンドの後に「commit」コマンドを指定時間（初期値は 30 秒）以内に入力しないと、変更は行われず、古い設定が自動的に復元されます。「2.1.2 管理アクセスの設定」でより詳しくこのトピックについて記載します。

注意 CLI による設定変更のコミットは Web インタフェースセッションを終了させる場合があります。

CLI により設定の変更をコミットする場合、コミット時にログインしている Web インタフェースブラウザセッションにて、再度ユーザのログインが要求される場合があります。これは Web インタフェースから参照したコンフィグレーションがもう有効でない可能性があるためです。

CLI を使用した NetDefendOS の再起動

コマンドを使用して NetDefendOS を再起動することもできます。

```
DFL-xxxx:/> shutdown
```

本コマンドは、再起動の前にすべての接続と VPN トンネルのグレースフルシャットダウンを実行します。これは、システムの再起動を必要とする多くの状況で十分です。これにはコンフィグレーションのリロード（再構成の操作）が含まれます。

shutdown コマンド実行後、コマンドが処理されるまで遅延（0 ～ 60 の整数値：秒）があります。

```
DFL-xxxx:/> shutdown 30
```

遅延の初期値は 5（秒）です。

NetDefendOS のシャットダウンと再起動の両方を行い、NetDefendOS ローダを含むハードウェアを完全に再初期化するためには、以下のコマンドを使用します。（ハードウェアをオフからオンに切り替えるのと同じ）

```
DFL-xxxx:/> shutdown -reboot
```

「-reboot」オプションは平常時はめったに必要ではありません。再起動により多くの時間を必要とするため、通常は使用しないことをお勧めします。NetDefendOS がアップグレードされる場合、「-reboot」オプションはアップグレードプロセスの間、自動的に実行されます。

Web インタフェースで **Status > Maintenance > Reset & Restore > Restart** メニューを選択し、再起動オプションを選択することによって、同様の再起動処理を実行することができます。

CLI を使用した NetDefendOS の再構成

以下のコマンドを使用して現在のコンフィグレーションの再読み込みとリロードを行います。

```
DFL-xxxx:/> reconf
```

コンフィグレーションのリロードとは別に、ルールとトラフィック処理に関連する NetDefendOS の内部データ構造の多くが初期化されます。
基本的には、通常のオペレーションで再構成を実行することはありませんが、NetDefendOS のメモリ管理に関連する一時的な問題を解決する手段として使用されることがあります。

上記で説明したシステム再起動とは異なり、再構成は通常、現在の接続または VPN トンネルには影響しません。しかし、IPsec トンネルの変更によっては、再構成によってトンネルが削除されトンネル SA が有効でなくなる場合があります。この場合は、トンネルが再確立される必要があります。

コンフィグレーションの整合性の確認

NetDefend OS におけるコンフィグレーションの変更後、「activate/commit」コマンド発行前に、以下のコマンドを使用してコンフィグレーション内に何か問題がないかを明示的に確認することができます。

```
DFL-xxxx:/> show -errors
```

本コマンドにより、アクティブ化されるコンフィグレーションをスキャンして、検出された問題を表示することができます。例えば、復元されたコンフィグレーションのバックアップには存在しない「Address Book」の IP オブジェクトを参照しているケースなどが考えられます。

CLI からログオフする

CLI による操作の終了後、他の人によるシステムへの許可のないアクセスを避けるためにログアウトする必要があります。「logout」コマンド使用してログオフします。

インタフェースにリモート管理アクセスを設定する

CLI を使用してリモート管理アクセスを設定することができます。ここでは管理アクセスが IP アドレス「10.8.1.34」を持つイーサネットインタフェース「if2」を通じて行われるものとします。

はじめに、NetDefendOS のアドレス帳に存在する「if2」に IPv4 アドレスオブジェクトの値を設定します。

```
DFL-xxxx:/> set Address IP4Address InterfaceAddresses/If2_ip Address=10.8.1.34
```

さらに、インタフェースのネットワーク IP アドレスに適切な値に設定する必要があります。

```
DFL-xxxx:/> set Address IP4Address InterfaceAddresses/If2_net Address=10.8.1.0/24
```

この例では、ローカルな IP アドレスが使用されていますが、代わりにパブリック IPv4 アドレスとすることもできます。また、アドレス帳フォルダ InterfaceAddresses に、コンフィグレーションのデフォルトのアドレスオブジェクト保存されているものとします。

次に、リモート HTTP 管理アクセスオブジェクト（この例では「HTTP_if2」とする）を作成します。

```
DFL-xxxx:/> add RemoteManagement RemoteMgmtHTTP HTTP_if2 Interface=if2
Network=all-nets LocalUserDatabase=AdminUsers AccessLevel=Admin HTTP=Yes
```

新しいコンフィグレーションをアクティブ化して、コミットすると、IPv4 アドレス 10.8.1.34 を通したリモート管理アクセスは、Web ブラウザを使用して可能になります。SSH 管理アクセスが必要な場合、RemoteMgmtSSH オブジェクトを追加する必要があります。

上のコマンドでは、all-nets ルートが ISP のゲートウェイに存在していると仮定しています。つまり、インターネットアクセスがファイアウォールで有効であるということを意味します。

sessionmanager で管理セッションを管理する

CLI は、管理セッション自体を管理するために sessionmanager と呼ばれるコマンドを提供します。本コマンドを使用して、以下を含む管理セッションのすべてのタイプを管理します。

- Secure Shell（SSH）CLI セッション
- ローカルコンソールインタフェース経由のすべての CLI セッション
- Secure Copy（SCP）セッション
- HTTP または HTTPS で接続する Web インタフェースセッション

本コマンドをオプションなしで実行した場合、現在オープン中のセッションのサマリを表示します。

```
DFL-xxxx:/> sessionmanager

Session Manager status
----------------------------------
Active  connections         : 3
Maximum allowed connections : 64
Local idle session timeout  : 900
```

「-list」オプションを使用してすべてのセッションのリストを参照します。ローカルコンソールセッションを示す典型的な出力を以下に示します。

```
DFL-xxxx:/> sessionmanager -list

User       Database         IP             Type     Mode     Access   Timeout
---------- ---------------- -------------- -------- -------- -------- --------
local      (none)           0.0.0.0        local    console  admin       -
admin      AdminUsers       192.168.1.12   SSH      console  admin       S
```

ユーザが完全な管理者権限を持つ場合、「sessionmanager」コマンドの「-disconnect」オプションを使用して強制的に別の管理セッションを終了することができます。

「sessionmanager」コマンドオプションは「CLI Reference Guide」にすべて記載されています。

2.1.7 CLI スクリプト

管理者は、NetDefendOS が提供する CLI スクリプティング機能を利用して、CLI コマンドセットの保存と実行を簡単に実施することができます。CLI スクリプトは、事前に定義した CLI コマンドのシーケンスであり、ファイルに保存して、D-Link ファイアウォールにアップロードした後に実行することができます。

CLI スクリプトの作成手順は以下の通りです。

1. テキストエディタを使用して 1 行に 1 コマンドで CLI コマンドの連続したリストを含むテキストファイルを作成します。D-Link が推奨する規則は、これらのファイルにファイル拡張子「.sgs」（Security Gateway Script）を使用することです。ファイル名は、拡張子を含めて 12 文字以内で指定してください。

2. Secure Copy（SCP）を使用して、D-Link ファイアウォールにファイルをアップロードします。多くのサードパーティ製のソフトウェア製品が、様々なコンピュータ環境のために SCP を提供しています。スクリプトファイルは、「script」という名前のルートディレクトリに保存する必要があります。例えば、アップロード用の代表的なコンソールコマンドは以下の通りです。

   ```
   > scp my_script.sgs admin1@10.5.62.11:script/
   ```

   詳しくは「2.1.8 セキュアコピー」を参照してください。

3. CLI コマンド「script -execute」を使用して、スクリプトファイルを実行します。

CLI スクリプトコマンドは、スクリプトの管理と実行に使用されるツールです。コマンドの完全な構文については、「CLI Reference Guide」で説明されており、具体的な使用例は以下のセクションで詳しく説明します。本マニュアルの「2.1.6 CLI の利用方法」も参照してください。

注意 アップロードしたスクリプトは、再起動後に失われます。
アップロードされた CLI スクリプトファイルは、不揮発性メモリに保持されないため、システム再起動後に消去されます。

CLI スクリプトで許可された 4 つのコマンド

スクリプトファイルで許可されるコマンドは以下の 4 つに制限されています。

- add
- set
- delete
- cc

これ以外のコマンドがスクリプトファイルに含まれている場合、実行中に無視されて、警告メッセージが出力されます。例えば、「ping」コマンドは無視されます。

スクリプトを実行する

上述の通り、「script -execute」コマンドは、ファイアウォールに事前にアップロードされた名前付きのスクリプトファイルを実行します。
例えば、事前にアップロードしてあるスクリプトファイル「my_sp.sgs」を実行するために、以下の通り CLI コマンドを指定します。

```
DFL-xxxx:/> script -execute -name=my_sp.sgs
```

スクリプトの変数

スクリプトファイルは以下のようなスクリプト変数を持つことができます。

```
$1, $2, $3, $4......$n
```

これらの変数名に置き換えられる値は、「script -execute」コマンドラインの最後にリストで指定されます。変数名の番号「n」は、ここのリストにおける変数の値の位置を示しています。$1 が 1 番目、$2 が 2 番目となります。

注意 シンボル $0 は、予約されています。
最初の変数名が $1 であることにご注意ください。変数 $0 は予約されていて、実行前にスクリプトファイル自体の名前に置き換えられます。

例えば、「my_sp.sgs」という名前のスクリプトは、スクリプトファイル内のすべての $1 をアドレス 126.12.11.01 に、またすべての $2 を文字列の If1 に置き換えて実行されます。

「my_sp.sgs」ファイルには、以下に示す一つの CLI コマンドラインが含まれています。

```
add IP4Address If1_ip Address=$1 Comments=$2
```

アップロード後にこのスクリプトファイルを実行するには、以下の通り CLI コマンドを指定します。

```
DFL-xxxx:/> script -execute -name=my_sp.sgs 126.12.11.01 "If1 address"
```

スクリプトファイルを実行する場合、変数の置き換えによりファイルの内容は以下のようになります。

```
DFL-xxxx:/> add IP4Address If1_ip Address=126.12.11.01 Comments="If1 address"
```

文字をエスケープする

コマンド内の特殊文字を通常の文字として実行する場合、エスケープする必要があります。これは特にドル記号「$」の場合に当てはまります。ここでは文字列「te$t」について考えてみます。ドル記号を普通の文字として扱うために、バックスラッシュ「\」文字を使用することでエスケープできます。文字列は「te\$t」となり、ドル記号は特殊文字として扱われません。

スクリプトの確認とコマンドの順序

CLI スクリプトはデフォルトでは検証されません。つまり、スクリプト内の記載順序が意味を持たないということです。スクリプトの最初で参照する構成オブジェクトをスクリプトの最後で作成する、といった記載になることも考えられます。

このアプローチは非論理的かもしれませんが、スクリプトの可読性のためにこうした設定になっています。オブジェクトなどが参照される前に作成されている必要があると、整理されていない支離滅裂なスクリプトファイルになる可能性があり、スクリプト量が多いファイルでは、関連する CLI コマンド同士をグループ化することが望ましいと言えます。

エラー処理

CLIのスクリプトファイルの実行によりエラー状態になった場合、動作の初期値としてはスクリプトを終了することになっています。「-force」オプションを使用することで、この動作を変更することができます。例えば、エラーによりスクリプトの実行が終了しないように、「my_sp2.sgs」というスクリプトファイルを実行します。CLI コマンドは以下の通りです。

```
DFL-xxxx:/> script -execute -name=my_sp2.sgs -force
```

「-force」が使用されると、スクリプトファイルのコマンドによってエラーが返されても、スクリプトは実行を続けます。

スクリプト出力

スクリプト実行による出力は CLI コンソールに表示されます。通常、この出力は実行中に発生するエラーメッセージにより構成されています。各コマンドの完了を確認するためには、「-verbose」オプションを使用します。

```
DFL-xxxx:/> script -execute -name=my_sp2.sgs -verbose
```

スクリプトの保存

スクリプトファイルがファイアウォールにアップロードされる場合、最初に一時的な RAM メモリだけに保持されます。NetDefendOS が再起動すると、アップロードされたスクリプトは、この揮発性メモリから失われ、これをもう一度実行するには再びアップロードしなければなりません。再起動時にスクリプトを保存するためには、「script -store」コマンドを使用して不揮発性の NetDefendOS ディスクメモリに移動させる必要があります。

例えば、不揮発性メモリに「my_sp.sgs」を移動するには、以下のコマンドを使用します。

```
DFL-xxxx:/> script -store -name=my_sp.sgs
```

または、以下のコマンドですべてのスクリプトを不揮発性メモリに移動することができます。

```
DFL-xxxx:/> script -store -all
```

スクリプトの削除

保存したスクリプトを削除するためには、「script -remove」コマンドを使用します。例えば、「my_sp」スクリプトを削除するには、以下のコマンドを使用します。

```
DFL-xxxx:/> script -remove -name=my_sp.sgs
```

スクリプトの表示

パラメータを含まない script コマンドを実行した場合、現在利用可能なスクリプト一覧と、各スクリプトのサイズ及び保存されているメモリを表示します（不揮発性メモリに存在する場合は "Disk" と表示されます）。

```
DFL-xxxx:/> script

Name           Storage      Size (bytes)
-------------- ------------ --------------
my_sp.sgs      RAM          8
my_sp2.sgs     Disk         10
```

特定のアップロード済みスクリプトファイル（例えば「my_sp.sgs」）の内容を表示するためには、以下のコマンドを使用します。

```
DFL-xxxx:/> script -show -name=my_sp.sgs
```

自動的にスクリプトを作成する

同じコンフィグレーションオブジェクトを複数の D-Link ファイアウォールの間でコピーする必要がある場合、CLI を使用して、必要なオブジェクトを生成するスクリプトファイルを作成し、各デバイスで同じスクリプトをアップロードして実行する方法があります。

いずれかの NetDefendOS システムに既に設定済みオブジェクトが存在し、それをコピーする必要がある場合には、そのシステムで「script -create」コマンドを実行することで、自動的に必要なスクリプトファイルを作成します。次に、このスクリプトファイルを、ローカルな管理ワークステーションにダウンロードし、オブジェクトを複製するためにファイアウォールにアップロードして実行することができます。

例えば、いずれかのユニットに既に存在する IP4Address オブジェクトと同じものを、複数のファイアウォール上で作成する必要があるケースを想定します。管理者は、CLI を使用してオブジェクトが存在するユニットに接続して、以下のコマンドを発行します。

```
DFL-xxxx:/> script -create Address IP4Address -name=new_sp.sgs
```

new_script_sgs というスクリプトが作成されます。このスクリプトには、ユニットが保持するコンフィグ内の全ての IP4Address を作成する CLI コマンドが含まれます。例えば、作成したファイルの内容は以下の通りです。

```
add IP4Address If1_ip Address=10.6.60.10
add IP4Address If1_net Address=10.6.60.0/24
add IP4Address If1_br Address=10.6.60.255
add IP4Address If1_dns1 Address=141.1.1.1
"
"
"
```

スクリプトを作成後、SCP 経由で「new_sp.sgs」をローカルの管理ワークステーションにダウンロードし、他の D-Link ファイアウォールにアップロード・実行することができます。これにより、すべてのユニット上でアドレス帳に同じ IP4Address オブジェクトを持つことができます。

以下は自動作成したスクリプトで注意すべき項目です。

- 自動作成したスクリプトではオブジェクトカテゴリが省略されます。
  上記の例題で作成されたスクリプトでは、以下のコマンドにより IP アドレスが追加されます。

  ```
  add IP4Address...
  ```

  カテゴリ名を使用してオブジェクトを指定する通常のコマンドは、以下の通りです。

  ```
  add Address IP4Address...
  ```

  両方ともコマンドの有効な形式です。オブジェクトが、オブジェクトタイプ名により一意に識別可能である場合、オブジェクトカテゴリを指定する必要はありません。自動生成されたスクリプトでは、常にそのようになります。また、この短縮形は、CLI コンソールで全体のコマンド文を入力する場合に使用することが可能ですが、Tab 補完では常にオブジェクトカテゴリが含まれます。

- スクリプトファイル名の長さには制限があります。
  「-create」を使用して作成するファイル名は、12 文字以内（拡張子を含む）で、ファイルタイプは「.sgs」になります。

- スクリプトに Set と Add の両方が含まれます。
  デフォルトのコンフィグレーションオブジェクトは Set アクションを持ち、デフォルトのコンフィグレーションに追加されたオブジェクトは Add アクションを持ちます。

- コンフィグレーション全体のスクリプトを作成します。
  以下のコマンドを使用して、コンフィグレーション全体のスクリプトを作成できます。

  ```
  DFL-xxxx:/> script -create -name=all_cnf.sgs
  ```

  これは全体のコンフィグレーションを再設定する場合に役立ちます。

  しかし、以下のオブジェクトは全体のコンフィグレーション用に作成されたスクリプトに含まれないことに注意してください。

  i. 追加された Certificate オブジェクト
  ii. 削除用にマークされたオブジェクト

- いくつかのオブジェクトは作成されるスクリプトファイルから常に除外されます。
  ハードウェアに依存するコンフィグレーションの場合では、「-create」オプションを使用してスクリプトを作成できないものがあります。これは、「script -create」コマンド内の CLI ノードタイプが以下のいずれかである場合に当てはまります。
  - COMPortDevice
  - Ethernet
  - EthernetDevice
  - Device

スクリプトファイルが作成されるときに、これらのノードタイプはスキップされ、NetDefendOS がメッセージ「No objects of selected category or type」を返します。

作成済みのスクリプトコマンドをコンソールに表示する

作成された CLI コマンドを、ファイルに保存せずにコンソール上で表示するには、「script-create」コマンドで「-name=」オプションを外します。

スクリプトファイル内のコメント

スクリプトファイルの「#」文字で始まる行は、コメントして扱われます。例えば以下のようになります。

```
# The following line defines the If1 IP address
add IP4Address If1_ip Address=10.6.60.10
```

他のスクリプトを実行するスクリプト

1 つのスクリプトが別のスクリプトを実行することができます。例えば、スクリプト「my_sp.sgs」には以下の行を含むことができます。

```
script -execute -name my_sp2.sgs
```

NetDefendOS では、スクリプトファイル「my_sp2.sgs」は別のスクリプトファイルを組み込んで実行することができます。このスクリプトのネストの最大値は 5 です。

Web インタフェースからスクリプトを実行する

Web インタフェースを通じて CLI スクリプトをアップロードし、実行することができます。スクリプトは実行後、メモリに保持されません。

本機能では、ファイルタイプ「.sgs」が必須ではありません。どのファイルタイプも許可されます。

例題 2.9

Web インタフェースから CLI スクリプトを実行する

この例題では、Web インタフェースを通じて、ローカルディスクストレージに CLI スクリプト my_script.sgs をアップロードして、実行します。

Web Interface

1. **Status >Maintenance > Import Script** の順にメニューをクリックします。
2. Browse を選択し、スクリプトファイル my_script.sgs を選択します。
3. Upload and Execute を選択します。
4. 実行に成功したことを示すメッセージが表示されます。
5. 変更したコンフィグレーションにはアクティブ化と保存を行う必要があります。

2.1.8 セキュアコピー

D-Link ファイアウォールにファイルをアップロード、または D-Link ファイアウォールからファイルをダウンロードするためには、Secure Copy（SCP）プロトコルを使用します。SCP は SSH プロトコルに基づいており、フリーで利用可能な多くの SCP クライアントが存在し、ほぼすべてのプラットフォームに対応しています。以下のコマンド行の例は、SCP クライアントソフトウェアの最も一般的なコマンド形式に基づいています。

SCP コマンド形式

SCP コマンドの構文は、ほとんどのコンソールベースのクライアントにとって分かりやすいものとなっています。scp コマンドと、それに続くファイル転送時の送信元 / 宛先の指定です。

アップロードは以下のコマンドで実行されます。

```
> scp <local_filename> <destination_firewall>
```

ダウンロードは以下のコマンドで実行されます。

```
> scp <source_firewall> <local_filename>
```

送信元または送信先のファイアウォールは以下の形式となります。

```
<user_name>@<firewall_ip_address>:<filepath>
```

例えば以下のようになります。

```
admin@10.62.11.10:config.bak
```

<user_name> は、管理者ユーザグループに定義されている NetDefendOS ユーザである必要があります。

注意 SCP の例ではパスワードプロンプトを表示しません。

SCP は、通常コマンド行の後にユーザパスワード用のプロンプトを表示しますが、そのプロンプトは本マニュアルの説明の中では記載していません。

以下の表に、SCP クライアントと NetDefendOS の間で実行できる操作をまとめています。

ファイルタイプ	アップロードの可否	ダウンロードの可否
コンフィグレーションのバックアップ（config.bak）	○（Web インタフェースでも使用可）	○（Web インタフェースでも使用可）
システムのバックアップ（full.bak）	○（Web インタフェースでも使用可）	○（Web インタフェースでも使用可）
ファームウェアの更新	○	×
証明書	○	○
SSH 公開鍵	○	×
Web 認証のバナーファイル	○	○
Web コンテンツフィルタのバナーファイル	○	○

NetDefendOS ファイル構成

NetDefendOS は、シンプルな 2 つのレベルのディレクトリ構造で、最上位のルートと多くのサブディレクトリで構成されています。しかし、「sshlclientkey」などの「ディレクトリ」は、より正確にはオブジェクトタイプとしてみなされるべきです。すべてのオブジェクトタイプ及び NetDefendOS のルートに保存されたすべてのファイルは、CLI コマンドの「ls」を使用することで表示することができます。

出力の結果は以下の通りです。

```
DFL-xxxx:/> ls
HTTPALGBanners/
HTTPAuthBanners/
SNMP_MIB/
certificate/
config.bak
factory.txt
full.bak
license.lic
script/
selftest.txt
sshclientkey/
```

個々のファイルとは別に、以下のオブジェクトタイプが表示されます。

オブジェクトタイプ	説明
HTTPAuthBanners/	ユーザ認証に利用される HTML バナーファイルが保存されているフォルダ。詳しくは、「6.2.5 WCF HTML ページのカスタム」を参照してください。
HTTPALGBanners/	HTML ALG のダイナミックコンテンツフィルタリングの HTML バナーファイルが保存されているフォルダ。詳しくは、「6.2.5 WCF HTML ページのカスタム」を参照してください。
SNMP_MIB/	MIB ファイルが保存されているフォルダ。
certificate/	VPN 用にアップロードされた X.509 デジタル証明書が保存されているフォルダ。
script/	CLI スクリプトが保存されているフォルダ。詳しくは「2.1.7 CLI スクリプト」を参照してください。
sshclientkey/	SSH クライアントの公開鍵ファイルが保存されているフォルダ。この公開鍵に一致するインストール済みの秘密鍵を持つ SSH クライアントの自動認証が許可されます。ファイル名には拡張子（ピリオドの文字）が含まれてはいけません。ファイルのアップロード後、管理者はユーザオブジェクトにファイルを紐付けて、ユーザの自動認証を有効化します。 証明書を使用した SSH 認証についての詳細は、「2.1.5 CLI 接続」を参照してください。

アップロードとダウンロードの例

いくつかのファイルは NetDefendOS ルートディレクトリに置かれています。コンフィグレーションバックアップファイル (config.bak) と完全なシステムバックアップファイル (full.bak) はルートディレクトリに保存されます。アップロードの際、これらのファイルに含まれる固有のヘッダによってファイルの識別が行われます。NetDefendOS がこのヘッダをチェックすることにより、該当するファイルはルートのみに保存されます。（すべてのファイルがヘッダを持つというわけではありません。）

管理者のユーザ名が「admin1」であり D-Link ファイアウォールの IPv4 アドレスが「10.5.62.11」である場合、コンフィグレーションのバックアップをアップロードする SCP コマンドは以下の通りとなります。

```
> scp config.bak admin1@10.5.62.11:
```

コンフィグレーションのバックアップを現在のローカルディレクトリにダウンロードには、以下のコマンドを実行します。

```
> scp admin1@10.5.62.11:config.bak ./
```

ルート配下にあるオブジェクトタイプにファイルをアップロードには、少し異なるコマンドを実行します。「my_sp.sgs」というローカルの CLI スクリプトファイルがある場合、アップロードコマンドは以下の通りとなります。

```
> scp my_sp.sgs admin1@10.5.62.11:script/
```

「my_sp.sgs」という名前の CLI スクリプトファイルがファイアウォールに保存されている場合、ダウンロードコマンドは以下の通りとなります。

```
> scp admin1@10.5.62.11:script/my_sp.sgs ./
```

アップロードのアクティブ化

すべてのコンフィグレーション変更と同様に、SCP アップロードも、CLI コマンド「activate」が発行された後にアクティブ化され、さらに続けて「commit」によって変更を確定する必要があります。

ファームウェア更新（「.upg」ファイルにパッケージされている）または完全なシステムのバックアップ（full.bak）のアップロードは例外です。これらのファイルタイプでは、自動的にシステムの再起動が発生します。もう一つの例外は、コンフィグレーションに影響しないスクリプトのアップロードです。

2.1.9 コンソールブートメニュー

NetDefendOS ローダは、基本ソフトウェアでありその上で NetDefendOS が動作しています。そして、これに対する管理者の直接インタフェースは、コンソールブートメニュー（または、単にブートメニュー）と呼ばれます。本セクションではブートメニューオプションについて説明します。

コンソールブートメニューにアクセスする

ブートメニューには、本製品のローカルコンソールポートに直接接続したコンソールデバイスを経由することでのみアクセスすることができます。ブートメニューには、本製品の電源をオンにした後、NetDefendOS の起動が終了する前にコンソールポートからアクセスします。

コンソールメニューは、本製品の電源をオンにした後、NetDefendOS の起動が終了する前にコンソールポートからアクセスします。電源オンの後に、NetDefendOS が完全に起動するまで 3 秒間あり、その間以下の通り「Press any key to abort and load boot menu」が表示されます。

```
Starting core in 3 seconds.
Press any key to abort and load boot menu


Loading bootmenu.cfx
```

図 2-4　ブート画面

この 3 秒間にコンソールキーのどれかを押すと、NetDefendOS の起動は中断し、コンソールメニューが表示されます。

パスワード設定のない初期メニューオプション

コンソール接続用に設定されたコンソールパスワードがない状態で、NetDefendOS を初回起動した場合、以下のコンソールメニューオプションのフルセットが表示されます。

```
================================================================
 D-Link serial console menu v2.02.03
================================================================
 1. Start firewall
 2. Reset unit to factory defaults
 3. Revert to default configuration
 4. Set console password

Select menu item:
```

図 2-5　ローカルコンソールメニュー画面

コンソールメニューで利用可能なオプションは以下の通りです。

1. Start firewall（ファイアウォールの開始）
本製品上で NetDefendOS ソフトウェアを完全に起動します。

2. Reset unit to factory defaults（工場出荷時設定にユニットをリセットする）
工場出荷時の状態にハードウェアをリストアします。本オプションが選択されると、以下の処理が実行されます。

- コンソールセキュリティを削除します。コンソールパスワードは削除されます。
- 初期設定及び初期状態の NetDefendOS プログラムをリストアします。

3. Revert to default configuration（初期設定に戻す）
コンフィグレーションを初期状態の NetDefendOS コンフィグレーションファイルになるようにリセットします。コンソールセキュリティなどの他のオプションは影響を受けません。

4. Set console password（コンソールパスワードの設定）
コンソール用のパスワードを設定します。パスワードが設定されないと、だれでもコンソールを使用できてしまうため、必ず設定してください。パスワードが設定されると、ブートメニュー及びコマンドラインインタフェース（CLI）でパスワードの入力が要求されます。

コンソールパスワード設定後の初期オプション

コンソールパスワードが設定されている場合、NetDefendOS ローディングがキーの押下によって中断された場合に表示する初期オプションは以下の通りです。

```
================================================================
 D-Link login
================================================================
 1. Start firewall
 2. Login

Select menu item:
```

図 2-6　Login 画面

コンソールメニューで利用可能なオプションは以下の通りです。

1. Start firewall（ファイアウォールの開始）
中断された NetDefendOS のスタートアッププロセスを再開します。

2. Login（コンソールメニューへのログイン）
コンソールパスワードを入力する必要があり、前述のフルブートメニューに進みます。

コンソールパスワードの削除
コンソールパスワードが設定された後は、ブートメニューで「Set console password」オプションを選択し、パスワードとして何も入力せずに Enter キーを押すだけで、コンソールパスワードを削除できます。

コンソールパスワードはコンソール専用
コンソールに設定されたパスワードは、Web ブラウザで管理者がアクセスするために使用される管理ユーザ名 / 管理パスワードとは関連づけされません。コンソールアクセスにだけ有効です。

2.1.10 RADIUS 管理認証

デフォルトの NetDefendOS コンフィグレーションに含まれるシステム管理タスクを使用するには、管理者が Web インタフェースまたは SSH 経由の CLI にログインする必要があります。SSH では、ローカルの NetDefendOS データベースに保存された資格情報に対して、ユーザ名とパスワードの検証が行われます。

NetDefendOS は、ローカルデータベースを使用する代わりに、外部の RADIUS サーバに対する資格情報の認証プロセスを実行することもできます。これは、Web インタフェースのアクセス用の Remote Management オブジェクト mgmt_http のプロパティ、および / または SSH 経由の CLI アクセス用の mgmt_ssh オブジェクトのプロパティを変更することで有効にすることができます。RADIUS 認証のためにこれらのオブジェクトのどちらかを設定する手順は以下の通りです。

- Authentication Source に RADIUS を指定します。

- Authentication Order プロパティを以下のオプションから選択します。
  i. **Local First** - ログイン資格証明書は最初にローカルユーザデータベースで調べられます。ローカルデータベースで検出されない場合、設定した RADIUS サーバに問い合わせます。

  ii. **Local Last** - 定義済みの RADIUS サーバのすべてが認証要求に応答しない場合にだけ、ローカルのデータベースに問い合せます。

- 認証に使用する 1 つ以上の RADIUS サーバを選択します。2 つ以上あると、1 つが利用できない場合に順番に試行されます。選択するサーバは、NetDefendOS に RADIUS サーバオブジェクトとして設定済みである必要があります。（詳しくは「9.2.3 外部 RADIUS サーバの設定」を参照してください。）

- Admin グループ、および / または Audit グループを指定して、ログイン資格証明書が RADIUS サーバによって認証された時に、付与するアクセス権の種類を決定します。NetDefendOS は、これらのグループ名を RADIUS サーバが返すユーザのグループ名と照合します。ワイルドカード文字であるアスタリスク「*」を 1 文字でこれらのプロパティのどちらかに設定すると、どんなグループもそのアクセス権を得ることを意味します。いずれかのプロパティを空白にすることは、アクセス権を持つユーザはいないことを意味します。

  管理者グループは監査グループより高い優先度を持っています。これは、ユーザが最初に管理者グループのメンバであることが認証されると、監査グループメンバシップは無視されることを意味します。そのため、Admin グループプロパティにアスタリスク「*」文字を指定すると、Audit グループのメンバシップが検証されないことを意味します。

  グループ名のすべてまたは一部の代わりにワイルドカード「*」文字を使用することができます。例えば、文字列の「sys*」は 3 つの文字列「sys」で始まる任意のグループ名を意味します。

重要 サーバにグループメンバシップを定義しなければなりません。

RADIUS サーバで認証されるすべての管理ユーザが、RADIUS サーバで定義されたグループメンバシップを必要とすることに注意してください。Admin Groups と Audit Groups で照合するグループメンバシップではない場合、認証されません。

注意 RADIUS Vendor ID をグループメンバシップに設定してください。

RADIUS サーバがグループメンバシップを送信する必要がある場合、サーバを設定する際にユーザグループのベンダ固有の属性ベンダを使用する必要があります。NetDefendOS Vendor ID は「5089」で、ユーザグループは vendor-type 1 として文字列タイプの値で定義されます。

グループ不一致用のログインメッセージの変更

管理者によるログインアクションは、RADIUS 認証と非 RADIUS 認証で同じようなアクションとなります。

しかし、1 つの例外があります。ユーザの資格証明書が正しいにも関わらず、RADIUS サーバが返したグループ名が Admin Groups または Audit Groups 内のどのグループにもマッチしないと、Web インタフェース、または CLI は以下のメッセージを表示します。

```
You do not have permission to access this device.
```

ログイベントメッセージの生成

ログメッセージは管理者のログイン成功またはログイン失敗を示します。RADIUS 管理認証では、ログメッセージは以下のフィールド値を表示します。

フィールド	説明
usergroups	RADIUS サーバの認証によって返されたすべてのグループメンバシップのリストを示します。多くの場合、ユーザがログインに失敗した理由を障害調査するのに役立ちます。
access_level	認証成功により与えられた特権を示します。
authsource	RADIUS サーバ名を示します。
userdb	使用される RADIUS サーバオブジェクト名を示します。
server_ip	クライアントが接続している NetDefendOS インタフェースの IP です。認証する RADIUS サーバの IP アドレスではありません。
client_ip	ログインしようとしているユーザコンピュータの IP です。

ログイベントメッセージの代表的な例は以下の通りです。

- Successful RADIUS Authentication

  system_admins グループの一部であるユーザでのログインに成功した。

```
event=admin_login authsystem=HTTP interface=If1 username=jdoe usergroups=sys_
admins access_level=administrator authsource=RADIUS userdb=radius_auth1 server_
ip=192.168.1.1 server_port=80 client_ip=192.168.1.30 client_port=6132
```

- Insufficient Access Rights

  ユーザは正しいユーザ名とパスワードを入力したが、RADIUS サーバ (以下の例では sys_admins) が返したグループ名が Admin Groups または Audit Groups リストのどちらにも見つけられなかった。

```
event=admin_authorization_failed action=disallow_admin_access authsystem=HTTP
interface=If1 username=jdoe usergroups=sys_admins authsource=RADIUS
userdb=radius_auth1 server_ip=192.168.1.1 server_port=80 client_ip=192.168.1.30
client_port=6042
```

- Servers Unreachable

  すべての定義済み RADIUS サーバは到達不能で、タイムアウトが発生した。

```
event=admin_authsource_timeout authsystem=HTTP interface=If1 username=jdoe
authsource=RADIUS server_ip=192.168.1.1 server_port=80 client_ip=192.168.1.30
client_port=5987
```

Local Console は Fallback Option である

RADIUS サーバが入力した資格証明書を認証せず、ローカルデータベースでも許可されないと、Web インタフェースまたは SSH 経由の CLI から管理者がログオンできない状態になります。そのような場合は、D-Link ファイアウォールのローカルコンソールポートを使用して管理アクセスを行うことができます。しかし、パスワードがローカルコンソールに設定されていると、ローカルコンソールで CLI 管理を行うためにパスワードが必要となります。（コンソールのパスワードは他の管理パスワードとは完全に異なることに注意してください。）

例題 2.10

RADIUS 管理認証を有効にする

この例題では、認証が 2 つの RADIUS サーバを使用して実行されるように、Web インタフェース管理アクセス用の現在のデフォルトルールを変更します。RADIUS サーバオブジェクトがコンフィグレーションに既に設定され、radius_auth1 と radius_auth2 という名前を持つものとします。radius_auth2 は、radius_auth1 が応答エラーになった場合のフォールバックサーバです。

Authentication Order には、NetDefendOS データベースが最初に参照されることを意味する Local First に設定します。ローカルデータベースでユーザが検出されない場合、RADIUS サーバへの問合せが行われます。

グループ「sys_admins」のメンバであるすべてのユーザがフルアクセス権限を許可され、他のすべての認証ユーザは、監査権限のみ持ちます。

CLI

ユーザを含むユーザデータベースになるように CLI コンテキストを変更する

```
DFL-xxxx:/> set RemoteManagement RemoteMgmtHTTP rmgmt_http AuthSource=RADIUS AuthOrder=LocalFirst
            RadiusServers=radius_auth1,radius_auth2 AdminGroups=sys_admins
```

Web Interface

1. **System > Device > Remote Management** の順にメニューをクリックします。
2. rmgmt_http オブジェクトを選択します。
3. Authentication Source に RADIUS を設定します。
4. Authentication Order に Local First を設定します。
5. RADIUS servers に radius_auth1 を選択し、Include をクリックします。
6. radius_auth2 を選択して、前の手順を繰り返します。
7. Admin Groups を sys_admins に設定します。
8. 「OK」ボタンをクリックします。

2.1.11 強化されたパスワード

システムのセキュリティを保つため、NetDefendOS にはローカルユーザデータベースのユーザに対し Strong Password（複雑なパスワード）を強制するグローバルオプションがあります。このオプションは、NetDefendOS V11.10.00 以降で利用可能です。

Strong Password では次のルールが適用されます。

- 8 文字以上
- ユーザ名の大部分が含まれていないこと
- 次の 4 つのうち、3 つ以上のルールに適合していること
  - 1 文字以上の小文字を含む
  - 1 文字以上の大文字を含む
  - 1 文字以上の数字（0 ～ 9）を含む
  - 1 文字以上の記号（!、$、% など）を含む

Strong Password の有効化

Strong Password は、NetDefendOS の新規インストール時の初期状態では有効化されています。この機能は手動で無効化することも可能であり、NetDefendOS のセットアップウィザードでも設定が可能です。

セットアップウィザードで無効化しない場合、初期値のパスワード「admin」を変更するように要求されます。Strong Password を有効化したままウィザードを中止すると、パスワードが Strong Password のルールに従っていない限り、他の設定をアクティブ化することができません。

Strong Password の検証

Strong Password が有効化されている場合、以下のタイミングでパスワードの強度が検証されます。

- ローカルユーザデータベースに新しいユーザが追加され、パスワードが設定された場合
- 既存ユーザのパスワードが変更された場合

「admin」ユーザの他に、NetDefendOS のコンフィグレーションには定義済みのユーザ「audit」が存在します。パスワードの初期値は audit です。管理者がユーザ「audit」のパスワードを変更し、上記で述べたルールに適合するまでは脆弱なままとなります。

古い NetDefendOS の更新

Strong Password の機能は NetDefendOS V11.10.00 以降で実装されています。それより古いバージョンを V11.10 以降にアップグレードした場合、Strong Password 機能は無効化された状態となります。必要に応じて、管理者により有効化することができます。

アップグレード後に本機能を有効化した場合、アップグレード前に作成された全てのユーザは、Strong Password が設定されていないものとしてフラグが付いています。古いコンフィグレーションの脆弱なパスワードに対して Strong Password フラグが設定された場合、そのユーザのパスワードについて、アップグレード後に Strong Password に適合するように変更する必要があります。Strong Password が有効化されている場合、NetDefendOS により、入力された新しいパスワードが Strong Password のルールに従っていることが検証されます。

ユーザパスワードのステータス検証

Web インタフェース上で表示されるローカルユーザデータベースのユーザリストには「Strong Password」の項目があります。本項目の値には「yes」または「No」が表示され、Strong Password に適合しているかどうかを示します。

例題 2.11

Strong Password を無効化する

この例題では、Strong Password を無効化し、ローカルユーザデータベースにおける複雑なパスワードの強制を行わないように設定します。

CLI

```
DFL-xxxx:/> set Settings MiscSettings EnforceStrongPasswords=No
```

Web Interface

1. **System > Advanced Settings > Device Settings > Misc. Settings** の順にメニューをクリックします。
2. Enforce Strong Passwords のチェックを外します。
3. 「OK」ボタンをクリックします。

2.1.12 詳細な管理設定

Web インタフェースの「Remote Management（リモート管理）」セクション配下の Advanced Settings には、以下のような詳細な設定が多数あります。

項目	説明
Local Console Idle Timeout	指定された時間（秒）内で何も操作が行われないと、ローカル（シリアル）コンソールユーザはログアウトします。 初期値 : 900
Validation Timeout	指定された時間（秒）内で管理者がログインしないと、元のコンフィグレーションに戻ります。 初期値 : 30
SSH Before Rules	設定した IP ルールにかかわらず、SSH トラフィックをファイアウォールに対して有効にします。 初期値 : Enabled（有効）
Web Before Rules	設定した IP ルールにかかわらず、HTTP（S）トラフィックをファイアウォールに対して有効にします。 初期値 : Enabled（有効）
WebUI Idle timeout	指定された時間（秒）内で何も操作が行われないと、HTTP(S）セッションが閉じられます。 初期値 : 900
WebUIHTTP port	Web インタフェース用の HTTP ポートを指定します。 初期値 : 80
WebUI HTTPS port	Web インタフェース用の HTTP（S）ポートを指定します。 初期値 : 443
WebUI Allow Login Auto Complete	Web ブラウザにユーザ名とパスワードの記録を許可します。 初期値：Enabled（有効）
HTTPS Certificate	HTTPS トラフィックに使用する証明書を指定します。RSA 証明書だけがサポートされています。 初期値 : HTTPSAdminCert
HTTPS Root Certificates	ルート証明書を指定します。

2.1.13 構成オブジェクトの設定

構成オブジェクト

システムコンフィグレーションは、コンフィグレーションオブジェクトによって構築されています。各オブジェクトはあらゆる種類の設定可能なオブジェクト（ルーティングテーブルエントリ、アドレス帳エントリ、サービス定義、IP ルールなど）を示しています。各構成オブジェクトは、多くのプロパティを持っています。

オブジェクトタイプ

構成オブジェクトは、明確に定義されたタイプを持っています。タイプにより、コンフィグレーションオブジェクトに利用可能なプロパティや、それらプロパティの制約が定義されます。例えば、IP4Address タイプは名前付きの IPv4 アドレスを示す全てのコンフィグレーションオブジェクトに使用されます。

オブジェクト構成

Web ユーザインタフェースでは、構成オブジェクトがオブジェクトタイプに基づいたツリー構造で体系化されています。

CLI では、類似の構成オブジェクトタイプが一つのカテゴリにグループ化されます。これらのカテゴリは、CLI では構成オブジェクトにすばやくアクセスできるように Web ユーザインタフェースで使用される構造とは異なります。例えば、IP4Address、IP4Group および EthernetAddress というタイプは、それらがすべて異なるアドレスを表すためものとして Address という名前のカテゴリにグループ化されます。同時に、Ethernet および VLAN オブジェクトは、すべてインタフェースオブジェクトとして、Interface という名前のカテゴリにグループ化されます。カテゴリは、システム設定には実際には影響を与えません。単に管理を簡単にする手段として提供されています。

以下の例は、オブジェクトを処理する方法を示しています。

例題 2.12

構成オブジェクトをリスト表示する

オブジェクトの一覧を取得し、存在する構成オブジェクトを参照することができます。ここでは、すべてのサービスオブジェクトを表示する方法を説明します。

CLI

```
DFL-xxxx:/> show Service
```

サービス一覧は、各タイプによってグループ化され、表示されます。

Web Interface

1. **Objects > Services** の順にメニューをクリックします。

2. すべてのサービスの一覧がメイン画面に表示されます。

このリストには、次のような基本的な要素があります。

- **Add ボタン**
  クリックすると、プルダウンメニューが表示されます。リストに追加可能なすべてのタイプの設定項目が選択肢として表示されます。
- **一覧のヘッダ**
  このヘッダ行はリストの各列のタイトルを表示します。各タイトル横の矢印 はリストをその項目でソートする場合に使用します。
- **行**
  リストの各行が 1 つの設定項目に対応しています。通常、各行は、(名前を持っている場合)オブジェクト名から始まり、各列の値が続きます。

リスト内の各行はハイパーリンクのない場所をクリックすることで選択でき、背景は濃い灰色に変わります。選択した行で右クリックすると、メニューが表示され、そのオブジェクトを「edit」(編集)または「delete」(削除)することができます。

例題 2.13

構成オブジェクトを表示する

構成オブジェクトに対する最も簡単な操作は、そのプロパティ値などを参照することです。ここでは、telnet サービスを表す構成オブジェクトの内容を表示する方法を説明します。

CLI

```
DFL-xxxx:/> show Service ServiceTCPUDP telnet

       Property   Value
---------------- -------------
           Name: telnet
DestinationPorts: 23
           Type: TCP
     SourcePorts: 0-65535
        SYNRelay: No
  PassICMPReturn: No
            ALG: <empty>
     MaxSessions: 1000
        Comments: Telnet
```

Property 列には、ServiceTCPUDP クラスの全プロパティ名が表示され、Value 列には、対応する値が表示されます。

Web Interface

1. **Objects > Services** の順にメニューをクリックします。
2. リスト内の「telnet」エントリを選択します。
3. 「telnet」サービスを表示するページが表示されます。

参照 CLI 経由でオブジェクトにアクセスする場合、カテゴリ名を省略し、タイプ名のみを使用することができます。例えば上の例題の CLI コマンドは以下のように簡略化することができます。

```
DFL-xxxx:/> show ServiceTCPUDP telnet
```

例題 2.14

構成オブジェクトを編集する

NetDefendOS の動作が変更された場合、いくつかのオブジェクトを編集する必要があるかもしれません。ここでは、telnet サービスの「Comments」を編集する方法を説明します。

CLI

```
DFL-xxxx:/> set Service ServiceTCPUDP telnet Comments="Modified Comment"
```

新しいプロパティ値の確認のために再度オブジェクトを参照します。

```
DFL-xxxx:/> show Service ServiceTCPUDP telnet

       Property   Value
---------------- -------------
           Name: telnet
DestinationPorts: 23
           Type: TCP
     SourcePorts: 0-65535
        SYNRelay: No
  PassICMPReturn: No
            ALG: <empty>
     MaxSessions: 1000
        Comments: Modified Comment
```

Web Interface

1. **Objects > Services** の順にメニューをクリックします。
2. リスト内の「telnet」エントリを選択します。
3. 「Comments」テキストボックスに新しいコメントを入力します。
4. 「OK」ボタンをクリックします。
5. 新しいコメントがリスト内で更新されたことを確認します。

注意 構成の変更を、アクティブ化する必要があります。
構成オブジェクトへの変更は、アクティブ化して変更をコミットするまで動作中のシステムには適用されません。

例題 2.15

構成オブジェクトを追加する

ここでは IPv4 アドレス 192.168.10.10 を IPv4 アドレスオブジェクトとしてアドレス帳に追加する方法を説明します。

CLI

```
DFL-xxxx:/> add Address IP4Address myhost Address=192.168.10.10
```

新しいオブジェクトを参照します。

```
DFL-xxxx:/> show Address IP4Address myhost

           Property   Value
-------------------- -------------
                Name: myhost
             Address: 192.168.10.10
      UserAuthGroups: <empty>
NoDefinedCredentials: No
            Comments: <empty>
```

Web Interface

1. **Objects > Address Book** の順にメニューをクリックします。

2. 「Add」ボタンをクリックし、プルダウンメニューから「IP4 Address」を選択します。

3. 以下の通り「Name」と「Address」を入力し、「OK」ボタンをクリックします。
< 入力例 >
General
   - Name : myhost
   - Address : 192.168.10.10

4. 新しい IPv4 アドレスオブジェクトがリストに追加されたことを確認します。

例題 2.16

構成オブジェクトを削除する

ここでは、IP4Address オブジェクトを削除する方法を説明します。

CLI

```
DFL-xxxx:/> delete Address IP4Address myhost
```

Web Interface

1. **Objects > Address Book** の順にメニューをクリックします。

2. 「myhost」オブジェクトを含む行で右クリックし、プルダウンメニューから「Delete」を選択します。

3. オブジェクトに削除を示す取り消し線が引かれます。

例題 2.17

構成オブジェクトの削除を取り消す

削除されたオブジェクトは、アクティブ化とコミットを行う前にリストアすることができます。ここでは、「例題 2.16」で削除した IP4Address オブジェクトをリストアする方法を説明します。

CLI

```
DFL-xxxx:/> undelete Address IP4Address myhost
```

Web Interface

1. **Objects > Address Book** の順にメニューをクリックします。

2. 「myhost」オブジェクトを含む行で右クリックし、プルダウンメニューから「Undo Delete」を選択します。

例題 2.18

変更した構成オブジェクトをリスト表示する

いくつかの構成オブジェクトの編集後に、最後のコミット以来、変更、追加および削除したオブジェクトの一覧を参照することができます。ここでは、変更を行った構成オブジェクトをリスト表示する方法を説明します。

CLI

```
DFL-xxxx:/> show -changes

  Type           Object
  -------------- -----
- IP4Address     myhost
* ServiceTCPUDP  telnet
+ RemoteMgmtSSH  ssh
```

各行の先頭のマークの意味は以下の通りです。

+ : オブジェクトが追加されたことを示します。
* : オブジェクトが変更されたことを示します。
- : オブジェクトに削除マークがついていることを示します。

Web Interface

1. メニューバーの **Configuration > View Changes** メニューをクリックします。

2. 変更一覧が表示されます。

設定をアクティブ化およびコミットする

設定オブジェクトの変更後、その変更が動作中のシステムに適用されるためにアクティブ化する必要があります。アクティブ化の処理中に、新しく提供された設定は有効になり、新しいコンフィグレーションデータによって、関連するサブシステムの初期化が行われます。

注意 IPsec 変更をコミットする

管理者は、アクティブな IPsec トンネルの設定に影響する変更がコミットされた場合、使用中のトンネル接続は終了され、再確立する必要があることに注意してください。

新しい設定が有効になると、NetDefendOS は、管理者が再度確立を行う間（初期値で 30 秒）待機します。前述の通り、設定が CLI 経由でアクティブ化される場合は、「commit」コマンドを期間内に発行する必要があります。接続が再度確立されなかったり、「commit」コマンドが発行されないと、NetDefendOS は以前の設定を使用するようにコンフィグレーションを元に戻します。これは、フェールセーフメカニズムであり、リモート管理者が自分自身をロックアウトするのを防ぐのに役立ちます。

例題 2.19

構成のアクティブ化とコミットを行う

ここでは、新しい構成のアクティブ化とコミットを行う方法を説明します。

CLI

```
DFL-xxxx:/> activate
```

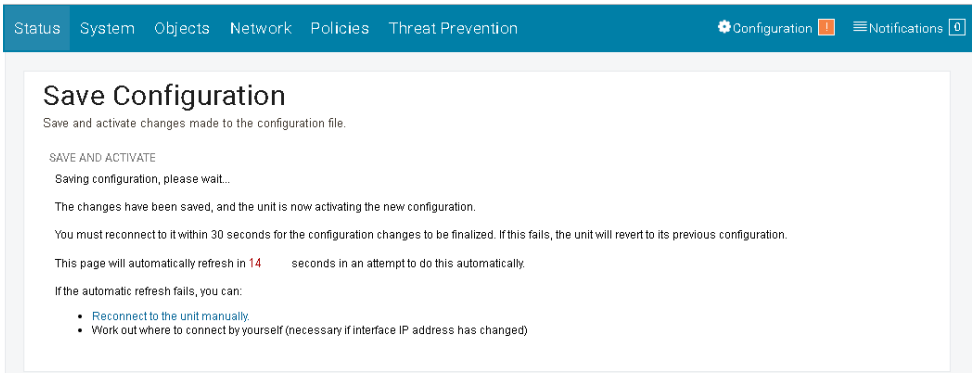
本システムは、新しい構成を検証し、使用を開始します。コマンド入力状態になった後、次のコマンドを実行します。

```
DFL-xxxx:/> commit
```

新しい構成がコミットされます。

Web Interface

1. メニューバーで **Configuration > Save and Activate** をクリックします。
2. 設定を確認するページが表示されますので、「OK」ボタンをクリックします。
3. 以下のページが表示され、新しい構成が保存されます。



Web ブラウザは 10 秒後に Web インタフェースに自動的に接続を行います。接続が成功すると、リモートマネジメントがまだ動作していると認識されます。新しい構成は、その後自動的にコミットされます。

注意 管理者アカウントの変更時など、Web インタフェースへの自動ログインが行われない場合には 30 秒以内に手動でログインを行う必要があります。ログインしない場合、システムの構成は以前の設定に戻ります。

4. 新しい構成がアクティブになると、以下の画面が表示されます。

参照 変更はコミットされる必要があります。

設定は、変更が保存される前にコミットされる必要があります。逆に、構成に対するすべての変更は、コミットしないことで無効とすることができます。

2.2 システムの日時設定

2.2.1 概要

NetDefendOS が正しく動作するためには、日付と時刻を正しく設定することが重要です。 スケジュールされたポリシー、IDP およびアンチウイルスデータベースの自動更新、およびデジタル証明書などのその他の製品機能では、システムクロックが正確に設定されている必要があります。

さらに、ログメッセージには、特定のイベントがいつ発生したかを示すためにタイムスタンプが付いています。 これは、時計が正確であるだけでなく、時計がネットワーク内の他の機器と正しく同期していることを前提としています。

時間設定の方法

NetDefendOS は 2 つの方法で時間を設定することができます。

- 手動で設定する
  管理者は手動で日時を設定できます。これは、「2.2.2 日時の手動設定」で説明します。

- 外部のタイムサーバを使用する
  NetDefendOS は、時間同期プロトコルを使用する外部のタイムサーバの使用をサポートしており、パブリックインターネットからこれらのサーバに送信されたクエリに対する応答を使用して自動的にローカルシステムクロックを調整します。これは「2.2.3 外部タイムサーバの使用」で、より詳しく説明します。

  NetDefendOS が使用できるタイムサーバには以下の 2 つのタイプがあります。

  i. パブリックサーバ - 誰でも使用できるサーバです。
  ii. D-Link サーバ - D-Link の所有するタイムサーバです。日時設定の推奨の方式です。

2.2.2 日時の手動設定

現在の日付と時刻の設定

管理者は手動で日時を設定することが可能であり、新しい NetDefendOS の使用を開始したときは、この方式が推奨されます。

例題 2.20

現在の日付と時刻を設定する

以下の手順に従って、現在の日付と時間を調節します。

CLI

```
DFL-xxxx:/> time -set YYYY-mm-DD HH:MM:SS
```

YYYY-mm-DD HH:MM:SS が新しい日付と時刻に設定されます。
日付の順番は年、月、日であることに注意してください。

例えば、2007 年 4 月 27 日午前 9:25 に日時を設定するためには、コマンドは以下の通りとします。

```
DFL-xxxx:/> time -set 2007-04-27 09:25:00
```

Web Interface

1. **System > Device > Date and Time** の順にメニューをクリックします。

2. Current Date and Time に現在の日時を入力し、「Set」ボタンをクリックします。

3. 「OK」ボタンをクリックします。

注意 再構成は必要ありません。
新しい現在の日付と時間が直ちに適用されます。システムの再構成または再起動は必要ありません。

タイムゾーン

世界は、ロンドンを経度 0 度としたグリニッジ標準時（GMT）に従っていくつかのタイムゾーンに分割されています。経度 0 度から東西のタイムゾーンは、グリニッジ標準時からプラス、マイナスの整数時で表されます。あるタイムゾーンに属するすべての場所は同じローカルタイムを持ち、グリニッジ標準時からの時間差が表示されます。

サマータイム（DST : Daylight Saving Time）

NetDefendOS では、タイムゾーンは Date and Time のオブジェクトである Location プロパティにより設定されています。NetDefendOS には利用可能な全てのタイムゾーンのデータベースが存在し、管理者は、システムの子午線の位置が一致する場所を選択するだけで設定することが可能です。

初期値では、Location プロパティは「DLinkHQ」（Taipei 時間）に設定されています。DST（サマータイム）プロパティについても初期値で有効化されており、選択したロケーションに合わせて自動的に設定されます。

管理者は、Location プロパティを変更することができます。また、NetDefendOS が最初に起動したときに実行されるスタートアップウィザードの設定でも変更することができます。

例題 2.21

タイムゾーンを変更する

この例題では、NetDefendOS のタイムゾーンを初期値から Tokyo に変更します。

CLI

```
DFL-xxxx:/> set DateTime Location=Asia/Tokyo
```

Web Interface

1. **System > Device > Date and Time** の順にメニューをクリックします。
2. Location で Asia/Tokyo を選択します。
3. 「OK」ボタンをクリックします。

2.2.3 外部タイムサーバの使用

NetDefendOS は 1 つ以上の外部タイムサーバから受信した情報を使用することで、自動的にシステム時間を調整できます。これらの時間は、通常、原子時計を使用して高精度な時間を提供します。NetDefendOS が他のネットワークデバイスと日時の整合性を確実にするためには、タイムサーバを使用することをお勧めします。

時刻同期プロトコル

時刻同期プロトコルは、外部のタイムサーバから時間情報を検索するために標準化された方法です。NetDefendOS は、以下のプロトコルをサポートしています。

プロトコル	説明
SNTP プロトコル（SNTP）	RFC 2030 によって定義された Simple Network Time Protocol（SNTP）は、NTP（RFC 1305）を簡易化したものです。SNTP は、NetDefendOS がタイムサーバにクエリを送信するために使用されます。多くの公共のタイムサーバは NTP サーバと呼ばれており、SNTP を使用することでアクセスが可能です。
UDP/TIME	UDP/TIME プロトコルはインターネット上で時刻同期化サービスを提供するのに使われてきた方法です。サーバは 1900 年 1 月 1 日真夜中以来の時間を秒単位で返信しています。

タイムサーバの設定方法

NetDefendOS は以下の 2 つのタイプのタイムサーバから 1 つを設定する機能を提供します。

- D-Link タイムサーバ
  D-Link は公的に利用可能なサーバの代わりに使用できる D-Link 自身のタイムサーバを運用しています。

- カスタムタイムサーバ
  特定のタイムサーバを指定できます。公に利用可能ないくつかのタイムサーバを設定することができます。

これらが 2 つのタイプのサーバを設定する方法を次に説明します。

D-Link タイムサーバの設定

D-Link タイムサーバの利用をオンまたはオフに切り換えるプロパティがあります。これは、他のどんなサーバの詳細も指定する必要がないので、タイムサーバを設定する最も簡単な方法です。NetDefendOS は、タイムサーバの FQDN に関する DNS ルックアップを実行することによって、タイムサーバの IP アドレスを検出します。

D-Link のタイムサーバの FQDN を解決することができるように、NetDefendOS に少なくとも 1 つの外部 DNS サーバを設定する必要があることにご注意ください。

例題 2.22

D-Link タイムサーバを使用する

D-Link NTP サーバの使用を有効にします。

CLI

```
DFL-xxxx:/> set DateTime TimeSynchronization=D-Link
```

Web Interface

1. **System > Device > Date and Time** の順にメニューをクリックします。
2. D-Link (pre-configured timesync server) を選択します。
3. 「OK」ボタンをクリックします。

カスタムタイムサーバを設定する

NetDefendOS が複数の外部タイムサーバにクエリを送信するように設定します。1 個以上のサーバを使用することで、到達不能のサーバが時間同期プロセスに失敗することを防ぐことができます。NetDefendOS は常に設定済みのすべてのタイムサーバにクエリを送り、返送された情報を元に平均時刻を算出します。公的に利用可能なタイムサーバのリストはインターネット検索エンジンを使って検索できます。

カスタムサーバの IP アドレスを設定する方法には以下の 2 通りがあります。

- IPv4 または IPv6 アドレスを直接指定します。
- サーバ URL の参照を含む FQDN アドレスを指定します。アドレスオブジェクトを解決するために、NetDefendOS 上に少なくとも 1 つ以上の外部 DNS サーバが設定されている必要があります。詳細は「3.1.7 FQDN アドレスオブジェクト」を参照してください。

例題 2.23

カスタムタイムサーバを設定する

この例では、SNTP プロトコルを使用してスウェーデン国立時刻周波数研究所のタイムサーバに接続し、時刻同期を設定します。タイムサーバの URL は、ntp1.sp.se および ntp2.sp.se です。以下の FQDN アドレスオブジェクトが既に定義されているものとします。

- ntp1_fqdn - ntp1.sp.se
- ntp2_fqdn - ntp2.sp.se

CLI

```
DFL-xxxx:/> set DateTime TimeSynchronization=custom TimeSyncServer1=ntp1_fqdn TimeSyncServer2=ntp2_fqdn TimeSyncIn-
            terval=86400
```

Web Interface

1. **System > Device > Date and Time** の順にメニューをクリックします。

2. TIME SYNCHRONIZATION の「Custom」をチェックして、タイムサーバの情報を入力します。

< 入力例 >

TIME SYNCHRONIZATION

- Primary Time Server : ntp1_fqdn
- Secondary Time Server : ntp2_fqdn

3. 「OK」ボタンをクリックします。

タイムサーバの URL は、FQDN アドレスオブジェクトとして指定する必要があります。

注意 同期間隔を設定するのに CLI を使用する時、「TimeSyncInterval」パラメータを指定しないと、初期値の 86400 秒 (=1 日) が使用されます。

例題 2.24

時間同期を手動で起動する

CLI から時間同期を手動で起動することができます。以下に一般的なレスポンスを示します。

CLI

```
DFL-xxxx:/> time -sync
Attempting to synchronize system time...
Server time:2007-02-27 12:21:52 (UTC+00:00)
Local time:2007-02-27 12:24:30 (UTC+00:00) (diff: 158)
Local time successfully changed to server time.
```

最大調整時間

誤ったタイムサーバにより製品が大きく間違った時間データに更新されないように、時間調整の最大値 (秒) を指定することができます。NetDefendOS の現在の時間とタイムサーバから受信した時間の差が最大調整時間 (Maximum Adjustment) より大きい場合、そのタイムサーバからの応答された時刻は破棄されます。例えば、最大調整値が 60 秒に設定され、NetDefendOS の現在の時刻が 16:42:35 であると仮定します。タイムサーバが 16:43:38 という時間で応答するならば、その差は 63 秒であり、それは最大調整時間に従い、破棄されます。

例題 2.25

最大調整時間を変更する

この例題では、最大の調整値は 40,000 秒に設定されます。これは外部のサーバが調整できる最大の時差です。不正な NetDefendOS コンフィグレーションなど顕著な違いには正当な理由があるかもしれません。

CLI

```
DFL-xxxx:/> set DateTime TimeSyncMaxAdjust=40000
```

Web Interface

1. **System > Device > Date and Time** の順にメニューをクリックします。

2. 「Max drift」に 40,000 を設定します。

3. 「OK」ボタンをクリックします。

最大調整値を無視する必要性が生じる場合があります。例えば時間同期は有効になったばかりで、開始時間の差が最大調整の値より大きい場合などです。その時は、手動で同期を実施し、最大調整パラメータを無視することができます。

例題 2.26

時間同期を強制的に実行する

ここでは、最大調整時間を使用せずに、強制的に時間同期を実行する方法を説明します。

CLI

```
DFL-xxxx:/> time -sync -force
```

同期間隔

同期間隔は、必要に応じて調節可能です。初期値では、この値は 86,400 秒（1 日）で、時刻同期は 24 時間に 1 回実行されます。

2.2.4 日時設定の概要

以下は、日時に関する主なプロパティの概要です。

項目	説明
Location	タイムゾーンオフセット。初期値 : DLinkHQ (Taipei)
Enable daylight saving time	サマータイムの有効 / 無効を設定します。有効にした場合、「Manual」または「Automatic」を選択します。 初期値：有効
Time Sync Server Type	時間同期のためのサーバのタイプ、Disabled（無効化）、D-Link (pre-configured timesync server) 、Custom。 初期値 : D-Link (pre-configured timesync server)
Primary Time Server	タイムサーバ 1 の DNS ホスト名または IP アドレス。初期値 : なし
Secondary Time Server	タイムサーバ 2 の DNS ホスト名または IP アドレス。初期値 : なし
Synchronization interval	時刻同期の間隔（秒）。初期値 : 86400
Max drift	サーバが調整できる最大の時間（秒）のずれ。初期値 : 600
Group interval	サーバレスポンスがグループ化される間隔。初期値 : 10

2.3 イベントとログ取得

2.3.1 概要

ログを取得し、システムアクティビティを解析する能力は、NetDefendOS の主要な機能の一つです。ログの取得は、システムステータスとその健全性のモニタを可能にするだけではなく、機能のデバッグの補助やネットワークの利用を監査します。

ログメッセージの生成

NetDefendOSは、対応するシステムイベントの結果として生成される多くのログメッセージを定義しています。例えば、接続の確立と切断、不正パケットの受信、フィルタリングポリシーに従うトラフィックの廃棄などのイベントがあります。

ログイベントは、バッファの使用状況、DHCP クライアント、高可用性および IPsec などの NetDefendOS の特定の処理について常に生成されます。IP ルールの処理など NetDefendOS サブシステムのイベント生成を必要に応じて有効または無効にすることができます。

イベントメッセージが生成される時はいつでも、フィルタされ、すべての設定済みのイベントレシーバに配信されます。複数のイベントレシーバが構成可能であり、レシーバ毎に固有のカスタムイベントフィルタを保持します。

2.3.2 ログメッセージ

イベントタイプ

NetDefendOS は、イベントメッセージを生成できる数百のイベントを定義します。イベントの範囲は、低レベルで業務的なシステムイベントから高レベルのカスタマイズ可能なユーザイベントまであります。

例えば、conn_open イベントは典型的な高レベルのイベントであり、一致するセキュリティポリシールールによってイベントメッセージが生成されるように設定されている場合、新しい接続が確立されると常にイベントメッセージを生成します。

また、startup_normal イベントは、システムの起動後すぐに業務的なイベントメッセージを生成する低レベルのイベントです。

メッセージの形式

すべてのイベントメッセージは、カテゴリ、ログレベル、推奨されるアクションなどの属性を持つ一般的なフォーマットを持っています。これらの属性により、以下のようなメッセージの簡単なフィルタリングを行うことができます。

- イベントレシーバに送信する前に NetDefendOS 内のイベントメッセージをフィルタします。
- ログを出力して外部ログレシーバ上に保存した後に、分析の一部をフィルタします。

「Log Reference Guide」ですべてのイベントメッセージの一覧を参照できます。さらに、本ガイドは、イベントメッセージの仕様、セベリティレベルの意味、利用可能な様々な属性についても説明しています。

イベントのシステムレベル

各ログイベントのセベリティの初期値は事前に定義され、最も高いセベリティから最も低いセベリティまで順番であり、以下のいずれかとなります。

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Info
- Debug

初期値では、NetDefendOS は定義済みのログサーバに生成した「Info」レベル以上のメッセージをすべて送信しますが、管理者によって送信するレベルを変更することができます。「Debug」セベリティは、システムトラブルシューティングのためだけに意図されたものであり、普通は使用されません。全てのログメッセージとその意味については、「NetDefendOS Log Reference Guide」で説明されています。

イベントメッセージのタイムスタンプ

NetDefendOS がログメッセージを外部ログサーバに送信するために生成する際、常に UTC/GMT（グリニッジ標準時）で表されるタイムスタンプがつきます。これにより、異なるシステム時間で設定される別のタイムゾーンにある他のファイアウォールからのイベントを比較できます。

これの例外は、ローカルな Memlog 機能を使用して表示されるログメッセージです。これらは常に現在のローカルシステム時間でタイムスタンプを行います。

2.3.3 ログレシーバのタイプ

NetDefendOS が生成したイベントメッセージは各種タイプのログレシーバに送信されます。メッセージを受信するためには、NetDefendOS にキャプチャするイベントとイベントの送信先を指定した 1 つ以上のログレシーバオブジェクトを定義する必要があります。

NetDefendOS は様々な種類のレシーバにイベントメッセージを配信することができます。また、以下の Log Receiver オブジェクトを作成することで、有効になります。

- **Memory Log Receiver**
  NetDefendOS には、Memlog として知られる自身のログ出力メカニズムがあります。これは、メモリ内にすべてのイベントを保持し、Web インタフェースを通じログメッセージを直接表示することができます。

  初期値では有効ですが、無効にすることもできます。

  このレシーバタイプについては、「2.3.4 Memory ログレシーバ（Memlog）」で詳しく説明します。

- **Syslog Receiver**
  Syslog は、ネットワークデバイスからのイベント出力に関して、ログメッセージのデファクトスタンダードです。 他のネットワークデバイスが既に Syslog サーバにログの出力をしている場合、NetDefendOS のログメッセージ用の Syslog を使用することで総合的な管理を簡単にします。

  このレシーバタイプについては、「2.3.5 Syslog ログレシーバ」で詳しく説明します。

- **Mail Alerting**
  メールアラート機能は、多くのログメッセージを 1 つのグループにまとめ、SMTP サーバ経由で指定のメールアドレスに送信することができます。

  このレシーバタイプについては、以下の「2.3.6 メールアラート」で詳しく説明します。

2.3.4 Memory ログレシーバ（Memlog）

Memory Log Receiver（または、Memlog として知られる）は、外部サーバにメッセージを送信する代わりに、ファイアウォール内のメモリに直接ログの出力を行う NetDefendOS におけるオプションの機能です。標準のユーザインタフェースを通じてこれらのメッセージを検証することができます。

Memlog の容量制限

新しいメッセージ用の有効な Memlog メモリは、事前に固定設定しているサイズに制限されます。割り当てられたメモリがログメッセージでいっぱいになると、最も古いメッセージが、新しい入力メッセージの場所を空けるために廃棄されます。これは、Memlog が最後にシステム初期化を行った後、最近のものだけがバッファにメッセージの制限数まで保持されることを意味します。また、NetDefendOS が、大量の VPN トンネルなどのシステムで大量のメッセージを作成している場合には、限定的に最近の期間を反映するだけのため、Memlog 情報はあまり意味がないと言えます。

Memlog タイムスタンプ

Memlog がコンソールの出力結果に表示されるタイムスタンプは、常にファイアウォールのローカルシステム時間です。これは、GMT 時間で常にタイムスタンプが付いている外部ログレシーバに送信されたログメッセージとは異なります。

Memlog の有効化と無効化

Memory Log Receiver オブジェクトは、NetDefendOS に初期値で存在しているため、memlog は初期値で有効です。memlog へのログ出力が必要でない場合、Memory Log Receiver オブジェクトを削除できます。すると、このタイプのログ出力は発生しません。memlog を再び有効にするためには、Memory Log Receiver オブジェクトをコンフィグレーションに追加し直します。Memory Log Receiver のインスタンスは常に 1 つだけです。

2.3.5 Syslog ログレシーバ

概要

Syslog は、ログメッセージのフォーマットは標準化されていませんが、ログデータを送信するために標準化されているプロトコルです。NetDefendOS で使用されるフォーマットは、処理、フィルタリングおよび検索をしやすくしています。

各ログエントリの厳密なフォーマットは Syslog レシーバの動作内容によって異なりますが、多くは似たようなフォーマットです。ログの読み出し方法もまた、Syslog レシーバの動作内容によって異なります。UNIX サーバの Syslog デーモンは、通常一行ずつテキストファイルにログを出力します。

メッセージログのフォーマット

多くの Syslog レシーバは、各ログエントリの最初にタイムスタンプとログデータを送信したデバイスの IP アドレスを持っています。

```
Feb 5 2000 09:45:23 firewall.example.com
```

その次のテキストは発生したイベントによって異なります。

```
Feb 5 2000 09:45:23 firewall.example.com EFW: DROP:
```

すべてのメッセージに自動化された処理を容易に行うために、NetDefendOS は、テキストの 1 行にすべてのログデータを記述しています。最初のテキストに続くすべてのデータは「フォーマット名 =value」というように表現されています。これによって自動フィルタは指定のデータがログエントリ内の特定の位置にあると推測しなくても必要な値を簡単に検索することができます。

注意 Prio と Severity フィールド

Syslog メッセージの「Prio= 」欄は D-Link Logger メッセージのための「Severity」欄と同じ情報を含んでいますが、番号付けの順番は逆になっています。

ファシリティの設定

Facility プロパティは Syslog メッセージを生成するプログラムのタイプをサーバに示します。指定しない場合、NetDefendOS によって local0（カーネルメッセージを意味する）が設定されます。Facility 名は通常多くの syslog デーモンでフィルタパラメータとして使用しています。

例題 2.27

Syslog ホストへのログ機能を有効にする

IP アドレス 192.168.6.1 の Syslog サーバに対して、重要度 Emergency または Alert を持つ全イベントのログ出力を有効にします。

CLI

```
DFL-xxxx:/> add LogReceiver LogReceiverSyslog my_syslog IPAddress=192.168.6.1 LogSeverity=Emergency,Alert
            Facility=local1
```

Web Interface

1. **System > Device > Log and Event Receivers > Add > Syslog Receiver** の順にメニューをクリックします。

2. Syslog サーバの設定を行います。

< 入力例 >

General

- Name : イベントレシーバに適した名前を指定します。例：my_syslog
- IP Address : Syslog サーバの IP アドレスを指定します。例：192.168.6.1
- Facility : Facility リストで「local1」を選択します。
- SeverityFilter を選択し、セベリティに Emergency および Alert を選択します。

3. 「OK」ボタンをクリックします。

注意 Syslog サーバを正しく設定する必要があります。

NetDefendOS からのログメッセージを受信するためには、Syslog サーバを設定する必要があります。正しく設定するためには、ご使用の Syslog サーバのマニュアルを参照してください。

RFC 5424 コンプライアンス

初期値では、NetDefendOS は多くの Syslog サーバに適した形式で Syslog にメッセージを送信します。しかし、いくつかのサーバが、RFC 5424 が定義するように、最新の Syslog 標準により厳しい遵守を必要とするかもしれません。このため、NetDefendOS は、厳しい RFC 5424 コンプライアンスを有効にするオプションを提供します。

ホスト名の設定

すべての Syslog メッセージのヘッダには、Syslog ホスト名である文字列欄があります。初期値では、NetDefendOS は、常にこれが送信インタフェースの IP アドレスになるように設定されています。

RFC 5424 コンプライアンスを有効にすると、ホスト名に特定の値を設定することも可能となります。以下の例で、これを行う方法を説明します。

例題 2.28

ホスト名を使用して Syslog RFC 5424 コンプライアンスを有効にする

この例題では、IPv4 アドレス 192.168.5.1 を持つ Syslog サーバに Emergency または Alert 以上のセベリティを持つすべてのイベントのログへの出力を有効にします。また、Syslog ヘッダにホスト名 my_host1 を使用して RFC 5424 コンプライアンスを有効にします。

CLI

```
DFL-xxxx:/> add LogReceiver LogReceiverSyslog my_syslog IPAddress=192.168.5.1 RFC5424=Yes Hostname=my_host1
            LogSeverity=Emergency,Alert
```

Web Interface

1. **System > Device > Log Receivers > Add > Syslog Receiver** の順にメニューをクリックします。
2. イベントレシーバ名（例：my_syslog_host）を指定します。
3. 「IP Address」に「192.168.5.1」を入力します。
4. Facility リストから適切な Facility を選択します。
5. Advanced を選択し、RFC 5424 Compliance オプションを有効にします。
6. Hostname に my_host1 を入力します。
7. SeverityFilter を選択し、セベリティに Emergency と Alert を選択します。
8. 「OK」ボタンをクリックします。

2.3.6 メールアラート

概要

Mail Altering オブジェクトを作成することで、NetDefendOS はログメッセージを指定の外部 SMTP サーバ経由で指定のメールアドレスに送信するように設定できます。Mail Altering オブジェクトは他のログレシーバのタイプと同様に考えることができます。また、送信されるログメッセージのタイプを選択することも可能です。

この機能の本来の目的は、迅速に重要な NetDefendOS イベントを管理者に警告する手段を提供することであるので、通常、この方法で送信されるイベントに選択されるセベリティレベルは非常に高くなります。

メールアラートオブジェクト

多くのメールアラートオブジェクトプロパティは、他のタイプのログレシーバオブジェクトと同じであるため、本セクションでは記載を省略します。固有のオブジェクトプロパティは以下の通りです。

オブジェクト	説明
SMTP Server	宛先メールアドレスに生成したメールを送信する SMTP サーバの IP アドレス。これは、FQDN アドレスオブジェクトまたは DNS で解決可能な FQDN どちらでも設定可能です。（いずれも、DNS サーバを NetDefendOS に設定する必要があることに注意してください。）
Server Port	SMTP サーバがリッスンするポート番号。初期値で標準のポート番号 25 に設定されます。
SMTP Recipient	送信メール用の 1 つの宛先メールアドレス。
SMTP Sender	メールで送信者名にする文字列。
Subject	メールで題名にする文字列。
Send Test Email	これはプロパティではなく、入力した SMTP プロパティをテストするのに使用する Web インタフェースのボタンです。CLI にも同等の機能があり、本セクションで後ほど説明します。

イベントトリガーモード

トリガー	説明
Single event trigger	少なくとも 1 つのメールが適切な各イベントのために送信されます。「Event count threshold」および「Event count period」の値は本オプションと共に使用されません。しかし、1 つのイベントが送信可能な状態である場合、これは、適切な他のイベントをメールに追加できるように「Keep collecting before sending period」の期間待機する必要があります。
Rate of events trigger	複数のイベントがまとめられて、E メールで送信されます。メール送信の前に収集するイベント数は、「Event count threshold 」および「Event count period」の値によって制御されます。
Event count threshold	この数のイベントが「Event count period」プロパティによって指定された時間（分）より前に発生した場合にだけ、メールは送信されます。従って、トリガーは指定したイベントのレートであり、単なるイベントの累計ではありません。送信メールに既に含まれているイベントは、再びカウントされません。 Mail Alerting オブジェクトが最初に作成されるとき、このカウントはゼロであり、NetDefendOS が再開するときにはいつもゼロにリセットされます。メールを Mail Alerting オブジェクトが送信すると、また、このカウントはゼロにリセットされます。 「Single event trigger」を選択すると、このプロパティと「Event count period」プロパティは使用されません。
Event count period	上記「Event count threshold」の説明で参照される時間（分）であり、イベントがカウントされている最近の期間です。
Send report emails	有効にすると、送信メールが 1 つのイベントを持たなくても、または、「Event count threshold」値に到達しなくても、「Report email interval」で指定した時間に常に少なくとも 1 通のメールが送信されます。 これは「Single event trigger」モードでは使用されません。
Report email interval	メールがイベントを含まない場合に、メールが送信されるまでに待機する最大時間（時）です。通常、この値は 24 に設定されており、メールの中身は空でも Mail Alerting オブジェクトは 1 日に少なくとも 1 つのメールを生成します。これは、システムが起動していることを管理者に通知し、希望するすべてのイベントを強調表示できます。
Report email subject	レポート送信時のメールの件名です。これにより、E メールがレポートメールであるのか、トリガーによって生成されたメールであるのかを簡単に識別することができます。 本プロパティは文字列を持つ必要があり、空のままにはできません。
Keep collecting before sending	メール送信の準備ができていると、それを送信する前に、NetDefendOS はこの時間（分）待機します。メールの送信を待つ間に起こる新しいイベントもすべてペンディング中のメールに追加されます。 どちらのトリガーモードでもこれを使用できます。「Single event trigger」モードの場合、最初のトリガーイベント後に発生した新しいイベントもメールに追加されます。 NetDefendOS は最短 1 分の間隔でメールを送信するため、本項目が 0 に設定されていてもメール送信には遅延が生じ、その間に新しいイベントが追加されます。

トリガー	説明
Minimum time between emails	連続したメールの送信において、メール間の経過時間をこれより小さくできません。このプロパティの値は、メールの過剰な送信を防ぐことができます。 メール送信の準備ができていても、この期間内であると送信できません。この期限が切れるまで、新しいイベントのすべてをメールに追加します。

高度なオプション

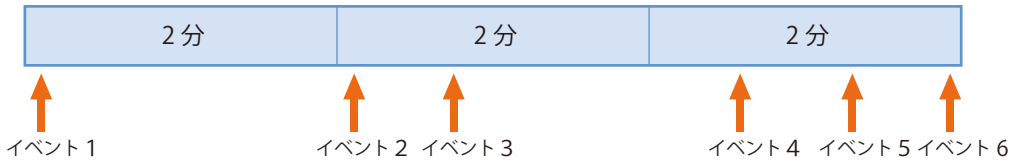
- **Identity**
  この文字列パラメータは、NetDefendOS が SMTP サーバに送信した HELO または EHLO コマンドで SMTP クライアントを特定します。指定しない場合、NetDefendOS の送信インタフェースの IPv4 アドレスが自動的に設定されます。

- **X-Mailer**
  SMTP サーバ通信しているソフトウェアの名前です。これは、オプションであり、初期値は空白です。

メールアラートの処理フロー

イベントトリガープロパティの設定の詳細について、以下の例題を参照してください。
NetDefendOS で Mail Alerting オブジェクトが構成済みであり、「Rate of events trigger」オプションにおいて Event count period が 2 分、Event count threshold が 3 イベントに設定されているとします。（E メールが送信されるには、2 分間の間に 3 つのイベントが発生する必要があります。）

最後のメールを送信してから、メールが送信されるために適切な 6 つのログイベントが発生し、これらが 6 分間にわたって発生するものと仮定します。下の図では 6 分を 2 分のセクションに分けて、イベントの発生を分かりやすく示しています。



処理のフローは以下の通りです。

1. NetDefendOS は最初のイベントの前にゼロからカウントを開始します。
2. 3 番目のイベントが発生すると、しきい値に到達します。しかし、最初のイベントが 2 分の時間枠の外にあり、2 番目と 3 番目のイベントが時間内にあるため、メールは送信されません。
3. 4 番目と 5 番目のイベントも同様です。それまでの 2 分間の枠において、イベント数がしきい値の 3 つに到達していません。
4. 6 番目のイベントの発生時だけ、2 分間にしきい値の 3 イベントに到達するため、E メールが送信されます（Keep collecting before sending（分）待機中に発生した新しいイベントも追加されます）。
5. NetDefendOS は 1 番目、2 番目、および 3 番目のイベントを破棄するため、これらはメールに含まれていません。
6. イベントカウンタをゼロにリセットし、再度「Event count period」内でイベントカウンタを開始します。

テストメールを送信

メールアラート機能には、テストメールをサーバに送信する Send Test Email 機能があります。Web インタフェースで「Send test email」ボタンを押すことで実行します。CLI では、テストメールは以下のコマンドで送信されます。

```
DFL-xxxx:/> smtp -sendmail -logreceiver=<mail-alerting-object-name>
```

テストメールの本文は以下と同様のテキストを含みます。

```
This is message #1 sent to test the SMTP Log Receiver "my_mail_alert"
```

テストメールがログレシーバから送信される度に、メッセージの番号「#1」が増加します。

Web インタフェースでは、Mail Alerting オブジェクトが作成されると、コンフィグレーションの変更のアクティブ化と保存の前でもテストボタンを押すことができます。これは同等の CLI テストメール機能とは異なります。

複数の E メールアドレスに送信

ログメッセージを複数のメールアドレスに送信するように複数の Mail Alerting オブジェクトを作成することができます。しかし、同じログメッセージ情報を複数のメールアドレスに送信するために、複数の Mail Alerting オブジェクトを作成することは推奨されません。代わりに、SMTP サーバにメーリングリストを作成し、そのアドレスに送信されたメールが複数の受信者に送信されるようにしてください。

メールサイズの制限

NetDefendOS がログメッセージのバッファリングとメール本文の作成に使用可能なメモリを制限するために、メールサイズに制限をが設けられています。この制限は 8k バイトです。この制限に到達すると、メールが未送信であっても、新しいログメッセージのすべてが破棄されます。イベントが破棄されると、以下のメッセージがメール本文に追加されます。送信時のサイズによって、破棄されたメッセージ数は異なります。

```
[100] message(s) have been discarded because of email body size limit
```

使用可能メモリがメール作成中に完全に使い果たされると、このメッセージはそれを示す若干異なるテキストとなります。メッセージが繰り返して破棄される場合、イベントフィルタをより制限するべきである、または、メール送信間隔を短くするべきであるという兆候であると言えます。

2 つ以上の Mail Alerting オブジェクトが作成されている場合、メール作成のために各オブジェクトに固有のメモリが割り当てられます。

例題 2.29

Mail Alerting オブジェクトの設定

この例題では、Emergency または Alert に等しいセベリティを持つすべてのイベントがメールに送信されるように Mail Alerting オブジェクト「my_smtp_receiver」を設定します。

受信者のメールアドレスを admn@example.com、SMTP サーバのアドレスを 203.0.113.10 と仮定します。しきい値と関連するプロパティの初期値を使用します。

他のすべての設定可能なプロパティも初期値のままにします。

CLI

```
DFL-xxxx:/> add LogReceiver LogReceiverSMTP my_mail_alert IPAddress=203.0.113.10 Recipient=admn@example.com
            Sender=device1@example.com Subject="Log message summary" LogSeverity=Emergency,Alert
```

Web Interface

1. **System > Device > Mail Alerting > Add >Mail Alerting** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_mail_alert
   - SMTP Server: 203.0.113.10
   - SMTP Recipient: admn@example.com
   - SMTP Sender: device1
   - Subject: Log message summary
3. SeverityFilter を選択し、セベリティに Emergency および Alert を指定します。
4. 「OK」ボタンをクリックします。

2.3.7 Severity フィルタとメッセージ例外

各ログレシーバに対して、どのログメッセージカテゴリとセベリティをレシーバに送信するかというルールを決めることが可能です。また、特定イベントのセベリティを低く、または高くすることもできます。

Severity フィルタ

Severity フィルタは、レシーバに送信するセベリティを指定する方法です。初期値では、Debug（デバッグ）以外の全ログメッセージが送信されます。例えば、Emergency、Alert、および Critical メッセージを送信するというように、より限定的にこれを制限することができます。

ログメッセージ例外

Severity フィルタが適用された後、生成されたメッセージに対してログメッセージ例外が適用されます。ログレシーバには複数のメッセージ例外を設定することが可能であり、それぞれが以下の項目から構成されます。

- カテゴリと ID
  これは例外により影響を受けるログメッセージを指定します。ログメッセージの ID を指定しないと、特定のカテゴリに対する全ログメッセージが含まれます。「Log Reference Guide」で特定のログメッセージを参照できます。
- タイプ
  これは以下のいずれかとなります。
  - Exclude - Severity フィルタが許可しても、特定のログメッセージを除外します。
  - Include - Severity フィルタが除外しても、特定のログメッセージを含めます。

    さらに、含めるように設定したメッセージの Severity を指定できます。これを Default に設定すると、元のセベリティが使用されます。そうでない場合、セベリティは指定値に設定されます。本機能は特定のログメッセージのセベリティを上げる (または下げる) ことができます。

2.3.8 SNMP トラップ

SNMP プロトコル

SNMP（Simple Network Management Protocol）は、NMS（Network Management System）と管理デバイスの間で通信するための手段です。SNMP は 3 つのタイプのメッセージを定義しています。

- Read - NMS が管理デバイスを検証します。
- Write - 管理デバイスの状態を変更します。
- Trap - 状態の変化について NMS に非同期にメッセージを送信するために管理デバイスによって使用されます。

NetDefendOS における SNMP トラップ

NetDefendOS は、イベントメッセージを SNMP トラップとして送信することが可能であり、SMTP トラップの概念をさらに進化させます。これは、管理者がネットワークの操作に重要であると考えるイベントの SNMP トラップ通知を設定できることを意味します。

MIB ファイル「DLINK-DFL-TRAPS-MIB.mib」では、NetDefendOS から送信される SNMP トラップを表すために使用される、SNMP オブジェクトやデータタイプを定義しています。

このファイルは NetDefendOS 自身にあり、Web インタフェースまたは Secure Copy (SCP) を使用して管理者用ワークステーションのローカルディスクに展開されます。「2.5 SNMP」でより詳しく説明されています。

D-Link ファイアウォール製品には、DLNNNosGeneric トラップと呼ばれる一般的なトラップオブジェクトがあり、すべてのトラップに使用されます。（NNN はファイアウォールの製品型番を示します。）

このオブジェクトには以下のパラメータがあります。

パラメータ	説明
System	トラップを生成するシステム。
Severity	メッセージのレベル。
Category	問題を報告する NetDefendOS サブシステム。
ID	カテゴリ内の一意の識別番号。
Description	短い説明文。
Action	NetDefendOS が行うアクション。

この情報については、個別の「Log Reference Guide」で ID を使用して参照することができます。

SNMP2c と SNMPv3 の使用

NetDefendOS は、SNMPv2 または SNMPv3 を使用した SNMP トラップの送信をサポートしています。これらの SNMP プロトコルバージョンはよく似ていますが、異なる点として、SNMPv3 では暗号化や認証がサポートされており、セキュリティの観点から SNMPv3 が推奨されます。

イベントレシーバの設定

SNMP トラップ機能は、SNMP2c イベントレシーバまたは SNMPv3 イベントレシーバのオブジェクトを定義する事で設定可能です。

リピートカウント

SNMP2c と SNMPv3 ログレシーバは Repeat Cout と呼ばれるプロパティを持っており、レシーバに対してイベントが何回送信されるかを指定しています。本設定の初期値は 0 であり、所定のイベントが発生する度にレシーバにメッセージが送信されます。

例えば Repeat Count プロパティが 3 に設定されている場合、イベントはシステムの最後の起動後に発生した最初の 3 回だけ送信されます。（システムの再起動によりカウントは初期化されます。）これにより、繰り返しのイベントであっても、レシーバに同じメッセージが不必要に送信されません。

インタフェース Up/Down のイベント

SNMP2c と SNMPv3 ログレシーバオブジェクトは Use interface link up/down traps と呼ばれるプロパティを持っており、有効化 / 無効化することができます。初期値では無効になっています。有効化した場合、コンフィグレーション内のイーサネットインタフェースがオンライン / オフラインステータスに移行したときに、レシーバに送信されるイベントが発生します。

SNMPv3 セキュリティオプション

SNMPv3 を使用する場合、3 つのレベルのセキュリティオプションが選択可能です。

- noAuthNoPriv - 認証と暗号化を行いません。（初期値）
- authNoPriv - SHA1 を使用した認証を行いますが、暗号化は行いません。認証は必須の Password プロパティを使用して実施されます
- authPriv - SHA1 を使用した認証と AES を使用した暗号化を有効化します。認証と暗号化は必須の Password プロパティを使用して実施されます。

例題 2.30

SNMPv3 イベントレシーバを設定する

NetDefendOS に、セベリティ Emergency または Alert を持つすべてのイベントについて、SNMP トラップを受信する SNMPv3 イベントレシーバを設定します。

レシーバが IPv4 アドレス 192.168.3.1 を持っていると仮定します。

CLI

```
DFL-xxxx:/> add LogReceiver EventReceiverSNMPv3 my_snmp_receiver
                    IPAddress=192.168.3.1
                    Username=my_name
                    Password=myunguessablepassword
                    Snmp3SecurityLevel=authPriv
```

Web Interface

1. **System > Device > Event Receivers > Add > SNMPv3 Event Receiver** の順にメニューをクリックします。

2. 以下の情報を入力します。

< 入力例 >

- Name : my_snmp_receiver
- IP Address : 192.168.3.1
- Security Level : authPriv
- Password : myunguessablepassword
- SeverityFilter を選択し、セベリティに Emergency および Alert を指定します。

3. 「OK」ボタンをクリックします。

2.3.9 詳細なログ設定

管理者は、以下のログの出力のために詳細な設定を行うことができます。

項目	説明
Send Limit	本設定は、NetDefendOS が 1 秒間に送信するログパケット数を制限します。これは重要なイベントがログに出力されない結果をもたらす可能性があり、本値を決して低く設定しすぎないようにします。 最大値を超過すると、超過したメッセージは破棄されてバッファには保持されません。管理者はその時々でログサーバが対処できるメッセージの負荷について判断する必要があります。これは、通常、使用されているサーバのハードウェアプラットフォームや、プラットフォームのリソースが別のタスクと共有されているかどうかによって異なります。 初期値 : 2000

2.3.10 Logsnoop

Web インタフェースを通してログイベントメッセージをモニタおよび参照する基本的な機能があります。「logsnoop」 CLI コマンドは、以下の方法のいずれかを使用してログメッセージを参照できるように、この能力を拡張します。

- Logsnoop は CLI コンソールにログメッセージをリアルタイムに表示できます。また、管理者が興味のあるメッセージだけを参照できるようにフィルタリングを適用できます。
- Logsnoop は時間をさかのぼって、指定された数の最近生成されたログメッセージを含む Memlog バッファの内容を表示できます。フィルタリングをこの出力結果に適用すると、管理者が興味のあるメッセージだけを表示できます。
- 上記の 2 つの機能を組み合わせることができるので、memlog バッファの内容と新たに生成しているメッセージの両方を一緒に表示できます。

リアルタイムな Logsnoop をオンまたはオフに切り換える

Logsnoop をオンに切り換えるためのコマンドの基本形式は以下の通りです。

```
DFL-xxxx:/> logsnoop -on
```

NetDefendOS が生成したすべてのログメッセージが CLI コンソールに表示されます。個々のメッセージの先頭には「LOG」が表示されます。
例 :

```
LOG:2014-01-13 13:53:39 SYSTEM prio=Alert id=03200021 rev=1
event=demo_mode action=shutdown_soon shutdown=halt time=7200
```

パラメータなしでコマンドを入力すると、logsnoop の現在の状態を調べることができます。

```
DFL-xxxx:/> logsnoop

Real time log snooping is enabled.   Filter:All
```

Logsnoop をオフに切り換えます。

```
DFL-xxxx:/> logsnoop -off
```

ログメッセージのフィルタリング

システムの稼働中にスヌーピングをオンに切り換えると、システムは大量のメッセージをコンソールに送信してしまいます。通常、メッセージをフィルタするために、メッセージをフィルタする追加のコマンドパラメータを単独または組み合わせて追加することが望ましいと言えます。多くのフィルタリングパラメータの内のいくつかを使用した例を以下に示します。

- **セベリティによるフィルタ**

```
DFL-xxxx:/> logsnoop -on -severity=warning
```

1 度に 1 つのセベリティレベルのみフィルタできることに注意してください。

- **ログ ID 番号によるフィルタ**

```
DFL-xxxx:/>  logsnoop -on -logid=1500001
```

別紙の「NetDefendOS Log Reference Guide」ですべての ID 番号を参照できます。先頭のゼロを指定する必要はありません。

- **ソース IP によるフィルタ**

```
DFL-xxxx:/>  logsnoop -on -srcip=192.168.1.10
```

ログメッセージが表示されるには、メッセージ内に「srcip」フィールドが存在しなければなりません。例えば、ログメッセージが IP ルールセットエントリから送信されると、表示されるメッセージの「srcip」フィールドには、ルールを起動した接続の送信元 IP が含まれます。

- **ソースインタフェースによるフィルタ**

```
DFL-xxxx:/>  logsnoop -on -srcif=If1
```

ログメッセージが表示されるには、メッセージ内に「srcif」フィールドが存在しなければなりません。例えば、ログメッセージが IP ルールセットエントリから送信されると、表示されるメッセージの「srcif」フィールドには、ルールを起動した接続の送信元インタフェースが含まれます。

- **パラメータの組み合わせによるフィルタ**

```
DFL-xxxx:/> logsnoop -on -severity=warning -srcip=192.168.1.10 -srcif=If1
```

1 つの「logsnoop」コマンド内にいろいろなフィルタリングパラメータを一緒に使用できます。

別紙の「NetDefendOS CLI Reference Guide」の logsnoop のエントリでコマンドパラメータに関する全リストを参照できます。もしくは、以下の CLI コマンドを使用できます。

```
DFL-xxxx:/> help logsnoop
```

ワイルドカードとフリーテキストによるフィルタリング

フィルタリングパラメータを指定する際に、以下のワイルドカードを使用できます。

* - アスタリスクは「none」(なし) または多くの文字を示します。
? - 疑問符は任意の 1 文字を示します。

例えば、文字の「warning」のどこか後ろに文字「udp」があるものを検索するコマンドは以下の通りです。

```
DFL-xxxx:/> logsnoop -on -pattern=*warning*udp*
```

「-pattern」パラメータはログメッセージでフリーテキストのフィルタを指定します。ワイルドカードは、「-pattern」に限らず他のフィルタリングパラメータで使用することも可能です。

ログメッセージ数の制限

フィルタリングを使用しても、コンソールに表示するメッセージ数を減らす必要がある場合があります。以下の 2 つの方法で表示メッセージの数を制限できます。

- **頻度の制限：**

```
DFL-xxxx:/> logsnoop -on -rate=5
```

表示するログメッセージを 1 秒に最大 5 回に制限します。

- **総数の制限：**

```
DFL-xxxx:/> logsnoop -on -num=100
```

最初の 100 個のログメッセージだけを示します。その後、logsnoop はオフに切り替わります。

Memlog ヒストリの検証

Memlog は、NetDefendOS が最近生成された多くのログメッセージを格納するために使用する ローカルメモリのバッファの名称です。初期値は「Enabled」です。「logsnoop」を使用すると、特別なパラメータ「-source=memlog」を使用して memlog の検証が行われます。

例えば、以下のコマンドを使用して memlog バッファの全コンテンツを調べることができます。

```
DFL-xxxx:/> logsnoop -on -source=memlog
```

「-on」パラメータを使用しても、本コマンドはリアルタイムのログへの出力に切り替えません。そのため「-off」パラメータを持つマッチングコマンドは必要ありません。

Memlog と新しいログメッセージの検証

memlog でログヒストリを調べて、同時にリアルタイムのログスヌーピングをオンにできます。以下のコマンドを使用してこれを実行します。

```
DFL-xxxx:/> logsnoop -on -source=both
```

これはまた memlog と続いて生成されたすべてのメッセージの内容を表示します。コマンドにはさらに詳細なフィルタリングパラメータを追加することをお勧めします。

「-source=both」を使用した場合、別途 off パラメータを指定してコマンドを実行し、リアルタイムログをオフにする必要があります。

タイムレンジの指定

表示するログメッセージには制限を設定することが可能であり、「-starttime」パラメータを使用すると指定日時以降の、または / および「-endtime」パラメータを使用すると指指定日時以前のログが生成されます。

以下の形式で時間の値自体を指定できます。

- **日時を使用する**

  日付と時間は "yyyy-mm-dd hh.mm.ss" の形式をとります。引用符で囲む必要があります。
  （例 : 2014-01-12 18:30:00）1 月 12 日 18:30 以降のログメッセージを参照するコマンドは以下の通りです。

  ```
  DFL-xxxx:/> logsnoop -on -starttime="2014-01-12 18:30:00"
  ```

  日付と時間の両方を入力する場合、引用符でパラメータ値を囲む必要がありますのでご注意ください。

- **日付を使用する**

  日付を時刻なしで指定できます。これは、引用符で囲まない形式 yyyy-mm-dd を取ります。（例 : 2014-01-12）時間の初期値は常に 00:00:00 であるため、この例は 2014 年 1 月 12 日 00:00:00 です。1 月 12 日の全ログメッセージを参照するコマンドは以下の通りです。

  ```
  DFL-xxxx:/> logsnoop -on -starttime=2014-01-12 -endtime=2014-01-13
  ```

memlog を検索しない場合、時刻の設定は、指定した将来の時刻に logsnoop のオン / オフをする動作となります。
「-source=memlog」オプションを使用する場合は、開始時間と終了時間を使用して memlog 履歴の特定の期間を検索します。

2.4 モニタリング

NetDefendOS のリアルタイムな性能を以下に示すいくつかの方法でモニタリングできます。
- リアルタイムモニタアラート
- リンクモニタ
- SNMP クライアントを介したモニタリング
- ハードウェアモニタリング

2.4.1 リアルタイムモニタアラート

多くの NetDefendOS の統計的な値がリアルタイムモニタ機能を通じてグラフィカルにモニタされます。リアルタイムモニタアラートのしきい値では、最大および / または最小数のしきい値を持つことができるように、これらのモニタされる値を NetDefendOS に指定することができます。

指定した最大または最小のしきい値を超えると、NetDefendOS は、定義済みのすべてのログレシーバに送信するログメッセージを自動的に生成します。それらのすべてのログメッセージが識別番号 54 を持つ REALTIMEMONITOR メッセージカテゴリに所属します。

したがって、ログメッセージの ID は、054XXXXX という形式になります。XXXXX の部分は、アラートルールのリスト内でイベントを生成する統計の位置を表します。
例えば、ID 05400003 を持つログメッセージはルールリストの 3 番目のルールを特定します。

モニタアラートルール

各 Monitor Alert Rule は以下のフィールドから成ります。

フィールド	説明
Name	ルールにユーザが割り当てた名前
Sample time	統計情報をチェックする間隔（秒）
Low threshold	低いしきい値（指定する場合）
High threshold	高いしきい値（指定する場合）
Backoff Interval	連続した Monitor Threshold Rule ログメッセージの間隔の最小値（秒）。この値は、統計データがしきい値を超えた後、続けてそれを下回る動作となった場合に、ログメッセージのフラッドを防ぐために役に立ちます。
Continuous	しきい値内に戻った際にもイベントを生成し続けるかどうかを指定します。「Yes」または「No」を指定します。
Log Message ID	生成されたログメッセージの ID

2.4.2 リンクモニタ

概要

リンクモニタは、D-Link ファイアウォールの外側にある 1 つ以上の IP アドレスへの接続性をモニタする NetDefendOS の機能です。このモニタリングは標準の ICMP「ping」要求を使用して行われ、NetDefendOS はこれらの IP アドレスに対するネットワーク経路の可用性を評価することができます。経路が何らかの理由で中断しているように見える場合、管理者は多くの操作から実施するものを 1 つ選択することができます。

リンクモニタの操作

リンクモニタポーリングに対して十分な応答が得られない場合、NetDefendOS は、これらの IP アドレスに対する通常のリンクがダウンしているものとして、以下の 3 つの実行可能な操作から 1 つを開始することができます。

1. Reconfigure（NetDefendOS の再構成）
2. HA Failover（高可用性（High Availability : HA）フェイルオーバ）
3. HA Failover and Reconfigure（HA フェイルオーバ及び NetDefendOS の再構成）

複数ホストのモニタ

1 つの Link Monitor オブジェクトが 1 つのホストまたは複数のホストをモニタすることができます。1 つのホストをモニタする場合、ホストのエラーまたはホストへの接続のエラーのいずれかが、モニタのアクションを起動します。

複数のホストが 1 つの Link Monitor オブジェクトに指定される時、オブジェクトのアクションが起動するためには、ホストの 50% 以上が到達不能である必要があります。これは、それぞれのホストというよりも、ホストへの接続の有効性が重要である場合に役に立ちます。ホストの 1 台が利用可能であることが重要である場合、そのホストのみをモニタする Link Monitor オブジェクトが作成されるべきです。

リンクモニタ再構成の違い

リンクモニタによってトリガされる再構成には特別な側面があります。リンクモニタの再構成には全インタフェースを再起動する追加のアクションがあります。特定のイーサネット NIC の過負荷などに関連する問題があると、インタフェースの初期化によりこれを解消することができるということを意味します。
これは、再構成が行われている間に処理能力に一時的な遅延だけを起こします。

リンクモニタの用途

リンクモニタは以下の 2 つの異なるシナリオで役に立ちます。

- 外部デバイスはファイアウォールとのリンクに時々問題を起こすため、物理リンクを再度ネゴシエーションする必要があります。そのような問題はADSLモデムなどの少し古い機器で時々発生する可能性があります。このシナリオに対する操作では「1. Reconfigure」を選択する必要があります。

  再構成はNetDefendOSのコンフィグレーションが再度ロードされることを意味します。すべての接続と状態は再構成のために保存されますが、リローディングは、すべてのトラフィックがしばらくの間中断し、外部デバイスへの全インタフェースを再度ネゴシエーションすることを意味します。

- HAクラスタ設定では、マスタから外部インターネット（または、ネットワークの他の部分）へのリンクが継続的にモニタされるため、リンク障害が発生すると、スレーブが引き継ぎます。（スレーブがモニタするアドレスに対して異なる物理接続を持つと仮定します。）HAに対し選択する操作は、「2. Failover」または「3. Failover and reconfigure」のいずれかとなります。HAクラスタに1番目の操作オプション「1. Reconfigure」を選択した場合、再構成中にマスターサーバの処理が一時的に保留となり非稼働状態が検出されると、スレーブサーバが引き継ぐため、Reconfigureアクションにおいても結果的にフェイルオーバが発生することになります。フェイルオーバを使用した再構成を希望する場合、オプション3の選択がより適しています。このオプションでは最初にフェイルオーバを実施し、その処理は一時的であるため、トラフィックの中断はほとんどありません。最初に再構成を実施すると処理が遅くなり、何らかのトラフィックの中断を引き起こします。

  VPNシナリオにおいてすべてのトンネルを保持するためには、再構成によりいくつかのトンネルを喪失してしまうことから、「2. Failover」オプションを選択するのが最適です。

HAクラスタを使用したリンクモニタリング

リンクモニタリングは上記のHAクラスタシナリオで使用されるのが最も一般的です。マスタとスレーブがリンクモニタのトリガーとなる同じ条件をコピーしないことが重要です。例えば、マスタのファイアウォールに接続する特定のルータをリンクモニタが「Ping」するとしたら、そのルータにスレーブを接続するべきではありません。もしそのような接続になっている場合、リンクモニタの継続的な再構成のトリガーによって、スレーブからマスターへのフェイルバック、次いで再度スレーブへのフェイルバック、というような挙動になります。

HAクラスタ内のアクティブなユニットが再構成する間、フェイルオーバを許可しないことが重要であり、「Advanced settings」の「Reconf Failover Time」には低過ぎない値、または高過ぎない値を設定する必要があります。

「Reconf Failover Time」はアクティブでないユニットが引き継ぐまでアクティブなユニットが再構成に対して待機する時間を制御します。これに低過ぎる値を設定すると、アクティブでないユニットの待機時間が十分でないことを意味します。高過ぎる値を設定すると、アクティブなユニットが再構成中に故障し、アクティブでないユニットが引き継ぐ必要がある場合に非常に長いダウンタイムとなることを意味します。

クラスタに関する詳細は、「第12章 High Availability（高可用性）」を参照してください。

IPsecトンネルと高可用性クラスタ

起動されたリンクモニタ操作が、「フェイルオーバ」または「フェイルオーバと再構成」であると、IPsecトンネルは自動的にクローズされて、トンネルSAは両端で削除されます。フェイルオーバが行われた後に、以下のことが起こります。

- IPsecトンネルがLAN-to-LANトンネルであったならば、トンネルに設定されたkeepalive timeの時間制限内にトラフィックが流れると、自動的に再確立されます。
- 外部クライアントからのIPsecトンネルは失われ、自動的に再確立されません。クライアントは新しい接続を開始しなければなりません。

リンクモニタオブジェクトプロパティ

リンクモニタ設定オブジェクトには以下のパラメータがあります。

項目	説明
Action	NetDefendOSが実行するアクションについて、「リンクモニタの操作」「リンクモニタの操作」で説明した3種類のアクションから指定します。
Addresses	このプロパティは、モニタする1台以上のホストのIPアドレスを指定します。複数のホストにおいて、半分（50%）以上が応答すれば、問題がないと見なされます。ホストの半分以上が応答しないと、NetDefendOSは、リンクに問題があると見なします。 ホストが1台の場合は応答するか、しないかで、50%のルールは関係ありません。 ホストは、最後のNetDefendOS再構成またはフル再起動以降少なくとも1度はNetDefendOSが到達できるまで、この50%ルールでは使用されません。これは、到達不能なホストが2回ではなく1回操作を始動する責任があることを意味します。 そのため、最後の構成後に1台が到達不能であった3台のホストグループは、3台目が到達可能になるまで2台のホストグループとして処理されます。これは、アクションがトリガされた後に問題が継続している場合に、その問題が解消されホストが到達可能になるまで、NetDefendOSが同じアクションを繰り返し実施しないことを意味します。
Max Loss	ホストへの連続したping応答回数。応答がない場合、単一のホストは到達不能と見なされます。初期値は7です。
Initial Grace Period	最後の再構成後、リンクモニタは指定時間（秒）、操作を始動することはできません。これにより初期リンクネゴシエーション中のFalse Positive（誤検知）を回避します。初期値は45（秒）です。
Ping Interval	Pingをホストに送信する間隔（ミリ秒）。初期値は250（ミリ秒）です。
Routing Table	ホストのIPアドレスのルートを調べるのに使用されるルーティングテーブルです。初期値は「main」ルーティングテーブルです。

項目	説明
Use Shared IP	HA クラスタでモニタするときだけ使用します。各ユニットの独立した IP を使用して送信する代わりに、リンクモニタの ping を共有 IP アドレスから送信することを許可します。これは、パブリック IPv4 アドレスがクラスタ内の各ユニットで利用できない場合に役に立ちます。「12.6 リンクモニタと HA」を参照してください。

例題 2.31

リンクモニタのセットアップ

この例題では、IPv4 アドレス「my_host」に設定されたホストの有用性をモニタする Link Monitor オブジェクトを作成します。この IPv4 アドレスが NetDefendOS アドレス帳に既に定義されているものとします。

ホストが無効であることを検出すると、モニタのアクションは HA Failover となります。

CLI

```
DFL-xxxx:/> add LinkMonitor Action=HAFailover Addresses=my_host
```

Web Interface

1. **System > Device > Link Monitors > Add > Link Monitor** の順にメニューをクリックします。
2. 以下を入力します。
   - Action: HA Failover
   - Addresses: my_host
3. 「OK」ボタンをクリックします。

2.4.3 ハードウェアモニタ設定

可用性

特定の D-Link ハードウェアモデルでは、管理者は、CLI を使用してファイアウォール内部の現在の温度などの様々なハードウェア操作パラメータの現在の値を問い合わせることができます。この機能は、ハードウェアモニタと呼ばれます。

注意 ハードウェアモニタリングはすべてのモデルで使用できるというわけではありません。
ハードウェアモニタリング機能は、DFL- 260E および DFL-860E では使用できません。

ハードウェアモニタリングの設定と実行は、CLI または Web インタフェースのいずれかを通じて行われます。

ハードウェアモニタの有効化

System > Device > Hardware Monitoring の Advanced Settings セクションは、利用可能である場合にハードウェアモニタを有効にするために以下の設定を提供します。

項目	説明
Enable Sensors	すべてのハードウェアモニタ機能を有効または無効にします。初期値 : Enalbled（有効）
Poll Interval	ハードウェアモニタのためのポーリング間隔。これは、ハードウェアモニタ値を読み取る間隔（ミリ秒）です。 最小値 : 100、最大値 : 10000、初期値 : 500

「hwm」CLI コマンドを使用する

利用可能なすべてのセンサから現在値のリストを取得するためには、以下のコマンドを使用します。

```
DFL-xxxx:/> hwm -all
```

これは以下のように省略できます。

```
DFL-xxxx:/> hwm -a
```

以下は、2 個の温度センサに対する本コマンドからの典型的な出力です。

```
DFL-xxxx:/> hwm -a
Name             Current value (unit) Enabled
---------------- ----------------------------
cpu_temp         =  53.000 (C)        (x)
```

SYS 温度はハードウェアユニット内部の全体的な温度用です。CPU 温度はユニットの中央プロセッサに関連しており、その冷却方式により全体の温度より低くなることがあります。

注意 "(x)" の意味

センサー一覧の左側にある (x) は、センサが有効であることを示しています。

「-verbose」オプションを使用すると現在値および設定範囲を表示します。

```
DFL-xxxx:/> hwm -a -v
2 sensors available
Poll interval time = 500ms
Name [type][number] = low_limit] current_value [high_limit (unit)     Enabled
------------------------------------------------------------------------------
sys_temp         [TEMP  ][  0] =    44.000]    45.000 [   0.000  (C)
cpu_temp         [TEMP  ][  0] =     0.000]    53.000 [   80.000 (C)     (x)
Time to probe sensors: 2.980000e-05 seconds
```

左に表示される各物理属性について、操作可能な範囲の最小値と最大値を示しています。ポーリング後の戻り値が範囲外である場合、NetDefendOSは、オプションで設定したログサーバに送信するログメッセージを生成します。

注意 各ハードウェアモデルは、異なるセンサと範囲を持っています。

各ハードウェアモデルは、それぞれ異なるセンサのセットと動作範囲を持っており、上記の出力とその値は参考例です。

範囲の最小値と最大値の設定

「hwm」コマンドからの出力に示される最小、最大値は、Web マネージャで **System > Device > Hardware Monitoring > Add** の順にメニューをクリックして画面を表示し、モニタするハードウェア項目を選択して設定します。希望する動作範囲を指定することができます。

センサは、Web インタフェースで以下の項目の固有な組み合わせを指定することによって識別されます。

項目	説明
Type	上記の CLI 出力で示したセンサのタイプであり、Web インタフェースで選択肢のリストに表示されます。例 : Temp
Sensor	上記の CLI 出力で示したように、センサの番号です。例 : SYS Temp 番号は 0 です。
Name	上記の CLI 出力で示したように、センサ名です。例 : SYS Temp
Enabled	本設定を使用して各センサを有効または無効にします。有効にすると、「hwm」コマンドにおける出力結果のセンサの横に「(x)」が表示されます。

2.4.4 メモリモニタ設定

Web マネージャの **System > Device > Monitoring > Hardware Monitoring> Advanced Settings** の MEMORY MONITORING SETTINGS セクションでは、利用可能なメモリのモニタに関連した多くの設定を以下の通り提供します。

項目	説明
Memory Poll Interval	メモリのポーリング間隔。メモリ値を読む間隔（分）です。最小値は 1、最大値は 200。初期値 : 15（分）
Use Percentage Limit	• True - メモリモニタはモニタリングのための単位として割合を使用します。（初期値） • False - メガバイトを使用します。 Alert レベル、Critical レベルおよび Warning レベルに適用します。
Log Repetition	Alert、Critical または Warning レベルにある各ポーリング結果に対するログメッセージを送信する必要があります。または新しいレベルに到着した場合にだけ送信する必要があります。 • True - Memory Poll Interval がトリガーとなる場合にメッセージを送信します。 • False - 値があるレベルから別のレベルに移行した場合にメッセージを送信します。（初期値）
Alert Level	空きメモリが本値（バイト）未満である場合、Alert ログメッセージを生成します。0 に設定すると無効になります。最大値は 10,000 です。初期値 : 0
Critical Level	空きメモリが本値（バイト）未満である場合、Critical ログメッセージを生成します。0 に設定すると無効になります。最大値は 10,000 です。初期値 : 0
Warning Level	空きメモリが本値（バイト）未満である場合、Warning ログメッセージを生成します。0 に設定すると無効になります。最大値は 10,000 です。初期値 : 0

2.5 SNMP

2.5.1 SNMP を使用した管理

簡易ネットワーク管理プロトコル（SNMP : Simple Network Management Protocol）は、ネットワークデバイスの管理における標準プロトコルです。SNMP に準拠したクライアントは、SNMP プロトコルをサポートするネットワークデバイスに接続して、管理タスクを実行できます。NetDefendOS は、SNMP プロトコルの以下のバージョンを使用することで SNMP クライアントによるアクセスをサポートします。

- バージョン 1
- バージョン 2c
- バージョン 3

ただし、クエリ操作はセキュリティ上の都合によりクライアントによって制限されます。具体的には、NetDefendOS は次の SNMP リクエスト操作をサポートしています。

- GET REQUEST 操作
- GET NEXT REQUEST 操作
- GET BULK REQUEST 操作（SNMP バージョン 2c および 3）

NetDefendOS で SNMP アクセスを設定する

SNMP クライアントによるアクセスを許可するために、NetDefendOS のコンフィグレーションで SNMP Management オブジェクトを作成する必要があります。これには、以下のオブジェクトプロパティがあります。

オブジェクトプロパティ	説明
Protocol	バージョン 1 と 2c（初期値）を選択するか、またはバージョン 3 を選択します。
Interface-SNMP	リクエストが到達する NetDefendOS インタフェース。
Network-SNMP	リクエストが到達する IP アドレスまたはネットワーク。

他のオブジェクトプロパティは、セキュリティのためにあり、SNMP プロトコルの選択に依存します。これらを次に説明します。

SNMP セキュリティオプション

選択したプロトコルによって、以下のセキュリティオプションがあります。

- **バージョン 1 と 2c**

  SNMP バージョン 1 と 2c の認証は Community String プロパティを使用します。Community String はパスワードと同等であり、推測するのを難しくするべきです。大文字小文字と数字の組み合わせを使い、一般のパスワードと同じように構成されます。

  SNMP バージョンの 1 と 2c は暗号化のためのオプションを提供していないため、トラフィックはプレーンテキストとして送信されます。このため、多くの場合 SNMP バージョン 3 がより良い選択といえます。SNMP バージョン 1 またはバージョン 2c を使用する必要がある場合、クライアントコンピュータと NetDefend Firewall の間で確立される VPN トンネルを経由して SNMP 接続を送信することが可能です。

- **バージョン 3**

  SNMPv3 をプロトコルに選択すると、Security Level プロパティを設定することができます。これは以下の値を取ることができます。

プロパティ	説明
noAuthNoPriv	認証も暗号化もありません。
authNoPriv	SHA-1 認証で、暗号化はありません。
authPriv	SHA-1 認証と AES 暗号化

  認証が有効であると、Local User Database オブジェクトを選択する必要があります。これには、クライアントアクセスに使用される有効なユーザ名 / パスワードのペアがあります。administrator または auditor のユーザ名 / パスワードの組み合わせが SNMPv3 資格証明として使用されるのであれば、多くの場合、定義済みの AdminUsers データベースで十分です。

  暗号化が有効であると、NetDefendOS は AES 暗号化だけを使用します。一般的に DES 暗号化は安全性が低いとみなされるため、SNMPv3 RFC で定義されるように、NetDefendOS ではサポートしていません。

NetDefendOS MIB ファイル

どの SNMP クライアントにも必要とされる重要コンポーネントは、MIB ファイルです。管理情報ベース（MIB: Management Information Base）は、通常プレーンなテキスト形式のデータベースで、SNMP クライアントがアクセスできるネットワークデバイス上のパラメータを定義します。

NetDefendOS の MIB ファイルは、NetDefendOS システム上に存在します。NetDefendOS フォルダ「SNMP_MIB」にあり、以下の名称を持っています。

- DLINK-DFL-MIB.mib
- DLINK-DFL-TRAPS-MIB.mib

MIB ファイルのダウンロード

リストのあるファイルは、Web インタフェースまたはセキュアコピー (SCP) のいずれかを使用して、直接 NetDefendOS から管理コンピュータのローカルディスクにダウンロードできます。Web インタフェースでこれを行うためには、**Status > Maintenance > Resources** メニューに行きます。

SCP クライアントを使用する代表的コマンドラインは以下の通りです。

```
> pscp -l admin -pw admin 192.168.1.17:SNMP_MIB/DLINK-DFL-MIB.mib .
```

管理コンピュータのディスクに保存されると、SNMP クライアントソフトウェアはファイルをインポートすることができます。

MIB エントリ

MIB の各エントリはその値が何であるかを説明するテキストを含んでいます。本マニュアルでは、すべてのリストについて再現しません。インタフェースによって送信されたパケットの総数のための典型的な MIB ファイルエントリは以下の通りです。

```
clvIfPktsTotCnt OBJECT-TYPE
  SYNTAX Counter32
  MAX-ACCESS read-only
  STATUS current
  DESCRIPTION "Total number of packets transmitted by the interface"
              ::= { clvIfStatsEntry 10 }
```

SNMP 用の IP ルールを有効にする

SNMP クライアントによるすべてのアクセスを IP ルールセットがチェックするか否かは、SNMP Before Rules という拡張設定が制御します。初期値では、これは有効であり、この設定を常に有効にすることを推奨します。

この設定を有効にすると、IP ルールセットの先頭に、暗黙の Allow ルールが追加され、ネットワークからポート 161 に入るアクセスおよび SNMP アクセスで指定したインタフェース上のアクセスを自動的に許可します。SNMP ではポート 161 が通常用いられ、NetDefendOS は常にこのポート上で SNMP トラフィックが発生すると想定します。

SNMP オーバロードを回避する

SNMPReqLimit という拡張設定により、1 秒あたりに許可される SNMP リクエストの数を制限します。これにより、SNMP のオーバロードによる攻撃を回避できます。

例題 2.32

SNMPv1/2c モニタリングを有効にする

この例題では、Mg1RQqR というコミュニティ名を用いて、ネットワーク mgmt-net から lan インタフェースを介する SNMP バージョン 1 および 2c のアクセスを有効にします。管理クライアントが内部ネットワーク上にいれば、そのために VPN トンネルを実装する必要はありません。

CLI

```
DFL-xxxx:/> add RemoteManagement RemoteMgmtSNMP my_snmp_v1-2 Interface=lan Network=mgmt-net SNMPGetCommunity=Mg1RQqR
```

SNMP Before Rules を必ず有効にする必要があります。初期値は有効です。コマンドを以下の通り入力します。

```
DFL-xxxx:/> set Settings RemoteMgmtSettings SNMPBeforeRules=Yes
```

Web Interface

1. **System > Device > Remote Management > Add > SNMP Management** の順にメニューをクリックします。
2. リモートアクセスタイプ、アクセスフィルタ、認証を入力します。

リモートアクセスタイプ

- Name : my_snmp_v1-2
- SNMP Version : SNMPv1 and SNMPv2c

Access Filter

- Interface : lan
- Network : mgmt-net

Authentication

- Community : Mg1RQqR

3. 「OK」ボタンをクリックします。

SNMP Before Rules を必ず有効にする必要があります。初期値は有効です。**System > Device > Remote Management > Advanced settings** で設定を参照できます。

例題 2.33

SNMP バージョン 3 のモニタリングを有効にする

この例題では、上記の SNMP バージョン 1 と 2c の例題と同様ですが、代わりに SNMP バージョン 3 を使用します。ネットワーク mgmt-net からの lan インタフェースを経由した SNMPv3 アクセスを有効にします。SNMPv3 認証と暗号化の両方を有効とし、認証はローカルデータベース AdminUsers を使用して行います。

CLI

```
DFL-xxxx:/> add RemoteManagement RemoteMgmtSNMP my_snmp_v3 Interface=lan Network=mgmt-net SNMPversion=SNMPv3
            LocalUserDatabase=AdminUsers Snmp3SecurityLevel=authPriv
```

SNMP Before Rules を必ず有効にする必要があります。初期値は有効です。コマンドを以下の通り入力します。

```
DFL-xxxx:/> set Settings RemoteMgmtSettings SNMPBeforeRules=Yes
```

Web Interface

1. **System > Device > Remote Management > Add > SNMPManagement** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_snmp_v3
   - SNMP Version: SNMPv3
   - Security Level: authPriv
3. アクセスフィルタを入力します。
   - Interface: lan
   - Network: mgmt-net
4. Authentication を入力します。
   - Local User Database: AdminUsers
5. 「OK」ボタンをクリックします。

SNMP Before Rules を必ず有効にする必要があります。初期値は有効です。**System > Device > Remote Management > Advanced Settings** で設定を参照できます。

2.5.2 永続する SNMP インタフェースインデックス

SNMP アクセスのために、NetDefendOS は、コンフィグレーションのインタフェース (すべてのインタフェースタイプ) を含むインデックステーブルを保持し、各インタフェースにはテーブル内の位置を示すインデックス番号があります。SNMP を使用するスクリプトを含む SNMP クライアントソフトウェアは、特定のインタフェースを参照するためにこれらのインデックス番号を使用します。

インタフェースの追加もしくは削除の問題

初期値では、NetDefendOS が再起動する度に、インデックステーブルが構築されますが、新しいインタフェースが設定に追加または削除されるため、そのインタフェースに新しいインデックス番号が割り当てられる可能性があることを意味します。これはインタフェースに同じインデックス番号があると予想している SNMP クライアントソフトウェアに問題を引き起こす可能性があります。

解決法は Persistence の有効化である

再起動後、インタフェースが常に同じインデックス番号を持つことを確実にするために、管理者は、SNMP Persist Interface Index 設定を有効にするべきです。これは、全体の構成で有効となるグローバル設定です。

永続インタフェースを HA クラスタで有効にする

NetDefendOS 高可用性クラスタでは、インタフェースインデックステーブルは同じ方法で構築され、テーブルはクラスタノードの間でミラーされます。しかし、マスタとスレーブの両方で HA 設定の「Enable High Availability」が有効である時だけ、有効化されたインタフェース永続が正しく機能します。これは、Web インタフェースで **System > Device > High Availability** メニューにあり、初期値は有効です。

削除された物理インタフェースを追加して戻す

ハードウェアから物理インタフェースを削除すると（これは拡張モジュールを利用している場合に起こりえます）、おそらくコンフィグレーションから削除されていないため、インタフェースはインデックステーブルにまだ存在します。インデックステーブルのエントリが失われるのは、コンフィグレーションからインタフェースを完全に削除する時だけです。

これは、物理インタフェースが後でハードウェアに追加して戻されると、同じインデックス番号を持続することを意味します。これは、追加されたインタフェースが、異なる物理ユニットであったとしてもそうなります。

インデックステーブルの圧縮

インタフェースの永続が有効である場合、各インタフェースにインデックステーブルの同じ位置を保持させることによって、正常に動作します。これは、インタフェースが削除されたときにテーブル（そしてインタフェースのインデックス番号）にずれが生じることを意味します。必要に応じて、管理者は、定期保守の期間、以下の CLI コマンドを使用することで手動でテーブルをデフラグすることができます。

```
DFL-xxxx:/> ifstat -snmpnewindexes
```

テーブルをデフラグするために、続けて Activate と Commit を実行する必要があります。

番号の連続したリストにインデックス番号をつけ直す以外に、デフラグを実行する他の理由はありません。フラグメント化のために付加的なリソースは消費されません。

警告 バックアップを復元すると、インタフェースインデックスはリナンバされる

NetDefendOS システムバックアップの復元が実行されると（完全またはコンフィグレーションのみのどちらでも）、インタフェースインデックス番号はバックアップの値に戻ってしまいます。

例題 2.34

SNMP のインデックス永続を有効にする

この例題では、SNMP インデックス永続を有効にする方法を示しています。

CLI

```
DFL-xxxx:/> set Settings RemoteMgmtSettings SNMPPersistentIfIndexes=Yes
```

Web Interface

1. **System > Device > Remote Management** の順にメニューをクリックします。
2. Advanced Settings を選択します。
3. SNMP セクションで、オプションの Persistent Interface indexes を有効にします。
4. 「OK」ボタンをクリックします。

2.5.3 SNMP の詳細設定

以下の SNMP の詳細設定は、Web マネージャの「Remote Management」セクションで行われます。CLI 経由で行うこともできます。

項目	説明
SNMP Before RulesLimit	設定した IP ルールにかかわらず、SNMP トラフィックをファイアウォールに対して有効にします。初期値 : Enabled
SNMP Request Limit	NetDefendOS が 1 秒間に処理する SNMP リクエストの最大数。SNMP リクエストがこの値を超過すると、NetDefendOS は、この超過リクエストを無視します。初期値 : 100
System Contact	管理ノード用の連絡窓口。初期値 : N/A
System Name	管理ノード名。初期値 : N/A
System Location	管理ノードの物理的な位置。初期値 : N/A
Interface Description	SNMP MIB-II ifDescr 変数に表示する内容。初期値 : Name
Interface Alias	SNMP ifMIB ifAlias 変数に表示する内容。初期値 : Hardware
Persistent Interface indexes	インタフェースインデックスの永続が有効であるかどうか判断するグローバル設定。初期値 :No

2.6 診断ツール

2.6.1 概要

ネットワーク問題を障害調査する場合に、NetDefendOS は問題解決を補助する切り分けツールを提供します。

本セクションは、管理者が利用可能な最も重要なトラブルシューティングツールについて説明します。これらの多くは CLI コマンドで使用されます。

2.6.2 ping コマンド

ICMP エコーリクエストとエコーリプライメッセージの組み合わせが ping として知られています。これらは、ホストに到達可能かどうかを検出する簡単な診断ツールを提供します。NetDefendOS CLI では、ping コマンドがこの機能を提供します。

最も簡単な形式では、リモート IP アドレスを ping する CLI コマンドは以下の形式を取ります。

```
DFL-xxxx:/> ping <ipaddress>
```

例えば、IPv4 アドレス 10.6.58.10 に ping します。

```
DFL-xxxx:/> ping 10.6.58.10

Sending 1 4-byte ICMP ping to 10.6.58.10 from 192.168.3.20
using PBR table “main”
ICMP Reply from 192.168.1.1 seq=0 time=<10 ms TTL=128

Ping Results: Sent: 1, Received:1, Avg RTT: 10.0 ms
```

ここで、RTT は ICMP エコー要求と応答メッセージの往復遅延時間です。TTL 値はホップカウンタである Time To Live です。初期の TTL 値は、送信側が設定しており、通過したルータごとに減少します。0 に到達すると、パケットが永遠に循環するのを防ぐために、パケットを破棄します。

「ping」コマンドの基本的な形式は、NetDefendOS Web インタフェースの **Status > Tools > Ping** でも使用できます。

ルーティングテーブルの選択

初期値では、ICMP ping 用の外向きソースインタフェースは、main ルーティングテーブル内の宛先 IP アドレスのルックアップを実行することで選択されます。「-pbr」オプションを使用して初期値を上書きし、ルックアップに使用するルーティングテーブルを指定することも可能です。
例えば、ルーティングテーブル「my_routing_table」を使用する場合、コマンドは以下の通りとなります。

```
DFL-xxxx:/> ping 10.6.58.10 -pbr=my_routing_table -verbose
```

注意 「-srcif」オプションと共に「-pbr」オプションは使用できません。
後で記述する「-srcif」オプションを使用したパケットシミュレーションで「-pbr」オプションは使用できません。これは、外向きインタフェース用のルーティングテーブルのルックアップは、入力パケットをシミュレートする際には意味がないためです。

外向き Ping メッセージの IP ルールとポリシー

ICMP ping メッセージが NetDefendOS から外向きに送信される場合、NetDefendOS は常に信頼されているため、トラフィックを許可する IP ルールまたは IP ポリシーは全く必要ありません。Stock_Allow_All_Rule を使用することで、NetDefendOS イベントメッセージログに、外向きの ping は conn_open と conn_close ログイベントを生成します。ソースインタフェースは常に（NetDefendOS 自身を意味する）core インタフェースになります。

内向き Ping メッセージの IP ルールとポリシー

内向きに送信される ping メッセージには NetDefendOS に応答を許可する IP ルールまたは IP ポリシーが必要で、関連する Service オブジェクトが定義済みサービス ping-inbound に設定されている必要があります。wan インタフェースに到着する ping メッセージ用の IP ルールの例は以下の通りです。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
Allow	wan	all-nets	core	wan_ip	ping-inbound

-verbose オプションの使用

ping 実行により最大限の情報を取得したい場合は、-verbose オプションを使用することをお勧めします。例題は以下の通りです。

```
DFL-xxxx:/> ping 10.6.58.10 -verbose

Sending 1 4-byte ICMP ping to 10.6.58.10 from 192.168.3.20
... using route “192.168.3.20 via lan, gw (Iface IP)” in PBR table “main”
ICMP Reply from 192.168.3.20 seq=0 time=<10 ms TTL=255

Ping Results: Sent: 1, Received:1, Avg RTT: 10.0 ms
```

ここでは、IPv4 アドレス 192.168.3.20 は ping が送信されるファイアウォールのイーサネットインタフェースの IP アドレスです。出力結果は、正しいインタフェースを検出するために実行されたルートルックアップを示しています。

パケットシミュレーションが「-scrif」オプション（後述）を使用して実行される場合、トリガとなるルールを表示するには「-verbose」オプションの指定する必要があります。

TCP と UDP の接続性のテスト

ICMP メッセージは UDP または TCP ではありませんが、IP トラフィックにおける独自の 3 番目のカテゴリであると言えます。しかしながら、NetDefendOS ping コマンドには、TCP または UDP の接続性のどちらかをテストするメッセージを送信する機能があります。

TCP として送信するために、「-port」オプションを「-tcp」オプションと共に使用します。接続性の確認に成功すると、宛先ホストと 3 ウェイ TCP ハンドシェークを行います。例題は以下の通りです。

```
DFL-xxxx:/> ping 10.6.58.10 -port=80 -tcp -verbose

Sending 0-byte TCP ping to 10.6.58.10:80 from 192.168.3.20:41207
using PBR table “main”
... using route “10.6.10.0/24 via aux, no gw” in PBR table “main”
TCP Reply from 10.6.58.10:80 to 192.168.3.20:41207 seq=0 SYN+ACK
time=>10 ms TTL=128
TCP Reply from 10.6.58.10:80 to 192.168.3.20:41207 seq=0 ACK
time=>10 ms TTL=128

TCP Ping Results: Sent: 1, RST/ACKs Received:1, Loss: 0%, Avg RTT: 10.0 ms
```

これにより、内向きの TCP 通信に対するリモートホストの応答性を確立することができます。

UDP の接続性をテストするには、「-port」オプションと共に「-udp」オプションを使用します。また、パケット数を指定するためには「-count」オプションを、各パケット長を指定するためには「-length」を使用して UDP メッセージのサイズを指定する必要があります。例題は以下の通りです。

```
DFL-xxxx:/>  ping 10.6.58.10 -udp -port=53 -verbose -count=1 -length=30

Sending 30-byte UDP ping to 10.6.58.10:53 from 192.168.3.20:22307
using PBR table “main”
... using route “0.0.0.0/0 via ext, gw 192.168.3.1” in PBR table “main”
UDP Reply from 10.6.58.10:53 to :192.168.3.20:22307 seq=0 time=50 ms TTL=58

Ping Results: Sent: 1, Received:1, Loss: 0%, Avg RTT: 50.0 ms
```

-srcif を使用した入力パケットのシミュレーション

リモートホストの応答をテストする代わりに、NetDefendOS ping コマンドを使用し、内向きの ICMP ping メッセージをシミュレートし、その結果により設定済みの IP ルールセットとルーティングテーブルをテストできます。「-srcif」オプションを使用することでこのシミュレーションを行うことができます。例題は以下の通りです。

```
DFL-xxxx:/> ping 10.6.58.10 -srcif=wan -verbose
```

本コマンドは宛先 IP10.6.58.10 を持つ ICMP パケットを構成し、NetDefendOS はまるでパケットが指定のソースインタフェース（この場合 wan）に到着したかのように反応します。

パケットが指定されたインタフェースに到着するように見えるので、管理者は、設定による動作や、トリガされる IP ルールセットのエントリ及びルートを観察することができます。
指定した IP アドレスは実際のホストであるかもしれません。その場合、ファイアウォールを通してパケットはそのホストに送信されます。

送信元 IP と受信インタフェース（-srcif パラメータ）の組み合わせにマッチするルートが何もないと、パケットはデフォルトのアクセスルールによって破棄されます。例題は以下の通りです。

```
DFL-xxxx:/> ping 10.6.58.10 -srcif=wan -verbose

Rule and routing information for ping:
PBR selected by rule “iface_member_main” - PBR table “main”
DROPPED by rule “Default_Access_Rule”
```

ping が破棄されないためには、IP アドレスとインタフェースの組み合わせにマッチするルートだけでなくそのインタフェースのパケットを許可する IP ルールセットのエントリにもマッチする必要があります。管理者が、wan インタフェースのパブリックインターネットから到来し保護された lannet 上のホストに向かうパケットをシミュレートする場合、許可する IP ルールセットのエントリは以下と類似しているかもしれません。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
Allow/NAT	lan	lannet	wannet	all-nets	ping-inbound

パケットを許可する IP ルールセットのエントリもなければ、パケットは破棄されます。例題は以下の通りです。

```
DFL-xxxx:/> ping 10.6.58.10 -srcif=wan -verbose

Rule and routing information for ping:
PBR selected by rule “iface_member_main” - PBR table “main”
DROPPED by rule “Default_Rule”
```

通常、-srcif オプションは次に説明する -srcip オプションと組み合わせて使用されます。

送信元 IP アドレスの指定

-srcip オプションを使用して、特定の送信元 IP アドレスを持つ ICMP ping パケットを構成して、送出することもできます。例題は以下の通りです。

```
DFL-xxxx:/> ping 10.6.58.10 -srcip=192.168.3.1 -verbose
```

前述の通り、これは、ネットワークテストの目的で管理者の使用を意図した機能です。

注意 ALG では、「-srcif」または「-srcip」を平行して使用できません。
「-srcif」と「-srcip」オプションの制限は、起動する IP ルールと共に ALG を使用できないということです。

「-srcif」と「-srcip」の組み合わせ

特定の送信元 IP を持つ指定インタフェースに到着するパケットをシミュレートするために -srcif オプションに「-srcip」を組み合わせることは可能です。これらのオプションの両方を使用するのがおそらく最も一般的な方法です。

この例題では、シミュレーションによって、トリガされるパイプルールの参照も可能であることを示しています。

```
DFL-xxxx:/>  ping 10.6.58.10 -srcif=lan -srcip=192.168.3.1 -verbose

Rule and routing information for ping:
PBR selected by rule “iface_member_main” - PBR table “main”
allowed by rule “nat_all_wan”
piped by rule “out_pipe” - Fwd Chain: out
piped by rule “out_pipe” - Ret Chain: in
Sending 1 4-byte ICMP ping to 10.6.58.10 from 192.168.3.20
sent via route “0.0.0.0/0 via lan, gw 192.168.3.1” in PBR table “main”
ICMP Reply from 10.6.58.10 seq=0 time= 10 ms TTL=247

Ping Results: Sent: 1, Received:1, Avg RTT: 10.0 ms
```

上記の出力結果は、Pipe Rule オブジェクト out_pipe がどのように起動されたかを示しています。

これらのオプションには、さらに「-tcp」と「-port」オプションを組み合わせることができます。

IPv6 を使用した Ping

今まで IPv4 アドレスの ping コマンドの使用について説明してきました。IPv6 アドレスでも ping できます。例題は以下の通りです。

```
DFL-xxxx:/> ping 2001:DB8::2
```

IPv6 の ping に関する詳しい情報は、「3.2 IPv6 のサポート」を参照してください。

FQDN 解決

NetDefendOS から ping 要求を発行する場合、完全修飾ドメイン名 (FQDN) として宛先を指定することができます。NetDefendOS は外部の DNS サーバを使用することで、数字の IP アドレスに解決します。例題は以下の通りです。

```
DFL-xxxx:/> ping server.example.com
```

注意 少なくとも 1 つの DNS サーバを設定する必要があります。

FQDN 解決が機能するためには、NetDefendOS に少なくとも 1 つの DNS サーバを設定する必要があります。DNS サーバの設定については、「3.10 DNS 設定」を参照してください。

DNS サーバが IPv4 アドレスまたは IPv6 アドレスのいずれか、または両方を返します。これら 3 つのパターンに対し、以下の通り処理が行われます。

- IPv4 アドレスだけを返す場合、ping コマンドは ICMP メッセージにその IPv4 アドレスを使用します。
- IPv6 アドレスだけを返す場合、ping コマンドは ICMP メッセージにその IPv6 アドレスを使用します。
- IPv4 と IPv6 アドレスの両方が利用可能であると、NetDefendOS は初期値では IPv4 アドレスを使用します。しかし、NetDefendOS は、「-6」コマンドオプションによって IPv6 アドレスを使用するように強制することができます。例題は以下の通りです。

```
DFL-xxxx:/> ping www.example.com -6
```

2.6.3 stats コマンド

重大な NetDefendOS の問題が疑われる場合、第 1 段階として以下の CLI コマンドを使用します。

```
DFL-xxxx:/> stats
```

「stats」コマンドは、システムのスナップショットを提供し、システムの最後のシャットダウンの日時を示します。また、NetDefendOS 操作において重大なエラーがあったかどうかを示すこともできます。しかし、「stats」が使用するバッファが、再構成のような特定の操作でクリアされてしまうため、本コマンドの出力結果には、バッファクリアの前に発生したイベントを示すことができないことにご注意ください。

以下はコマンドから出力された代表的な例です。

```
DFL-xxxx:/> stats
Uptime              : 7 days, 02:12:38
Last shutdown       : 2014-06-17 16:05:00: Activating configuration changes
CPU Load            : 4%
Connections         : 23 out of 512000
Fragments           : 0 out of 16384 (0 lingering)
Buffers allocated   : 43280
Buffers memory      : 43280 x 2636 = 111412 KB
Fragbufs allocated : 32
Fragbufs memory     : 32 x 10040 = 313 KB
Out-of-buffers      : 0
```

Last shutdown 行の最後には、シャットダウンの理由が記述されています。

Poll Offloading を使用したときの stats コマンドの出力

NetDefendOS が動作するハードウェアプラットフォームによっては、性能を上げるために poll offloading として知られている技術を利用できます。poll offloading では、アクティブな 2 つの CPU コアがあります。1 つの CPU コアが NetDefendOS の機能の大部分を実行しており、2 つ目はイーサネットインタフェースのポーリングを処理する NetDefendOS の部分を実行しています。

poll offloading がアクティブな状態で stats コマンドを使用すると、コマンド出力における CPU Load の行は、1 つではなく 2 つの割合を示します。最初の割合は NetDefendOS の大部分を実行している CPU コアの負荷です。2 番目の割合はインタフェースのポーリングサブシステムを実行している CPU コアの負荷を示しています。以下は、この表示例です。

```
CPU Load            :12%, 1%
```

ハードウェアプラットフォームがこれをサポートしていれば、Poll offloading は NetDefendOS によって自動的に有効になるため、管理者が有効にする必要はありません。

2.6.4 connections コマンド

「connections」コマンドを使用することで、管理者は、NetDefendOS ステートエンジンに現在設定されているすべての接続のスナップショットを取得することができます。コマンドは「conn」に省略できます。出力例は以下の通りです。

```
DFL-xxxx:/> conn

State    Proto   Source                       Destination             Tmout
-------- ------- -------------------------- ---------------------- ------
TCP_OPEN TCP     If1:10.4.4.24:54047          If2:192.168.9.3:338     261772
UDP      UDP     If2:192.168.109.11:4500      If3:10.152.0.22:450     130
PING     ICMP    vlan1:192.168.1.1:512        If3:90.152.1.1:512      8
FIN_RCVD TCP     If1:10.4.4.121:55679         core:10.4.0.31:444      69
TCP_OPEN TCP     If2:192.168.96.77:35217      If3:10.93.2.49:463      70855
UDP      UDP     vlan1:192.168.100.163:560    vpn-A:10.45.1.2:161     9
UDP      UDP     vlan1:192.168.100.163:582    vpn-B:10.25.1.2:161     76
```

コマンド出力の各行は 1 つの接続に対応しています。
各フィールドは以下の通りです。

フィールド	説明
State	これは、接続の状態を示しており、実際に各ステータスを確認できるのは TCP 接続のみです。表示される値は以下の通りです。 **i.** UDP - UDP 擬似接続 **ii.** PING - ICMP ping 接続 **iii.** TCP_OPEN - TCP 接続がオープン状態です。 **iv.** SYN_RCVD - TCP 接続は、SYN パケットを受信し、オープン状態です。 **v.** FIN_RCVD - TCP 接続はクローズしました。接続が再開できるように NetDefendOS がすべてのデータをクリーンアップするまで 80 秒間（初期値）待機します。80 秒の値は、NetDefendOS に設定した TCP FIN Idle Lifetime によって制御されます。接続の再開は、NetDefendOS に設定した Allow TCP Reopen（初期値では無効）によって制御されます。 **vi.** RAW IP - Protocol 欄で指定された他のプロトコル。
Proto	接続に使用されたプロトコルで、State 欄と同じものもあります。表示される値は以下の通りです。 **i.** UDP - UDP 擬似接続 **ii.** ICMP - ICMP ping 接続 **iii.** TCP - TCP 接続 **iv.** ESP - IPsec VPN トンネルに使用されています。 **v.** 使用されるプロトコルを示す番号または名前。State 欄は、RAW IP の値となります。
Source	これは以下の項目から成ります。 **i.** ソースインタフェース。これは VLAN または IPsec トンネルなどの NetDefendOS インタフェースオブジェクトのタイプの名称であるかもしれません。また、NetDefendOS 自身が接続のソースであることを示す Core であるかもしれません。 **ii.** 接続のソース IP アドレス **iii.** 接続のソースポート番号
Destination	これは以下の項目から成ります。 **i.** 宛先インタフェース。これは VLAN または IPsec トンネルなどの NetDefendOS インタフェースオブジェクトのタイプの名称であるかもしれません。また、NetDefendOS 自身が接続の宛先であることを示す Core であるかもしれません。 **ii.** 接続の宛先 IP アドレス **iii.** 接続の宛先ポート番号
Tmout	トラフィックが検出されない状態で接続がタイムアウトになるまでの時間（秒）。接続のいずれか一方が送信した何らかのトラフィックが検出されると、直ちにこの値はタイムアウトの初期値にリセットされます。初期値は以下の NetDefendOS 設定に従って制御されます。 **i.** TCP Idle Lifetime - TCP 接続用。初期値は 262144（秒）です。 **ii.** UDP Idle Lifetime - UDP 接続用。初期値は 130（秒）です。 **iii.** Ping Idle Lifetime - ICMP Ping 接続用。初期値は 8（秒）です。 **iv.** Other Protocols Idle Lifetime - 他のすべてのプロトコル。初期値は 130（秒）です。

フィルタリング接続

「connections」コマンドでは、接続の表示フィルタを指定する機能を提供します。プロトコル TCP との接続だけを表示するコマンドは以下の通りです。

```
DFL-xxxx:/> conn -show -protocol=TCP
```

ソースインタフェース If3 との接続だけを参照します。

```
DFL-xxxx:/> conn -show -srciface=If3
```

接続のクローズ

「connections」コマンドを使用すると、管理者は、すべて、または選択した接続をクローズすることができます。すべてをクローズするコマンドは以下の通りです。

```
DFL-xxxx:/> conn -close -all
```

ソースインタフェース If3 との接続だけをクローズします 。

```
DFL-xxxx:/> conn -close -srciface=If3
```

-verbose オプション

「-verbose」オプションを使用すると、「connections」コマンドは、各接続について「 ...term:」で始まる行を追加します。この行では、接続がファイアウォールを通過するためにインタフェース、IP またはポート番号に NetDefendOS が行った変更があれば表示します。例えば、以下の出力では 1 つの接続を示しています。

```
DFL-xxxx:/> conn -show -verbose

State    Proto   Source                      Destination             Tmout
-------- ------- --------------------------- ----------------------- ------
TCP_OPEN TCP     If1:10.4.0.16:60848         If3:192.168.96.82:80    262119
        ...term: If1:192.168.96.1:39097      If3:192.168.96.82:80    262119
```

ここでは、オリジナルの接続は NAT IP ルールセットのエントリの対象となり、If1:10.4.0.16:60848 が If1:192.168.96.1:39097 に変換されます。宛先は同じですが、送信元 IP とポートは NetDefendOS によって変更されています。この例題では、プライベート IP アドレスが使用されましたが、192.168.96.1 は、通常、パブリック IP アドレスとします。

「connections」コマンドの全オプションの一覧については、「CLI Reference Guide」を参照してください。

2.6.5 dconsole コマンド

次の段階では、以下の CLI コマンドを使用します。

```
DFL-xxxx:/> dconsole
```

これは以下のように省略できます。

```
DFL-xxxx:/> dcon
```

「dconsole」コマンドは、NetDefendOS 操作中に発生した重要なイベントのリストを提供して、深刻な問題を引き起こすイベントの日付、時間、および特徴を立証することに役立ちます。以下のような一覧が表示されます。

```
Showing diagnose entries since 2008-05-22:
2008-06-21 11:54:58                Start (11.04.01-0:131)
2008-06-21 11:56:16                Stop (RECONFIGURE)
2008-06-21 11:56:21                Start (11.04.01-0:131)
2008-06-21 11:57:29                Stop (RECONFIGURE)
2008-06-21 11:59:31                Start (11.04.01-0:131)
2008-06-21 11:59:49                Stop (NORMAL)
"
"
```

「dconsole」の出力結果には、重大なランタイムエラーの場合、システムメモリのダンプを含めることもできます。以下のようなダンプが表示されます。

```
‘
’
Reason: Exception ‘DataAbort’ occurred at address 0x7aaea34
Generation date/time: 2008-07-04 14:23:56 List of loaded PE-modules:
fwloader(1.07.04): BA:0x00100000, EP:0x00101028, SS:0x0, IS:0xe7000
fwcore(811.04.01-2336): BA:0x07761038, EP:0x0007c630 Register dump:
-------------------------------------------------
r0 : 0xe1a0003c, r1 : 0x07c685dc, r2 : 0x00000004, r3 : 0x50013700,
r4 : 0x06cb2d04, r5 : 0x0753a740, r6 : 0x050ce1f8, r7 : 0x00000000,
r8 : 0x0753a79c, r9 : 0x050ce1f8, r10: 0x00000000, r11: 0x0775ff34,
r12: 0x00000004, sp : 0x0775fcec, lr : 0x079de7e4 Stack dump:
5da89306 c33613f4 c330cfc5 04411507 45515a49 86619f8b c0db0a81
4e395861 cb25b796 e3108934 932766c5 4dcff9e9 711c3463 b9cd5d1e
52149961 9324dea3 d340dc25 15458610 63582ded 689a0c54 dfb43131
02c7d971 a0ebb72c bfaae832 db216923 08ba693b 95e4de97 98d121a2
‘
’
```

dconsole の出力結果は管理者が確認するには難しいかもしれませんが、調査のために D-Link サポートに送付することも可能です。

「dconsole」コマンドは、NetDefendOS の前バーションにあった「crashdump」コマンドに代わるものです。

Status > Maintenance > Diagnostic Console の順にメニューをクリックし、「dconsole」を Web インタフェースで動作させます。
本画面を開くと、自動的に「dconsole」を実行し、直ちにテキストボックスに出力結果を表示します。Refresh ボタンを押すと、「dconsole」が再び実行されて、テキストボックスに新しい出力結果が表示されます。

2.6.6 pcapdump コマンド

有効な診断ツールは、D-Link ファイアウォールのインタフェースに入出力されるパケットを検証する機能です。この目的のため、NetDefendOS は、CLI コマンド「pcapdump」により、入出力するパケットストリームの検証を行うだけでなく、指定した基準に従って、これらのストリームにフィルタリングを行います。「pcapdump」CLI コマンドの使用法のみ本セクションで説明しますが、本機能は Web インタフェースにもあります。

また、「pcapdump」によってフィルタされたパケットは、パケットキャプチャ用の事実上の標準である libpcap ライブラリファイル形式のファイルタイプ「.cap」で保存することができます。

「pcapdump」CLI コマンドの完全な構文については、「CLI Reference Guide」を参照してください。

シンプルな例題

pcapdump 使用の例題は以下の通りです。

```
DFL-xxxx:/> pcapdump -size 1024 -start lan
DFL-xxxx:/> pcapdump -stop lan
DFL-xxxx:/> pcapdump -show
DFL-xxxx:/> pcapdump -write lan -filename=cap_lan.cap
DFL-xxxx:/> pcapdump -cleanup
```

1 行ずつ行っていきます。

1. 記録の取得は、1024kbyte のバッファサイズを使用して「lan」インタフェースに対して開始されます。

```
DFL-xxxx:/> pcapdump -size 1024 -start lan
```

2. lan インタフェースの記録の取得を停止します。

```
DFL-xxxx:/> pcapdump -stop lan
```

3. 要約された形式でコンソールにダンプ出力します。

```
DFL-xxxx:/> pcapdump -show
```

4. これと同じ情報が cap_lan.ca と呼ばれるファイルに完全な形で記載されています。

```
DFL-xxxx:/> pcapdump -write lan -filename=cap_lan.cap
```

分析をするためには、この時点で「cap_lan.cap」ファイルを管理ワークステーションにダウンロードする必要があります。

5. 最終的なクリーンアップが実行され、取得したすべてのメモリが解放されます。

```
DFL-xxxx:/> pcapdump -cleanup
```

キャプチャファイルの再使用

ファイアウォールからファイルを削除する唯一の方法は、ローカルコンソールを経由したものであるため、「pcapdump -write」オプションを使用する場合には、いつも同じファイル名を使用することをお勧めします。新しい書込み操作は、古いファイルを上書きします。

マルチプルインタフェース上の動作

複数の「pcapdump」を同時に実行することができます。以下の項目は、本機能に関する説明です。

1. すべての実行から取得したすべてのキャプチャは、同じメモリバッファに登録されます。

本コマンドは、異なるインタフェースを指定して複数回起動することができます。この場合、異なった実行に対するパケットフローはレポートの別セクションにまとめられます。

インタフェース間を流れるパケットのより明確な出力が必要である場合、希望するインタフェースを指定して 1 つの pcapdump コマンドを実行することが最適です。

2. インタフェースを指定しないと、すべてのインタフェースでキャプチャが行われます。

3. インタフェースを指定しないで「-stop」オプションを使用すると、すべてのインタフェースでキャプチャを停止します。

4. 「pcapdump」は、コマンドの重複を検出することによって、同じインタフェースで複数回キャプチャが実行されることを防ぎます。

フィルタオプション

特定のインタフェースを通過するすべてのパケットをキャプチャすると、有用な情報以上の過剰な情報が提供されることになります。特定のトラフィックのタイプに照準を合わせるために、「pcapdump」コマンドに対して、以下の形式のいずれかのフィルタオプションを追加することができます。

フィルタ	説明
-eth=<macaddr>	送信元または送信先 MAC アドレスでフィルタします。
-ethsrc=<macaddr>	送信元 MAC アドレスでフィルタします。
-ethdest=<macaddr>	送信先 MAC アドレスでフィルタします。
-ip=<ipaddr>	送信元または送信先 IP アドレスでフィルタします。
-ipsrc=<ipaddr>	送信元 IP アドレスでフィルタします。
-ipdest=<ipaddr>	送信先 IP アドレスでフィルタします。
-ipversion=<1...15>	IP バージョンでフィルタします。
-port=<portnum>	送信元または送信先ポート番号でフィルタします。
-srcport=<portnum>	送信元ポート番号でフィルタします。
-destport=<portnum>	送信先ポート番号でフィルタします。
-proto=<id>	id が 10 進数のプロトコル ID であるプロトコルをフィルタします。
-<protocolname>	「-proto=」を使用する代わりに、プロトコル名だけで指定することができます。「-tcp」、「-udp」または「-icmp」の 1 つを指定することができます。

複数ポートの検証

ポート番号のリストでポートを指定します。

```
DFL-xxxx:/> pcapdump -size 1024 -start lan -port=67,68
```

ポート範囲で指定することもできます。

```
DFL-xxxx:/> pcapdump -size 1024 -start lan -port=8080-8088
```

出力ファイルをダウンロードする

上記例題の 1 つに示した通り、「pcapdump」の「-write」オプションは、バッファリングしたパケット情報をファイアウォールのファイルに保存することができます。

これらの出力ファイルは、NetDefendOS ルートディレクトリに置かれ、ファイル名は「pcapdump」コマンド行で指定されます。通常は「.cap」のファイルタイプを使用します。出力ファイル名は、以下で記述する指定ルールに従う必要があります。Secure Copy（SCP）を使用してファイルをローカルワークステーションにダウンロードすることができます。「2.1.8 セキュアコピー」を参照してください。「ls」CLI コマンドを発行することによって、NetDefendOS のルートディレクトリのすべてのファイルリストを参照することができます。

「-cleanup」オプションは、ファイルを消去するためのオプションであり、ファイルのダウンロード終了後に行う必要があります。

出力ファイル名の制限

「pcapdump」出力に使用されるファイル名は、以下のルールに従う必要があります。

- ファイル名の拡張子を除き、名前は 8 文字以内とします。
- ファイル名の拡張子は 3 文字以内とします。
- ファイル名と拡張子は、半角英数字 (A-Z、0-9,「-」、および「_」を使用します。

フィルタの組み合わせ

対象とするパケットを精査するために、複数のフィルタ表現を一緒に使用することができます。例えば、特定の宛先 IP アドレスで特定の宛先ポートに向かうパケットを調べることができます。

Wireshark との互換性

オープンソースツールの Wireshark（以前は Ethereal と呼ばれていた）は、キャプチャしたパケットに関するログを調べるための非常に有益な解析ツールです。「pcapdump」コマンドを「-write」オプションで実行したときに出力される業界基準の「.pcap」ファイルの形式は、Wireshark と互換性があることを意味します。

詳しくは、http://www.wireshark.org を参照してください。

Web インタフェースで pcap を使用する

Web インタフェースの **Status > Tools > Packet Capture** で上で説明したすべての機能を使用することができます。また、直接 .cap ファイルを管理ワークステーションにダウンロードすることも可能です。Wireshark がインストールされていて、ファイルの関連付けが設定されていれば、直接ソフトウェアでファイルを開くことができます。

2.6.7 traceroute コマンド

概要

NetDefendOS の「traceroute」 CLI コマンドは、外部ネットワークのルータを通過する際にパケットが取得するルートおよびこれらのルータからのラウンドトリップタイムに関する情報を提供します。

Traceroute は、1 で始まる time-to-live（TTL）値を持つパケットを送信することで機能し、その後連続的にパケットを増加させます。パケットが通過するのに従って、ルータは time-to-live を減少させます。値が 0 になると、パケットはルータによって破棄され、ICMP time-exceeded メッセージが送信元に送り返されます。送信元は、次のルータに到達できるように TTL が 2 である別のパケットを送信します。意図する宛先に到達するまで、time-to-live の増加は続きます。ソースと宛先の間のルータによって返送された ICMP time-exceeded メッセージは、traceroute 出力のベースを提供します。

「traceroute」コマンドは Microsoft Windows™ などの他の多くのシステムにもあります。Windows のように、ICMP ping メッセージとして、NetDefendOS は traceroute パケットを送信します。NetDefendOS の CLI コマンドの基本形式は以下の通りです。

```
DFL-xxxx:/> traceroute <destination>
```

<destination> は IPv4 または IPv6 アドレスです。例題は以下の通りです。

```
DFL-xxxx:/> traceroute 192.168.4.1
```

または、DNS が解決できる Fully Qualified Domain Name（FQDN）を指定することも可能です。例題は以下の通りです。

```
DFL-xxxx:/> traceroute server.example.com
```

FQDN と共に traceroute を使用する場合、アドレス解決を実行するためには少なくとも 1 つの DNS サーバを NetDefendOS に設定する必要があります。詳しくは、「3.10 DNS 設定」を参照してください。

トレースルートの出力

FQDN として指定される宛先を持つ、初期設定を使用した traceroute からの代表的な出力結果は以下の通りです。

```
DFL-xxxx:/> traceroute server.example.com

Tracing server.example.com [10.194.40.247], 30 hops max, 32 bytes of data
Hop#   RTT     RTT     RTT     Host
  1   10 ms   10 ms   10 ms    10.4.16.1
  2   10 ms   10 ms   10 ms    10.4.0.2
  3   10 ms    0 ms   10 ms    10.194.40.247
Trace complete.
```

ここで、出力結果の各行は、次のルータに到達するために traceroute が行った試行に対応します。

初期値では traceroute は各ルータホップを 3 回試み、ミリ秒で表された Round Trip Time は対応する RTT の見出しの下に表示されます。上の出力結果のターゲットの宛先へのパスには 2 つのルータがあります（ホップ番号 1 と 2）。最終的なホップ（番号 3）は DNS が IPv4 アドレス 10.194.40.247 にアドレス解決された宛先です。

ルートは変更可能

パケット交換ネットワークの動的性質を考えると、「traceroute」コマンドが送信した連続したパケットが異なるルータのセットを通過することが考えられます。このような処理が発生していることを知るのは困難であり、「traceroute」コマンドの出力結果には表示されません。

指定したホップ値で異なる複数のルータが応答する可能性もあります。traceroute の出力結果の行の最後にある Host 欄の下に表示されたアドレスは、常にそのホップに送信された最後の ICMP メッセージに対応したルータのものです。

traceroute オプション

traceroute コマンドの重要なオプションは以下の通りです。

- **-6**

  宛先を FQDN として指定する場合、NetDefendOS は解決する DNS サーバから IPv4 アドレスを要求するだけであり、そのアドレスを宛先アドレスとして使用します。IPv6 アドレスが DNS サーバから要求され、宛先アドレスとして使用される場合は、本オプションを使用しなければなりません。

  ```
  DFL-xxxx:/> traceroute server.example.com -6
  ```

  または、「traceroute」コマンドの後に直接 IPv6 アドレスを入力できます。

- **-maxhops**

  送信されたパケットの time-to-live パラメータに最大値を指定します。

  ```
  DFL-xxxx:/> traceroute server.example.com -maxhops=20
  ```

  初期値は 30 です。

  NetDefendOS が設定したタイムアウト（初期値は 1（秒））以内にルータから何の応答も取得しないと、maxhops の制限に到達するまで time-to-live 値を増やしながら ICMP ping メッセージを送信し続けるため、Maxhops による制限は重要です。

- **-count**

  各ホップに試行する回数を指定します。

  ```
  DFL-xxxx:/> traceroute server.example.com -count=1
  ```

  初期値は 3 です。

- **-size**

  送信されるペイロードのサイズを指定します。ペイロードはランダムデータから作成されます。

  ```
  DFL-xxxx:/> traceroute server.example.com -size=128
  ```

  初期値は 32 です。

- **-nodelay**

  各クエリが遅延なく送信されるように指定します。

```
DFL-xxxx:/> traceroute server.example.com -nodelay
```

  初期値は無効です。

  「-count」パラメータにより指定した traceroute ICMP メッセージの数が、最初に遅延なしで連続的に送信されます。そして、メッセージの次のセットが増加した time-to-live 値で送信される前に 1 秒の固定遅延があります。「-nodelay」を指定することで、1 秒の遅延は削除され、メッセージのセットは遅延なしで連続的に送信されます。この連続したパケットストリームは denial-of service（DOS）攻撃をシミュレートできます。

- **-starthop**

  ホップを開始する time-to-live（TTL）値を指定します。

```
DFL-xxxx:/> traceroute server.example.com -starthop=3
```

  初期値は 1 です。

- **-stop**

  進行中のすべての traceroute を終了させます。

```
DFL-xxxx:/> traceroute -stop
```

- **-timeout**

  time-to-live を増やして、再試行する前に、NetDefendOS がルータまたは宛先から応答を待つ時間です。

```
DFL-xxxx:/> traceroute server.example.com -timeout=2000
```

  あらゆるタイムアウト条件が traceroute の出力結果に示されます。以下はこの出力例です。

```
DFL-xxxx:/> traceroute example.com

Tracing example.com [10.120.184.11], 30 hops max, 32 bytes of data
Hop#    RTT       RTT     RTT   Host
  1     0 ms      0 ms   10 ms  10.4.16.1
  2    10 ms     10 ms   10 ms  10.4.0.2
  3    10 ms     10 ms   10 ms  10.131.48.2
  4      *         *       *    Request timed out
```

  以下の場合にタイムアウトが発生します。

  i. ルータまたは宛先が ICMP ping メッセージに応答するように設定されていない可能性がある。

  ii. 宛先ホストがオフラインの可能性がある。

オプションの組み合わせ

単一のコマンドに上記のオプションのいずれも組み合わせられます。例題は以下の通りです。

```
DFL-xxxx:/> traceroute server.example.com -count=2 -starthop=3 -maxhops=4

Hop#    RTT     RTT    Host
  3    10 ms   10 ms   10.131.48.2
  4    10 ms   10 ms   ge1-1-0-617.cty-pe3.una.se.ip.tzc.net [10.88.215.44]
  5    10 ms   10 ms   te2-1-80.zty-p2.sfl.se.ip.tzc.net [10.131.143.226]
  6   120 ms  120 ms   10.82.35.201
Maximum hops reached.
```

コマンドの全オプションについては、「CLI Reference Guide」を参照してください。

2.6.8 frags コマンド

IP データのフラグメント化は、大きいパケットが横断するネットワーク機器の Maximum Transmission Unit（MTU）サイズ内に適合する小さいデータフラグメントに分解されることから起こります。そのようなフラグメントを NetDefendOS が受信すると、パケットリアセンブリでは、それを転送する前に、完全なパケットに修復するように再び組み立てます。

CLI コマンド「frags」により、管理者はリアセンブリプロセスの現在の状態を調べることができます。パラメータなしで frags コマンドを使用すると、現在アクティブなリアセンブリの状態を、以下の例題の通り出力結果に示します。

```
DFL-xxxx:/> frags

RecvIf Num  State   Source       Destination   Protocol Next  Timeout
------ ---- ------- ------------ ------------- -------- ----- -------
If1    886  Unknown 192.168.1.6  192.168.2.1       ESP      0 593/593
If2    890  Accept  10.0.1.60    192.168.3.1       UDP   7280 592/591
If3    345  Drop    192.168.0.2  10.1.1.2          UDP   1494 581/101
```

本コマンドの各行の出力は、個々のリアセンブリ処理のステータスを示しており、少なくとも一つのパケットフラグメントが IP データグラムとして受信されています。リアセンブリプロセスにある各データは、ソース / 宛先 IP アドレスとそのプロトコル番号で識別されます。まださらにフラグメントを受信する可能性がある限り、リアセンブリ操作はコマンドの出力に残ります。

リアセンブリの状態

frags コマンドの結果出力で参照される再組み立ての State は以下の項目のいずれかです。

状態	説明
Done	リアセンブリは終了したが、リアセンブリは、2 重化フラグメントのある場合に備え、少しの間 alive 状態を維持します。
Drop	NetDefendOS は、組み立て直されたパケットを設定ルールに基づいて破棄することを決定しました。これは Accept 状態の反対で、受信したフラグメントでマッチするものすべてが破棄されます。
Unknown	パケットを破棄するか、または受け付けるかをまだ判断していないことを示します。
Accept	設定ルールに基づいてパケットを破棄しないように決定していることを示します。これは Drop 状態の反対で、受信したフラグメントでマッチするものすべてを受け付けます。
Free	新しいリアセンブリの開始に利用可能なリアセンブリスロットを示します。

frags コマンドのオプション

Free 状態にあるリアセンブリスロットを参照するためには、「-free」オプションを使用します。

```
DFL-xxxx:/> frags -free
```

完了したリアセンブリ操作を参照するには、「-done」オプションを使用します。

```
DFL-xxxx:/> frags -done
```

最大長の設定

NetDefendOS は以下の設定を使用して、指定サイズを超過するパケットを破棄するように、様々なプロトコルに入力するパケットの最大サイズを制御することができます。

パラメータ	説明
Max TCP Length	TCP パケットの最大サイズ（ 初期値 :1480 バイト）
Max UDP Length	UDP パケットの最大サイズ（ 初期値 :60000 バイト）
Max ICMP Length	ICMP パケットの最大サイズ（ 初期値 :10000 バイト）
Max ICMPv6 Length	ICMPv6 パケットの最大サイズ（ 初期値 :10000 バイト）
Max GRE Length	GRE パケットの最大サイズ（ 初期値 :2000 バイト）
Max IPsec ESP Length	Psec ESP パケットの最大サイズ（ 初期値 :2000 バイト）
Max IPsec AH Lenth	IPsec AH パケットの最大サイズ（ 初期値 :2000 バイト）
Max SKIP Length	SKIP パケットの最大サイズ（ 初期値 :2000 バイト）
Max OSPF Length	OSPF パケットの最大サイズ（ 初期値 :1480 バイト）
Max IPIP/FWZ Length	IPIP/FWZ パケットの最大サイズ（ 初期値 :2000 バイト）
Max IPsec IPComp Length	IPsec IPComp パケットの最大サイズ（ 初期値 :2000 バイト）
Max L2TP Length	L2TP パケットの最大サイズ（ 初期値 :2000 バイト）
Max Other Length	その他のパケットの最大サイズ（ 初期値 :1480 バイト）
Log Oversized Packets	最大サイズを超えた場合のログ生成

しかし、個々の NetDefendOS インタフェースの MTU 値では、パケットサイズがどのように分割されるかを決定しています。例えば、最大の UDP 長を 60,000 に設定できますが、インタフェースの MTU サイズが 1500 であると、パケットは 41 のフラグメント（60,000/1500）に分割されます。

法外に大きいパケットは攻撃の形式として使用され、設定した最大値を超過する場合は、NetDefendOS が直ちにそれらを廃棄するため、これらの最大値を可能な限り低い値に維持することが有益です。

TCP Length

TCP を使用すると、正常に設定されているすべての TCP スタックは、TCP パケットのサイズをネゴシエートされた Maximum Segment Size（MSS）値に制限します。通常、この MSS 値は MTU 値から 20 バイトの IP ヘッダサイズを引いた値になります。1500 バイトの MTU 値では、MSS は 1480 バイトになり、通常、これはフラグメント化の必要がなくなります。

2.6.9 selftest コマンド

動作の問題は NetDefendOS ではなく、ハードウェアプラットフォームに関する問題によって引き起こされる場合があります。このため、ハードウェア機能を様々な観点からテストを実行するのに、CLI コマンドの selftest を提供します。

警告 ライブトラフィックでテストを行わないでください！

「selftest」コマンドはライブトラフィックを送信するシステムで使用するべきではないことを覚えておくことが重要です。本コマンドにより接続と関連データが失われ、テスト結果自身の信頼性は低くなります。

ハードウェアの準備

「selftest」の信頼性を完全に保証するには、ユニットのすべてのネットワーク接続を切断すると共に、現在の構成をすべてバックアップし、ハードウェアユニットを基本の構成にリセットすることをお勧めします。

これは HA クラスタ内のユニットについても同様です。クラスタは 2 つの別のハードウェアユニットに分割し、それらをそれぞれの基本構成にリセットするべきです。

基本構成へのリセットは CLI、または Web インタフェースを通じて実行できます。CLI を使用したコマンドは以下の通りです。

```
DFL-xxxx:/> reset -configuration
```

シンプルな例題

「selftest」の簡単な使用は、システムメモリをテストすることです。

```
DFL-xxxx:/> selftest -memory
```

これは、1 メガバイトのデータブロックをメモリに書き込み、それを読み戻します。「-num=」オプションを使用することで書かれるメガバイト数を変更できます。初期値では、メモリテストは 1 回ですが、以下の例題に示すコマンドでは 10 回繰り返されます。

```
DFL-xxxx:/> selftest -memory -num=10
```

スループットテスト

以下のコマンドオプションはトラフィックのスループットをテストします。

- **-throughout**
  これは、最大パケットサイズを使用して、指定したすべてのインタフェースを通過する実行可能な最大トラフィックフローを生成します。本オプションは受信パケットを検証しません。
- **-traffic**
  このテストは、60 ～ 1,518 バイト間で混在するパケットサイズのトラフィックを生成し、各受信フレームのコンテンツを検証します。本オプションでは、受信パケットを検証します。

「-throughput」または「-traffic」オプションを使用する場合、インタフェース同士が接続し、1 つのインタフェースからの出力を別のインタフェースが受信するようにテストを実行する必要があります。これは、以下に示す 2 つの方法のうちのいずれかで実現できます。

- **スイッチを通じた接続**
  すべてのインタフェースは、他のどのネットワークにも接続していない同じスイッチに接続します。インタフェースの速度によって差が出る可能性があるため、ハードウェアがすべてのイーサネットインタフェースに同じ最大リンク速度を持っている場合にだけ、この方法が適切に動作します。

- **ペアでイーサネットインタフェースに接続する**
  混在したイーサネットインタフェース速度を持つハードウェアを使用する場合、隣接するペアで同じ最大リンク速度でインタフェースに接続する必要があります。スイッチを使用するべきではありません。一度に 1 つのインタフェースのペアをテストするべきです。例えば、「-throughput」オプションが If1 と If2 インタフェース間に適用される場合、コマンドは以下の通りです。

```
DFL-xxxx:/> selftest -interfaces=If1,If2 -throughput
```

-burnin オプション

「-burnin」オプションを使用すると、テストサブセットとして知られる一式のテストが連続的に繰り返されます。テスト期間の初期値は 2 時間で、サブセットの初期値は以下の通りです。

- -memory
- -ping
- -throughput
- -traffic
- -cryptoaccel

テストのサブセットで「-burnin」テストの期間を変更できます。30 分間メモリとメディアのテストを繰り返す例は以下の通りです。

```
DFL-xxxx:/> selftest -burnin -minutes=30 -memory -media
```

例えば、時々発生するだけのエラー、またはあるハードウェアの部品が、あるクリティカルな動作温度に到達した後にだけ発生するエラーを検出するのに「-burnin」オプションを使用できます。

「selftest」CLI コマンドの全オプションのリストについては、「CLI Reference Guide」をご参照下さい。多くのコマンドラインの例題と共に記載されています。

2.6.10 techsupport コマンド

techsupport コマンドは、問題をトラブルシューティングするための一般的なコマンドです。複数のトラブルシューティングコマンドを単一のコンソール出力としてまとめたものになります。この出力結果は管理者が利用することも可能ですが、通常は問題を解決するために、適切なサポートに送付します。

techsupport コマンドは以下のいずれかの方式で実行できます。

- CLI コンソールで techsupport コマンドを入力します。
  コンソールに結果が出力されます。長い出力結果となる可能性があるため、この方法はあまり適切なコマンド実行方式ではないかもしれません。

- Web インタフェースからコマンドを実行します。
  NetDefendOS の Web インタフェースでは、ボタンを 1 回押すだけで techsupport コマンドを実行することができます。出力結果は、ブラウザを実行している管理コンピュータのローカルでディスクにファイルとして保存されます。
  分析用にサポート宛にファイルを送る場合は、このコマンド実行形式が最も最適なファイル取得方法と言えます。
  NetDefendOS により生成されたファイル名の形式は、「techsupport-yyyymmdd.txt」となります。「yyyymmdd」部分は作成日時です。ファイルのヘッダにもタイムスタンプが含まれ、ファイル作成時の正確なシステム時間を示しています。

例題 2.35

techsupport 出力を作成する

この例題では、CLI 及び Web インタフェースで techsupport コマンドを実行します。

CLI

```
DFL-xxxx:/> techsupport
```

Web Interface

1. **System > Maintenance > Technical Support** の順にメニューをクリックします。
2. 「Download support file」ボタンをクリックします。
3. ファイルがコンピュータにダウンロードされます。

2.7 メンテナンス

2.7.1 バージョン更新のアラート

概要

NetDefendOS では、関連するアップグレードに関して D-Link サーバから情報を受信するように設定することが可能です。この情報は、Web インタフェースを介して管理者に表示されます。これにより、管理者に対してアップグレードが利用可能であることが通知されます。本機能は初期値で有効化されており、無効化するには管理者が手動で設定を変更する必要があります。手順については、本セクションの最後に例題で説明します。

D-Link サーバとの通信は暗号化され、定期的である

NetDefendOS と D-Link サーバ間の通信は暗号化されており、以下のタイミングで行われます。

- システム起動の直後
- 起動後 1 日あたり一度

必要な前提条件

以下のすべての条件に合う場合にだけ、この機能は動作します。

- NetDefendOS はパブリックインターネットにアクセスできる。
- 機能が管理者によって無効にされていない。

ログイベントメッセージの生成

管理者に対し、バージョンの更新が可能であることのアラートが生成される際、ログメッセージも生成されます。メッセージのセベリティレベルは Notice で、ログイベント名は new_firmware_available です。

例題 **2.36**

サービスの自動更新を有効にする

この例題では、NetDefendOS の各サービスの自動更新を有効化します。

Web Interface

1. **Status > Maintenance > Update Center** の順にメニューをクリックします。
2. SERVICES セクションで自動更新を有効にするサービスにチェックを入れます。
3. 「OK」ボタンをクリックします。

2.7.2 自動更新メカニズム

多くの NetDefendOS セキュリティ機能は、自動更新とコンテンツフィルタリングのために、外部サーバに依存しています。侵入検知と防御（IDP: Intrusion Prevention and Detection）システムとアンチウィルスモジュールは、最新の脅威からの防御を提供するために、更新されたシグネチャデータベースにアクセスする必要があります。

自動更新機能を容易にするために、D-Link は、D-Link ファイアウォールに更新サービスを提供するグローバルな組織サーバを構築しています。入手しやすく、少ないレスポンス回数で、NetDefendOS の更新を提供するために、最適なサーバを自動的に選択するメカニズムを採用しています。

これらの機能に関する詳細は、以下のセクションを参照してください。

- 「7.6 侵入検知と防御」
- 「6.4 アンチウィルススキャン」
- 「6.2 Web コンテンツフィルタリング」

2.7.3 コンフィグレーションのバックアップ

管理者は、任意の時点で NetDefendOS システムのスナップショットを取得し、必要に応じてそれを復元することができます。

スナップショットには 2 つのタイプがあります。

- コンフィグレーションのバックアップ
  これは、1 つのファイルに保存されている現在の全 NetDefendOS コンフィグレーションであり、インストールされた NetDefendOS バージョンを含みません。コンフィグレーションのみを復元する場合に役に立ちます。

  ハードウェアのリプレースの際に容易に再作成できるように定期的に最低限のコンフィグレーションをバックアップすることが重要です。そうでない場合、1 つ 1 つコンテンツを手動で追加してコンフィグレーションを再作成することになります。

- システムのバックアップ
  これは、1 つのファイルに保存されたコンフィグレーションとインストール済み NetDefendOS ソフトウェアの両方の完全なバックアップです。これは、コンフィグレーションと更新された NetDefendOS バージョンの両方を復元する場合に便利です。

  完全なシステムバックアップは、コンフィグレーションのバックアップよりはるかに大きいファイルであり、数十メガバイトであるかもしれません。そのため、それに伴う時間を考えると定期的にこれを実行することは推奨されません。しかし、D-Link ファイアウォールが初めて設定されて動作した段階で、少なくとも一度これを作成することをお勧めします。完全なシステムバックアップにより、現在のコンフィグレーションを新しいハードウェアに復元することが簡単になります。

注意 バックアップ機能はすべてを含まない

DHCP サーバのリースデータベースやアンチウィルス /IDP データベースなどのダイナミックな情報はバックアップされません。

バージョンの互換性

完全なシステムバックアップには NetDefendOS バージョンが含まれるため、これらのバックアップのタイプに関して互換性の問題はありません。

コンフィグレーションのみのバックアップに関しては、以下の項目について注意することが必要です。

- 新しい NetDefendOS バージョンで作成されたコンフィグレーションのバックアップは、それより古い NetDefendOS バージョンには絶対にアップロードしないでください。例えば、NetDefendOS 11.20.00 バージョンが動作するファイアウォールから作成したバックアップを 11.10.02 バージョンが動作するファイアウォールに絶対にアップロードしないでください。

- 古いバージョンで作成されたコンフィグレーションのバックアップは、常にそれより新しいバージョンにアップロードできますが、特定の場合に互換性の問題があり、アップロードしたコンフィグレーションをアクティベートする場合に NetDefendOS からメッセージが表示されます。そのようなケースでは、NetDefendOS の再起動が発生することがあります。

- そのため、新しい NedDefendOS が搭載済みの新しいハードウェアに、保存済みコンフィグレーションを転送する場合に完全なシステムバックアップが有用です。最初に、完全なシステムバックアップをアップロードして、正しいバージョンのシステムを取得し、次に、最新のコンフィグレーションのバックアップをアップロードします。より新しい NetDefendOS バージョンに移行させたい場合には、NetDefendOS のアップグレードを実行できます。

使用する管理インタフェース

SCP(Secure Copy)、または Web インタフェースを使用してファイアウォールから直接ファイルをダウンロードすることにより、コンフィグレーションおよびシステムの両方についてバックアップファイルを作成することができます。バックアップは CLI コマンド経由で行うことはできません。

同様に、反対の手順（アップロード）によって、バックアップの復元が行われます。SCP または Web インタフェースを使用してバックアップファイルをアップロードします。CLI コマンドでは復元はできません。

注意 異なるハードウェアにシステムのバックアップをアップロードしないでください。

完全なシステムバックアップ（コンフィグレーションと NetDefendOS）を取得したものと同じモデルではないハードウェアにアップロードしないようにしてください。

異なるハードウェアにアップロードした場合、コンフィグレーションの自動的なアクティブ化と NetDefendOS の再起動を引き起こし、システムが到達不能になる可能性があります。アクティブ化前にコンフィグレーションを変更する機会がないため、完全なシステムバックアップは同じハードウェアにだけ行う必要があります。

操作の割込み

NetDefendOS の処理を妨害せずに、いつでもバックアップを作成できます。しかし、復元では、復元されたコンフィグレーションがファイアウォールのセキュリティポリシーを大幅に変更する可能性があるため、アクティブなトラフィックフローがある状況で実施することをお勧めしません。

バックアップを復元した後は、通常のコンフィグレーション変更を行うように新しい変更をアクティブ化する必要があります。

完全なシステムの復元はより複雑で、既存のすべての接続の損失を伴う NetDefendOS の再初期化を必要とします。初期化は、ハードウェアタイプにより完了するまでに数秒を必要とし、通常の操作はこの間に行うことはできません。

SCP を使用したバックアップとリストア

NetDefendOS ルートディレクトリには 2 つのファイルが置かれています。

- config.bak - 現在のコンフィグレーションのバックアップです。
- full.bak - 完全なシステムのバックアップです。

SCP は、これらのファイルのどちらかをダウンロードするために使用されます。ダウンロード完了後、管理者は手動でファイル名にダウンロード日付を含むようにリネームする必要があります。

バックアップファイルを復元するためには、管理者はバックアップファイルを本製品にアップロードする必要があります。NetDefendOS はファイルのヘッダを読むことでファイルを識別することができるため、日付を含めてファイル名の変更は不要です。SCP によるバックアップファイルのアップロードにより、ファイルコンテンツのリストアが実行されます。

Web インタフェースを使用したバックアップとリストア

SCP の使用に代わる手段として、管理者は Web マネージャ経由で直接コンフィグレーションまたは全システムのバックアップとリストアを行うことができます。Web インタフェースを使用する場合、前述の 2 つのファイルに対し、NetDefendOS により自動的に現在の日付が付けられます。例えば、full.bak は 2008 年 11 月 21 日の状態のスナップショットであることを示すために「full-20081121.bak」となります。

例題 2.37

システムの完全なバックアップをダウンロードする

システムのバックアップを行います。

Web Interface

現在動作中の構成のバックアップを作成する :

1. メニューバーの **Status > Maintenance > Backup & Restore** の順にメニューをクリックします。
2. SYSTEM BACKUP セクションの Backup System をクリックします。
3. コンピュータにファイルがダウンロードされます。

コンフィグレーションのバックアップファイルを調べる

「.bak」ファイルのコンフィグレーションファイルのみ通常のテキストエディタで開くことが可能であり、コンテンツを検証することができます。ただし、ファイルには修正及び保存ができないバイナリ情報が含まれます。

コンフィグレーション「.bak」ファイルは初期値と異なるオブジェクトのプロパティ値のみを示します。したがって、「.bak」ファイルのコンフィグレーションを調べる最も良い方法は、それを NetDefendOS にロードして、保存およびアクティブ化せずに、参照用として Web インタフェースを使用することです。

2.7.4 工場出荷時設定にリセットする

「restore to factory defaults」を適用して、D-Link ファイアウォールを購入した時の元のハードウェア状態に設定を戻すことができます。リストアを適用すると、IDP やアンチウィルスデータベースなどのデータはすべてなくなるため、再ロードする必要があります。

例題 2.38

ハードウェアを完全に工場出荷時設定にリセットする

CLI

```
DFL-xxxx:/> reset -unit
```

Web Interface

1. **Status >Maintenance > Reset & Restart** の順にメニューをクリックします。
2. RESET TO FACTORY DEFAULTS セクションで「Reset the entire unit to factory defaults. This includes firmware version and configuration.」オプションを選択します。
3. 「Reset to Factory Defaults」ボタンを押下し、確認後リセット処理が完了するまでしばらく待ちます。

工場出荷時設定にリセットすると、すべての更新が失われます。

すべての設定が工場出荷時設定に戻ります。本製品が工場から出荷された後に行われたあらゆる NetDefendOS の更新が失われます。

基本のコンフィグレーションにリセットする

完全な工場リセットに代わる別の手段は、基本コンフィグレーションにファイアウォールをリセットすることだけです。これは、NetDefendOS コンフィグレーションだけが工場出荷時設定にリセットされることを意味します。

基本構成へのリセットは CLI、または Web インタフェースを通じて実行できます。CLI を使用したコマンドは以下の通りです。

```
DFL-xxxx:/> reset -configuration
```

DFL-260E、860E、および 870 をリセットする

D-Link DFL-260E、860E、および 870 モデルをリセットするには、電源を入れたときに 10-15 秒間、ユニットのリセットボタンを押さえたままにします。その後、リセットボタンを放すと、ユニットは読み込みを続け、初期の工場出荷設定で起動します。

DFL-1600、2560、および 2560G をリセットする

DFL-1660/2560/2560G モデルをリセットするためには、前面のディスプレイ上に「Press keypad to Enter Setup」メッセージが表示されたら、キーパッド上のキーを押下します。次に「Reset firewall」オプションを選択し、確認後、「Yes」を選択します。リセット処理が完了した後、ユニットが工場出荷時設定で起動します。

警告 初期化（リセット）を中止しないでください

工場出荷時設定へのリセット処理を終了前に中止すると、ファイアウォールは、保存されているユーザデータのすべてを完全に喪失して適切な動作は中止されてしまいます。

インタフェース IP アドレスをリセットする

初期値へのリセットは、管理インタフェースと管理アクセスの IP アドレスを初期値にリセットします。

また、本操作により、管理インタフェースの他に、ネットワーク 127.0.x.0/24 で 127.0.x.1 になるようにすべてのイーサネットインタフェースの IPv4 アドレスをリセットします。「x」の値は 1 から始まり、連続したインタフェース毎に 1 つずつ増加していきます。管理インタフェースはスキップされます。

IPv4 アドレス 127.0.0.1 はループバックインタフェースの予約アドレスであるため使用されません。

廃棄処理の手続き

また、工場出荷時設定へのリストアオプションは、本製品が運用を終了し、もう使用しない場合に廃棄処理の手続きの一部として使用されるべきものです。

廃棄処理の手続きの一部として、工場出荷時設定へのリストアは、VPN 設定のような注意を要する情報のすべてを削除するために行われます。また、製品の廃棄に向けた予防措置として、本製品の記憶媒体を破壊し、またコンピュータ処分のサービスを行う適切な業者により破棄し、それを証明してもらうことをお勧めします。

2.8 言語

NetDefendOS のグラフィカルな管理インタフェースは多くの言語で利用可能です。インタフェースを開く際に、言語をプルダウンメニューから選択できます。

グラフィカルインタフェースに表示された選択言語は、NetDefendOS によってファイアウォールの不揮発性メモリにある個別の言語ファイルのセットの 1 つから読まれます。これらのファイルは CLI の「languagefiles」コマンドを使用して表示および管理されます。これらのすべてがファイルタイプ「.RC」を持っています。

すべての利用可能な言語ファイルを参照するには、オプションなしでコマンドを使用してください。

```
DFL-xxxx:/> languagefiles
Language files
LNG-CH.RC --> “Chinese”
```

この出力は、中国語ファイルだけが存在することを示しています。

言語ファイルを削除するには、「-remove」オプションを使用します。

```
DFL-xxxx:/> languagefiles -remove=LNG-CH.RC
Removing “LNG-CH.RC” ...OK
```

1 つも言語ファイルがなければ、以下の出力が表示されます。

```
DFL-xxxx:/> languagefiles
Language files
No language files found
```

デフォルト言語である英語は、NetDefendOS にハードコード化されており、リストにファイルとして現れません。

注意 R11.10.01.06 以降のバージョンでは、日本語 GUI 言語ファイルが用意されていません。ログイン画面で English を選択してご使用ください。

2.9 診断と品質向上

概要

D-Link は NetDefendOS 及び関連するサービスを向上するために、NetDefendOS に Diagnostics と Improvements として知られる機能を提供します。これは、NetDefendOS インストールに関する情報メッセージを D-Link サーバに自動的に送信するための NetDefendOS のオプションから成ります。

本機能は初期値で有効で、本セクションの終わりの例題で示すとおり、無効にする場合は管理者により手動で設定する必要があります。

通信は暗号化され定期的に送信される

NetDefendOS と D-Link サーバ間の通信は暗号化されており、以下の場合に起こります。

- システム起動の直後
- 起動に続いて 1 日あたり一度

上記の例外として、変則的なイベントが起こった後に、一度だけ送信されるクラッシュのレポートがあります。

D-Link に送信される情報

診断と品質向上機能が有効であると、NetDefendOS が D-Link に返す情報は以下のタイプになります。

情報	説明
匿名の診断報告	この情報は、NetDefendOS に関するスタティックパラメータに関連しており、NetDefendOS バージョン番号や、アンチウィルスまたは IDP データベースなどのあらゆるインストールされたデータベースとバージョン番号も含んでいます。
匿名の診断報告と利用統計情報	初期値は「Enabled」です。利用統計情報は、システム運用に関するより高いレベルの詳細情報を提供し、以下のようなパラメータを含んでいます。 • システム使用時間 • インストールされた RAM メモリ量 • CPU 負荷 • RAM メモリ使用量 • Web コンテンツフィルタリング（有効な場合）
クラッシュレポート	初期値で有効であり、変則的なシステムイベントが起こると、暗号化されて匿名の情報を D-Link に送信します。クラッシュレポートは、イベントの後に 1 度だけ送信されます。このレポートは D-Link のエンジニアが NetDefendOS で問題が発生した箇所や理由を判断するのに役立ちます。

注意 ログイベントメッセージは生成されません。

診断と品質向上情報が NetDefendOS によって D-Link に送信される場合に、ログメッセージは何も生成されません。

例題 **2.39**

診断と品質向上メッセージの作成を無効にする

この例題では、診断と品質向上機能を無効にする方法を示しています。

CLI

```
DFL-xxxx:/> set Settings DiagnosticsSettings EnableDiagnostics=No
```

Web Interface

1. **System > Advanced Settings > Diagnostic Settings** の順にメニューをクリックします。
2. Anonymous Diagnostics Reporting 設定を無効にします。
3. 「OK」ボタンをクリックします。

第 3 章 基本機能

この章では、NetDefendOS のコンフィグレーションを構成する基本的な論理オブジェクトについて記載しています。これらのオブジェクトには、IP アドレスや IP ルールセットのエントリなどの項目があります。初期状態で存在するものもありますが、いくつかは管理者が定義する必要があります。さらに、異なるインタフェースタイプやセキュリティポリシーの構築方法ついて記載しています。

- 「3.1 アドレス帳」
- 「3.2 IPv6 のサポート」
- 「3.3 サービス」
- 「3.4 インタフェース」
- 「3.5 ARP」
- 「3.6 IP ルールセット」
- 「3.7 アプリケーションコントロール」
- 「3.8 スケジュール」
- 「3.9 証明書」
- 「3.10 DNS 設定」

3.1 アドレス帳

3.1.1 概要

NetDefendOS のアドレス帳には名前を持つオブジェクトがあり、IP アドレス範囲をはじめ IP アドレス、ネットワークを含む各種 IP アドレスのタイプを表しています。アドレス帳にはイーサネット MAC アドレスを定義することもできます。

アドレス帳オブジェクトを使用することには、以下に示す多くの重要な利点があります。

- 意味のある英字名を使用することによって、コンフィグレーションの理解が深まります。
- 数字のアドレスを入力する代わりにアドレスオブジェクト名を使用すると、誤りが抑制されます。
- アドレス帳に IP アドレスオブジェクトを定義することで、この定義を変更した場合、自動的にすべての参照先にも変更が行われます。

3.1.2 IP アドレス

IP アドレスオブジェクトは、IP アドレスの各タイプにシンボル名を定義するために使用されます。アドレスを指定する方法によって、IP アドレスオブジェクトは IP アドレス（指定ホスト）、ネットワーク、または IP アドレス範囲も意味します。

さらに、IP アドレスオブジェクトは、ユーザ認証で使用するユーザ資格証明書を指定するためにも使用されます。詳しくは、「第 9 章 ユーザ認証」を参照してください。

シンプルな IP アドレスのアドレスオブジェクトは以下の 2 通りがあります。

- IPv4 アドレス用の IP4 Address オブジェクト
- IPv6 アドレス用の IP6 Address オブジェクト

本セクションでは IPv4 アドレスオブジェクトが使用される様々なパターンを説明します。IPv6 アドレスオブジェクトについては「3.2 IPv6 のサポート」で説明します。

IPv4 アドレスタイプ

以下のリストは、IP アドレスオブジェクトが持ち得る様々なタイプのアドレス及び、その特定のタイプを示すために使用されるフォーマットについて記載しています。

アドレスタイプ	内容
ホスト	1 台のホストが IP アドレスによって示されます。 例 : 192.168.0.14
IP アドレス	IP ネットワークは、CIDR（Classless Inter Domain Routing）形式を使用して示されます。CIDR は、ネットワークのサイズ（ネットマスク）を表すために「/」と数字「0-32」を使用します。/24 は、256 アドレス（ネットマスク 255.255.255.0）を持つクラス C のネットワークに、/27 は、32 アドレスネット（ネットマスク 255.255.255.224）に相当します。0-32 の番号は、ネットマスク内の 2 進数を表します。 例：192.168.0.0/24
IP 範囲	IPv4 アドレスの範囲は、a.b.c.d - e.f.g.h の形式で示されます。範囲がネットマスクバウンダリに限定されず、IP アドレスのあらゆる範囲を含んでいることにご注意ください。 例 : 192.168.0.10-192.168.0.15 は連続する 6 個のホストを示しています。

例題 3.1

シンプルな IPv4 アドレスを追加する

ここでは、IP アドレス 192.168.10.16 の IPv4 ホスト wwwsrv1 をアドレス帳に追加します。

CLI

```
DFL-xxxx:/> add Address IP4Address wwwsrv1 Address=192.168.10.16
```

Web Interface

1. **Objects** > **Address Book** > **Add** > **IP4 Address** の順にメニューをクリックします。
2. 「Name」に「wwwsrv1」と「Address」に「192.168.10.16」を入力し、「OK」ボタンをクリックします。

例題 3.2

IPv4 ネットワークを追加する

ここでは、アドレス 192.168.10.0/24 を持つ wwwsrvnet という名前の IPv4 ネットワークをアドレス帳に追加します。

CLI

```
DFL-xxxx:/> add Address IP4Address wwwsrvnet Address=192.168.10.0/24
```

Web Interface

1. **Objects** > **Address Book** > **Add** > **IP4 Address** の順にメニューをクリックします。
2. 「Name」に「wwwsrvnet」、「Address」に「192.168.10.0/24」を入力し、「OK」ボタンをクリックします。

例題 3.3

IPv4 アドレス範囲を追加する

ここでは、IPv4 アドレス範囲（192.168.10.16 - 192.168.10.21）を追加し、wwwservers という範囲名をつけます。

CLI

```
DFL-xxxx:/> add Address IP4Address wwwservers Address=192.168.10.16-192.168.10.21
```

Web Interface

1. **Objects** > **Address Book** > **Add** > **IP4 Address** の順にメニューをクリックします。
2. 「Name」に IP 範囲名「wwwservers」、「Address」に IP アドレス範囲「192.168.10.16-192.168.10.21」を入力し、「OK」ボタンをクリックします。

例題 3.4

アドレスオブジェクトを削除する

以下の手順でアドレス帳の wwwsrv1 という名前のオブジェクトを削除します。

CLI

```
DFL-xxxx:/> delete Address IP4Address wwwsrv1
```

Web Interface

1. **Objects** > **Address Book** の順にメニューをクリックします。
2. アドレスオブジェクト「wwwsrv1」を右クリックし、「Delete」を選択します。

使用中の IP オブジェクトの削除

別のオブジェクトで使用中の IP オブジェクトが削除されると、NetDefendOS はコンフィグレーションが展開されることを許可せず、警告メッセージを生成します。つまり、オブジェクトの削除には成功したように見えますが、NetDefendOS は、コンフィグレーションのファイアウォールへの保存を許可しません。

3.1.3 イーサネットアドレス

イーサネットアドレスオブジェクトは、イーサネットアドレス（MAC アドレス）にシンボル名を定義するために使用されます。これは、スタティック ARP エントリを ARP テーブルに登録する場合や、数字のイーサネットアドレスをシンボリック名で表したい設定のために使用します。

イーサネットアドレスは aa-bb-cc-dd-ee-ff の形式を使用します。イーサネットアドレスが表示される際もこの形式となります。

例題 3.5

イーサネットアドレスを追加する

ここでは、MAC アドレス 08-a3-67-bc-2e-f2 を持つイーサネットアドレスオブジェクトを wwwsrv1_mac という名前でアドレス帳に追加します。

CLI

```
DFL-xxxx:/> add Address EthernetAddress wwwsrv1_mac Address=08-a3-67-bc-2e-f2
```

Web Interface

1. **Objects > Address Book > Add > Ethernet Address** の順にメニューをクリックします。

2. 「Name」に「wwwsrv1_mac」、「MAC Address」に「08-a3-67-bc-2e-f2」を入力し、「OK」ボタンをクリックします。

3.1.4 アドレスグループ

グループ簡素化設定

構成をシンプルにするために、アドレスオブジェクトをグループ化できます。インターネットからアクセス可能にする必要がある多数のサーバについて考えてみます。各サーバは連続的でない IP アドレスを割り振られており、1 つの IP 範囲で参照することはできません。そのため、個別の IP アドレスオブジェクトを各サーバに作成する必要があります。

各サーバにトラフィックを許可する個別のセキュリティポリシーを作成し維持するという負担を軽減するために、web-server などと名付けたアドレスグループを作成し、グループメンバとして Web サーバホストを含めることができます。このようにまとめることで、 1 つの IP ルールセットのエントリの中でフィルタ条件としてグループを指定することが可能になるため、それにより管理コストを大幅に削減することができます。

アドレスグループのタイプ

アドレスグループのオブジェクトは、以下のいずれかのタイプになります。

- IPv4 Group オブジェクト - メンバには IPv4 アドレスオブジェクトのみ含めることができます。
- IPv6 Group オブジェクト - メンバには IPv6 アドレスオブジェクトのみ含めることができます。
- Ethernet Address Group オブジェクト - メンバにはイーサネットアドレスオブジェクトのみ含めることができます。
- FQDN Group オブジェクト - メンバには FQDN アドレスオブジェクトのみ含めることができます。

IP アドレスの除外

グループを Web インタフェースで作成する場合、アドレスオブジェクトをグループに追加することが可能なだけでなく、グループから明示的にアドレスを除外することができます。しかし、CLI を使用してグループを作成する場合には除外することはできません。

グループからの除外は、グループからメンバーを削除することとは異なります。除外されたアドレスオブジェクトはグループのメンバーのままですが、グループにより記述された IP アドレス空間からは除外されます。

例えば、ネットワークオブジェクトがネットワーク「192.168.2.0/24」であり、これをグループに追加する場合、明示的に IPv4 アドレス「192.168.2.1」を除外するのは可能です。これは、グループには「192.168.2.2」から「192.168.2.255」までの範囲が含まれることを意味します。

グループは異なるサブタイプを持つことが可能

アドレスグループオブジェクトは、同じタイプのオブジェクト（IP4 アドレスなど）を持つ必要がありますが、グループ内でサブタイプが分かれることも可能です。例えば、IPv4 アドレスは、IPv4 アドレスの範囲と IPv4 ネットワークを組み合わせて IP4 Group とすることができます。グループは全てのメンバオブジェクトのアドレスの集合体を表しています。

例えば、IP4 グループが 2 つの IP4 アドレスオブジェクトを持つ場合、以下のようになります。

- 192.168.0.10 - 192.168.0.15
- 192.168.0.14 - 192.168.0.19

これらの 2 つを組み合わせた結果は、192.168.0.10 - 192.168.0.19 という 1 つのアドレス範囲となります。

CLI からグループメンバを追加または削除する

グループが定義された後、メンバを追加したり削除したりすることが必要になる場合があります。Web インタフェースを利用すると、利用可能なオブジェクト及びグループのオブジェクトが表示されているため、簡単に作業を行うことができます。CLI を利用することも可能ですが、特別なコマンド構文が必要となります。

my_ip_group という名前の IP4Group が既に定義されているものとします。これには my_ip_1、my_ip_2、my_ip_3 という名前の 3 つの IP4Address オブジェクトが含まれています。my_ip_2 のオブジェクトがグループから削除する場合、コマンドは以下のようになります。

```
DFL-xxxx:/> set Address IP4Group my_ip_group Members-=my_ip_2
```

「Members=」オプションにより、1 つ以上のメンバをグループから削除します。メンバを追加する場合は、「Members+=」オプションを使用します。IP4Address オブジェクト「my_ip_4」と「my_ip_5」をグループに追加する場合、以下のコマンドを実行します。

```
DFL-xxxx:/> set Address IP4Group my_ip_group Members+=my_ip_4,my_ip_5
```

例題 3.6

IP4 グループオブジェクトを作成する

この例題では、IP4 アドレスグループオブジェクト my_ip4_address1 と my_ip4_address2 がアドレス帳に定義済みであると仮定して、IP4 グループ ip4_group に追加します。

CLI

```
DFL-xxxx:/> add Address IP4Group my_ip4_group Members=my_ip4_address1,my_ip4_address2
```

Web Interface

1. **Objects > Address Book > Add > IP4 Group** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_ip4_group
3. Available から my_ip4_address1 を選択し、Include をクリックします。
4. Available から my_ip4_address2 を選択し、Include をクリックします。
5. 「OK」ボタンをクリックします。

3.1.5 自動生成されるアドレスオブジェクト

設定を簡便にするために、システムがはじめに起動した際に自動的にいくつかのアドレスオブジェクトがアドレス帳に生成されます。これらのオブジェクトは、初期構成の段階で既にいくつかの設定に使用されています。

以下のアドレスオブジェクトが自動的に生成されます。

オブジェクト	内容
Interface address	システム内の各イーサネットインタフェースのために、2つの IP アドレスが事前に定義されています。一つは実際のインタフェースの IPv4 アドレスに対するオブジェクトで、もう一つはそのインタフェースのローカルネットワークを表しています。インタフェース IPv4 アドレスオブジェクトは、「**インタフェース名** _ip」という名前で、ネットワークオブジェクトは「**インタフェース名** _net」という名前が付けられています。例えば、「lan1」という名前のインタフェースは、「lan1_ip」という名前の IP オブジェクトと「lan1_net」というネットワークを持ちます。 これらのアドレスは InterfaceAddresses と呼ばれるアドレス帳フォルダに保存されます。 イーサネットインタフェースの IP アドレスを変更する場合、直接イーサネットインタフェースで IP アドレスを変更せずに、デフォルトアドレス帳オブジェクトのアドレスを変更することを強くお勧めします。
Default Gateway	「_gw」を持つ IP アドレスオブジェクトは、パブリックインターネットへの接続に使用されるデフォルトインタフェースに対して自動的に生成されます。例えば、インターネット接続がインタフェース「wan」にあるとすると、デフォルトゲートウェイアドレスは、「wan_gw」という名前を取得します。この IP アドレスは、インターネットへのゲートウェイとして機能する外部ルータを示します。 このアドレスは、ルーティングテーブルによって優先的に使用されますが、DHCP サーバから要求されるゲートウェイアドレス情報を保存するために、DHCP クライアントサブシステムによっても使用されます。デフォルトゲートウェイアドレスが設定過程で提供されると、デフォルトゲートウェイオブジェクトはそのアドレスに設定されます。そうでない場合、オブジェクトは「0.0.0.0/0」のままになります。
all-nets アドレスオブジェクト	「all-nets」オブジェクトはアドレス「0.0.0.0/0」に初期化され、すべての想定される IPv4 アドレスを表します。このオブジェクトは、NetDefendOS を設定する際に広く使用されており、その意味を理解することが重要です。

3.1.6 Address Book フォルダ

アドレス帳における大量のエントリの構成を助けるために、Address Book フォルダを作成することができます。これらのフォルダはコンピュータのファイルシステム内のフォルダによく似ています。アドレス帳は、指定された名称で作成され、グループとして関連するすべての IP アドレスオブジェクトを含めるために使用されます。

フォルダの使用は、管理者が簡単に Address Book エントリを分割できる方法であり、個々のフォルダのエントリに対して特別なプロパティが設定されている訳ではありません。NetDefendOS は、まるでそれらが IP アドレスオブジェクトの大規模テーブルであるかのようにすべてのエントリを参照し続けます。

また、NetDefendOS は、IP ルールセットにおいてフォルダの概念を使用します。そこでは、管理者が作成したフォルダに、関連する IP ルールをグループ化します。

前述の通り、初回起動時に作成されたデフォルトフォルダ「InterfaceAddresses」があり、NetDefendOS によって検出されたイーサネットインタフェースのデフォルトアドレスオブジェクトを含みます。

例題 3.7

アドレスフォルダオブジェクトを作成する

この例題では、アドレスフォルダオブジェクト my_address_folder を作成します。

CLI

```
DFL-xxxx:/> add Address AddressFolder my_address_folder
```

Web Interface

1. **Objects > Address Book > Add > Address Folder** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_address_folder
3. 「OK」ボタンをクリックします。

3.1.7 FQDN アドレスオブジェクト

概要

アドレスオブジェクトを IP アドレスとして指定する代わりに、FQDN Address オブジェクトに FQDN（例：server1.example.com）として指定できます。他の構成オブジェクトがそのオブジェクトを参照する場合に、NetDefendOS は FQDN を自動的に IP アドレスに解決します。

FQDN アドレスオブジェクトプロパティ

FQDN Address オブジェクトには、以下のプロパティがあります。

オブジェクト	内容
Name	オブジェクトの論理名。これは管理者によって指定されます。
Address	オブジェクトの FQDN。これは管理者によって指定されます。
Active Address	FQDN が解決されると、これは FQDN の IP アドレスになります。解決されないと、このプロパティは値を割り当てられません。NetDefendOS だけがこのプロパティを設定できます。

FQDN アドレスオブジェクトの使用ルール

現在、次の種類の NetDefendOS オブジェクトだけが、FQDN Address オブジェクトへの参照を含めることができます。

- IP Policy オブジェクトの送信元 / 宛先ネットワーク
- IP ルールセットにおける Goto Rule または Return Rule オブジェクトの送信元 / 宛先ネットワーク
- Routing Rule の送信元 / 宛先ネットワーク
- IDP Rule オブジェクトの送信元 / 宛先ネットワーク
- トラフィックシェーピング機能で使用される Pipe Rule オブジェクトの送信元 / 宛先ネットワーク
- トラフィックレート制限で使用される Threshold Rule オブジェクトの送信元 / 宛先ネットワーク
- IPsec Tunnel オブジェクトのリモートエンドポイント
- Mail Alerting オブジェクトの SMTP Server プロパティ
- システム日時構成で使用されるカスタムタイムサーバの IP アドレス

FQDN 解決には設定済みの DNS サーバが必要である

FQDN Address オブジェクトが正しく機能するためには、DNS Server オブジェクトを作成して少なくとも 1 つのが外部 DNS サーバを設定する必要があります。NetDefendOS の DNS サーバの設定については、「3.10 DNS 設定」を参照してください。

DNS ルックアップは一貫性があるべきである

管理者は、IP Policy オブジェクトによって参照される FQDN Address オブジェクトに対する DNS ルックアップの結果が、これらのポリシーで影響を受けるホストで使用される DNS ルックアップの結果と同じであることを確認する必要があります。DNS ルックアップの一貫性を確実にするには、NetDefendOS で使用されている DNS サーバが、保護する対象のホストと同じ DNS サーバと同じであるようにします。

FQDN Address オブジェクトの利用は FQDN 解決のトリガーとなる

新しいコンフィグレーションが展開されて、そのコンフィグレーションが FQDN Address オブジェクトを利用する時だけ、NetDefendOS は DNS 解決を実行しようとします。つまり、現在の NetDefendOS のコンフィグレーションには FQDN Address オブジェクトが既にあるかもしれませんが、コンフィグレーションを変更する時だけ、DNS ルックアップを実行するため、アドレスオブジェクトは、例えば IP Policy オブジェクトによって参照されます。

DNS サーバが設定されていない場合、FQDN Address オブジェクトを使用する設定（IP Policy オブジェクトなど）を展開しようとすると、NetDefendOS でエラーが発生します。

DNS 解決が失敗したときの動作

NetDefendOS により、FQDN アドレスオブジェクトから IP アドレスへの解決ができなかった場合、オブジェクトを参照するすべてのルールは、トラフィックに対してトリガされません。つまり、設定にルールが存在しないように処理されます。

同様に、IPsec トンネルにおいて FQDN アドレスオブジェクトを使用してエンドポイントを設定している場合、FQDN が解決できないと、このトンネルは失敗します。また、Mail Alerting オブジェクトで FQDN アドレスオブジェクトが解決できない場合もアラートが送信されません。

FQDN Address オブジェクトは複数の IP を保存できる

FQDN に応じて、DNS ルックアップは IPv4 および IPv6 アドレスの両方を返すことができます。1 つの DNS 応答の中で、複数の IPv4/IPv6 アドレスが存在する場合があります。DNS クエリにおいて、1 つの応答の中で複数の IP アドレスが返された場合、NetDefendOS によって、クエリを開始した FQDN アドレスオブジェクトに対していずれかのアドレスが割り当てられます。NetDefendOS は 1 つの DNS 応答で最大 128 個の IPv4 アドレス、そして / または、128 個の IPv6 アドレスを処理することができます。いずれのタイプについても、DNS サーバから送信される IP アドレスで 128 個の制限を超過したものは破棄されます。DNS 応答によって返された全てのアドレスは、FQDN キャッシュに保存され、後で参照することができます。

ルールの処理にはすべての FQDN アドレスが含まれる

FQDN Address オブジェクトを参照するルールに対してトラフィックが一致した場合、その FQDN に紐づくすべての IP アドレスに対して検証が行われます。つまり、単一または複数の応答の中で、DNS サーバが 2 つ以上のアドレスを返した場合、いずれかの IP アドレスがルールによって正しくトリガされます。

この動作は、FQDN Address オブジェクトが単一のエンドポイントとして使用される場合は適用されません。例えば、IPsec Tunnel や Mail Alerting オブジェクトなどが該当します。

FQDN アドレスキャッシング

NetDefendOS は、内部の FQDN Address Cache を使用することで、参照される度に、同じ FQDN Address オブジェクトが解決される必要はないことを保証します。以下の CLI コマンドを使用することで現在のキャッシュコンテンツを調べることができます。

```
DFL-xxxx:/> dns -cache
```

以下は、このログメッセージの出力例です。

```
DFL-xxxx:/> dns -cache

Name                              Status     IP Cnt Address
--------------------------------- ---------- ------ --------------------
my_fqdn_address1                  Resolved        1 server1.example.com
my_fqdn_address2                  Unused          0
```

以下のコマンドでキャッシュ内の特定の FQDN の状態を調べることができます。

```
DFL-xxxx:/> dns -cache <FQDN>
```

<FQDN> はアドレス帳にあるアドレスオブジェクトの論理的構成名です。以下はコマンドの出力の例です。

```
DFL-xxxx:/> dns -cache my_fqdn_address1

Address   : my_fqdn_address1
Status    : Resolved

IP address                                        LifeTime
------------------------------------------------- --------
203.0.113.3                                       299
```

また、Web インタフェースで **Status > Run-time Information > DNS Cache** メニューを使用して、DNS キャッシュに関するこの情報にアクセスできます。

Minumum TTL 設定

また、DNS サーバが FQDN Address オブジェクトに対して IP アドレスを返すとき、Time To Live（TTL）の値も返します。この値は DNS キャッシュの中の FQDN Address オブジェクト用のエントリと共に保存されます。TTL の期限が切れる時、NetDefendOS は、新しい DNS クエリを発行することによって、キャッシュエントリをリフレッシュします。

DNS サーバから返された TTL は、非常に低い値かゼロであるかもしれません。このため、NetDefendOS はグローバルな DNS 設定 Minimum TTL（初期値：1 秒）を提供します。DNS サーバから返された TTL が、Minimum TTL 値以下であれば、TTL は、Minimum TTL 値になるようにリセットされます。

Minimum Cache Time 設定

また、Minimum Cache Time と呼ばれる 2 番目のグローバルな DNS 設定があります。初期値は 86,400 秒（1 日）です。NetDefendOS は、新しいエントリの追加時、キャッシュが一杯である場合にのみ、Minimum Cache Time の期限を待たずにエントリを削除します。

Minimum Cache Time 設定は、複数の DNS クエリが 1 つの FQDN に対して異なる IP アドレスを返したときに、重要になってくる可能性があります。DNS サーバによっては、所定の FQDN に対してラウンドロビン形式で動作し、連続するクエリにおいて異なる IP アドレスを返してサーバ負荷を分散します。最小キャッシュ時間の値を高くすると、所定の FQDN に対して想定されるすべての IP アドレスがキャッシュ内に共存できるようになります。

キャッシュエントリの TTL が期限切れとなっても最小キャッシュ期間に到達していない場合、FQDN に対する新しい DNS リクエストが NetDefendOS によって発行され、DNS サーバによって返された新しい IP アドレスに対して追加のキャッシュエントリが作成されます。

FQDN にワイルドカードを使用する

FQDN Address オブジェクトの FQDN に対し、ワイルドカードとしてアスタリスクの記号を使用することができます。アスタリスクはあらゆる文字の組み合わせを意味します。以下のルールに基づき、ワイルドカードが使用されます。

- ワイルドカードは FQDN の最初や最後の文字として使用することができます、例えば、*.example.com 及び www.example.* はどちらも有効な値です。as is *.example.*
  しかし、www.*.com は無効であり、NetDefendOS によって拒否されます。最初や最後の文字として指定されたワイルドカードは、文字列の一部としても使用されます。例えば、*server.example.com という文字列は client_server.example.com や vpn_server.example.com に一致します。

- ワイルドカードは、NetDefendOS 設定において FQDN Address オブジェクトがフィルタの一部である場合にのみ使用することができます。例えば、*.example.com は、IP Policy オブジェクトの Destination Network プロパティに対する FQDN の値となり得ます。
  単一の IP アドレスのみが適用されるアドレスオブジェクトについては、ワイルドカードは使用できません。例えば、ネットワークタイムサーバの IP アドレスは FQDN Address オブジェクトとして設定することは可能ですが、この FQDN にはワイルドカードを含めることはできません。

- ワイルドカードが使用される際、ワイルドカードを含む URL の対象となる Web サイトにクライアントがアクセスする際の DNS クエリを許可する IP Policy に対して、適切な DNS Control Profile が関連づけられている必要があります。さらに、プロファイルの Populate DNS Cache プロパティを有効にしている必要があります（初期値で有効）。プロファイルの設定方法については、「6.1.12 DNS ALG」を参照してください。
  クライアントから DNS サーバへ送信される DNS クエリからのエントリとともに DNS キャッシュを展開するためには、DNS Control Profile を設定する必要があります。DNS Control Profile オブジェクトと一緒に設定された DNS ALG は、DNS クエリ処理を取り次いで、ワイルドカードによって生成された複数の DNS 応答をキャッシュに置き換えます。

DNS Control Profile が使用されない場合、FQDN のワイルドカードは動作しません。

注意 FQDN で非常に多数のワイルドカードが使用されている場合、リソースが消費され、システムのパフォーマンスに影響が出る可能性があります。

関連するログメッセージ

NetDefendOS は、FQDN Address オブジェクトに関連している以下のログメッセージを生成します。

ログメッセージ	説明
ipv4_max_addresses	128 個の IPv4 アドレス制限を超えたため、DNS サーバからのアドレスは破棄されました。
ipv6_max_addresses	128 個の IPv6 アドレス制限を超えたため、DNS サーバからのアドレスは破棄されました。
dns_no_record	DNS サーバに FQDN のレコードがないため、解決することができません。
dns_timeout	DNS サーバは FQDN ルックアップ中にタイムアウトになりました。
dns_error	DNS ルックアップ中に、不明なエラーが発生しました。
ip6_address_added	FQDN の IPv6 アドレスは、解決されてキャッシュに追加されます。
ip6_address_removed	FQDN IPv6 アドレスの生存時間は期限が切れたので、キャッシュから削除されました。
ip4_address_added	FQDN の IPv4 アドレスは、解決されてキャッシュに追加されます。
ip4_address_removed	FQDN IPv4 アドレスの生存時間は期限が切れたので、キャッシュから削除されました。

例題 3.8

FQDN Address オブジェクトを追加する

この例題では、FQDN Address オブジェクト「my_fqdn_address1」を NetDefendOS アドレス帳に追加する方法を示しています。

FQDN Address オブジェクトは FQDN「server.example.com」のアドレスを含みます。FQDN を IP アドレスに解決できるように、少なくとも 1 つの DNS サーバが NetDefendOS に既に設定されているものとします。

CLI

```
DFL-xxxx:/> add Address FQDNAddress my_fqdn_address1 Address=server.example.com
```

Web Interface

1. **Objects > Address Book > Add > FQDN Address** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_fqdn_address1
   - Address: server.example.com
3. 「OK」ボタンをクリックします。

例題 3.9

DNS Minimum TTL と Minimum Lifetime を設定する

この例題では、Minimum TTL に 10 秒、Minimum Cache Time に 1000 秒を設定します。

CLI

```
DFL-xxxx:/> set DNS MinTTL=10 MinCacheTime=1000
```

Web Interface

1. **System > Device > DNS** の順にメニューをクリックします。
2. Advanced 設定を選択します。
3. 以下の情報を入力します。
   - Minimum TTL: 10
   - Minimum Cache Time: 1000
4. 「OK」ボタンをクリックします。

例題 3.10

IP ポリシーを持つ FQDN オブジェクトを使用する

この例題では、lannet ネットワークの内部のクライアントから Web サイト www.example.com までの接続は許可されません。

CLI

A. www.example.com のために FQDN オブジェクトを作成する

```
DFL-xxxx:/> add Address FQDNAddress example_website Address=www.example.com
```

B. サイトへの接続を破棄する

```
DFL-xxxx:/> add IPPolicy Name=deny_lan_to_example SourceInterface=lan SourceNetwork=lan_net
            DestinationInterface=any DestinationNetwork=example_website Service=all_services
```

Web Interface

A. www.example.com のために FQDN オブジェクトを作成する

1. **Objects > Address Book > Add > FQDN Address** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: example_website
   - Address: www.example.com
3. 「OK」ボタンをクリックします。

B. サイトへの接続を破棄する

1. **Policies > Firewalling > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: deny_lan_to_example
   - Action: Deny
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: any
   - Destination Network: example_website
   - Service: all_services
3. 「OK」ボタンをクリックします。

3.1.8 FQDN グループ

通常の IP アドレス帳オブジェクトは Address Group オブジェクトにまとめることができます。同様に、FQDN アドレスオブジェクトも FQDN Group オブジェクトにまとめることができます。例えば、複数の FQDN アドレスオブジェクトを使用したポリシーを適用する場合、複数の IP ポリシーを設定する必要はありません。

注意 IP ルールでは FQDN グループはサポートされません。

FQDN Address オブジェクトと同様に、FQDN Group オブジェクトは IP Rule オブジェクトで使用することはできません

例として、FQDN「example.com」「www.example.com」「server.example.com」を参照する FQDN Address オブジェクトを想定します。これらのオブジェクトは FQDN Group オブジェクトにまとめることが可能であり、それぞれの URL への / からの接続を許可する単一の IP Policy オブジェクトによって使用することができます。

注意 FQDN グループには FQDN グループを含めることはできません。

FQDN Group オブジェクトには FQDN Address オブジェクトのみ含めることができます。他の FQDN Group オブジェクトを含めることはできません。

例題 3.11

FQDN Group オブジェクトを作成する

この例題では、FQDN Group オブジェクト my_fqdn_group を作成します。このグループには my_fqdn_address1 と my_fqdn_address2 オブジェクトが含まれます。

CLI

```
DFL-xxxx:/> add Address FQDNGroup my_fqdn_group Members=my_fqdn_address1,my_fqdn_address2
```

Web Interface

1. **Objects > Address Book > Add > FQDN Address** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_fqdn_group
3. Available から my_fqdn_address1 を選択し、Include をクリックします。
4. Available から my_fqdn_address2 を選択し、Include をクリックします。
5. 「OK」ボタンをクリックします。

3.2 IPv6 のサポート

今まで説明した IP アドレスはすべて IPv4 タイプです。IP アドレスの標準 IPv6 は、128 ビットよりもはるかに大きいアドレス空間を提供するという最も重要な利点を持ち IPv4 の後継として設計されています。多くの利点がありますが、IPv6 では、グローバル IP アドレスを大量に使用できるため、IPv4 のように NAT を使って限られた数のグローバル IPv4 アドレスを共有する必要がありません。

本セクションでは、IPv6 の利用を有効にする方法、IPv6 オブジェクトを作成する方法、クライアントによるステートレス自動構成を有効にする方法、IPv6 アドレスオブジェクトを使用する IP ルールとルートを作成する方法を記載しています。

注意 プレフィックス「2001:DB8::/32」はドキュメンテーションのために予約されています。

RFC 3849 で記載されている通り、IPv6 プレフィックス「2001:DB8::/32」は文書記述用に予約されています。そのため、本書のすべての IPv6 の例ではこのネットワークまたはこのネットワークのアドレスを使用します。

IPv6 をサポートする NetDefendOS コンフィグレーションオブジェクト

NetDefendOS の以下に示すオブジェクトが IPv6 をサポートしています。

- アドレス帳
- ルーティングテーブル（スイッチルートを除く）
- ルーティングルール
- IP ルールセット（いくつかのアクションを除く）
- HTTP と LW-HTTP ALG
- IPsec トンネル
- リモート管理（所定の IPv6 ネットワークやホストからの通信を許可するリモート管理オブジェクトを定義する必要があります。HTTP/HTTPS 通信に対して設定することができます。）

IPv6 は各インタフェースで有効にする

IPv6 が動作するためには、各 NetDefendOS インタフェース上で明示的に IPv6 を有効化する必要があります。具体的には、あるイーサネットインタフェースにルーティングされる Pv6 トラフィックに対し、インタフェースで IPv6 が有効になっている必要があります。IPsec の場合、トンネル内を流れるフローのトラフィックに対してではなく、トンネルを確立するトラフィックに対して有効化する必要があります。初期値ではすべてのインタフェース上で IPv6 が無効化されています。

また、インタフェースで IPv6 を有効化することに加えて、IPv6 アドレスと IPv6 ネットワーク（プリフィックス）が割り当てられている必要があります。これらの設定が行われていると、IPv6 プロパティを持つルールやルールの中でインタフェースを使用することができます。

例題 3.12

インタフェースで IPv6 を有効にする

定義済みのアドレスオブジェクトを使用して、wan イーサネットインタフェースで IPv6 を有効にします。

CLI

```
DFL-xxxx:/> set Interface Ethernet wan1 EnableIPv6=Yes IPv6IP=wan_ip6 IPv6Network=wan_net6
```

Web Interface

1. **Network > Interfaces and VPN > Ethernet** の順にメニューをクリックし、メイン画面の「wan1」のリンクをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。
   - Enable IPv6 : チェックし、IPv6 を有効にします。
   - IP Address: wan_ip6
   - Network: wan_net6

さらに、ISP ルータに接続している場合にはインタフェースに対して IPv6 ゲートウェイアドレスを入力します。

インタフェースルートを自動的に追加する

IPv6 アドレスとネットワークがイーサネットインタフェースに割り当てられると（両方が必要）、そのインタフェースのための IPv6 ルートを main ルーティングテーブルに追加する必要があります。

インタフェースのための自動ルート作成が有効であると（初期値では有効）、ルートが追加されます。

Interface Address オブジェクトを作成する別の方法

IPv6 アドレスオブジェクトは IPv4 オブジェクトと異なるオブジェクトとして NetDefendOS アドレス帳に作成されます。

all-nets6 オブジェクト（IPv6 アドレス「::/0」）がアドレス帳に事前に定義されています。これは、インタフェースに関連付ける IPv6 アドレスとネットワークオブジェクトを作成しなければならないことを意味します。これは、以下の方法のいずれかで行われます。

- 手動でアドレス帳にアドレスオブジェクトを追加した後に、関連インタフェースにこれらのオブジェクトを割り当てます。これは、既に例題で示した通りです。
- イーサネット、VLAN、リンクアグリゲーションインタフェースに対して、DHCPv6 クライアント機能を個々のインタフェースで有効にすることができ、クライアントリースを外部の DHCP サーバから受信する時、必要に応じて IPv6 アドレスオブジェクトが作成されます。DHCPv6 クライアント機能に関する詳細は、「5.6.1 DHCPv6 クライアント」で説明します。
- イーサネット、VLAN、およびリンクアグリゲーションインタフェースに対して、インタフェースで Autoconfigure プロパティを有効にすることで行います。本オプションは次に説明します。

Auto Configure オプション

DHCP クライアントオプションがインタフェースで有効でない場合、自動的に IPv6 アドレスをインタフェースに割り当てるための代替方法があります。インタフェースで Auto Configure IP Address プロパティを有効することによって、NetDefendOS は Extended Unique Identifier（EUI-64）アルゴリズムを使用して IPv6 アドレスを算出します。

EUI-64 アルゴリズムは IP アドレスを選択するのに /64（64 bit）IPv6 ネットワークを必要とします。この /64 ネットワークは以下の 2 つのソースのいずれかを元にしています。

- インタフェースの IPv6 Network プロパティとしてスタティックに定義されます。
- Router Discovery オプションを有効にすることで、インタフェースからアクセス可能な、Neighbor ディスカバリメカニズムを通して検出される外部ルータから取得できるようになります。

例題 3.13

手動で IPv6 インタフェースアドレスを追加する

IPv6 アドレスとネットワークを wan イーサネットインタフェースに関連付ける必要があるものとします。この例題では、アドレス帳に新しい IPv6 アドレスオブジェクト 2 つ：ネットワーク「wan_net6」（IPv6 プレフィックス「2001:DB8::/32」）とそのネットワーク内の単一の IP アドレス「wan_ip6」（2001:DB8::1）を追加します。

CLI

```
DFL-xxxx:/> add Address IP6Address wan_net6 Address=2001:DB8::/32
DFL-xxxx:/> add Address IP6Address wan_ip6 Address=2001:DB8::1
```

Web Interface

ネットワークアドレス（IPv6 プレフィックス）を追加します。

1. **Objects > Address Book > Add > IP6 Address** の順にメニューをクリックします。
2. オブジェクトに適当な名前（ここでは wan_net6）を指定します。
3. IPv6 アドレスに「2001:DB8::/32」を入力します。
4. 「OK」ボタンをクリックします。

IP アドレスを追加する

1. **Objects > Address Book > Add > IP6 Address** の順にメニューをクリックします。
2. オブジェクトに適切な名前（ここでは wan_ip6）を指定します。
3. IPv6 アドレスに「2001:DB8::1」を入力します。
4. 「OK」ボタンをクリックします。

IPv4 と IPv6 はアドレスグループオブジェクトを共有できない

IPv6 アドレスオブジェクトは IPv4 オブジェクトと同様の方法で作成され、管理されます。それらを IP6 Address と呼び、IPv4 アドレスと同様に NetDefendOS ルールと他のオブジェクトに使用できます。しかし、これら 2 つのアドレスオブジェクトを 1 つの設定オブジェクトにまとめることはできません。

例えば、両方を含むアドレスグループを作成することはできません。標準のアドレスグループオブジェクトは IPv4 アドレスオブジェクトしか含むことができません。IPv6 では、IPv6 アドレスしか含むことができない IP6 グループオブジェクトと呼ばれる特別なオブジェクトがあります。

all-nets6 アドレスオブジェクト

定義済みの「all-nets」アドレスオブジェクトはすべての IPv4 アドレス用の「catch-all」オブジェクトです。別のオブジェクト「all-nets6」はすべての IPv6 アドレスを示しており、これには IPv6 アドレスのみ含まれます。

その上、単一のアドレスグループオブジェクトでは「all-net」（すべての IPv4 アドレス）を「all-nets6」と組み合わせることはできません。例えば、「DropAll」ルールが IP ルールセットの最後の「catch-all」ルールとして必要とされる場合、2 つのルールがすべての IPv4 と IPv6 トラフィックの取得のために必要です。詳しくは「3.6 IP ルールセット」を参照してください。

同様に、ルーティングテーブルは、IPv4 または IPv6 いずれかのネットワークに対するトラフィックを同じインタフェースに送信できますが、ルーティングテーブルを 2 つ（IPv4 用と IPv6 用）に分けて行う必要があります。一つのルートだけを使用して実行することはできません。

IPv6 ルータ通知の有効化

イーサネットインタフェースの追加オプションとして、IPv6 ルータ通知を有効にすることも可能です。これは、インタフェースに接続する外部クライアントが Stateless Address Auto-Configuration（SLAAC）を実行するために、IPv6 メッセージの要求および受信が可能であることを意味します。SLAAC プロセスでは、クライアントは接続する NetDefendOS インタフェースの MAC アドレスと IPv6 アドレスのプレフィックスに基づいてクライアント自身の固有なグローバル IPv6 アドレスを作成することができます。

例題 3.14

IPv6 通知の有効化

この例では、wan イーサネットインタフェースで IPv6 通知を有効にします。

CLI

```
DFL-xxxx:/> set Interface Ethernet wan EnableRouterAdvertisement=Yes
```

Web Interface

1. **Network > Interfaces and VPN > Ethernet** の順にメニューをクリックし、メイン画面の「wan1」のリンクをクリックします。
2. Advanced タブを開き、Enable router advertisement for this interface オプションを有効にします。
3. 「OK」ボタンをクリックします。

ICMP エラーのパススルーを有効にする

IPv4 と異なり、IPv6 パケットのフラグメント化は、送信元ホスト側でのみ、自身の MTU サイズの選出を使用して行われます。万一、パケットが、選択された MTU サイズを処理できないネットワーク機器に到達した場合、MTU を減らし、パケットの再送が必要であることを示すために ICMP エラーメッセージを送信元ホストに返送します。

このため、IPv6 トラフィックの IP ルールセットエントリで使用される Service オブジェクトに対しては常に Pass returned ICMP errors messages from destination プロパティを有効化しておくことをお勧めします。これの代替手段として、明示的に両方向の ICMP エラーメッセージを許可する IP ルールセットのエントリを設定することが可能です。

これの例外は、MTU が初めは IPv6 がサポートする最小の MTU である 1280 に設定されている場合です。この場合、エラーは起こらないので、ICMP エラーメッセージが通過できるように設定する必要はありません。

IPv6 Neighbor 探索

IPv6 Neighbor Discovery（ND）は IPv4 ARP プロトコルに相当します。

特定のイーサネットインタフェースで IPv6 を有効にすると、NetDefendOS は、そのインタフェースに設定された IPv6 アドレス用の IPv6 Neighbor Advertisements（NA）で、インタフェースに送信されたどの IPv6 Neighbor Solicitations（NS）にも応答します。また、NetDefendOS は Proxy Neighbor 探索を使用して、設定されたどのネットワークにも Neighbor 通知で応答します。

Proxy Neighbor 探索

NetDefendOS の IPv6 機能である Proxy Neighbor Discovery（ Proxy ND）は、IPv4 用の Proxy ARP（「4.2.6 プロキシ ARP」で説明されています。）と同じように動作します。
プロキシ ND を有効にする方法は以下の 2 つです。

A. 直接インタフェースにアドレスをパブリッシュする
これは、イーサネットインタフェースにオプションを設定することで行われる ARP パブリッシュとまさに同じ方法で行われます。オプションの Publish と Xpublish の両方が IPv6 のためにサポートされます。これらのオプションは「3.5.3 ARP パブリッシュ」で説明されています。

B. スタティックルートの一部としてアドレスをパブリッシュする
特定のイーサネットインタフェース上の IPv6 アドレスのためのルートが作成されると、そのインタフェースで IPv6 は既に有効になっていて、IPv6 Neighbor 探索が使用可能であることを意味します。オプションで、Proxy Neighbor Discovery（Proxy ND）を IPv6 ルートに対して有効にすることもできます。これにより、すべてまたは選択したインタフェースが、ルートのネットワークのために Neighbor Solicitations にも応答します。

この 2 番目の方式を使用した例題は以下の通りです。

例題 3.15

IPv6 ルートを追加し、プロキシ ND を有効にする

main ルーティングテーブルにルートを追加して、IPv6 を有効化した既存のインタフェース If1 上で、IPv6 ネットワーク my_ipv6_net がルーティングされるように設定します。

さらに、my_ipv6_net 用の proxy neighbor discovery が、If3 インタフェースで有効とします。

CLI

まず、main ルーティングテーブルになるように CLI コンテキストを変更します。

```
DFL-xxxx:/> cc RoutingTable main
```

IPv6 ルートを追加します。

```
DFL-xxxx:/main> add Route6 Network=my_ipv6_net Interface=If1 ProxyNDInterfaces=If3
```

最後に、デフォルトの CLI コンテキストに戻します。

```
DFL-xxxx:/main> cc
DFL-xxxx:/>
```

Web Interface

1. **Network > Routing > Routing Tables > main > Add > RouteIPv6** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Interface: If1
   - Network: my_ipv6_net
3. Proxy ND タブを開き、インタフェース If3 を選択して「Include」をクリックし、Available から Selected に移動します。
4. 「OK」ボタンをクリックします。

ICMP ping を使用した IPv6 のトラブルシューティング

CLI コマンドの ping は IPv4 と IPv6 アドレスの両方に対して使用できます。
例 :

```
DFL-xxxx:/> ping 2001:DB8::2
```

IPv6 ホストが到達可能で応答するかどうかを判断するための手段として利用することができます。

ping を Web インタフェースの **Status > Tools > Ping** で開始することもできます。

ゲートウェイが信頼済みであるため、ファイアウォールからの外向き ICMP メッセージを許可する IP ルールは必要ありません。しかし、ファイアウォールが外部ホストにより ping される場合には、IPv4 と同様に、これを許可する IP ルールセットのエントリを設定する必要があります。そのようなエントリは、定義済みの Service オブジェクト ping6-inbound を使用します。Service オブジェクト all_icmpv6 は、モバイル ICMP メッセージ以外のすべての IPv6 ICMP メッセージをカバーしています。

NetDefendOS が IPv6 ping メッセージに応答するのを許可する適切な IP ルールセットのエントリは以下の通りです。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
Allow	wan	all-nets6	core	wan_ip6	ping6-inbound

上のルールは、IPv6 が wan インタフェースで有効であるものと仮定します。

IPv6 使用制限

NetDefendOS の現在のバージョンにおける IPv6 制限の概要は以下の通りです。

- IPv4 と IPv6 アドレスを使用した IP ルールは同じ IP ルールセットに共存できますが、単一のエントリに IPv4 と IPv6 を組み合わせることはできません。
- IPv6 アドレスは、現在、以下のアクションを行う IP ルールではサポートされていません。
  - NAT
  - SAT
  - SLB SAT
  - Multiplex SAT
- IPv4 と IPv6 アドレスを使用したルートは同じルーティングテーブルに共存できますが、単一のルートに IPv4 と IPv6 を組み合わせることはできません。
- IPv4 と IPv6 アドレスを使用したルーティングルールは共存できますが、単一のルールに IPv4 と IPv6 を組み合わせることはできません。
- IPv6 は以下に示す項目と共に使用できません。
  - IDP
  - トラフィックシェーピング（パイプとパイプルール）
  - 多くの ALG。HTTP と LW-HTTP ALG は IPv6 をサポートしています。

IPv6 と高可用性

NetDefendOS High Availability (HA) は IPv6 をサポートしており、どの IPv6 設定オブジェクトも HA マスタおよびスレーブユニットの両方に反映されます。

アドレス帳オブジェクト IP6 HA Address は、IP4 HA Address オブジェクトに相当するものです。これは、共有およびプライベート IPv6 の両方が HA クラスタでインタフェースのペアに割り当てられることを許可します。

管理アクセスのため、またはログ出力の送信元アドレスとしてプライベートインタフェース IPv6 アドレスを使用できませんが、クラスタがアクティブである場合に ICMP ping メッセージに応答するため、または、クラスタが非アクティブの時にそのようなメッセージを送信するために使用できます。

HA クラスタで IP6 HA Address オブジェクトを使用することに関する詳細は「12.3 High Availability（高可用性）設定」を参照してください。

IPv6 と透過モード

経路交換を IPv6 ネットワークでは定義できないため、NetDefendOS の透過モードは直接 IPv6 をサポートしません。（「4.9 透過モード」を参照してください。）

しかし、Proxy ARP が IPv4 で使用されるのと同様の方法で、透過的にネットワークを分割することは可能です。IPv4 のこの手順については、「4.2.6 プロキシ ARP」で説明されています。IPv6 における唯一の違いは、Neighbor Discovery（ND）がプロキシ ARP の代わりに使用されるということです。その他の方式は同じです。同時にこれらは、IPv4/IPv6 ネットワークを分割するためにお互いに一緒に使用することが可能です。

IPv4 ネットワークに IPv6 をトンネルする

NetDefendOS は IPv4 トラフィックだけをサポートするネットワークに IPv6 トラフィックのトンネリングを許可します。これは、IP6in4 Tunnel オブジェクトを使用して行われます。詳しくは、「3.4.8 6in4 トンネル」を参照してください。

Neighbor 探索詳細設定を使用する

本セクションでは、IPv6 の Neighbor Discovery（ND）の設定について、さらに細かく検討します。特に、NetDefendOS Neighbor ディスカバリキャッシュについて説明します。

NetDefendOS における Neighbor 探索の取り扱いは、外部ホストのリンクレイヤと IP アドレスのタプルに関する情報を保有するキャッシュが IPv6 ホストのローカルメモリの中に維持されるという点で ARP の取り扱いに類似しています。NetDefendOS ND キャッシュ状態の概要は以下の通りです。（これらは RFC 4861 で定義されています。）

状態	説明
INCOMPLETE	アドレス解決は進行中で、Neighbor のリンクレイヤアドレスはまだ決定していない。
REACHABLE	Neighbor が最近（最後の 10 秒以内に）到達可能になったことが確認された。
STALE	Neighbor の到達可能性はもう確認されないが、トラフィックが送信されるまで、到達可能性を検証する試みは行わない。
DELAY	Neighbor の到達可能性はもう確認されず、トラフィックは最近送信されていた。到達性を調べる前に、到達性の確認を許可されるまで少し待機してください。
PROBE	Neighbor の到達可能性はもう確認されず、unicast neighbor solicitation probes は到達性を検証するために送信されている。

Neighbor エントリは以下の理由でキャッシュの中に現れます。

- NetDefendOS が Neighbor にパケットを送信しようすると、エントリが作成されます。
- NetDefendOS が、ソースのリンクレイヤアドレスオプションを含む Neighbor solicitation を受信すると、エントリが作成されます。
- スタティックなエントリが管理者によって追加される時。これらは、常に REACHABLE 状態にあると見なされます。

Neighbor 探索のための高度な設定は、ARPNDSettings オブジェクトに含まれ、以下のプロパティを含んでいます。

プロパティ	説明
NDMatchEnetSender	イーサネット送信側アドレスが、パケットの送信元/送信先のリンクレイヤアドレスオプションから得られた送信側イーサネットアドレスにマッチしていないかどうかをチェックします。これは、IP スプーフィングの兆候の可能性があるため、初期値では、マッチしないパケットを破棄するようにこの設定は有効にされています。このチェックをスキップすることが望ましい場面もあります。
NDValSenderIP	有効であると、NetDefendOS は、Neighbor 探索パケットの non-link local 送信元アドレスがルーティングテーブルのルートにマッチすることを要求します。マッチしないと、パケットは破棄されます。 そのような一致するルートが何も設定されていない時に、Neighbor 探索パケットを処理するのであれば、この設定を無効にする必要があります。
NDChanges	時々発生するあるホストへの接続性の損失を経験しているのであれば、この設定を AcceptLog の値にするべきです。これは、原因がハードウェアイーサネットアドレス間を移動する同じ IPv6 アドレスであるかどうか特定するのに役立ちます。
NDCacheSize	Neighbor 探索キャッシュは、Neighbor 探索トラフィックとこのトラフィックを処理するのに要する時間を削減することで、より高いトラフィックのスループット速度を提供します。キャッシュのサイズはこの設定で調整され、異なるネットワークの規模を持つ特定のシナリオに適応することができます。 大きいキャッシュほど、物理メモリの割り当てが大きいことを意味します。しかし、キャッシュが小さ過ぎると、適応できずに項目は破棄されるかもしれません。その結果、より長い待ち時間と、より多くの Neighbor 探索トラフィックにつながってしまいます。
Timing Settings	Neighbor 探索に関連している多くのタイミング設定があります。 - NDMulticastSolicit - NDMaxUnicastSolicit - NDBaseReachableTime - NDDelayFirstProbeTime - NDRetransTimer これらは、低い値ほど短時間通信するだけの迷子のホストにうまく対応できますが、Neighbor 探索トラフィックの増加を引き起こすことを意味します。タイムアウトまたは Probe の送信前にエントリをキャッシュにおく時間を増やすためには、NDBaseReachableTime の値を増やすことをお勧めします。

別紙の「NetDefendOS CLI Reference Guide」で ARPNDSettings オブジェクト名の下に Neighbor 探索に関連している全設定が記載されています。

3.3 サービス

3.3.1 概要

サービスオブジェクトは、関連するパラメータを持つ特定の IP プロトコルを参照します。サービスの定義は、通常指定した送信元および（または）送信先ポート番号に関連付けされた TCP または UDP などの主要な転送プロトコルの一つをベースにしています。例えば、HTTP サービスは関連する送信先ポート 80 といずれかの送信元ポートを持つ TCP プロトコルを使用しているものとして定義されます。

しかし、サービスオブジェクトは TCP や UDP プロトコルに限定されず、ユーザ定義可能な IP プロトコルはもちろん ICMP メッセージを包含するように使用することができます。

サービスはパッシブである

サービスは、コンフィグレーション内のどんなアクションも実行できないパッシブな NetDefendOS オブジェクトです。代わりに、サービスオブジェクトは、様々な NetDefendOS ルールセットによって定義されたセキュリティポリシーに関連付けられ、特定のトラフィックタイプにだけルールを適用するフィルタとして機能します。

例えば、多くのセキュリティポリシーにはフィルタリングパラメータとしてサービスオブジェクトが関連付けられており、特定のプロトコルに対してルールがトリガされるかどうかを決定します。IP ルールセットエントリのフィルタの一部として設定することは、サービスオブジェクトの主要な用途の 1 つです。

IP ルールに関しては、サービスによって ALG が IP ルールに関連付けられます。ALG は、IP ルールに直接ではなくサービスに関連します。サービスオブジェクトが IP ルールにどのように使用されるかについての詳しい情報は、「3.6 IP ルールセット」を参照してください。

一方で、IP ポリシーについては直接 ALG オプションを設定することができます。IP ポリシーに紐づく Service が、ALG の Protocol プロパティに設定されている場合、ALG オプションが設定可能になります。

定義済みサービス

NetDefendOS では多くのサービスオブジェクトが事前に定義されています。これには HTTP と FTP などの一般的なサービスオブジェクトが含まれます。この事前に定義されたサービスは、ユーザが定義したサービスと同じように使用、および編集することができます。しかし、事前に定義されたサービスには変更を行わず、代わりに必要とされるパラメータを使用して新しいサービスを作成することをお勧めします。

カスタムサービスの作成については、「3.3.2 カスタムサービスの作成」を参照してください。

バージョン 11.01 以降で定義済みのサービスに変更する

NetDefendOS バージョン 11.01 以降で、定義済みの Service オブジェクトに変更が行われました。11.01 以降、以下の定義済みのサービスと関連する定義済みの ALG は新しい NetDefendOS の実装から取り外されました。

- http(ALG のみ削除)
- http-outbound（サービスと ALG を削除）
- ftp-inbound（サービスと ALG を削除）
- ftp-outbound（サービスと ALG を削除）
- ftp-internal（サービスと ALG を削除）
- ftp-passthrough（サービスと ALG を削除）

11.01 以前のコンフィグレーションが 11.01 以降にアップグレードされる場合、これらの定義済みのオブジェクトは従来と同様に存続して、従来と同様使用できるため、変更はありません。

新しい NetDefendOS11.01 以降では、必要に応じてこれらの削除されたサービスと ALG はカスタムサービスとして再作成することができます。しかし、より良いオプションは IP Policy オブジェクトを使用することです。例えば、IP ポリシーと共に定義済みの http サービスを利用できます。ALG 経由で以前に利用できた設定のすべてをポリシーに直接利用できます。

11.01 以降の新しいインストールでは、個別の ALG を使用する必要性をなくし、以下の Service オブジェクトのいずれも、直接 IP Policy オブジェクトと共に使用することができます。

- http
- https
- smtp
- imap
- pop3
- ftp
- tftp

上のサービスのすべてにおいて対応する ALG の設定は、関連する IP Policy オブジェクトで利用可能になります。

11.01 より前の NetDefendOS バージョンからアップグレードする場合では、管理者は、Service オブジェクトの Protocol プロパティを正しい値に設定することによって、これらの新しいバージョンのサービスを作成することができます。これにより、NetDefendOS の新規インストールと同様に、サービスを IP ポリシーと一緒に利用できます。

このトピックは、「6.1 アプリケーションレイヤゲートウェイ」でも記載されます。

例題 3.16

有効なサービスを表示する

NetDefendOS で現在有効なすべてのサービスの一覧を表示します。

CLI

```
DFL-xxxx:/> show Service
```

以下のようにサービスグループがはじめに表示され、タイプごとにグループ化されてサービスの一覧が表示されます。

```
ServiceGroup
    Name        Comments
   ------------ --------------------------------------------------
   all_services All ICMP, TCP and UDP services
   all_tcpudp   All TCP and UDP services
   ipsec-suite  The IPsec+IKE suite
   l2tp-ipsec   L2TP using IPsec for encryption and authentication
   l2tp-raw     L2TP control and transport, unencrypted
   pptp-suite   PPTP control and transport
ServiceICMP
...
```

Web Interface

1. **Objects > Services** の順にメニューをクリックし、サービス一覧を表示します。

例題 3.17

特定のサービスを参照する

echo システム内のプロパティを参照します。

CLI

```
DFL-xxxx:/> show Service ServiceTCPUDP echo
```

以下のような一覧が表示されます。

```
 Property           Value             Remarks
 -----------------  ----------------  ---------
             Name:  echo              Read-only
 DestinationPorts:  7
             Type:  TCPUDP (TCP/UDP)
      SourcePorts:  0-65535
         SYNRelay:  No
   PassICMPReturn:  No
              ALG:  <empty>
         Comments:  Echo service
```

Web Interface

1. **Objects > Services** の順にメニューをクリックし、サービス一覧を表示します。

2. 特定のオブジェクトのリンクをクリックし、サービスの内容を表示します。

3.3.2 カスタムサービスの作成

定義済みの NetDefendOS サービスオブジェクトのリストで特定のトラフィックの条件を満たしていない場合、新しいサービスを作成することができます。本セクションでは、新しいサービスの作成方法だけではなく、定義済みサービスのプロパティの理解のために説明も行います。

作成されるサービスタイプは以下の通りです。

- TCP/UDP サービス - UDP、TCP、または両方のプロトコルに基づくサービス。このセクションで、より詳しくこのサービスタイプについて説明します。
- ICMP サービス - ICMP プロトコルに基づくサービス。これは、「3.3.3 ICMP サービス」で、より詳しく説明します。
- IP プロトコルサービス - ユーザ定義プロトコルに基づくサービス。これは、「3.3.4 カスタム IP プロトコルサービス」で、より詳しく説明します。
- サービスグループ - 多くのサービスから構成されるサービスグループ。これは、「3.3.5 サービスグループ」で、より詳しく説明します。

TCP と UDP ベースサービス

多くのアプリケーションが IP ネットワーク経由でアプリケーションデータを転送するために転送プロトコルとして TCP/UDP を使用しています。

TCP（Transmission Control Protocol）は、信頼性のある PtoP 転送のためのメカニズムを含むコネクション型プロトコルです。TCP は、HTTP、FTP および SMTP などのエラーフリー転送が必須である多くの一般的なアプリケーションに使用されています。

UDP プロトコルのアプリケーション

UDP（User Datagram Protocol）は、ストリーミングオーディオやビデオサービスなどのデータの転送速度が非常に重要であるアプリケーションタイプによく使用されるプロトコルです。UDP は、コネクションレス型プロトコルで、わずかなエラーリカバリサービスしか提供しないため、TCP を使用するよりも非常に小さいオーバヘッドでトラフィックを転送します。このため、UDP はストリーミングでないサービスにも使用され、一般的にアプリケーション自身がエラーリカバリメカニズムを提供する場合に使用されます。

TCP と UDP サービスの定義

NetDefendOS ファイアウォールで TCP または UDP サービスを定義するためには、TCP/UDP サービスオブジェクトを使用します。このオブジェクトのタイプは、サービスを記述する固有名の一部、プロトコルの種類（TCP、UDP または両方）、サービスに適用する送信元と送信先ポートなどの情報を含んでいます。

ポート番号の指定

ポート番号はすべてのサービスタイプで指定されるため、ユーザインタフェースにこれらを入力する方法を理解することが有効です。以下の方法でサービスの送信元ポートおよび（または）送信先ポートの両方に指定されます。

項目	説明
シングルポート	多くのサービスについては、一つの送信先ポートで十分です。HTTP サービスでは、例えば TCP 送信先ポート 80 を使用し、SMTP は TCP 25 を使用します。これらのサービスタイプのためには、1 つのポート番号を 1 つの番号として単純にサービス定義に指定します。
ポート範囲	いくつかのサービスは送信先ポートの範囲を使用します。例えば、Microsoft Windows™ で使用される NetBIOS プロトコルは送信先ポートに 137 から 139 を使用します。TCP/UDP サービスオブジェクトでポート範囲を定義するために、フォーマット mmm-nnn が使用されます。ポート範囲は範囲内のすべてのポートを含み、例えば「137-139」は、ポート 137、138、139 を表します。
マルチポートとポート範囲	複数ポート範囲または個別のポートは、「,」で区切られて入力されます。これにより単一の TCP/UDP サービスオブジェクトだけを使用してポートが広い範囲をカバーできるようになります。 例えば、すべての Microsoft Windows™ ネットワーキングは、「135-139,445」のように指定されたポート定義を使用してカバーされます。HTTP とセキュアな HTTP（HTTPS）は、送信先ポート 80,443 を記述することによってカバーされます。

参照 送信元ポートの指定

多くのサービスでは、送信元ポートとしてデフォルト値 0-65535（利用可能な全ての送信元ポートに対応）が用意されています。

特定のアプリケーションを使用する場合、送信元ポートが限定的な範囲に定められていると、指定する際に役に立ちます。サービス定義をできるだけ狭くすることが、お勧めの手法であると言えます。

他のサービスプロパティ

基本プロトコルとポート情報の他に、TCP/UDP サービスオブジェクトには、いくつかの別のプロパティもあります。

- Forward ICMP Errors
  TCP 接続のオープンがファイアウォール背後のユーザアプリケーションによって行われ、リモートサーバが動作中でない場合、ICMP エラーメッセージがレスポンスとして戻ります。そのような ICMP メッセージは、新しい接続として NetDefendOS によって解釈されて、IP ルールが明示的にそれらを許可しない場合に破棄されます。

  「Forward ICMP Errors」によって、ICMP メッセージが要求アプリへ自動的に返されるようになります。ICMP メッセージが破棄されないようにした方が良いケースもあります。例えば、トラフィックフローのレートを低下させるために ICMP 抑制メッセージが送信される場合があります。これに対して、ICMP メッセージを破棄することは、攻撃手段としての使用を防止し、セキュリティを向上させます。

- Enable IPv4 Path MTU Discovery
  Allow ICMP Errors プロパティが有効であり、Path MTU Discovery ICMP メッセージのリレーを許可する場合にだけ、これは有効とすることができます。詳しくは「3.3.7 Path MTU Discovery」を参照してください。

- SYN flood protection（SYN Relay）（SUN フラッド防御 : SYN リレー）
  TCP ベースのサービスが SYN フラッド攻撃に対する防御を有効にするために設定します。本オプションは TCP/IP サービスタイプのためだけに存在します。詳しくは、「7.4.3.6 TCP SYN Flood 攻撃」を参照してください。

- ALG
  TCP/UDP サービスは、Application Layer Gateway（ALG）にリンクし、特定のプロトコルによるさらに詳しい検閲を有効にします。これは ALG を IP ルールのオブジェクトに関連付ける方法です。最初に、サービスに ALG を関連付け、次に、サービスに IP ルールを関連付けます。

  詳しくは、「6.1 アプリケーションレイヤゲートウェイ」を参照してください。

- Max Sessions（最大セッション数）
  サービスに関連する重要なパラメータは最大セッション数です。サービスが ALG に関連付いている場合は、このパラメータには初期値が割り当てられます。初期値は関連している ALG により異なります。例えば初期値が 100 の場合、これは、合計 100 個の接続だけがすべてのインタフェース上で許可されていることを表しています。

  例えば HTTP ALG に関わるようなサービスの場合、ファイアウォールを経由して接続しているクライアントが多数だとデフォルト値では低過ぎることがよくあります。従って、より高い値が必要になる場合の特別なシナリオを想定しておくことをお勧めします。

すべてのサービスの利用

サービスごとにフィルタするルールを設定する場合、すべてのプロトコルを参照するために「all_services」と呼ばれるサービスプロジェクトを利用することができます。しかし、これの使用をお勧めしません。より狭いサービスの指定がより良いセキュリティを提供するからです。

例えば、TCP、UDP、および ICMP という主なプロトコルだけをフィルタしたい時は、サービスグループの「all_tcpudpicmp」を代わりに利用することができます。

参照 「http-all」サービスには DNS は含まれません。

一般的な誤りは、定義済みサービスの「http-all」が DNS プロトコルを含んでいると見なすことです。このサービスには DNS プロトコルは含まれないため、定義済みサービス「dns-all」が、通常、多くの Web サーフィンに必要とされます。これを http-all が設定されたグループに含めて、Web サーフィンを許可する IP ルールセットのエントリに関連付けることができます。

必要最小限にサービスを制限する

IP ルールなどのポリシーの構成のためにサービスオブジェクトを選択する場合、トラフィックフィルタリングオブジェクトを実行するためにそのオブジェクトに含めるプロトコルは必要最小限とします。「all_services」オブジェクトの使用は便利ですが、より特定したサービスオブジェクトがもたらすセキュリティの利点を排除してしまいます。

最もよい方法は、セキュリティポリシーにおけるサービスのフィルタの幅を絶対に必要なプロトコルだけを許可するように狭めることです。「all_tcpudpicmp」サービスオブジェクトは、たびたび通常のトラフィック用として最初に選択しますが、これでさえ通常必要とするよりもずっと多くのプロトコルを許可している可能性があり、管理者はさらに許可するプロトコルの範囲を狭めることができます。

例題 3.18

TCP/UDP サービスを追加する

ここでは、MySQL によって使用される宛先ポート 3306 を使用している TCP/UDP サービスを追加する方法を説明します。

CLI

```
DFL-xxxx:/> add Service ServiceTCPUDP MySQL DestinationPorts=3306 Type=TCP
```

Web Interface

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。
   - Name : MySQL
   - Type : TCP
   - Source : 0-65535
   - Destination : 3306

3.3.3 ICMP サービス

カスタムサービスとして作成可能なもう 1 つのタイプのサービスは、ICMP サービスです。ICMP（Internet Control Message Protocol）は、エラーレポートや転送コントロール情報のために IP と統合されたプロトコルです。例えば PING サービスはインターネット接続性をテストするために ICMP を使用します。

ICMP タイプと Code

ICMP メッセージは IP パケット内に送信され、ICMP のフォーマットを特定する Message Type と、メッセージの詳細を記述する Code を含んでいます。例えば、メッセージタイプ「Destination Unreachable」は、エラーの正確な原因を指定するために Code パラメータを使用します。

サービスがすべての ICMP メッセージのタイプ（256 個の可能なタイプがあります。）を受け付けるか、またはフィルタすることが可能です。

Code の指定

タイプを選択すると、ポート番号の指定方法と同じように、タイプへのコードを指定できます。例えば、「Destination Unreachable」タイプがカンマで区切ったコードリスト 0,1,2,3 で選択されると、これは「Network unreachable」（ネットワーク未到達）、「Host unreachable」（ホスト未到達）、「Protocol unreachable」（プロトコル未到達）、および「Port unreachable」（ポート未到達）をフィルタします。

メッセージタイプを選択し、コード値を指定しない場合には、そのタイプのすべてのコードとみなされます。

ICMP メッセージのタイプ

NetDefendOS で設定可能な ICMP メッセージのタイプは以下の通りです。

パラメータ	説明
Echo Request	接続性を確認するために PING によって宛先に送信されます。
Destination Unreachable	送信元はパケットの送信時に問題が発生したことを通知されます。0 から 5 までのコードのタイプがあります。 • コード 0：ネットワークに到達不能 • コード 1：ホストに到達不能 • コード 2：プロトコルに到達不能 • コード 3：ポートに到達不能 • コード 4：フラグメント不能 • コード 5：送信元ルートの失敗
Redirect	送信元は特定のパケットにより適切な経路があることを通知されます。以下のコードがあります。 • コード 0：ネットワークに対するデータグラムの経路変更 • コード 1：ホストに対するデータグラムの経路変更 • コード 2：ToS（Type of Service）とネットワークに対するデータグラムの経路変更 • コード 3：ToS（Type of Service）とホストに対するデータグラムの経路変更
Parameter Problem	データグラムの不正なパラメータを識別します。
Echo Reply	Echo Request の結果として送信される到達先からのリプライ。
Source Quenching	送信元が受信先に非常に速くデータを送信しているため、バッファはフル状態になっています。
Time Exceeded	パケットは送信するために非常に時間がかかったため廃棄されました。

3.3.4 カスタム IP プロトコルサービス

IP 上で動作し、アプリケーション / トランスポート層の機能を実行するサービスは IP プロトコル番号によって定義されます。IP は異なるプロトコル番号にデータを送信することができます。これらのプロトコルは、IP ヘッダフィールドで指定されている固有の IP プロトコル番号でそれぞれ識別されます。例えば ICMP、IGMP および EGP は、それぞれプロトコル番号 1、2 および 8 を所有しています。

前述の TCP/UDP ポート範囲と似ていますが、IP プロトコル番号を範囲として指定することで、1 つのサービスに複数のアプリケーションを設定することも可能です。例えば、範囲 1-4,7 を指定すると、プロトコルの ICMP、IGMP、GGP、IP-in-IP、および CBT に一致します。

IP プロトコル番号

一般的に割り当てられている IP プロトコル番号とその説明については、IANA（Internet Assigned Numbers Authority）のホームページで公表されています。

http://www.iana.org/assignments/protocol-numbers

例題 3.19

IP プロトコルサービスを追加する

VRRP（Virtual Router Redundancy Protocol）の IP プロトコルサービスを作成する方法を説明します。

CLI

```
DFL-xxxx:/> add Service ServiceIPProto VRRP IPProto=112
```

Web Interface

1. **Objects > Services > Add > IP Protocol Service** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : VRRP
- IP Protocol : 112

Comments

Virtual Router Redundancy Protocol と入力します。

3.3.5 サービスグループ

「Service Group」は、名前が示すようにサービスの集合を構成する NetDefendOS のオブジェクトです。グループの概念はシンプルですが、グループを個々のサービスの代わりに使用できるため、セキュリティポリシーを構成する場合に非常に便利です。

グループの長所

例えば、サービスパラメータを除いて互いに同じである IP ルールセットが必要であるかもしれません。各ルールで使用する全てのサービスオブジェクトを含むサービスグループを定義し利用することで、それらルールを 1 つの IP ルールセットとして置き換えることができます。

SMTP、POP3、および IMAP 用に 3 つのサービスオブジェクトを組み合わせた「email-services」サービスと呼ばれるサービスグループを作成すると仮定します。その場合、全てのメールに関連したトラフィックフローを許可するためには、このグループを使用する 1 つの IP ルールセットのエントリのみを定義すれば良いことになります。

グループに他のグループを含める

グループを定義する際、そのグループには個々のサービスおよび（または）サービスグループを含めることもできます。グループ内にグループを持つという機能は、構成の複雑性を増し、問題のトラブルシューティングを行うことが難しくなってしまうため、慎重に使用する必要があります。

例題 3.20

Service を作成する

この例題では、2 つの定義済みサービス my_first_service および my_second_service から構成される Service Group オブジェクト「my_service_group」を作成する方法を示しています。

CLI

```
gw-world:/> add Service ServiceGroup my_service_group Members=my_first_service,my_second_service
```

Web Interface

1. **Objects > Services > Add > Service Group** の順にメニューをクリックします。
2. Name に my_service_group を入力します。
3. Available から my_first_service を選択し、Include を押します。
4. Available から my_second_service を選択し、Include を押します。
5. 「OK」ボタンをクリックします。

3.3.6 カスタムサービスのタイムアウト

どんなサービスも、カスタムタイムアウトの設定を持つことができます。また、これらを NetDefendOS にグローバルに設定することもできますが、通常、カスタムサービス毎に個別に値を変更します。

カスタマイズ可能なタイムアウト設定は以下の通りです。

項目	説明
Initial Timeout	これは、新しい接続のオープンが許可される時間です。
Establish (Idle) Timeout	指定時間にアクティビティが全くないと、クローズされたものと見なされ、NetDefendOS State テーブルから削除されます。TCP/UDP 接続の場合、初期値は 3 日です。
Closing Timeout	接続のクローズを許可される時間です。

管理者は特定のプロトコルに対し、許可する値を決定する必要があります。例えば、クライアントが接続するサーバの予想される応答に依存するかもしれません。

3.3.7 Path MTU Discovery

概要

Path MTU Discovery（本セクションでは省略して MTU Discovery とも言う）は、インターネットを経由して送信される IPv4 または IPv6 パケットの MTU サイズを、自身が通過するネットワーク装置の MTU 制限に合うように調整する方式で、フラグメント化の必要性を回避します。パケットが 1 台のネットワーク装置の next-hop MTU limit を超過し、パケットの DF（Don't Fragment）フラグが設定されると、ICMP メッセージは調整された MTU サイズを使用して再送信するように、パケットの送信側に送り返されます。これは、RFC 1191（IPv4 用）と RFC 1981（IPv6 用）によって定義されます。

NetDefendOS における実行

NetDefendOS の Path MTU Discovery 実行により以下の 2 つの機能の両方を許可します。

- 2 台の外部ネットワーク装置間の MTU Discovery に関係する ICMP メッセージを転送できます。
- DF（Don't Fragment）がセットされ、パケットサイズが NetDefendOS の外向きインタフェース（next-hop MTU）の MTU サイズよりも大きい場合、NetDefendOS は送信者に MTU Discovery ICMP メッセージを送り返します。

D-Link ファイアウォールは、MTU Discovery メッセージの交換においてはエンドポイントとして機能できません。NetDefendOS は ICMP メッセージを転送するか、またはそれ自身の外向きインタフェースで受け付けられる MTU を示すメッセージを生成するだけです。

Path MTU Discovery は、すべての NetDefendOS インタフェースの IPv6 の初期値として常に有効であり、本セクションでは詳しく説明しません。IPv4 に関しては、次にも説明する通り、有効でなければなりません。

Service オブジェクトで IPv4 MTU Discovery を有効にする

MTU Discovery は、IPv4 では初期値で有効ではありません。代わりに、接続を許可する IP ルールセットのエントリに関連している Service オブジェクトで明示的に有効にする必要があります。Service オブジェクトの以下の 2 つのプロパティを有効にすることで、本設定を行います。

- Forward ICMP Errors
- Enable IPv4 Path MTU Discovery

最初のプロパティを有効にした後にだけ、2 番目のプロパティは有効にできます。サービスが使用されている IP ルールセットのエントリは、ステートレスポリシー（FwdFast IP ルール）以外のすべてのタイプとすることができます。

MTU Discovery プロセス

代表的な Path MTU discovery メッセージ交換を図で説明するために、ルータと同様に D-Link ファイアウォールとパブリックインターネットを経由したサーバに接続しようとするクライアントコンピュータを考えてみます。以下の図はこれについて説明しています。

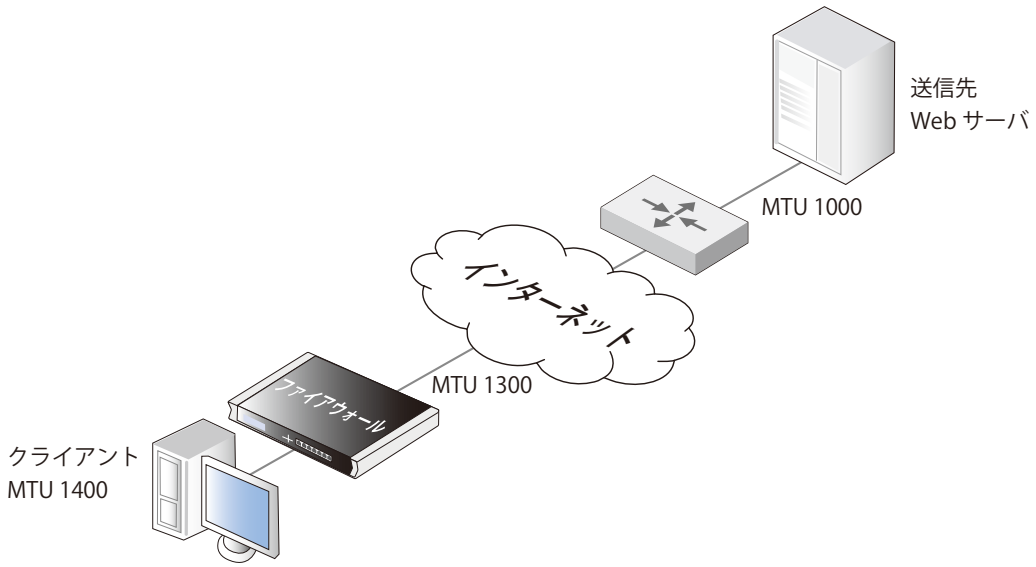


図 3-1　Path MTU Discovery 処理

関連する NetDefendOS IP ルールまたは IP ポリシーの上で MTU Discovery が有効であったと仮定して、以下の連続したイベントは MTU discovery がどう機能するかを示しています。

1. クライアントは、1400 バイトのパケットサイズを使用し、ファイアウォールを経由してサーバに接続しようとします。送信されたパケットが、DF（Don't Fragment）フラグを持っています。
2. NetDefendOS はネクストホップに使用されるインタフェースオブジェクトの MTU プロパティ値を見ます。これが 1300 であると、クライアントのパケット MTU が高過ぎるため、フラグメント化は実行できません。
3. NetDefendOS は、ICMP メッセージをクライアントに送ることにより、フラグメント化が必要であり、ネクストホップのための許容できる MTU が 1300 以下であることを示します。
4. クライアントは、要求された 1300 のサイズと共にパケットを再送し、これを NetDefendOS がサーバに送ります。
5. サーバのルータは NetDefendOS に対し、パケットサイズが大きすぎること、MTU サイズの許容が 1000 以下であることを示すために ICMP メッセージを送り返します。
6. NetDefendOS はこの ICMP メッセージをクライアントに転送します。
7. クライアントが再びファイアウォールとルータの両方に許容できるパケットサイズ 1000 を再送すると、サーバはアクセス可能になります。

DF フラグをオフする

NetDefendOS には Strip Don't Fragment と呼ばれるグローバルな IP 設定があり、パケットの DF（Don't Fragment）フラグを無効にするために使用されます。Strip Don't Fragment 設定は、DF フラグが常に無効となる、MTU サイズを下回る整数値を設定します。初期値では、このプロパティには 65535 の値があるので、DF フラグは常に無効とされます。

DF フラグを無効にすることは、Path MTU discovery がそのパケットに使用されないため、ネットワーク装置の許容できる MTU サイズより上のパケットの断片化が可能になることを意味します。多くの場合、これはパフォーマンスの低下のみ引き起こします。

しかし、Service オブジェクトで明示的に Path MTU discovery を有効にすると、Strip Don't Fragment 設定を書き換えるため、MTU discovery のためにこれを変更する必要はありません。

注意 MTU discovery を有効にしないと問題が起こる可能性があります

Path MTU discovery を無効にすると、意図しない副作用が起きるかもしれません。ICMP エラーの転送を無効にした場合、上流のデバイスが MTU 値を下げるために ICMP エラーを送信した際にパケットフローは停止するため、トラフィックの送信元に送信されません。

この潜在的な問題に対処する 1 つの方法は、必要に応じて、長過ぎるパケットを断片化できるように DF フラグを無効にするようにグローバルな Strip Don't Fragment 設定を使用することです。

例題 3.21

Path MTU Discovery を有効にする

この例題では、定義済みの IP ルール「int_to_ext_http」に path MTU discovery を設定する方法を示しています。このルールは、内部のクライアントをパブリックインターネットに NAT 変換します。クライアントがインターネット検索を行うため、path MTU discovery を有効にした Service オブジェクト「my_http_pmd_service」を作成し、IP ルールに関連付けます。

CLI

まず、Service オブジェクトを作成します。

```
DFL-xxxx:/> add Service ServiceTCPUDP my_http_pmd_service Type=TCP DestinationPorts=80,443 ForwardICMPErrors=Yes
            EnableIPv4PathMTUDiscovery=Yes
```

次に、新しいサービスを使用するために NAT IP ルールを編集します。

```
DFL-xxxx:/> set IPRule int_to_ext_http Service=my_http_pmd_service
```

Web Interface

まず、Service オブジェクトを作成します。

1. **Objects > Services > Add > TCP/UDP service** の順にメニューをクリックします。
2. 以下を入力します。
   - Name : my_http_pmd_service
   - Type : TCP
   - Destination : 80,443
   - Forward ICMP Errors を有効にします。
   - Enable IPv4 PathMTU Discovery を有効にします。

次に、新しいサービスを使用するために NAT IP ルールを編集します。

1. **Policies > Firewalling > Main IP Rules** の順にメニューをクリックします。
2. IP ルール int_to_ext_http を選択します。
3. Service セクションに移動します。
4. Service リストから my_http_pmd_service を選択します。
5. 「OK」ボタンをクリックします。

3.4 インタフェース

3.4.1 概要

インタフェースは、NetDefendOS において重要な論理的構成要素です。D-Link ファイアウォールを通過する、出発する、またはシステムに到達するすべてのネットワークトラフィックは、1 個以上のインタフェースを通過します。

送信元と送信先インタフェース

インタフェースは、NetDefendOS から、または NetDefendOS へのネットワークトラフィックの出入り口のようなものです。

NetDefendOS インタフェースでは、以下の 2 つの機能のうちいずれかの役割を持つことができます。

- 送信元インタフェース
  トラフィックがインタフェース経由でシステムに到着する場合、そのインタフェースは、（receiving または incoming インタフェースとしても知られる）送信元インタフェースとして NetDefendOS 内で参照されます。

- 宛先インタフェース
  トラフィックが NetDefendOS のセキュリティポリシーに対するチェックの後に送信される場合、トラフィックの送信に使用されるインタフェースは、NetDefendOS 内で（sending インタフェースとしても知られる）宛先インタフェースとして参照されます。

NetDefendOS を通過するすべてのトラフィックが、送信元と宛先インタフェースの両方を持っています。NetDefendOS 自身がトラフィックの送信元または宛先である場合に、後で詳しく説明されるように、特別な論理インタフェース「core」が使用されます。

インタフェースタイプ

NetDefendOS は多くのインタフェースタイプをサポートしており、以下の 4 つの主なグループに分類することができます。

- イーサネットインタフェース
  各イーサネットインタフェースは、NetDefendOS ベースの製品内の物理ポートを表しています。そのため、D-Link ファイアウォールから生成される、または到達するすべてのネットワークトラフィックは、物理インタフェースのいずれかを通過します。

  NetDefendOS は通常物理インタフェースタイプとしてイーサネットをサポートしています。イーサネットに関する詳しい情報は、「3.4.2 イーサネットインタフェース」を参照してください。

- サブインタフェース
  いくつかのインタフェースは、データの転送のために物理的なインタフェースへの接続が必要です。このインタフェースグループは物理サブインタフェースと呼ばれます。

  NetDefendOS は 2 つのタイプの物理サブインタフェースをサポートしています。

  - IEEE 802.1Q によって規定されている Virtual LAN（VLAN）インタフェース。VLAN インタフェース上の IP パケットをルーティングする場合、タグ付きの VLAN イーサネットフレーム内にカプセル化されます。VLAN インタフェースに関する詳しい情報は、「3.4.4 VLAN」を参照してください。
  - PPPoE サーバに接続するための PPPoE（PPP-over-Ethernet）インタフェース。PPPoE に関する詳しい情報は、「3.4.6 PPPoE」を参照してください。

- トンネルインタフェース
  トンネルインタフェースは、ネットワークトラフィックが最終到達先への決まった経路に送信される前に、システムとネットワーク内の別のエンドポイント間でトンネルする場合に使用されます。VPN トンネルは、2 つのファイアウォール間の通信を保証できる VPN（virtual private network）を実行するためにしばしば使用されます。

  トンネリングを実行するために、追加のヘッダがトンネルされるトラフィックに付加されます。さらに、各種変換がトンネルインタフェースのタイプに従って、ネットワークトラフィックに適用されます。例えば IPsec インタフェース上のトラフィックがルーティングされる時、ペイロードは通常安全性のために暗号化されます。

  NetDefendOS は以下のトンネルインタフェースタイプをサポートしています。

  - IPsec インタフェースは、IPsec VPN トンネルに対するエンドポイントとして使用されます。IPsec VPN に関する詳しい情報は、「10.3 IPsec」を参照してください。
  - PPTP/L2TP インタフェースは、PPTP または L2TP トンネルに対するエンドポイントとして使用されます。PPTP/L2TP に関する詳しい情報は、「10.4 PPTP/L2TP」を参照してください。
  - GRE インタフェースは、GRE トンネルを確立するために使用されます。GRE に関する詳しい情報は、「3.4.7 GRE トンネル」を参照してください。

- ループバックインタフェース
  ループバックインタフェースは特別なインタフェースのタイプで、パケットを通過させ、ループ先として設定されたループバックインタフェースを経由して送信します。これらは仮想ルーティングのシナリオでほとんど排他的に使用されます。

  詳しくは、「3.4.9 ループバックインタフェース」を参照してください。

すべてのインタフェースが論理的に等価である

たとえインタフェースの各タイプが実行される方法に大きな違いがあっても、NetDefendOS は論理的に等価であるとしてすべてのインタフェースを処理します。これは、重要で強力な概念で、すべてのインタフェースタイプが様々な NetDefendOS ルールセットやコンフィグレーションオブジェクト内で互換性を持って使用可能であるということを意味します。この結果、トラフィックが検証、制御、および経路制御される方法に非常に高い柔軟性を持つことができます。

インタフェースには固有な名称がある

NetDefendOS 内の各インタフェースは固有の名前を付与され、コンフィグレーション内の他の NetDefendOS オブジェクトで使用するために識別され、選択されることが可能です。NetDefendOS では、物理的なイーサネットインタフェースなどのいくつかのインタフェースタイプについて、必要に応じて変更可能な意味のあるデフォルト名が提供されています。管理者が定義する新しいインタフェースには、通常ユーザが提供する名称を指定します。

重要 インタフェースの削除前に参照先を削除する

NetDefendOS 構成から論理インタフェースを削除する場合、そのインタフェースの参照は最初に削除するか、変更しておくことが重要です。例えば、そのインタフェースを参照する IP ルールセット内のルールは、削除、または変更してください。

any インタフェース

IP Policy オブジェクトなどのルールに対してフィルタ条件を指定する際に、Interface プロパティに any を指定することができます。これは、（物理インタフェースだけではなく）すべての論理インタフェースがフィルタ条件に一致することを意味します。

core インタフェース

IP Policy オブジェクトなどのルールに対してフィルタ条件を指定する際に、Interface プロパティに core を指定することもできます。これは、そのインタフェースで送受信するトラフィックを処理するのが NetDefendOS 自身であることを意味します。

core インタフェースを指定する必要があるケースの一例としては、D-Link ファイアウォールが PPTP または L2TP サーバとして動作する場合か、ICMP "Ping" テストに応答する場合が考えられます。ルートの Destination Interface に core を指定することで、NetDefendOS は自身がトラフィックの宛先であり、何らかの処理（ICMP Ping テストへの応答など）を行わなければならないことを認識します。
物理インタフェースの IP アドレスがトラフィックの Destination Network である場合、通常、対応する Destination Interface は core となります。初期値ではすべての物理インタフェースの IP アドレスが core routed であるためです。「core routed」という用語は、イーサネットインタフェースで自動的に作成されたネットワークアドレス帳オブジェクトが既にそのインタフェースにルーティングされていることを、ルーティングテーブルで示すことを意味しています。

core インタフェースが指定されるケースとしてよくあるのは、コンフィグレーションルールにおいて、物理インタフェースに割り当てられたパブリック IP アドレスのインターネットから送信されたトラフィックを対象にしている場合です。インターネットに接続されたインタフェースが wan であり、そのインタフェースに割り当てられたパブリック IPv4 アドレスが wan_ip であると仮定します。この場合、このトラフィックをターゲットにしたルールは以下のようになります。

送信元インタフェース	送信元ネットワーク	宛先インタフェース	宛先ネットワーク
wan	all-nets	core	wan-ip

NetDefendOS によってアドレス wan_ip は自動的に core インタフェースでルーティングされるため、core インタフェースが指定されています。上記の例では Service プロパティを設定していませんが、実際には特定のプロトコルやすべてのプロトコルを許可するように設定します。

インターネットからの ICMP Ping リクエストを許可したり、プライベート IP アドレスを持つ保護されたサーバに到達しようとするインターネットトラフィックに対して SAT 変換が適用されていた場合、通常、上記のようなフィルタリングプロパティが IP ルールセットのエントリと一緒に使用されます。

インタフェースの無効化

インタフェースを無効化してトラフィックが送信されるないように設定することができます。

```
DFL-xxxx:/> set Interface Ethernet <interface-name> -disable
```

<interface-name> には無効化するインタフェースを指定します。

インタフェースを有効化するには、以下のコマンドを実行します。

```
DFL-xxxx:/> set Interface Ethernet <interface-name> -enable
```

インタフェースの無効化は Web インタフェースからも設定することができます。

3.4.2 イーサネットインタフェース

IEEE 802.3 イーサネット規格は、各種デバイスを同軸ケーブルなどの物理的転送メカニズムに任意の接点またはポートを割り当てることができます。デバイスが接続された各イーサネットは、CSMA/CD プロトコルを使用してネットワークを「listen」し、他に送信しているデバイスが存在しない場合、データを送信します。同時に 2 つのデバイスがブロードキャストすると、アルゴリズムにより時間をずらして再送が行われます。

注意 「インタフェース」と「ポート」用語の使用

「イーサネットインタフェース」と「イーサネットポート」の用語は互換性があります。本マニュアルでは、IP 通信に関連するポートと混同しないように「イーサネットインタフェース」を全体にわたって使用します。

イーサネットフレーム

デバイスはイーサネットフレームとしてデータをブロードキャストし、他のデバイスは、これらのフレームの予定された送信先であるかどうかを判定するために、「listen」（確認）します。フレームは、データの送信元デバイス、送信先デバイス、データペイロード及びエラーをチェックするビットを指定するビットシーケンスです。各フレームのブロードキャスティングの間の休止時間により、各フレームは次のフレーム到達の前に処理されます。また、通常のイーサネット、ファストイーサネット、ギガイーサネットの順で、より早いデータ転送速度となるほど、この休止時間は小さい値となります。

物理イーサネットインタフェース

各 NetDefendOS イーサネットインタフェースは、システム内の物理イーサネットポートと通信します。ポート数、リンク速度などは、D-Link のハードウェアタイプによって異なります。

注意 スイッチのファブリックを経由して接続するインタフェースソケット

NetDefendOS のいくつかのハードウェアプラットフォームは、物理イーサネットソケットを追加できる統合型のレイヤ 2 スイッチを使用しています。 外部的に、数個の独立したソケットを持ち得ますが、これらは内部のスイッチファブリック経由で結合されます。

そのような結合したインタフェースは、NetDefendOS によって 1 つのインタフェースとして認識され、NetDefendOS コンフィグレーションはそれらのすべてを参照するために 1 つの論理インタフェース名を使用します。各ハードウェアモデルの仕様にこれを示しています。

イーサネットプロパティ

NetDefendOS 構成の Ethernet オブジェクトは物理的なイーサネットインタフェースに対応しています。以下は、このオブジェクトタイプに設定できるプロパティです。

- **Name（インタフェース名）**

  イーサネットインタフェースの名前は、システムによって事前に定義されており、物理ポートの名前にマップされています。wan ポートを持つシステムは「wan」という名前のイーサネットインタフェースを持っています。

  イーサネットインタフェースの名前は、それらの使用用途を反映するように変更されることがよいと言えます。例えば、「dmz」という名前のインタフェースが無線 LAN に接続している場合は、インタフェース名を「radio」に変更する方が便利かもしれません。メンテナンスやトラブルシューティングのためには、対応する物理ポートに新しい名前を付けることをお勧めします。

参照 インタフェース一覧

システムの開始処理時、すべての有効なイーサネットインタフェース一覧を生成します。ご使用のファイアウォールが 1 つ以上のインタフェースを持つ場合、各インタフェースは、lanN、wanN および dmz の形式（N はインタフェース番号を示します。）で名前を付与されます。このマニュアル内の多くの例題で、lan が LAN トラフィック用、wan が WAN トラフィック用に使用されています。ご使用のファイアウォールがこれらのインタフェース名を持っていない場合、実際のインタフェースの名前に読み替えて参照してください。

- **IP address（IP アドレス）**

  各イーサネットインタフェースは、固定のアドレスまたは DHCP によって供給されるアドレスのインタフェース IP アドレスを持つことが必要です。インタフェース IP アドレスは、特定のイーサネットインタフェースを経由するシステムと通信するためのプライマリアドレスとして使用されます。

  標準ではイーサネットインタフェースの IPv4 アドレスを定義するために、NetDefendOS IPv4 アドレスオブジェクトを使用します。これらのオブジェクトは、通常システムに自動的に生成されます。詳しくは「3.1.5 自動生成されるアドレスオブジェクト」を参照してください。

参照 インタフェースにおける複数 IP アドレスの指定

ARP パブリッシュ機能を使用することで、複数の IP アドレスをイーサネットインタフェースに指定できます。詳細は「3.5 ARP」を参照してください。

- **Network（ネットワークアドレス）**
  インタフェース IP アドレスに加え、ネットワークアドレスがイーサネットインタフェースに指定されます。ネットワークアドレスは、インタフェース経由で直接到着する IP アドレスの情報、つまり、インタフェースと同じ LAN セグメントに存在する IP アドレスの情報を NetDefendOS に供給します。NetDefendOS は、インタフェースに関連するルーティングテーブルに実際のインタフェースの指定ネットワークへの直接経路を自動的に作成します。

- **Default Gateway（デフォルトゲートウェイ）**
  デフォルトゲートウェイアドレスをイーサネットインタフェースに指定できます。通常は、インターネットへのゲートウェイとして機能するルータのアドレスです。

  デフォルトゲートウェイを指定すると、初期値では、ネットワーク all-nets へのルートがそのインタフェースの NetDefendOS ルーティングテーブルに自動的に作成されます。これは、明確にマッチするルートを持たないどんなトラフィックも、そのインタフェースを経由してデフォルトインタフェースに送信されることを意味します。自動的にデフォルトルート作成用のインタフェースにおける高度なオプションを無効にすることで、この動作を変更することができます。

  通常、デフォルトゲートウェイへの 1 つのデフォルトルート「all-nets」だけが、ルーティングテーブルに存在する必要があります。

注意 all-nets IP アドレスオブジェクト

all-nets IP オブジェクト (IP アドレス : 0.0.0.0/0) はマルチキャスト IP アドレス範囲（224.0.0.0 => 239.255.255.255）を含みます。このトピックに関する詳しい情報については、「4.8 マルチキャストルーティング」を参照してください。

- **マルチキャストトラフィックの受信**
  本オプションはインタフェースにおけるマルチキャスト IP パケットの受信を制御します。3 つのオプションがあります。

オプション	説明
Off	プロミスキャスモードをオフに変更すると、マルチキャストパケットは警告なしで破棄されます。プロミスキャスモードは、OSPF または HA を使用すると自動的にオンに変更されます。
On	インタフェースは常にマルチキャストトラフィックを受信することができます。プロミスキャスモードは常にインタフェースの受信モードです。
Auto	マルチキャストパケットの宛先 IP アドレスに適用される IP ルールセットのエントリが存在する場合、イーサネットインタフェースは、マルチキャストパケットを受信するために自動的にプロミスキャスに設定された受信モードを取得します。（初期値）

本設定は OSPF または HA を使用したプロミスキャスモードの自動的な使用には影響しません。プロミスキャスモードの詳細については、以下に説明します。

- **Enable DHCP Client（DHCP クライアントを有効にする）**
  NetDefendOS には、接続する DHCP サーバによってアドレス情報をダイナミックに割り当てられる DHCP クライアント機能があります。この機能は、パブリックインターネット接続で ISP の DHCP サーバから外部の IP アドレス情報を受信するためにたびたび使用されます。

  DHCP を使用して設定される情報には、IPv4 アドレスだけでなくインタフェースのブロードキャストアドレス、インタフェースに接続したローカルネットワーク、およびデフォルトゲートウェイがあります。

  DHCP サーバから受信したすべてのアドレスは、対応する IPv4 アドレスオブジェクトに割り当てられます。この方法でダイナミックに割り当てられたアドレスは、スタティックアドレスと同様にコンフィグレーションで使用することができます。初期値で使用できるオブジェクトは、「3.1.5 自動生成されるアドレスオブジェクト」内に定義されているものと同じです。

  初期値ではイーサネットインタフェースにおいて DHCP は無効です。インタフェースが、固定 IP アドレスを使用した ISP 経由のパブリックインターネットへの接続に使用されている場合、DHCP を使用するべきではありません。

  さらに、IPv6 アドレスの DHCPv6 は、インタフェースコンフィグレーションオブジェクトの別のプロパティとして利用できるもので、初期値では無効です。（「5.6.1 DHCPv6 クライアント」を参照）

重要 DHCP クライアントは HA クラスタではサポートされません。

IPv4 DHCP クライアントと DHCPv6 クライアントの両方が高可用性クラスタでサポートされません。いずれかのプロパティがインタフェースで有効であると、コンフィグレーションのコミットを行う時に Shared HA IP アドレスが設定されないというエラーが発生します。

<interface-name> という名前のインタフェースにおいて、DHCP を通じて受信された DNS サーバアドレスは、<interface-name>_dns1 と <interface-name>_dns2 という名前を持つ NetDefendOS アドレスオブジェクトに割り当てられます。

注意 DHCP が有効な場合、ゲートウェイ IP アドレスを削除することはできません。

指定したイーサネットインタフェースで DHCP を有効にすると、そのインタフェースに定義したどのゲートウェイ IP アドレス（例えば ISP のアドレス）も削除できなくなります。ゲートウェイアドレスを削除するためには、はじめに DHCP オプションを無効にする必要があります。

DHCP を有効にすると、以下のようなインタフェースの詳細設定が可能となります。
- 希望する IP アドレスの要求
- 希望するリースタイムの要求
- DHCP サーバからスタティックルートの送信
- スタティックルートを持つ IP アドレスのコリジョンの拒否
- スタティックルートを持つネットワークのコリジョンの拒否
- DHCP リースに対して許可された IP アドレスの指定
- リースが受け付けられる DHCP サーバのアドレス範囲の指定

- **DHCP Host Name（DHCP ホスト名）**
  まれに、DHCP サーバは、DHCP クライアントによるホスト名の送信が必要な場合があります。

- **Enable transparent mode（透過モードの有効化）**
  「4.9 透過モード」で説明する通り、透過モードを有効にするためには switch ルートを追加することを推奨します。

  別の方法は、このオプションを使用してインタフェースの透過モードを直接有効にすることです。有効にすると、デフォルトの switch ルートは、自動的にインタフェースのルーティングテーブルに追加され、すべての対応する non-switch ルートが自動的に削除されます。

- **Hardware Settings（ハードウェアの設定）**
  何らかの事情で、インタフェースのハードウェア設定を変更する必要があるかもしれません。この場合に、以下のオプションが利用できます。

  - リンクのスピードを設定できます。通常、Auto のままにするのが最適です。
  - MAC アドレスは、ハードウェアに実装された MAC アドレスと別にする必要がある場合に設定することができます。いくつかの ISP 接続でこれを必要とする可能性があります。

- **仮想ルーティング**
  異なるインタフェースに関連するルートが別々のルーティングテーブルに保持されている仮想ルーティングを実行するために、多くのオプションがあります。

  - インタフェースを「all」ルーティングテーブルのメンバにします。このオプションは、初期値で有効であり、インタフェースに到着するトラフィックは「main」ルーティングテーブルに従って送信されることを意味します。インタフェース IP のルートは「all」ルーティングテーブルに挿入されます。
  - 上記の代替手段は、特定のルーティングテーブルだけにこのインタフェースのルートを挿入することです。ルーティングルールによって上書きされない限り、指定されたルーティングテーブルはすべてのルート索引に使用されます。

- **Automatic Route Creation（自動ルートの作成）**
  インタフェースに自動的にルートを追加することができます。この追加には以下のタイプがあります。

  - 指定したネットワークの本インタフェースにルートを追加します。初期値は有効です。
  - 指定したデフォルトゲートウェイを使用することで本インタフェースにデフォルトルートを追加します。初期値は有効です。

- **MTU Settings（MTU 設定）**
  これはこのインタフェースに送信されるパケットの最大サイズ（バイト）を決定します。初期値では、インタフェースはサポートされる最大サイズを使用します。

- **High Availability（高可用性）**
  高可用性クラスタには特定の 2 つのオプションがあります。

  - このインタフェースにプライベート IPv4 アドレスを指定できます。
  - 追加オプションは、このインタフェースから HA クラスタハートビートの送信を無効にすることです。

- **Quality Of Service**
  オプションは、あらゆる VLAN パケットの VLAN 優先度フィールドに IP DSCP 優先度をコピーするために存在しています。初期値では無効になっています。

- **Promiscuous Mode**

  多くの状況で、インタフェースは non-promiscuous モードで普通に動作しています。これは、到着パケットが受信したインタフェースの MAC アドレスにマッチしない宛先 MAC アドレスを持っていると、パケットは処理用の NetDefendOS に渡されずにインタフェースによって破棄されることを意味します。しかし、この動作は以下の NetDefendOS 機能を使用した場合には間違いです。

  - Multicast
  - High Availability
  - OSPF

  これらの機能では、パケットは、MAC アドレスのミスマッチがあっても NetDefendOS に渡される必要があります。これを行うためには、プロミスキャスモードがインタフェースで有効でなければなりませんが、管理者は手動で有効にする必要はありません。必要に応じて、NetDefendOS は自動的にインタフェースをプロミスキャスモードに切り換えます。マルチキャストだけの場合、プロミスキャスモードの自動的な使用は Auto の初期値を持つ Ethernet オブジェクトのプロパティ Receive Multicast Traffic を使用することで制御できるので、正しいモードが NetDefendOS によって選択されます。

  「ifstat<ifname>」コマンドを使用して、Receive Mode の値を参照することによって、イーサネットインタフェースの現在のモードを参照できます。この値を non-promiscuous モードで「Normal」にするか、または以下の CLI の例題に示すように NetDefendOS によって自動的に「Promiscuous」に設定します。（下記の例では途中を省略しています。）

```
DFL-xxxx:/> ifstat If1
Iface If1
Builtin e1000 - Gigabit Ethernet Bus 0 Slot 4 Port 0 IRQ 0
Media        : “Autonegotiated”
Link Status  : 100 Mbps Full Duplex
Receive Mode : Promiscuous
```

イーサネットインタフェースの IPv4 アドレスの変更

インタフェースにおける IPv4 アドレスを変更するためには、以下の 2 つの方式のうち 1 つを使用できます。

1. インタフェースで直接 IPv4 アドレスを変更する

例えば、lan インタフェースの IPv4 アドレスを 10.1.1.2 に変更する場合、CLI コマンドを使用することができます。

```
DFL-xxxx:/> set Interface Ethernet lan IP=10.1.1.2
```

次に説明する通り、この IPv4 アドレスの変更方法は推奨されません。

2. 代わりに、IP ルールなど多くの他の NetDefendOS オブジェクトで使用される、NetDefendOS Address Book の lan_ip オブジェクトを新しいアドレスに対して割り当てるべきです。以下の CLI コマンドでこれを行います。

```
DFL-xxxx:/> set Address IP4Address lan_ip Address=10.1.1.2
```

また、Web マネージャ経由でも同じ操作を行うことができます。

イーサネットインタフェースに使用できる CLI コマンドの概要については、以下の「イーサネットインタフェースに便利な CLI コマンド」を参照してください。

論理イーサネットインタフェースと物理イーサネットインタフェースの違い

論理イーサネットインタフェースと物理イーサネットインタフェースの違いはわかりにくいかもしれませんが、論理イーサネットインタフェースは、NetDefendOS コンフィグレーションで参照されるインタフェースです。Web インタフェースを使用する場合には、論理インタフェースのみ表示され、管理が可能です。

CLI を使用する場合には、論理および物理的インタフェースの両方を管理することができます。例えば、論理インタフェース「If1」の名前を「lan」になるように変更する CLI コマンドは以下の通りです。

```
DFL-xxxx:/> set Interface Ethernet If1 Name=lan
```

これは、インタフェースの論理名（およびそれを参照するすべて）を変更しますが、基礎となる物理名は変更しません。例えば、CLI コマンド「ifstat」は物理インタフェースの名称だけを表示しますが、このリストは上記名称の変更による影響を受けません。

CLI では、物理インタフェースはオブジェクト「Interface Ethernet」によって表されます。例えば、インタフェース「If1」のすべての特性を表示するためには、CLI コマンドは以下の通りとなります。

```
DFL-xxxx:/> show Interface Ethernet If1
```

このコマンドからの出力は使用されているイーサネットドライバをはじめカードのバス、スロット、およびポート番号を含む物理イーサネットカードに関して詳細を表示します。これらの詳細は物理インタフェースに関連している論理インタフェースのオブジェクトには関連しません。

イーサネットインタフェースに便利な CLI コマンド

本セクションでは、NetDefendOS イーサネットインタフェースの検証や操作に最も一般的に使用される CLI コマンドをまとめています。
また、CLI を使用しなければならないいくつかの操作を除き、Web インタフェースを通じてイーサネットインタフェースを検証することもできます。

割り当てたインタフェースの参照

IP アドレス「wan_ip」に割り当てられている現在のインタフェースを参照します。

```
DFL-xxxx:/> show Address IP4Address InterfaceAddresses/wan_ip
              Property  Value
 --------------------  ----------------------------
                 Name:  wan_ip
              Address:  0.0.0.0/0
       UserAuthGroups:  <empty>
 NoDefinedCredentials:  No
             Comments:  IP address of interface wan
```

ネットワーク「wan_net」に割り当てられている現在のインタフェースを参照します。

```
DFL-xxxx:/> show Address IP4Address InterfaceAddresses/wan_net
              Property  Value
 --------------------  ----------------------------
                 Name:  wan_ip
              Address:  0.0.0.0/0
       UserAuthGroups:  <empty>
 NoDefinedCredentials:  No
             Comments:  The network on interface wan
```

ゲートウェイ「wan_gw」に割り当てられている現在のインタフェースを参照します。

```
DFL-xxxx:/> show Address IP4Address InterfaceAddresses/wan_gw
This object is updated from Ethernet "wan".
              Property  Value
 --------------------  --------------------------------
                 Name:  wan_gw
              Address:  0.0.0.0
       UserAuthGroups:  <empty>
 NoDefinedCredentials:  No
             Comments:  Default gateway for interface wan
```

行の終わりで「Tab」キーを使用する「Tab 補完」機能によりコマンドを完成させることができます。

```
DFL-xxxx:/> show Address IP4Address InterfaceAddresses/wan_<tab>
[<Category>] [<Type> [<Identifier>]]:

InterfaceAddresses/wan_br    InterfaceAddresses/wan_gw
InterfaceAddresses/wan_dns1  InterfaceAddresses/wan_ip
InterfaceAddresses/wan_dns2  InterfaceAddresses/wan_net
```

以下の例においても、コマンド行の最後で「Tab 補完」機能を使用しています。

```
DFL-xxxx:/> show Address IP4Address <tab>
[<Category>] [<Type> [<Identifier>]]:

dnsserver1_ip              InterfaceAddresses/wan_br timesyncsrv1_ip
InterfaceAddresses/aux_ip  InterfaceAddresses/wan_dns1
InterfaceAddresses/aux_net InterfaceAddresses/wan_dns2
InterfaceAddresses/dmz_ip  InterfaceAddresses/wan_gw
InterfaceAddresses/dmz_net InterfaceAddresses/wan_ip
InterfaceAddresses/lan_ip  InterfaceAddresses/wan_net
InterfaceAddresses/lan_net Server
```

インタフェースアドレスの設定

インタフェースのアドレスを設定するためには、以下の CLI を使用します。

```
DFL-xxxx:/> set Address IP4Address InterfaceAddresses/wan_ip Address=172.16.5.1
Modified IP4Address InterfaceAddresses/wan_ip.
```

DHCP の有効化

インタフェースで DHCP を有効にするためには、以下の CLI を使用します。

```
DFL-xxxx:/> set Interface Ethernet wan DHCPEnabled=yes
Modified Ethernet wan.
```

イーサネットデバイスコマンド

いくつかのインタフェース設定は、イーサネット設定自身の直接的管理をします。D-Link 製ハードウェアの交換、およびイーサネットカード設定の変更、または D-Link 製以外のハードウェアで NetDefendOS を実行する場合のインタフェース設定に特に便利です。例えば、イーサネットインタフェース情報を表示するために、以下のコマンドを使用します。

```
DFL-xxxx:/> show EthernetDevice
```

本コマンドはすべてのイーサネットインタフェースを表示します。これらは現在のコンフィグレーション内に論理インタフェースとして定義されており、リストの左に「+」記号でマークされます。物理的に存在しているが、コンフィグレーションの一部ではないインタフェースは左に「-」記号で示されます。これらは、コンフィグレーションがアクティベートされた後に削除されます。

各インタフェースの詳細情報を表示します。例えば、インタフェース「If1」のコマンドは以下の通りです。

```
DFL-xxxx:/> show EthernetDevice If1
       Property Value
-------------- ----------------------
          Name: If1
EthernetDriver: E1000EthernetPCIDriver
        PCIBus: 0
       PCISlot: 17
       PCIPort: 0
               "
               "
```

「set」コマンドは、イーサネットインタフェースを制御するのに使用されます。例えば、インタフェース「lan」を無効にするためには、以下の通りコマンドを使用します。

```
DFL-xxxx:/> set EthernetDevice lan -disable
```

インタフェースを有効にするためには、以下の通りコマンドを使用します。

```
DFL-xxxx:/> set EthernetDevice lan -enable
```

イーサネットインタフェースカードにドライバを設定するためには、以下の通りコマンドを使用します。

```
DFL-xxxx:/> set EthernetDevice lan EthernetDriver=<driver>
PCIBus=<X> PCISlot=<Y> PCIPort=<Z>
```

例えば、WAN インターフェース上でバス、スロット、ポートの組み合わせ「0,0,2」のドライバ名 IXP4NPEEthernetDriver に対するコマンドは以下の通りです。

```
DFL-xxxx:/> set EthernetDevice lan EthernetDriver=IXP4NPEEthernetDriver
PCIBus=0 PCISlot=0 PCIPort=2
```

復元されたコンフィグレーションが新しいハードウェアのインタフェース名と一致しないインタフェース名を含む場合にこのコマンドが役に立ちます。物理インタフェースのバス、スロット、ポート、およびドライバの値をコンフィグレーション内の論理インタフェースに割り当てることによって、論理インタフェースは物理インタフェースにマップされます。しかし、コンフィグレーションをアクティベートする前にこのマッピングを行う必要があります。

すべての CLI オプションを参照するためには、「CLI Reference Guide」を参照してください。

高度なイーサネットインタフェース設定

NetDefendOS イーサネットに利用可能な高度な設定を詳述します。本設定はグローバルであり、すべての物理インタフェースに影響します。

DHCP 設定

NetDefendOS イーサネットインタフェース用の高度な DHCP 設定のリストは以下の通りです。

設定	説明
DHCP_AllowGlobalBcast	DHCP サーバにブロードキャストとして 255.255.255.255 の割り当てを許可します。（標準的ではありません。） 初期値 : 無効
DHCP_DisableArpOnOffer	提供された IP 上の NetDefendOS が行う ARP チェックを無効にします。チェックは、IP アドレスが既に使用中であるかどうか確認するために ARP リクエストを発行します。 初期値 : 無効
DHCP_UseLinkLocalIP	これを有効にすると、NetDefendOS はリースを待っている間、「0.0.0.0」の代わりに Link Local IP（169.254.*.*）を使用します。 初期値 : 無効
DHCP_ValidateBcast	割り当てられたブロードキャストアドレスが割り当てられたネットワークで最も大きい値のアドレスであることが必要です。 初期値 : 有効
DHCP_MinimumLeaseTime	DHCP サーバから許可された最小リースタイム（秒）。 初期値 : 60

ハードウェアの設定

NetDefendOS イーサネットインタフェースで利用可能な高度なハードウェア設定のリストは以下の通りです。これらの設定は D-Link 社以外のハードウェアで動作する NetDefendOS にのみ関連しています。

設定	説明
Ringsize_e1000_rx	e1000 カードの rx バッファのサイズ。 初期値 : 128
Ringsize_e1000_tx	e1000 カードの tx バッファのサイズ。 初期値 : 256
Ringsize_r8169_rx	r8169 カードの rx バッファのサイズ。 初期値 : 256
Ringsize_r8169_tx	r8169 カードの tx バッファのサイズ。 初期値 : 256

インタフェースモニタ設定

NetDefendOS イーサネットインタフェースで利用可能なモニタ設定のリストは以下の通りです。

設定	説明
IfaceMon_e1000	e1000 インタフェースのモニタを有効にします。 初期値 : 有効
IfaceMon_BelowCPULoad	CPU 負荷がこの割合を超えると、一時的に ifacemon を無効にします。 初期値 : 80
IfaceMon_BelowIfaceLoad	インタフェースのネットワーク負荷がこの割合を超えると、一時的に ifacemon とインタフェースを無効にします。 初期値 : 70
faceMon_ErrorTime	エラーの継続がこの時間を経過するとインタフェースはリセットを開始します。 初期値 : 10
IfaceMon_MinInterval	同じインタフェースのリセットの最小間隔。 初期値 : 30
IfaceMon_RxErrorPerc	問題であると判断すべき受信パケットのエラーの割合。 初期値 : 20
IfaceMon_TxErrorPerc	問題であると判断すべき送信パケットのエラーの割合。 初期値 : 7

3.4.3 リンクアグリゲーション

はじめに

D-Link ファイアウォールの個別の物理イーサネットインタフェースで、特定のトラフィックのストリームに必要とされる帯域を提供できない場合、NetDefendOS のリンクアグリゲーション機能を使用して、2 つ以上の物理インタフェースを 1 つにまとめることで可能となります。その結果、1 つの論理的な NetDefendOS インタフェースとして動作します。この機能は、他のセキュリティ製品ベンダでは Link Bundling や NIC Teaming などの名前を使用することがあります。

NetDefendOS では、集約されたイーサネットインタフェースは Link Aggregation 構成オブジェクトによって示されます。単体のイーサネットインタフェースと同様に、インタフェースの種類は L2 です。

例題のユースケース

例題のユースケースは、D-Link ファイアウォールが複数の 1 ギガイーサネットインタフェースしか持っていないが、特定のトラフィックフローの要求が 3 ギガビットの帯域幅である場合です。論理的な Link Aggregation オブジェクトを作成し、3 つの物理インタフェースの容量を 1 つにまとめることができます。このオブジェクトを他のインタフェースのように NetDefendOS コンフィグレーションで使用でき、トラフィックフローを管理する Route および IPRule や IPPolicy オブジェクトの一部とすることができます。すると、NetDefendOS は自動的に物理インタフェース間のトラフィックを拡大します。

以下の図は、3 つの 1 ギガバイトのネットワークが 1 ギガバイトのインタフェースしか持っていないファイアウォールを通じて 10G バイトのバックボーンと通信する必要があるという代表的なシナリオを示しています。ファイアウォールの 3 つの 1 ギガバイトのインタフェースは外部スイッチに接続し、Link Aggregation コンフィグレーションオブジェクトにグループ化されます。その後、スイッチはバックボーンへの 10 ギガバイトのリンクを提供します。

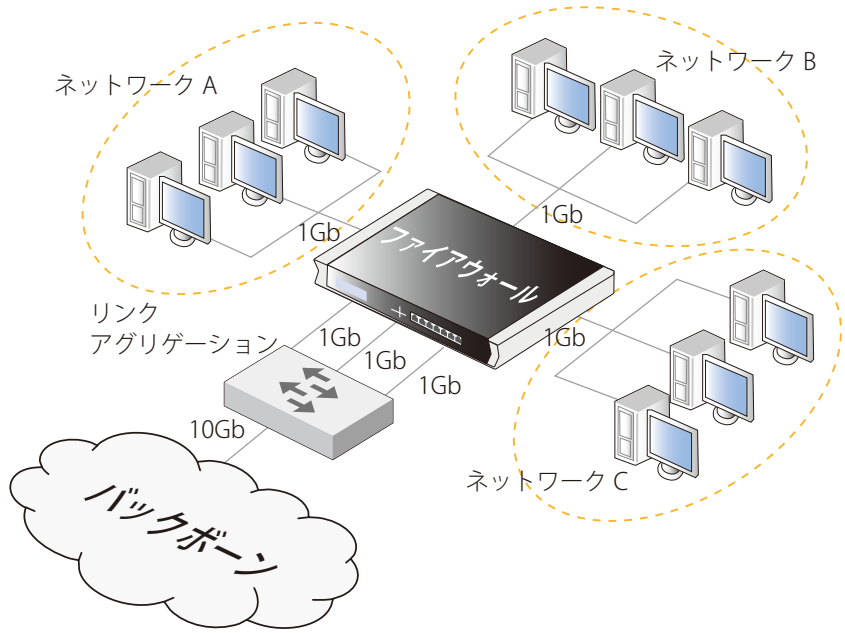


図 3-2　リンクアグリゲーション

注意 **複数のインタフェースを接続するスイッチファブリックは使用できません。**

1 つの論理インタフェースが D-Link のハードウェアモデル上のスイッチファブリックを通じて接続する多くの物理インタフェースから構成される場合、その論理インタフェースをリンクアグリゲーションオブジェクトのパーツにはできません。

これは NetDefend DFL-260E および DFL-860E の論理 lan インタフェースの事例です。

物理インタフェースの要件

以下は NetDefendOS の LinkAggregation コンフィグレーションオブジェクトに関連している物理イーサネットインタフェースの要件です。

- 1 つの LinkAggregation コンフィグレーションオブジェクトを使用して最大 16 個の物理インタフェースを集約できます。
- すべての物理インタフェースが同じリンク速度で動作する必要があります。
- すべての物理インタフェースを同じ外部スイッチに接続する必要があります。

モードの設定

LinkAggregation オブジェクトの Mode プロパティと外部スイッチは以下のモードのどちらかで設定します。

- **Static**

  アグリゲーションが static の場合、NetDefendOS はアグリゲーション内のインタフェースの 1 つが正常に動作していないことを知ることはできず、とにかくトラフィックを送信しようとします。集約されたインタフェースに接続する NetDefendOS とスイッチ間には、ネゴシエーションは起こりません。

  つまり、リンクエラーでは接続が完全に破棄されます。

- **LACP（Negotiated）**

  ネゴシエートされるアグリゲーションでは、集約されたインタフェースに接続するスイッチは、LACP（Link Aggregation Control Protocol）を使用するように設定されます。つまり、1 つの物理リンクが無効になると、NetDefendOS は残りの動作中のリンクにトラフィックを送信しようとします。

  Static 設定より優れた点は、代わりとなる動作中リンクに切り替える前に、NetDefendOS でエラーになった接続に送信するパケット数は限られていることです。これは、接続が破棄されても、接続の外部エンドポイントが受けるパケット損失は少ないことを意味します。

個別のインタフェースの参照は無視されます。

EthernetInterface オブジェクトが LinkAggregation オブジェクトの一部になると、もう個別のオブジェクトとして使用できません。コンフィグレーションがアグリゲーション後にこの個々のインタフェースの用途を保持している場合、基本的なコンフィグレーションは変更されませんが、動作中は NetDefendOS コンフィグレーション内の参照は無視されます。

例えば、以下の通りです。

- 集約されたインタフェースを参照するどの IP ルールセットもルールセット検索で無視されます。
- 集約されたインタフェースを参照するどのルートもルート検索で無視されます。無視されるルートは、CLI コマンドの「show routes」の出力結果に表示されますが、CLI コマンドの「routes」には表示されません。
- リンクアグリゲーションの各インタフェースに対してではなく、アグリゲーションオブジェクトに対して DHCP クライアント機能を有効にします。個別インタフェース上で DHCP が有効化されている場合、リンクアグリゲーションのグループに所属した際に自動的に無効化されます（グループから削除されたときに自動的に再有効化されます）。

個々のルートの参照を削除することをお勧めします

コンフィグレーション変更がコミットする度に、NetDefendOS は無視されるどんな集約インタフェースの参照に関しても警告を発行します。
例えば、インタフェース If1 は、Route オブジェクトに使用されているので、以下のような警告が表示されます。

```
If1 is not a valid routing interface because it's a Link Aggregation member
```

コンフィグレーションを明確にするためには、管理者が NetDefendOS のコンフィグレーションからそのような余分なインタフェースの使用を削除することをお勧めします。

個々のインタフェースのアドレスは 0.0.0.0 になる

EthernetInterface オブジェクトが LinkAggregation オブジェクトの一部になると、個々の IPv4 アドレスは「0.0.0.0」になります。これは CLI コマンド「ifstat」の出力結果で参照できます。

しかし、基本的な NetDefendOS コンフィグレーションは変更されません。例えば、関連するアドレス帳オブジェクトは変更されないため、インタフェースが LinkAggregation から外れた場合には、IP アドレスは元のアドレスに戻ります。

分散方式

管理者は集約した物理インタフェースを経由して伝播されるトラフィックについて判断を行い、以下の分散条件を選択する必要があります。

- DestinationMAC
- SourceIP
- DestinationIP
- SourcePort
- DestinationPort
- IP とポート（初期値）

分散方式の選択

集約されたインタフェース間のトラフィックを伝播するアルゴリズムは、入力として選択された分散方式を持つハッシュ法を使用します。したがって、最適な分散方式は、最も変動する方式です。例えば、トラフィックのソースが ISP 経由でインターネットに NAT 変換される大量の内部クライアントであると、分散方式の最適な選択は SourcePort かもしれません。これは、クライアントが各接続をオープンするため、ランダムに選択されるためです。

上のシナリオの代わりに SourceIP とすることができますが、十分多くのクライアントがある場合だけです。わずかなクライアントでは、SourceIP は使用される集約インタフェースの 1 つだけで終了するかもしれません。

パブリックインターネット上を経由してリモートクライアントからの外部要求を受信する、保護された Web サーバのためにアグリゲーションが行われている場合、すべての接続がサーバのアドレスを持つため、DestinationIP は適当ではありません。代わりに、様々な値を持ち得る SourceIP は分散方式には適切な選択であると言えます。

新しい接続がオープンするたびに、使用する物理イーサネットインタフェースを選択するハッシュプロセスは行われます。これは、ある接続のすべてのパケットが同じ物理インタフェースに送信されることを意味します。選択されたモードがダイナミックの場合、接続に失敗すると、続いて変更だけを行います。

デフォルト IP とポート分配方式

デフォルトの分散方式は「IP and Port」で、これは送信元と宛先 IP アドレスの両方はもちろん、送信元と宛先のポート番号も利用されます。一般的な多目的ソリューションになるように設計されており、トラフィックタイプが可変かつ管理者がどれが最適な分散方式かわからない場合にも対応可能です。

物理的なスイッチ接続

ファイアウォールと外部スイッチ間の物理的なケーブル接続は、LinkAggregation オブジェクトを作成し、コンフィグレーションの変更をアクティブ化する前後いずれでも行うことができます。コンフィグレーションの変更がアクティブになると、直ちに NetDefendOS は収集したインタフェースにデータを送信しようとします。

しかし、LinkAggregation オブジェクトをアクティブ化して保存する前に、所定の位置で物理的なケーブル接続を行うことをお勧めします。これは、negotiated（LACP）を使用すると、機能から予想され、関連する動作を提供します。

高可用性を持つ設定

HA を持つリンクアグリゲーションを使用する場合、HA クラスタ内にある各ファイアウォールのイーサネットポートからの接続は、同じまたは異なるスイッチに接続できます。しかし、同じスイッチを使用する場合、スイッチに 2 つのリンクアグリゲーショングループを作成することで各ファイアウォールから接続を分けるように設定する必要があります。

MTU 値の設定

特定の MTU プロパティの値をリンクアグリゲーションインタフェースに設定することができます。しかし、個別のイーサネットインタフェースの MTU プロパティがリンクアグリゲーションの MTU よりも低い値にセットされている場合、この値は集約されたイーサネットインタフェースの 1 つには使用されません。これは、モードが static または negotiated（LACP）であっても関係ありません。

例題 3.22

リンクアグリゲーション

この例では、イーサネットインタフェースの If1 と If2 が LinkAggregation オブジェクト la_if1_if2 の一部になります。この新しいオブジェクトに定義済みの IPv4 アドレスオブジェクト la_if1_if2_ip を割り当て、このアドレスはネットワーク la_if1_if2_net に所属するものとします。

リンクしているスイッチは、リンクネゴシエーションができます。

CLI

```
DFL-xxxx:/> add Interface LinkAggregation la_if1_if2 Mode=LACP IP=la_if1_if2_ip Network=la_if1_if2_net
            DistributionAlgorithm=DestinationIP
```

Web Interface

1. **Network > Interfaces and VPN > Link Aggregation > Add > Link Aggregation** の順にメニューをクリックします。
2. 以下を入力します。
   - Name: la_if1_if2
   - Distribution Algorithm: Destination IP
   - Mode: LACP
   - IP address (IPv4): la_if1_if2_ip
   - Network (IPv4): la_if1_if2_net
3. Members から If1 を選択し、Include を押します。
4. 前の手順を繰り返して、If2 インタフェースを追加します。
5. 「OK」ボタンをクリックします。

3.4.4 VLAN

概要

NetDefendOS の VLAN では、特定の物理インタフェースに関連する 1 個以上の VLAN インタフェースを定義することが可能です。そのため、これらは NetDefendOS の論理インタフェースであると考えられ、ルールセットやルーティングテーブルにおける他のインタフェースのように扱うことができます。

VLAN は様々なシナリオで便利です。代表的な使用法は、1 つのイーサネットインタフェースを多くの独立したインタフェースとして表すことができることです。つまり、D-Link ファイアウォールの物理的なイーサネットインタフェース数により、独立した外部ネットワークの合計接続数が制限されるということはありません。

もうひとつの VLAN の典型的な使い方は、組織に属する複数のクライアントグループとしての使い方です。そのため、異なるグループに属するトラフィックは異なる VLAN で完全に分割されます。NetDefendOS の制御下において異なる VLAN 間のトラフィックは分割され、NetDefendOS ルールセットで定義されたセキュリティポリシーを使ってフィルタされます。

以下で詳しく説明するように、NetDefendOS を使用した VLAN 構成は、ファイアウォールからスイッチまでの VLAN トランキングの組み合わせを含み、これらのスイッチはインタフェースにポートベース VLAN を構成します。どの物理的なファイアウォールインタフェースも、VLAN でないトラフィックと単一またはマルチプル VLAN の VLAN トランキングトラフィックの両方を同時に送信することができます。

VLAN 処理

NetDefendOS は VLAN の IEEE 802.1Q 仕様に準拠しており、これは、VLAN トラフィックの一部であるイーサネットフレームヘッダに VLAN 識別子 (VLAN ID) を追加することで VLAN がどのように機能するかを指定しています。

VLAN ID は 0 から 4095 までの番号で、そのフレームが所属する特定の VLAN を識別するために使用されます。このメカニズムを使用して、イーサネットフレームは異なる VLAN に所属しながらも、同じ物理インタフェースを共有します。

以下は、物理インタフェースで VLAN のタグ付けをされたイーサネットフレームを NetDefendOS が処理する時の原則です。

- NetDefendOS が物理インタフェースで受信するイーサネットフレームは、VLAN ID を調査されます。VLAN ID が検出され、一致した VLAN インタフェースがそのインタフェースに定義されていると、NetDefendOS は、後続のルールセットの処理のために VLAN を論理インタフェースとして使用します。
- インタフェースで受信したイーサネットフレームに割り当てられた VLAN ID がない場合は、フレームの送信元が物理インタフェースであり、VLAN ではないと見なされます。

- VLAN タグ付きトラフィックを物理インタフェースが受信し、NetDefendOS コンフィグレーション内のインタフェースに対応する VLAN ID を持つ定義された VLAN がなければ、NetDefendOS はそのトラフィックを廃棄し、「unknown_vlanid」ログメッセージが生成されます。

- VLAN ID は 1 つの NetDefendOS の物理インタフェースに対し固有でなければなりませんが、同じ VLAN ID を複数の別の物理インタフェースで使用することができます。つまり、同じ VLAN は多くの物理インタフェースに及ぶことができます。

- 物理インタフェースを VLAN 専用にする必要はなく、VLAN トラフィックおよび VLAN でないトラフィックを混ぜて送信することができます。

VLAN との物理的な VLAN 接続

以下の図では典型的な NetDefendOS の VLAN のシナリオに対する接続を示しています。

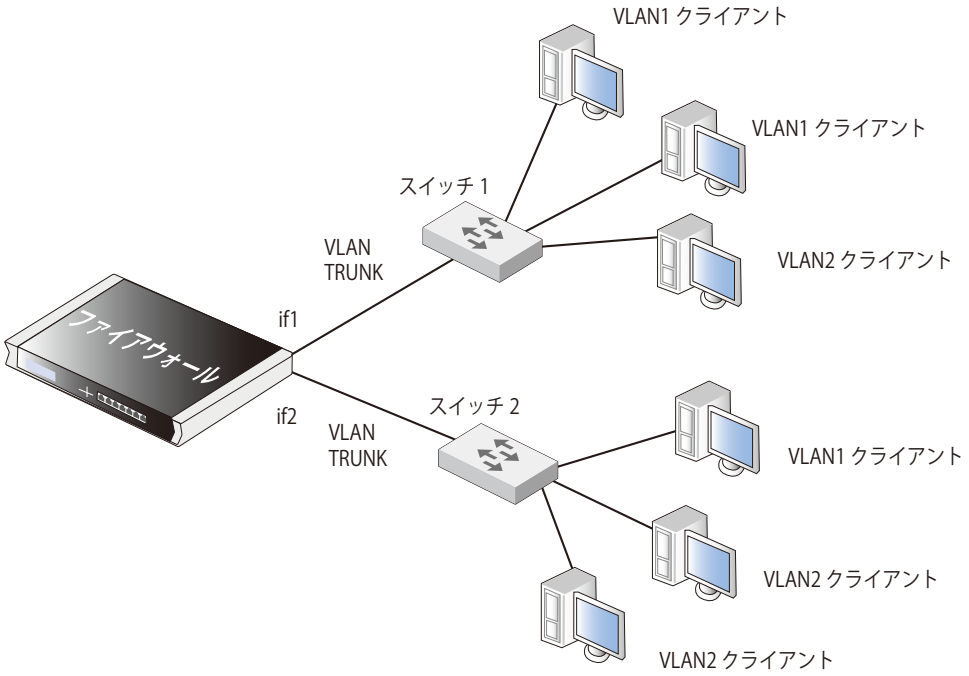


図 3-3　VLAN 接続

NetDefendOS の VLAN を使用した物理的な接続は以下の通りです。

- 1 つ以上の VLAN が物理的にファイアウォールインタフェースに構成され、これが直接スイッチに接続されています。この接続は VLAN トランクとして動作します。使用されるスイッチは、ポートベースの VLAN をサポートしている必要があります。これは、スイッチのポート毎に接続する VLANID を設定できることを意味します。トランクを通じて流れる VLAN ID を許可するように、ファイアウォールに接続するスイッチのポートを設定する必要があります。

  上の図において、スイッチ 1 とスイッチ 2 へのインタフェース if1 と if2 の間の接続は、VLAN トランクです。

- VLAN クライアントに接続するスイッチの他のポートは、それぞれ VLAN ID が設定されます。これらのポートの 1 つに接続するどのデバイスも、自動的にそのポートに設定された VLAN の一部となります。Cisco 社製スイッチでは、これをスタティックアクセス VLAN の設定と呼んでいます。

  上の図におけるスイッチ 1 では、1 つのインタフェースが VLAN2 用に、他の 2 つが VLAN1 用に設定されています。

  必要に応じて、スイッチはトランクトラフィックをファイアウォールから別のトランクに送信することができます。

- ファイアウォール上の 1 つ以上のインタフェースで VLAN トランクのトラフィックを送信することが可能であり、これらのインタフェースはそれぞれ別のスイッチに接続します。複数のトランクで同じ VLAN のトラフィックを送信するように設定することができます。

許可される VLAN 総数の制限

NetDefendOS のインストールに際し定義される VLAN インタフェースの数は、NetDefendOS のライセンスタイプによって制限されます。異なるハードウェアモデルは、VLAN に対し異なるライセンスと異なる制限を持つことになります。

VLAN 設定の概略

以下は、VLAN インタフェースのセットアップにおいて重要な手順です。

1. VLAN インタフェースに名前をつける。
2. VLAN に物理インタフェースを割り当てる。
3. その物理インタフェースに一意の VLAN ID を割り当てる。
4. VLAN に任意の IP アドレスを指定する。
5. VLAN に任意の IP ブロードキャストアドレスを指定する。
6. VLAN に適切なルーティングテーブルで必要なルートを作成する。
7. IP ルールセットに、VLAN インタフェースでトラフィックの通過を許可するルールを作成する。

注意 ポートベース VLAN

NetDefend DFL-260E および DFL-860E の LAN インタフェース上の VLAN は標準の NetDefendOS VLAN とは異なる設定となります。設定は、「付録 E DFL-260E/860E のポートベース VLAN」で詳しく記載しています。

これらの LAN インタフェースに対する VLAN 処理のオーバヘッドは、NetDefendOS によってではなく、これらのインタフェースを接続するスイッチのファブリックによって行われます。これにより、インタフェースを多くの異なる VLAN に分割することができます。この機能は、ポートベース VLAN と呼ばれます。

VLAN インタフェースにおけるトラフィックフローに対しては、物理インタフェースと同様に、適切な IP ルールとルートの両方が設定されている必要があることを認識することが重要です。例えば、送信元インタフェースとして特定の VLAN インタフェースを持つ IP ルールがトラフィックのフローを許可することを定義していないと、到着したパケットは破棄されます。

VLAN の詳細設定

VLAN に以下の詳細設定を行います。

項目	説明
Unknown VLAN Tags	不明な ID でタグ付けされた VLAN パケットへの対応を指定します。 初期値 : DropLog

例題 3.23

VLAN を定義する

ここでは、VLAN ID に 10 を使用した VLAN を定義します。VLAN の IP アドレスが、オブジェクト「vlan10_ip」としてアドレス帳に既に定義されているものとします。

CLI

```
DFL-xxxx:/> add Interface VLAN VLAN10 BaseInterface=lan IP=vlan10_ip Network=all-nets VLANID=10
```

Web Interface

1. **Network > Interfaces and VPN > VLAN > Add > VLAN** の順にメニューをクリックします。
2. 以下の通り入力し、「OK」ボタンをクリックします。

General

- Name : VLAN10
- Base Interface : lan1
- VLAN ID : 10

アドレス設定

- IP address : vlan10_ip
- Network : all-nets

3.4.5 サービス VLAN

あるシナリオでは、1 つの親 VLAN 内部で複数 VLAN からのトラフィックを包括することが望ましいと言えます。これは Q-in-Q VLAN または Stacked VLAN と呼ばれることがあります。NetDefendOS では、サービス VLAN と呼ばれ、IEEE 802.1ad で定義される標準に準拠しています。サービス LAN は他の VLAN へのトンネルと言うことができ、1 つのイーサネットインタフェース上の 1 つの論理的接続を使用して複数の VLAN がフローできる便利な方法を提供します。

サービス VLAN の使用例

D-Link ファイアウォールはサービス VLAN のための終端として機能できます。サービス VLAN 終端の代表的なユースケースの例は、以下の図で示します。

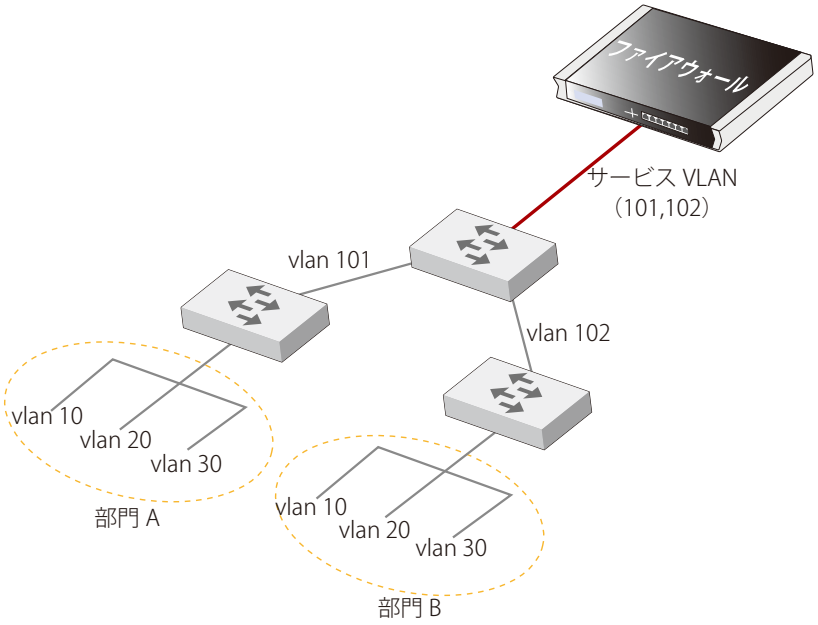


図 3-4　サービス VLAN の使用例

ここでは、会社の部門 A と B はそれぞれ VLAN ID10 と 20 を複製できる 2 つの VLAN を使用します。各部門のスイッチは、固有な VLAN ID 101 と 102 を使用することで中央にある別のスイッチにそれらを接続します。この中央のスイッチは、101 と 102VLAN にトンネル接続する 1 つのサービス LAN を使用することで D-Link ファイアウォールに接続できます。

サービス VLAN を定義する

標準の NetDefendOS VLAN オブジェクトは、サービス VLAN を定義するのに使用されますが、オブジェクトの Type プロパティは 0x88a8 に設定されます。この Type プロパティは VLAN タグに設定する TPID に対応しています。詳しくは、本セクションの終わりで説明します。

サービス VLAN オブジェクトを定義した後に、Base Interface プロパティをサービス VLAN オブジェクトに設定することで、内部に non-service VLAN オブジェクトを置くことができます。以下の例題でこれを示します。

例題 3.24

サービス VLAN を定義する

例題では、物理インタフェース If3 に ID100 を持つサービス VLAN svlan_A を定義します。

CLI

```
DFL-xxxx:/>  add Interface VLAN svlan_A Type=0x88a8 BaseInterface=If3 VLANID=100 IP=svlan_A_ip Network=svlan_A_net
```

VLAN オブジェクトをこれに追加します。

```
DFL-xxxx:/> add Interface VLAN vlan1 BaseInterface=svlan_A VLANID=1 IP=vlan1_ip Network=vlan1_net
```

Web Interface

1. **Network > Interfaces and VPN > VLAN > Add > VLAN** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: svlan_A
   - Type: 0x88a8
   - Base Interface: If3
   - VLANID: 100
   - IP Address: svlan_A_ip
   - Network: svlan_A_net

3. 「OK」ボタンをクリックします。

VLAN オブジェクトをこれに追加します。

1. **Network > Interfaces and VPN > VLAN > Add > VLAN** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: vlan1
   - Base Interface: svlan_A
   - VLANID: 1
   - IP Address: vlan1_ip
   - Network: vlan1_net

3. 「OK」ボタンをクリックします。

重要 ネットワークのジャンボフレームサポートを有効にしてください。

最適な性能のためには、サービス VLAN トラフィックを処理する外部ネットワーク装置でジャンボフレームのサポートを有効にすることをお勧めします。これはサービス VLAN トラフィックが標準サイズの 1500 バイトを超過するイーサネットの MTU 値を使用するためです。

タイプ値に関する全リスト

VLAN オブジェクトの Type プロパティに使用できる値に関する全リストは以下の通りです。

TPID（16 進数）	Decimal Equivalent（10 進数）	説明
0x8100	33024	IEEE 802.1Q VLAN（初期値）
0x88a8	34984	IEEE diffserv Service VLAN
0x9100	37120	0x9100 VLAN
0x9200	37376	0x9200 VLAN
0x9300	37632	0x9300 VLAN

Type プロパティは VLAN タグに Tag Protocol Identifier（TPID）を指定します。

VLAN オブジェクトは 0x8100（標準の VLAN）の Type を初期値とするため、通常、サービス VLAN を指定するために必要とされる Type は 0x88a8 だけです。リストの最後の 3 つのエントリが、他のメーカーの外部装置との相互運用性を提供するのに必要となる場合があります。

サービス VLAN 内のサービス VLAN

サービス VLAN オブジェクトの BaseInterface プロパティを別のサービス VLAN オブジェクトにすることができます。つまり、1 つのサービス VLAN に別のサービス VLAN を含めることができます。

ネストのレベルが多くなることは稀ですが、最大 15 レベルにネストされたサービス VLAN オブジェクトによってラップされた最初のレベルの VLAN オブジェクトを使用することで NetDefendOS は最大 16 レベルのネストを許可します。

3.4.6 PPPoE

Point-to-Point Protocol over Ethernet（PPPoE）は、通常のローカルインタフェース（例えば DSL 回線、無線デバイスまたはケーブルモデム）を経由してイーサネットワーク上の複数ユーザをインターネットに接続するために使用されるトンネリングプロトコルです。イーサネット上のすべてのユーザは一般の接続を共有し、一方、アクセス制御は各ユーザを基本として行われます。

インターネットサービスプロバイダ（ISP）は、顧客が自身のブロードバンドサービスに PPPoE 経由で接続することを要求します。PPPoE を使用して、プロバイダは以下のことを行います。

- ユーザ名 / パスワード認証を使用したセキュリティとアクセス制御の実行。
- IP アドレスを特定ユーザまで追跡する。
- PC ユーザのための自動 IP アドレス割り当て（DHCP に類似）。IP アドレスをユーザグループごとに用意する。

PPP プロトコル

PPP（Point-to-Point Protocol）は、シリアルインタフェース（例えば PC がサーバに電話線を使用して接続するダイヤルアップ接続）を使用している 2 台のコンピュータ間の通信用プロトコルです。OSI 参照モデルと関連して、PPP は、IP ネットワーク経由でどんなプロトコルのパケットも許可するために、レイヤ 2（データリンク層）カプセル化メカニズムを提供します。PPP は、リンクの確立、設定およびテストのための Link Control プロトコル（LCP）を使用します。一度 LCP が初期化されると、1 つ以上の Network Control Protocols（NCP）が特定のプロトコル群にトラフィックを転送するため、複数のプロトコルが同じリンク上で情報交換を行うことができます。例えば、IP と IPX 両方のトラフィックが PPP リンクを共有することができます。

PPP 認証

PPP 認証は、PPP 通信のオプションとして使われます。サポートされる認証プロトコルは、Password Authentication Protocol（PAP）、Challenge Handshake Authentication Protocol（CHAP）、Microsoft CHAP（version 1 と 2）です。認証されると、ネットワーク層プロトコルパラメータが NCP を使用して処理される前に、少なくとも 1 つのピアが自身を認証する必要があります。LCP と NCP のネゴシエーション中、暗号などのオプションパラメータがネゴシエートされます。

PPPoE クライアント設定

物理イーサネットインタフェースまたは VLAN インタフェースのどちらかで NetDefendOS PPPoE クライアントが動作することが可能です。

各 PPPoE トンネルは、NetDefendOS によって通常のインタフェースと同じルーティングと設定機能を持ち、すべてのトラフィックに適用する IP ルールセットを持つ論理インタフェースと解釈されます。PPPoE トンネルからファイアウォールに到着しているネットワークトラフィックは、その送信元インタフェースとして PPPoE トンネルインタフェースを持っています。外向きのトラフィックには、PPPoE トンネルインタフェースが送信先インタフェースとなります。

どのインタフェースにも 1 個以上の経路が提供されるため、NetDefendOS はどの IP アドレスからのトラフィックが許可され、PPPoE トンネルを経由してどこに送信されるかがわかります。PPPoE クライアントには、同じネットワークの異なるサーバを区別するために、サービス名を使用する設定を行うことも可能です。

IP アドレス情報

PPPoE は、DHCP と類似している自動 IP アドレス割り当てを使用します。NetDefendOS が ISP からこの IP アドレス情報を受信する場合、ネットワークオブジェクト内にそれを保存し、インタフェースの IP アドレスとして使用します。

ユーザ認証

ユーザ認証が ISP に要求される場合、PPPoE サーバに自動的に送信するために、ユーザ名とパスワードを NetDefendOS に設定することができます。

ダイヤルオンデマンド

ダイヤルオンデマンドが有効であると、PPPoE インタフェースにトラフィックがある場合にだけ PPPoE 接続は起動します。ファイアウォールがインタフェース上のアクティビティ（外向きトラフィック、内向きトラフィック、または両方のいずれか）をどのように検出するかを設定できます。さらに、トンネル切断までの非アクティビティ時間を設定可能です。

Unnumbered PPPoE

NetDefendOS が PPPoE クライアントとして動作する場合、unnumbered PPPoE が初期値で提供されます。また、PPPoE セッションで unnumbered PPPoE の使用を強制するためのオプションも設定可能です。

unnumbered PPPoE は、通常 ISP がユーザに対して事前に取得した 1 つ以上の IP アドレスを割り当てたい場合に使用されます。これらの IP アドレスを手動でクライアントのコンピュータに入力します。ISP は、接続時に PPPoE クライアントに対して IP アドレスを割り当てません。

NetDefendOS における unnumbered PPPoE 機能の追加オプションは、PPPoE クライアントインタフェースのアドレスとして使用される一つの IP アドレスの仕様を許可することです。このアドレスは以下の目的に役立ちます。

- IP アドレスは、「preferred IP」として PPPoE サーバに送信されます。unnumbered PPPoE の強制的な実行が有効となっていない場合、サーバは「preferred IP」を許可せず、代わりに PPPoE に新しい IP アドレスを割り当てる可能性があります。

  unnumbered PPPoE を実行するオプションを選択する場合、クライアント（すなわち、NetDefendOS）は、サーバによる別の IP アドレスの割り当てを受け付けません。

- unnumbered PPPoE が実行されない場合に、指定された IP アドレスまたは PPPoE サーバによって割り当てられたアドレスは、PPPoE クライアントインタフェースの IP アドレスとして機能します。これは、D-Link ファイアウォールによってトラフィックが送信または NAT された場合に、インタフェースから送信されるトラフィックのローカル IP アドレスとして使用されます。

注意 PPPoE には、discovery プロトコルが含まれます。

イーサネットにポイントツーポイント接続を供給するためには、固有のセッション識別番号を確立する他に、各 PPP セッションでリモートピアのイーサネットアドレスを学習する必要があります。PPPoE には、そうした機能を提供する discovery プロトコルがあります。

PPPoE は HA と共に使用できない

高可用クラスタの NetDefendOS では IP アドレスが共有される接続方式のため、PPPoE は正しく動作しません。そのため、HA と共に設定するべきではありません。

例題 3.25

PPPoE クライアントを設定する

PPPoE を経由して送信されるトラフィックを持つ WAN インタフェースに PPPoE クライアントを設定します。

CLI

```
DFL-xxxx:/> add Interface PPPoETunnel PPPoEClient EthernetInterface=wan Network=all-nets
            Username=exampleuser Password=examplepw
```

Web Interface

1. **Network > Interfaces and VPN > PPPoE > Add > PPPoE Tunnel** の順にメニューをクリックします。

2. 以下の通り入力します。
   - Name : PPPoEClient
   - Physical Interface : wan
   - Remote Network : all-nets（トンネル内にすべてのトラフィックを送信するため）
   - User Name : ISP から通知されているユーザ名を入力します。
   - Password : ISP から通知されているパスワードを入力します。
   - Confirm Password : パスワードを再度入力します。
   - Service Name : ISP から通知されているサービス名を入力します。
   - Authentication : 使用する認証プロトコルを正確に指定します。指定しない場合は、初期設定が使用されます。
   - Enable Dial-on-demand : チェックを外します。
   - Advanced の Automatically add a route for this interface using the given remote network.: チェックすると、新しい経路がインタフェースに追加されます。

3. 「OK」ボタンをクリックします。

3.4.7 GRE トンネル

概要

GRE（Generic Router Encapsulation）プロトコルは、ネットワークデバイスの通過やネットワークを行き来するトラフィックをトンネル化する必要がある時にいつも使用される簡単なカプセル化されたプロトコルです。GRE はセキュリティ機能を提供しないため、非常に低いオーバーヘッドで使用できます。

GRE の使用

GRE は、インターネットなどの第三のネットワークを通じて、2 つのネットワークを 1 つに接続する方法を提供するものです。接続される 2 つのネットワークは、介在するネットワークを通じて、GRE を使用してトンネルしている一般的なプロトコルと通信します。GRE は以下のように使用されます。

- 特定のプロトコルを妨げるネットワーク装置を横断します。
- IPv4 ネットワークで IPv6 トラフィックをトンネルします。
- UDP データストリームがマルチキャストされる場合に、マルチキャスティングをサポートしないネットデバイスを通過する必要があります。GRE により、ネットワークデバイス経由でトンネリングを行うことが可能です。

GRE セキュリティとパフォーマンス

GRE トンネルは、通信にどんな暗号も使用しないため、それ自身は安全ではありません。セキュリティはトンネルしているプロトコルから受ける必要があります。GRE に暗号化が備わっていないことの利点は、裏で処理されるトラフィックが少ないので高いパフォーマンスを発揮できることです。公共性のない内部ネットワークでトンネリングするような環境などでは、暗号化が備わっていなくても許容できるかもしれません。

GRE のセットアップ

NetDefendOS における IPsec トンネルのような他のトンネルと同様に、各 GRE トンネルは、同じフィルタリング、トラフィックシェーピング、および標準的なインタフェースで可能な設定を持ち、NetDefendOS によって論理的なインタフェースとして扱われます。GRE のオプション項目は以下の通りです。

項目	説明
IP Address	ローカル側のトンネル内部の IPv4 アドレスです。これは、空白のままにできないため、値を指定する必要があります。指定した IP アドレスは以下に使用されます。 • このトンネルのエンドポイントに ICMP Ping を送信することができます。 • トンネルに関連するログメッセージは送信元としてこの IP アドレスを使用して生成されます。 • NAT が使用されている場合、トンネルを通過しているトラフィックに NAT を実行する IP ルールにおいて送信元 IP を設定する必要はありません。この IP アドレスは、NAT の送信元アドレスとして使用されます。
Remote Network	GRE トンネルが接続するリモートネットワーク。
Remote Endpoint	トンネルが接続するリモートデバイスの IPv4 アドレス。
Outgoing Routing Table	送信するトラフィック用ではなく、トンネル自身に使用するためにルーティングテーブルを定義します。つまり、テーブルはトンネルのエンドポイントをルックアップするために使用されます。
Use Session Key	トンネルに任意に指定する一意の数字。これにより、2 つのエンドポイント間で 2 つ以上の GRE トンネルを設定できます。セッションキー値は、それらを認識するためのものです。
Additional Encapsulation Checksum	GRE プロトコルは IPv4 チェックサムに加えて、追加のチェックサムを提供します。これはデータ保全の特別なチェックを提供します。

仮想ルーティングオプションはイーサネットインタフェースなど他のどのインタフェースにも使用されます（「3.4.2 イーサネットインタフェース」を参照）。ここで指定したルーティングテーブルはトンネル自身ではなく、トンネルによって送信されたトラフィックに適用します。トンネル自身のルート検索は上で示す「Outgoing Routing Table」オプションで指定します。

GRE インタフェースのアドバンスド設定は以下の通りです。

項目	説明
Add route dynamically	このオプションは、ルーティングテーブルが自動的にアップデートされるように通常チェックされます。Route metric を指定することができます。
Address to use as source IP	GRE トンネルの送信元インタフェース IP として特定の IP アドレスを指定することができます。トンネル確立時、実際に使用されるインタフェースアドレスではなく、本設定値で開始されているように見えます。 例えば、ARP パブリッシュを使用していて、ARP パブリッシュした IP アドレスによってトンネルをセットアップしたい場合、これが行われるかもしれません。

GRE と IP ルールセット

確立された GRE トンネルというのは、GRE トンネルから到達または GRE へ到達するすべてのトラフィックが自動的に信頼されるということを意味している訳ではありません。そうではなく、GRE トンネルから到着するネットワークトラフィックは、評価のために NetDefendOS の IP ルールセットに転送されます。ネットワークトラフィックの送信元インタフェースは、関連する GRE トンネルの名前です。逆方向、すなわち GRE トンネルに向かっているトラフィックについても同じことが言えます。さらに、どの IP アドレスを許可され、トンネルを経由して送信されるかということを NetDefendOS が理解するように経路が定義される必要があります。

GRE シナリオの例

以下の図は典型的な GRE シナリオを示しています。ここでは、2 つの D-Link ファイアウォール A と B が介在する内部ネットワーク 172.16.0.0/16 を通してお互いに通信しています。2 つのファイアウォールの設定を次に説明します。

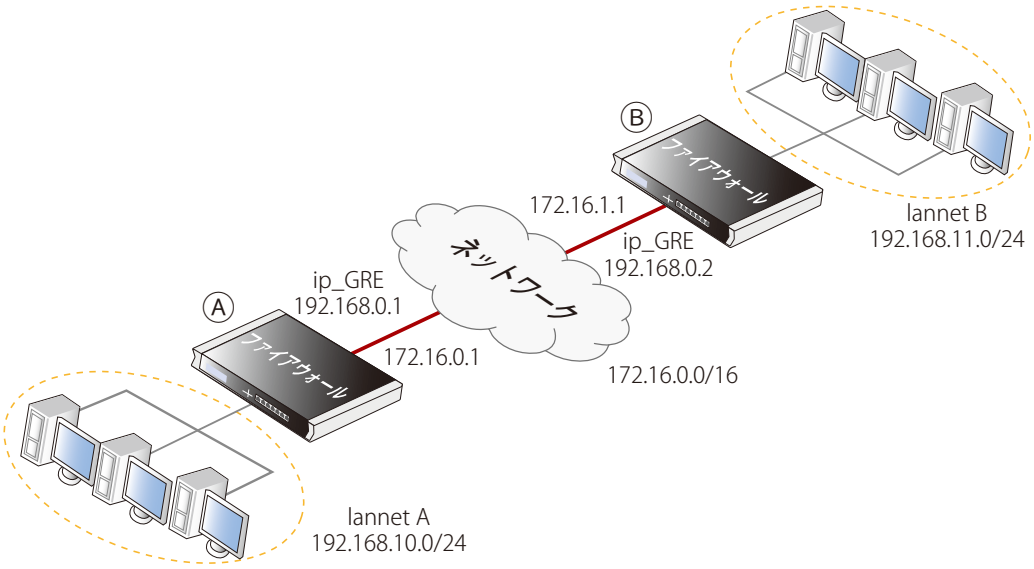


図 3-5　GRE 利用の例

GRE トンネルを使用して、A と B の間を通過するトラフィックは間にあるネットワークを通じてトンネリングされます。ネットワークは内部にあり、パブリックインターネットを通過しないため、暗号化の必要はありません。

パート 1. ファイアウォール「A」のセットアップ

ネットワーク 192.168.10.0/24 が LAN インタフェースの lannet であると仮定し、「A」に NetDefendOS をセットアップするためのステップは以下の通りです。

1. アドレス帳で以下の IP オブジェクトを作成します。
- remote_net_B : 192.168.11.0/24
- remote_gw : 172.16.1.1
- ip_GRE : 192.168.0.1

2. 以下のパラメータで GRE_to_B という GRE オブジェクトを作成します。
- IP Address : ip_GRE
- Remote Network : remote_net_B
- Remote Endpoint : remote_gw
- Use Session Key : 有効
- Session Key : 1

3. メインルーティングテーブル上に、GRE インタフェースの GRE_to_B にある remote_net_B にすべてのトラフィックを送るルートを定義します。GRE トンネルの Advanced タブで「Automatically add a route for this interface using the given remote network.」オプションを有効にしている場合は、自動的にルートが追加されるので必要ありません。

4. IP ルールセットにトラフィックがトンネルを通ることを許可するルールを作成します。

名称	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
To_B	Allow	lan	lannet	GRE_to_B	remote_net_B	all_services
From_B	Allow	GRE_to_B	remote_net_B	lan	lannet	all_services

パート 2. ファイアウォール「B」のセットアップ

ネットワーク 192.168.11.0/24 が lan インタフェースの lannet であると仮定して、B に NetDefendOS をセットアップするためのステップは以下の通りです。

1. アドレス帳に以下の IP オブジェクトを作成します。
- remote_net_A : 192.168.10.0/24
- remote_gw : 172.16.0.1
- ip_GRE : 192.168.0.2

2. GRE_to_A と呼ばれる GRE トンネルオブジェクトを以下のパラメータで作成します。
- IP Address : ip_GRE
- Remote Network : remote_net_A
- Remote Endpoint : remote_gw
- Use Session Key : 有効
- Session Key : 1
- Additional Encapsulation Checksum : Enabled

3. メインルーティングテーブル上に、GRE インタフェースの GRE_to_A にある remote_net_A にすべてのトラフィックを送るルートを定義します。GRE トンネルの Advanced タブで「Automatically add a route for this interface using the given remote network.」オプションを有効にしている場合は、自動的にルートが加えられるので必要ありません。

4. トラフィックがトンネルを通り抜けられるよう IP ルールセットに以下のルールを作成します。

名称	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
To_A	Allow	lan	lannet	GRE_to_A	remote_net_A	all_services
From_A	Allow	GRE_to_A	remote_net_A	lan	lannet	all_services

GRE トンネルステータスのチェック

IPsec トンネルには、稼働している、または稼働していない状態があります。NetDefendOS で GRE トンネルを使用する場合、これは実際には適用されません。コンフィグレーションで存在していると、GRE トンネルが稼働しています。

しかし、GRE トンネルのステータスをチェックできます。例えば、トンネルに gre_interface という名前が付いている場合、CLI コマンド「ifstat」を使用することができます。

```
DFL-xxxx:/> ifstat gre_interface
```

これは、トンネルで何が起こっているかを表示し、「ifstat」コマンドのオプションにより各種詳細を表示します。

3.4.8 6in4 トンネル

6in4 トンネルは IPv4 トラフィックだけをサポートするネットワークに IPv6 トラフィックのトンネリングを許可します。ISP が IPv4 パブリック IP アドレスだけを提供できる状況であっても、ホストが IPv6 アドレスでパブリックインターネットに接続する必要があるかもしれません。これは、RFC 4213（IPv6 ホストとルータのための IPv6 ホストとルータの基本的な移行メカニズム）の実装である 6in4 トンネルを使用することによって、解決されます。この機能は、NetDefendOS では 6in4 Tunnel コンフィグレーションオブジェクトによって提供されます。D-Link ファイアウォールが 6in4 トンネルのカプセル化装置として機能すると言えます。

この機能を使用する代表的なシナリオは、多くの IPv6 ホストコンピュータがあるファイアウォールの背後にある保護されたネットワークです。各ホストは自身の固有な IPv6 アドレスを必要とし、このアドレスはパブリックインターネットをまたがる他のホストにアクセスするものです。この IPv6 トラフィックはファイアウォールから（次に説明する）トンネルサーバまで広がる 1 つの 6in4 トンネルを通じて送信されます。これは、最初に本セクションで議論するシナリオです。

トンネルサーバとトンネルのブローカー

トンネルサーバは、パブリックインターネットを介して IPv4 での接続が可能な外部のコンピュータであり、IPv6 トラフィックに対してパブリックインターネットへのゲートウェイを提供します。トンネルサーバは、サーバ使用に課金が必要な、または無料でサービスを提供するサードパーティの組織であるトンネルブローカーによって提供されます。このサービスを提供する ISP もあるかもしれません。

必須のトンネルブローカー情報

外部のトンネルサーバに NetDefendOS 6in4 Tunnel オブジェクトを設定する前に、サーバを所有しているトンネルのブローカーは、設定に必要な以下の情報を提供します。

- IPv6 プレフィックス。ファイアウォールの背後にある IPv6 ホストが使用できるアドレス範囲です。NetDefendOS DHCPv6 サーバを設定することによって、アドレスはスタティックまたはダイナミックに割り当てられます。トンネルブローカーは、既にブローカー自身に割り当てられた広い範囲の固有の IPv6 プレフィックスを持っており、そのプレフィックスを使用して割り当てを行います。

- トンネルサーバコンピュータ上のインタフェースの IPv4 アドレス。これは、6in4 Tunnel オブジェクトを設定する時に Remote Endpoint プロパティとして使用されます。IPv4 アドレスの代わりに、DNS 解決可能なアドレスを利用することも可能です。この場合、DNS サーバが設定済みであるならば、NetDefendOS は自動的にアドレスを解決します。

- オプションで、ブローカーによりクライアント側のトンネルの内部ローカルエンドポイントの IPv6 アドレスが提供されます。これは 6in4 Tunnel オブジェクトの IP Address プロパティです。トンネルが有効であるかどうかを確認するために、トンネルサーバが ping を行います。

以下の図は、トンネルのブローカーを使用した IP6in4 トンネルの使用例を示しています。D-Link ファイアウォールの背後にある LAN ネットワークと DMZ ネットワークは、パブリックインターネットへの IPv6 アクセスを必要としますが、ISP のルータには IPv4 アクセスだけが利用可能です。

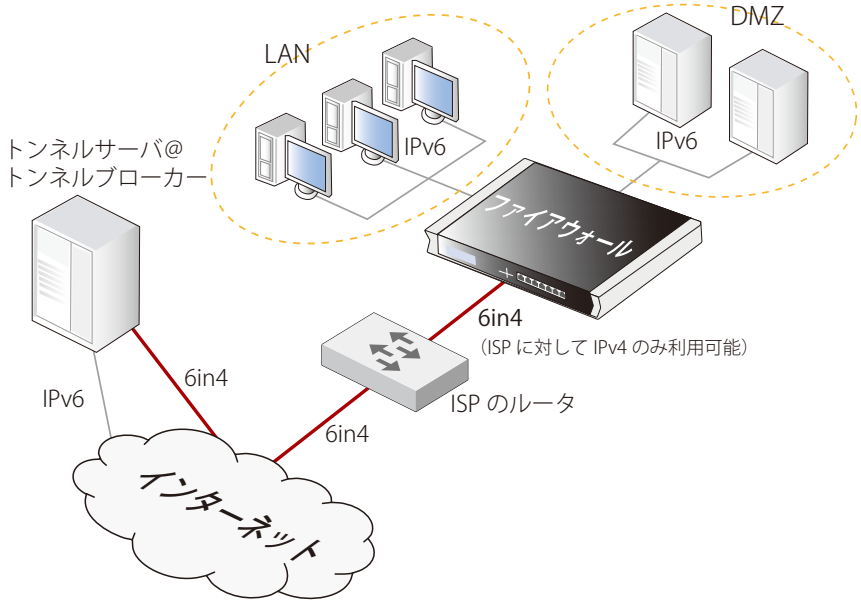


図 3-6　IP6in4 Tunnel 使用法

6in4 Tunnel オブジェクトの設定

オブジェクト名の他に、値を割り当てるべき 3 個の主なプロパティがあります。

プロパティ	説明
Remote Network	トンネルオブジェクトが定義された時に NetDefendOS によって自動的に追加されるルートのネットワークを指定します。ここで説明する代表的なクライアントのシナリオについては、通常、これはパブリックインターネットへの IPv6 ゲートウェイを示す all-nets6 になります。 自動的にルートを追加するオプションを無効にすると、手動で追加されたルート内でネットワークが指定されるため、このプロパティは設定不要となります。 トンネルのローカルエンドポイントであるインタフェースは、このプロパティのルートルックアップから取得されます。多くの場合、パブリックインターネットへのデフォルトルートがルックアップされ、インタフェースは ISP に接続するイーサネットインタフェースになります。
IP Address	トンネル内部のローカル IPv6 アドレス。トンネルが生存しているかどうかを確認するのに ping を実行できる場合、トンネルのブローカーによって提供されている可能性があります。提供される場合は、ICMP ping が応答できるように適切な NetDefendOS IP ルールまたはポリシーを設定する必要があります。 ブローカーが特定のアドレスを必要としないのであれば、これはブローカーが付与するプレフィックスに所属するどんな IPv6 アドレスにも設定されます。
Remote Endpoint	これはトンネルサーバ用の IPv4 アドレスであり、NetDefendOS はパブリックインターネットを経由して連絡する方法がわかります。IPv4 トラフィック専用の ISP を経由して NetDefendOS がパブリックインターネットにアクセスする手段を持っているものとします。

例題 3.26

6in4 トンネルコンフィグレーション

この例題では、6in4 Tunnel オブジェクトは、インターネットを経由してリモートトンネルサーバに接続するように設定されます。

多くのアドレスオブジェクトが NetDefendOS のアドレス帳で既に設定されているものとします。これらには、トンネルのローカルな内側 IPv6 エンドポイントには local_endpoint_ip6、トンネルサーバの IPv4 アドレスには tunnel_server_ip4 という名称のオブジェクトがあります。

CLI

```
DFL-xxxx:/> add Interface IP6in4Tunnel my_6in4_tunnel IP=local_endpoint_ip6 Network=all-nets6
            RemoteEndpoint=tunnel_server_ip4
```

Web Interface

1. **Network > Interfaces and VPN > 6in4 > Add > 6in4 Tunnel** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_6in4_tunnel
   - IP Address: local_endpoint_ip6
   - Remote Network: all-nets6
   - Remote Endpoint: tunnel_server_ip4
3. 「OK」ボタンをクリックします。

6in4 トンネルを持つルーティングテーブルの利用

初期値では、NetDefendOS の main ルーティングテーブルで IPv4 リモートエンドポイントにルックアップが行われます。特定のルーティングテーブルになるようにこれを変更することができます。トンネルの Remote Network プロパティのルートは、初期値で main テーブルを含むすべてのルーティングテーブルにも追加されます。また、特定のルーティングテーブルに追加されるように変更することもできます。

MTU 値の変更

保護された IPv6 クライアントが使用する MTU をあまり大きくするべきではありません。これは、トンネリングプロセスの間、過度のフラグメント化を行う結果、不要なオーバヘッドを引き起こすためです。ファイアウォールの背後にある IPv6 クライアントの MTU 値を調整するために、以下の方法があります。

- トラフィックフローを制御する IP ルールセットのエントリで使用される Service オブジェクトで、Foward ICMP errors プロパティが有効化されている場合、IPv6 ホストは最初に 6in4 Tunnel オブジェクトの MTU プロパティの初期値を使用します。初期値は 1280 であり、IPv6 における最小値となります。他のダウンストリームのネットワーク機器で異なる MTU が要求される場合、ICMP メッセージを介して通信することが可能です。
- NetDefendOS Router Advertisement オブジェクトを IPv6 ホストに接続するインタフェースに対して設定することができます。これは、推奨される MTU 値を提供できます。この方式は、不適当な MTU サイズが理由の ICMP エラーのメッセージを受信しても再送する必要がないため、ホストによる最も速い応答を提供します。

これらのオプションは一緒に使用することができます。そのため、ルータ通知が提供した最初の MTU 値が受け付けられない場合、推奨される MTU 値が ICMP エラーメッセージを通じて送信されます。

NetDefendOS がトンネルサーバとして機能する

ここまでは NetDefendOS が外部トンネルサーバ用のクライアントとして動作しているものと仮定してきました。しかし、D-Link ファイアウォール自身がトンネルサーバであることも可能です。この代表的な用途は、会社の支店のクライアントが IPv6 アクセスを必要とする場合です。これを以下の図で説明します。

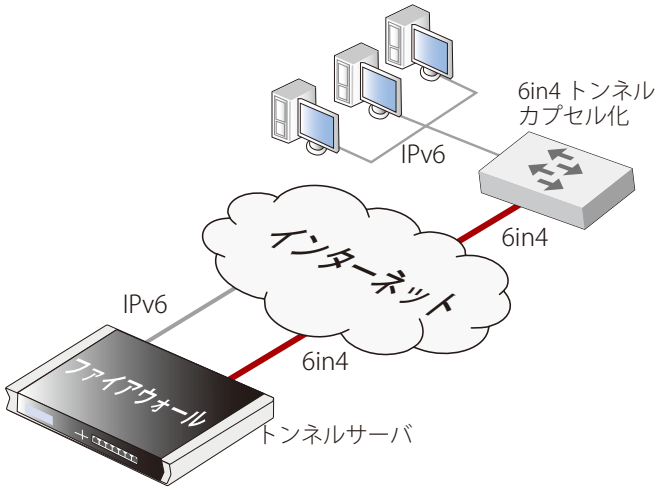


図 3-7　6in4 トンネルサーバとして機能する

上の図の 6in4 トンネルカプセル化装置は、リモートネットワークトラフィックのために 6in4 トンネルを行うことができるネットワーク装置です。例えば、ルータ、適切なソフトウェアを持つサーバ、または以前に説明したように設定された D-Link ファイアウォールといった機器によって実現することができます。

このトンネルサーバ機能を提供するように NetDefendOS を設定するには、以下のコンフィグレーションの要素が必要です。

- リモートホストの IPv6 トラフィックを送信するために接続する各トンネルの 6in4 Tunnel オブジェクト。
- IPv6 をサポートする ISP ゲートウェイに接続されるインタフェースのための all-net6 ルート。トンネルからの内向き IPv6 トラフィックを、ルートのインタフェースを経由してインターネットに送信することができます。このインタフェースは、通常 ISP に接続するイーサネットインタフェースですが、別のインタフェースのタイプであるかもしれません。
- all-net6 ルートを使用したトンネルから来たトラフィックが出ていくことを許可する少なくとも 1 つの IP ルールまたは IP ポリシー。これは、必要に応じて MTU サイズを調整できるように Forward ICMP errors プロパティが有効であるオブジェクトを使用しなければなりません。

  IPv6 トラフィックを制御する IP ルールまたは IP ポリシーは、特定の IPv6 トラフィックのタイプを許可、または拒否する NetDefendOS Application Control 機能を使用できます。詳しくは「3.7 アプリケーションコントロール」を参照してください。

NetDefendOS の設定には、以下の方法で使用されているオブジェクトプロパティで 6in4 Tunnel オブジェクトを設定することが必要です。

プロパティ	説明
Remote Network	クライアントホストが使用する IPv6 プレフィックスです。
IP Address	ブローカーファイアウォールへのエンドポイントのローカルな内側 IPv6 アドレス。他の誰からもアクセスできないようにするべきです。NetDefendOS は自動的にインタフェース core を持つルートを作成します。（つまり、core ルート）
Remote Endpoint	接続トンネルのリモートイーサネットインタフェースの IPv4 アドレスです。また、これは DNS 解決可能なアドレスであるかもしれません。

サーバとして機能する時、1 つの 6in4 Tunnel オブジェクトは、1 つの内向きなトンネルだけから接続を受け付けることができます。他の内向きなトンネルには別々のトンネルオブジェクトを設定しなければなりません。また、NetDefendOS がサーバとして機能する場合、正しく MTU サイズを調整できるように ICMP エラーメッセージを許可しなければなりません。

3.4.9 ループバックインタフェース

ループバックインタフェースは論理的な NetDefendOS インタフェースで、このインタフェースを通じてすべての送信トラフィックを取得し、2 番目に設定されたループバックインタフェースを通じて送出します。その結果、ループバックインタフェースはペアで常に設定され、双方が互いに参照します。

例えば、Loopback Interface オブジェクトのペア LB1 と LB2 を設定し、それぞれペアとなるように定義するものとします。トラフィックを LB1 インタフェースを通して送信する場合、NetDefendOS 内で仮想的に発生する転送を使用して、同時に LB2 インタフェースが受信します。同様にトラフィックが LB2 を通じて送信される場合、LB1 が受信します。これはまさに 2 つのインタフェースが相互に接続する 2 つの物理的なイーサネットインタフェースのようです。

Loopback インタフェースに IPv6 を使用できる

IPv4 と IPv6 トラフィックの両方でループバックインタフェースを使用できます。Loopback Interface オブジェクトには常に IPv4 アドレスとネットワークが必要です。Loopback Interface オブジェクトの Enable IPv6 プロパティをオンにすることで、必須の IPv4 情報に加えて、IPv6 アドレスとネットワークも定義することができます。Loopback Interface オブジェクトに IPv4 および IPv6 アドレス情報の両方をグループ化しても、それらの間に何の関係も含意しません。IPv6 ループバックアドレスはコンフィグレーションを簡潔にするために定義されるものです。

仮想ルーティングを使用したループバックインタフェースの使用法

通常、ループバックインタフェースは NetDefendOS 仮想ルーティングと共に使用されます。仮想ルーティングでは、1 つの D-Link ファイアウォールの動作を分割することが可能で、複数の仮想ファイアウォールのように振る舞います。複数のルーティングテーブルを持つことによりこのような動作が可能となり、各テーブルが 1 セットのインタフェースのルーティングを処理します。

仮想ルーティングでは、それぞれルーティングテーブルとそれに関連するルートを完全に分離することができるので、関連するトラフィックフローは完全に別々となります。しかし、あるトラフィックが、個別のルーティングテーブル内のインタフェース間でフローする必要があると、ループバックインタフェースのペアを使用しなければなりません。（「4.6 仮想ルーティング」も参照してください。）

ループバックインタフェースパラメータ

以下は、ループバックインタフェースに指定できるプロパティです。

プロパティ	説明
Name	NetDefendOS における表示と参照用のインタフェースの論理名。
Loop To	これはペアのもう片方のループバックインタフェースの名前です。もう片方のインタフェースは Loop to プロパティ用にこのループバックインタフェースを持ちます。 各ペアにおいて、最初のインタフェースを作成するときには、Loop to プロパティは空白のままにしておきます。パートナーの作成後に設定します。
IP Address	ループバックインタフェースに割り当てる IPv4 アドレス。これは、「Ping」可能であり、ダイナミックに変換される接続に送信元アドレスとして使用できるアドレスです。このアドレスは、インタフェースに割り当てられた Network の任意の IP にできますが、ループバックペアのもう片方のインタフェースに割り当てられたアドレスと同じにはできません。
Network	ループバックインタフェースに割り当てるネットワークで、上記の IP Address が属するものです。これはループバックペアの片方のインタフェースと同じネットワークである必要はありません。
Enable IPv6	有効にすると、本オプションで、IPv6 アドレスとネットワークを入力できます。IPv4 がループバック設定に使用されなくても、IPv4 アドレスとネットワークを入力する必要があります。

ループバックインタフェースがどのようにルーティングテーブルで使用されるかによって、2 つのオプションのいずれかを選択できます。

- **Make the interface a member of all routing tables**
  main ルーティングテーブルに従って、このループバックインタフェースに到着するトラフィックが送信されます。このループバックインタフェースの IP アドレス用のルートが自動的にすべてのルーティングテーブルに挿入されます。

- **Make interface a member of a specific routing table**
  本オプションにより、このインタフェースの IP 用のただ 1 つのルートが自動的に特定のルーティングテーブルに挿入されます。そして、特定のルーティングテーブルだけがこのインタフェースに到着するトラフィックのルートルックアップに使用されます。

注意 ルーティングルールはテーブルセクションを上書きできます。
トラフィック用のトリガーとなる Routing Rule は、上記のルートルックアップの設定を上書きできます。

IP アドレスのためのルートだけが自動的に追加される

ループバックインタフェースが作成されると、自動的にルーティングテーブルにルートが挿入されますが、これは、ループバックインタフェースの IP アドレスプロパティによってのみ実現できます。他のルートは手動で追加する必要があります。例えば、インタフェースがインターネットへのアクセスを提供する場合に、ネットワーク all-nets にループバックインタフェースを関連付けるルートを手動で追加する必要があるかもしれません。

ループバックインタフェースの IP アドレス

ループバックインタフェースは、他のインタフェースタイプと同じように、IP アドレスを含めて設定します。Loopback Interface オブジェクトに割り当てられた IP Address プロパティに割り当てられる IPv4 アドレスへの注意事項は以下の通りです。

- IPv4 アドレスは架空のものを使用できますが、異なるアドレスでなければなりません。インタフェースペアのアドレスは同じネットワーク上に設定できます。
- ループバックインタフェースに割り当てられた IP アドレスは、IP ルールセットのエントリが指定するどのアドレス変換にも送信元アドレスとして使用されます。
- アドレス変換を使用していないなら、標準のループバック IPv4 アドレスの範囲にある IP にインタフェースの IP アドレスを設定することをお勧めします。これは 127.0.0.0 ～ 127.255.255.255 の範囲内にあります。例 : 127.0.1.1

ループバックインタフェースのための使用例

この使用例で、以下のように 1 つの保護されたローカルネットワーク LAN1 を持つ 1 つの D-Link ファイアウォールについて考えます。このネットワークへのルートは、RT1 と呼ばれるルーティングテーブルに含まれています。RT1 は、他のすべてのルーティングテーブルから分離し、Ordering パラメータは Only に設定されているルーティングテーブルです。

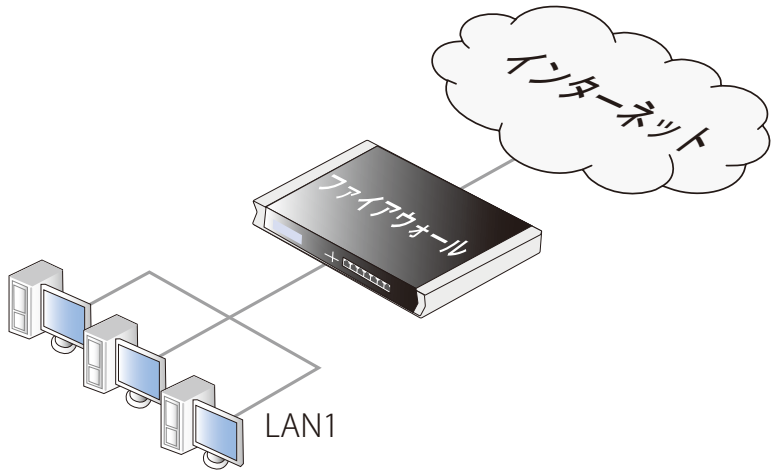


図 3-8　ループバックインタフェースのための使用例

また、ファイアウォールはインターネットに接続されていますが、インターネットへの all-nets ルートは完全に分けられていて、ルーティングテーブル RT2 も同様に分けられています。この状況では、RT1 には all-nets ルートが何もないので、LAN1 のクライアントがインターネットに到達する方法はありません。

LAN1 クライアントがインターネットにアクセスするためには、ループバックインタフェースを使用しなければなりません。その設定プロセスを以下の通り 3 つの部分にまとめることができます。

- 異なるルーティングテーブルにメンバシップを持つループバックインタフェースのペアを定義します。
- トラフィックをループバックインタフェースに送るルートを定義します。
- トラフィックがループバックインタフェースへ（から）フローすることを許可する IP ルールセットのエントリを定義します。

以下の図ではこの設定を示しています。

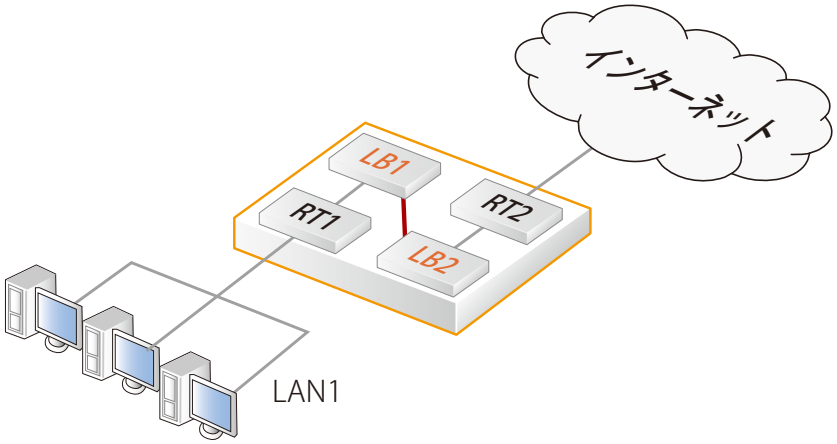


図 3-9　ルーティングテーブルを使用したループバックインタフェースの設定

これらの手順をより詳しく説明します。

1. 1 組のループバックインタフェース LB1 と LB2 を作成し、それぞれの Loop to パラメータでもう片方のインタフェースを指定します。また、ルーティングテーブル RT1 のメンバに LB1 を、RT2 のメンバとして LB2 を定義します。

2. 以下の 2 つのコンフィグレーションの追加が必要です。

i. all-nets トラフィック（インターネットへのトラフィック）をループバックインタフェース LB1 に送信するルートを RT1 に定義します。
ii. インターネットトラフィックが LAN1 から LB1 までフローすることを許可する IP ルールセットのエントリを作成します。

3. ループバックインタフェース LB1 を通じて送信されるインターネットトラフィックは、自動的にパートナー LB2 に到着します。LB2 が all-nets ルートを含むルーティングテーブル RT2 のメンバであるので、トラフィックをインターネットに送信することに成功します。

上記に加えて、以下の 2 つの設定を行う必要があります。

i. LB2 からインターネットまでトラフィックがフローすることを許可する IP ルールセットのエントリを定義する必要があります。これは、前のルールと同じ IP ルールセットに含めることも可能であり、ただ 1 つの外部 IP アドレスを利用する NAT ルールとなるでしょう。
ii. LB2 インタフェースに LAN1 トラフィックを送信するルートを定義する必要があります。これはインターネットから戻るトラフィックに必要です。

ループバックインタフェースとルーティングテーブルの関係図および、ここでの説明におけるネットワークは以下の通りです。

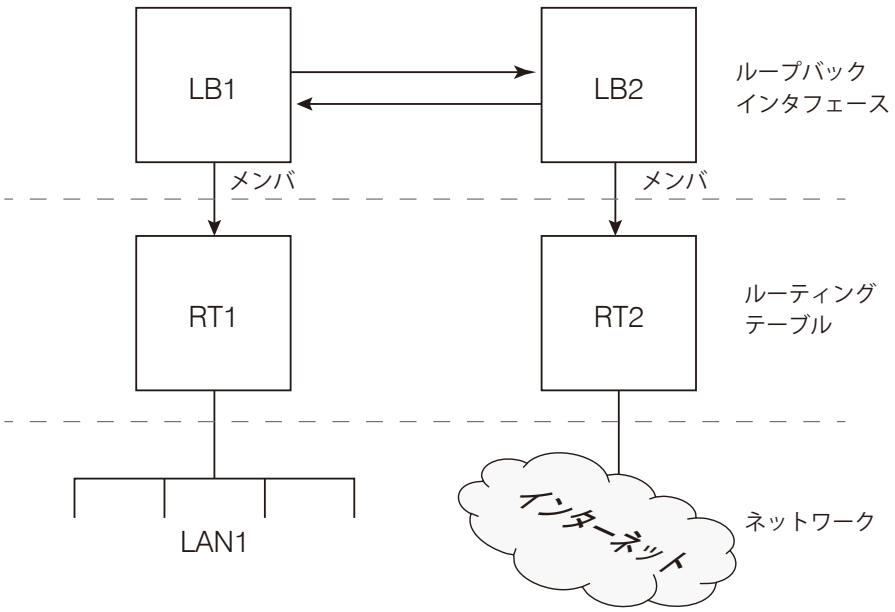


図 3-10　ループバックインタフェース設定の要素

例題 3.27

ループバックインタフェースのペアを作成する

この例題では、ループバックインタフェースのペア（RT1 ルーティングテーブルに所属する LB1 と RT2 ルーティングテーブルに所属する LB2）を作成する方法を示します。

LB1 には、IPv4 アドレス 127.0.6.1 とネットワーク 127.0.6.0/24 を設定します。LB2 には、IPv4 アドレス 127.0.5.1/24 とネットワーク 127.0.5.0/24 を設定します。

LB1 インタフェースに RT1 テーブルによって送信されたトラフィックは、LB2 インタフェースに行き、RT2 ルーティングテーブルを使用して送信されます。

CLI

A. 1 つ目のループバックインタフェースを作成します。

```
DFL-xxxx:/> add Interface LoopbackInterface LB1 IP=127.0.5.1 Network=127.0.5.0/24 MemberOfRoutingTable=Specific
            RoutingTable=RT1
```

B. 2 つ目のループバックインタフェースを作成します。

```
DFL-xxxx:/> add Interface LoopbackInterface LB2 IP=127.0.6.1 Network=127.0.6.0/24 LoopTo=LB1
            MemberOfRoutingTable=Specific RoutingTable=RT2
```

C. 今度は、最初のループバックインタフェースに戻り、LoopTo プロパティを設定します。

```
DFL-xxxx:/> set Interface LoopbackInterface LB1 LoopTo=LB2
```

3.4.10 インタフェースグループ

NetDefendOS インタフェースのセットは、インタフェースグループにまとめられます。そして、1 つの NetDefendOS コンフィグレーションオブジェクトのように動作して、セキュリティポリシーを作成する際に、1 つのグループの代わりに使用されます。例えば、グループが送信元インタフェースとして IP ルールセットのエントリに使用される場合、グループに含まれるいずれのインタフェースも、ルールに適合する可能性があります。

グループは通常のイーサネットインタフェースから構成されるか、または VLAN インタフェースや VPN トンネルなどの他のタイプから構成されることが可能です。さらに、グループのメンバは同じタイプである必要はありません。グループは、例えば 2 つのイーサネットインタフェースと 4 つの VLAN インタフェースの組み合わせで構成されることも可能です。

Security/Transport Equivalent オプション

インタフェースグループを作成する時、オプションの Security/Transport Equivalent を有効にすることができます。（初期値では無効です。）オプションを有効にするということは、接続が 2 つのインタフェース間で移動する必要があるかもしれない NetDefendOS ルール内の送信先インタフェースとしてグループを使用可能であることを意味します。例えば、インタフェースはルートフェイルオーバまたは OSPF によって変更が生じるかもしれません。

接続がグループ内の 1 つのインタフェースから別のインタフェースに移動し、Security/Transport Equivalent が有効になっている場合、NetDefendOS は新しいインタフェースを持つ NetDefendOS ルールセットに対して接続をチェックしません。

オプションが無効の場合、接続は、グループ内の別のインタフェースに移動されず、代わりに破棄されて、再オープンされる必要があります。この新しい接続は、次に NetDefendOS ルールセットに対してチェックされます。非常に遅い代替インタフェースなどいくつかの場合では、新しいインタフェースに特定の接続を許可することは賢明ではないかもしれません。

例題 3.28

インタフェースグループを作成する

CLI

```
DFL-xxxx:/> add Interface InterfaceGroup examplegroup Members=exampleIf1,exampleIf2
```

Web Interface

1. **Network > Interfaces and VPN > Interface Groups > Add > Interface Group** の順にメニューをクリックします。

2. 以下の通りの情報を入力し、グループを定義します。

General

- Name : 使用するグループ名を入力します。
- Security/Transport Equivalent : チェックして有効にすると、インタフェースは、接続がインタフェース間で移動する必要があるルールで送信先インタフェースとして使用されます。

Interfaces

- グループ内に定義するインタフェースを「Available」リストから選択し、「Selected」リストに移動します。

3. 「OK」ボタンをクリックします。

3.4.11 レイヤ 2 のパススルー

いくつかのインタフェースタイプでは、NetDefendOS は DHCP と non-IP プロトコルのいずれか、または両方にレイヤ 2 パススルーをする機能を提供します。初期値では両方とも無効ですが、以下のインタフェース構成タイプでは有効にできます。

- Ethernet
- VLAN
- Link Aggregation
- L2TPv3

また、これらのオプションが機能するために、直接インタフェースで透過モードは有効にされる必要があります。（これは、手動でスイッチルートを追加することによって、有効にするべきではありません。）

注意 L2TPv3 インタフェースは透過モードが有効である必要はありません。

NetDefendOS コンフィグレーションの L2TPv3 インタフェースには透過モードを有効にするプロパティがないので、DHCP または no-IP プロトコルパススルーが有効になる前に、有効にする必要はありません。

以下の例の通り、パススルーは個別または一緒に有効とすることができます。

例題 3.29

レイヤ 2 のパススルーを有効にする

この例題では、インタフェース if1 に対して transparent モード、DHCP パススルー、non-IP プロトコルを有効にします。

CLI

```
DFL-xxxx:/> set Interface Ethernet if1 AutoSwitchRoute=yes DHCPPassthrough=Yes NonIPPassthrough=Yes
```

Web Interface

1. **Network > Interfaces and VPN > Ethernet** の順にメニューをクリックします。
2. インタフェース if1 を選択します。
3. 以下を有効にします。
   - 「Enable Transparent Mode」を有効にします。
   - 「DHCP Passthrough」を有効にします。
   - 「L2 Passthrough for Non-IP Protocols」を有効にします。
4. 「OK」ボタンをクリックします。

3.5 ARP

3.5.1 概要

ARP（Address Resolution Protocol）は、ネットワーク層プロトコル（OSI レイヤ 3）アドレスをデータリンク層ハードウェアアドレス（OSI レイヤ 2）にマップし、IP アドレスを対応するイーサネットアドレスに解決するために使用されるプロトコルです。データネットワークでは、IPv4 アドレスを対応するイーサネットアドレスに解決するために使用されます。ARP は、OSI データリンク層（レイヤ 2）で動作し、転送のためにイーサネットヘッダによってカプセル化されます。

OSI レイヤ

OSI レイヤの概要については「付録 D OSI 参照モデル」を参照してください。

イーサネット上の IP アドレス指定

イーサネットネットワーク内のホストは、別のホストのイーサネットアドレス（MAC アドレス）を知っている場合だけ、そのホストと通信することができます。IP のようなより上位のプロトコルは IP アドレスを使用します。これらは、MAC アドレスのような下位のハードウェアアドレッシングスキームとは異なります。ARP は、その IP アドレスからホストのイーサネットアドレスを取得するために使用されます。

ホストが IPv4 アドレスを対応するイーサネットアドレスに解決する必要がある場合、ARP リクエストパケットをブロードキャストします。ARP リクエストパケットには、送信元 MAC アドレス、送信元 IPv4 アドレスおよび送信先 IPv4 アドレスがあります。ローカルネットワークの各ホストは、このパケットを受信します。指定された送信先アドレスを持つホストは、送信元 MAC アドレスを持ち ARP を生成したホストに ARP リプライパケットを送信します。

3.5.2 ARP キャッシュ

スイッチやファイアウォールといった、ネットワーク装置の ARP キャッシュは ARP の実行に重要なコンポーネントです。それは IP アドレスとイーサネット MAC アドレス間のマッピングを保存するダイナミックなテーブルから成っています。

NetDefendOS は他のネットワーク装置と同じように ARP キャッシュを使用します。最初に、ARP キャッシュは、NetDefendOS 起動時には空で、必要に応じてトラフィックフローとしてエントリと共に置かれます。

典型的な（最小限の）ARP キャッシュの内容は、以下の表のようになります。

タイプ	IP アドレス	イーサネットアドレス	Expire
Dynamic	192.168.0.10	08:00:10:0f:bc:a5	45
Dynamic	193.13.66.77	0a:46:42:4f:ac:65	136
Publish	10.5.16.3	4a:32:12:6c:89:a4	-

上記表の内容に関する説明は以下の通りです。

- ARP キャッシュ内にある最初の項目は、IPv4 アドレス 192.168.0.10 がイーサネットアドレス 08:00:10:0f:bc:a5 にマップされることを我々に通知するダイナミック ARP エントリです。

- テーブルの 2 個目の項目は、IPv4 アドレス 193.13.66.77 をイーサネットアドレス 0a:46:42:4f:ac:65 にダイナミックにマップします。

- 3 個目の項目は IPv4 アドレス 10.5.16.3 をイーサネットアドレス 4a:32:12:6c:89:a4 に結びつけるスタティック ARP エントリです。

期限欄

上記表内の 4 列目の Expire（期限）は ARP エントリが有効である期間を示すために使用されます。

例えば、最初の項目は Expire の値が 45 で、これはこのエントリが無効な場合、45 秒で ARP キャッシュから削除されることを意味します。トラフィックが、期限後に IPv4 アドレス 192.168.0.10 に送信される予定である場合、NetDefendOS は新しい ARP リクエストを発行します。

ARP エントリの期限の初期値は 900 秒（15 分）です。これは、「Advanced Settings」の「ARP Expire」設定を編集することで変更できます。「ARP Expire Unknown」設定は、NetDefendOS が到達できないメンバアドレスを記憶する時間を指定します。これは、NetDefendOS が連続でそのようなアドレスをリクエストしないことを保証するため使用されます。この設定の初期値は 3（秒）です。

例題 3.30

ARP キャッシュを表示する

ARP キャッシュの内容を CLI で表示します。

CLI

```
DFL-xxxx:/> arp -show
ARP cache of iface lan
 Dynamic 10.4.0.1   = 1000:0000:4009 Expire=196
 Dynamic 10.4.0.165 = 0002:a529:1f65 Expire=506
```

ARP キャッシュをフラッシュする

ネットワーク内のホストが同じ IP アドレスを保持したまま新しいハードウェアにリプレイスされる場合、MAC アドレスは新しくなります。NetDefendOS が ARP キャッシュ内にそのホストの古い ARP エントリを持っている場合、そのエントリは変更された MAC アドレスであるため無効となり、イーサネット上のホストに送信されたデータが決して送信先に到着しないということが発生します。

当然、ARP エントリ期限後は、NetDefendOS はホストの新しい MAC アドレスを学習しますが、時には更新を手動で動作させる必要があります。手動で更新を行う最も簡単な方法は、ARP キャッシュをフラッシュすることです。これは、キャッシュからすべてのダイナミック ARP エントリを削除し、接続ホストへの MAC/IP アドレスマッピングを検出するために NetDefendOS で新しい ARP クエリを発行させます。

フラッシュは CLI コマンドの arp -flush を使用して行われます。

例題 3.31

ARP キャッシュをフラッシュする

CLI で ARP キャッシュをフラッシュする方法を説明します。

CLI

```
DFL-xxxx:/> arp -flush
ARP cache of all interfaces flushed.
```

ARP キャッシュのサイズ

初期値では、ARP キャッシュは同時に 4096 個の ARP エントリを保持できます。これは多くのシナリオにおいて適切な値ですが、ファイアウォールに直接接続している非常に広域の LAN が複数ある場合、この値を大きく調節する必要があるかもしれません。これは **Network > ARP/Neighbor Discover** の「Advanced Settings」アイコンをクリックし、「ARP/Neighbor Discovery Settings」画面で「ARP cache size」設定を修正することで行われます。

いわゆる「ハッシュテーブル」は、ARP キャッシュ内のエントリを迅速に検索します。最大限の効率のためには、ハッシュはインデックスを付けているテーブルの大きさの 2 倍とするべきで、直接接続している最大広域の LAN が 500 個の IP アドレスを持っている場合は、ARP エントリハッシュのサイズを少なくとも 1000 エントリにする必要があります。**Network > ARP/Neighbor Discover** の「Advanced Settings」アイコンをクリックし、「ARP/Neighbor Discovery Settings」画面で「ARP Hash Size」設定を修正し、特定のネットワーク要件に反映することができます。

「ARP Hash Size VLAN」設定は、「ARP Hash Size」設定に似ていますが、VLAN インタフェースに対するハッシュサイズだけに反映されます。初期値は 64 です。

3.5.3 ARP パブリッシュ

概要

NetDefendOS は、IP アドレスが実際に接続するインタフェース以外のインタフェースへの IP アドレスパブリッシュをサポートします。オプションで、インタフェースの MAC アドレスをパブリッシュする代わりに特定の MAC アドレスをパブリッシュすることも可能です。NetDefendOS は、パブリッシュした IP アドレスのインタフェースで受信した ARP リクエストに対して ARP リプライを送信します。この機能は、NetDefendOS では ARP パブリッシュと呼ばれます。

摘要

ARP パブリッシュは、以下の項目などさまざまな理由で使用されます。

- ファイアウォールのインタフェースが複数の IP アドレスを持っているという印象を与えること。

  複数の分かれた IP 範囲が一つの LAN 上にある場合に有効となります。このゲートウェイアドレスがファイアウォールインタフェースでパブリッシュされる場合、各 IP 範囲にあるホストはその IP 範囲内のゲートウェイを使用する可能性があります。

- また、外部インタフェース上で複数のアドレスをパブリッシュし、NetDefendOS がこれらのアドレスに対するトラフィックをスタティックにアドレス変換できるようになり、プライベート IPv4 アドレスを持つ内部サーバに送信します。

- あまり一般的でない目的は、間違った方法で ARP に応答する近傍のネットワークデバイスを救済することです。

ARP パブリッシュを有効にする方法

ARP パブリッシュは以下の方法のいずれかで有効となります。

- パブリッシュされるアドレスを定義することで、インタフェースに対して ARP オブジェクトを作成することができます。

- スタティックルートが IPv4 アドレスまたはネットワークに作成される場合、すべてまたは選択インタフェースのアドレスまたはネットワークをパブリッシュするために Proxy ARP と呼ばれるルートオプションを使用できます。

  ARP オブジェクトを使用する場合、IP アドレスは 1 回に 1 つパブリッシュされるだけです。しかし、Proxy ARP 機能は全体のネットワークをパブリッシュできます。すべてのインタフェースに対し、1 回のステップでパブリッシュすることができます。

  Proxy ARP は、「4.2.6 プロキシ ARP」でより詳しく説明されています。

ARP オブジェクトプロパティ

ARP オブジェクトには、以下のプロパティがあります。

プロパティ	説明
Mode	ARP オブジェクトのタイプ。上で説明したとおり、以下のいずれかに設定できます。 - Static - ローカルな ARP キャッシュ内に固定のマッピングを作成します。 - Publish - 特定の MAC アドレス（または、このインタフェース）で IP アドレスを発行します。 - XPublish - 特定の MAC アドレスで IP アドレスを発行し、ARP 応答を含むイーサネットフレームの MAC アドレスについて偽ります。
Interface	ARP オブジェクトのローカルな物理イーサネットインタフェース。
IP Address	MAC/IP マッピング用の IP アドレス。
MAC Address	MAC/IP マッピング用の MAC アドレス。省略すると、イーサネットインタフェースの MAC アドレスを使用します。

ARP オブジェクトのための 3 つのパブリッシュモードオプション（Static、Publish、および XPublishare）は次で詳しく説明します。

Static モードの ARP オブジェクト

Static ARP オブジェクトは、NetDefendOS ARP キャッシュに対して、関連するイーサネットインタフェースの MAC アドレスに特定の IP アドレスを接続するマッピングを挿入します。

このモードは、外部デバイスのためにアドレスをパブリッシュするのではなく、むしろ外部デバイスに到達する方法を NetDefendOS 自身に伝えるためのものです。スタティックな ARP エントリは、特定の MAC アドレスを使用することで特定のインタフェースを通じて特定の IP アドレスに到達できることを NetDefendOS に伝えます。これは、NetDefendOS がそのアドレスとの通信を希望する場合に、ARP テーブルのスタティックなエントリを参照して、特定のインタフェースに存在する特定の MAC アドレスに到達することができるかどうかを判断することを意味します。

スタティックな ARP オブジェクトの最もよくある使用方法は、ある外部のネットワークデバイスが正しく ARP リクエストに応答していない状況にあって、不正な MAC アドレスを報告することです。無線モデムなどいくつかのネットワークデバイスには、このような問題があります。

さらに不正ユーザがネットワークに存在する場合、安全性を高めるために特定の MAC アドレスに対して IP アドレスをロックするため、または DoS 攻撃を避けるために使用されます。しかし、そのような保護はその IP アドレスに送信されるパケットに対してのみ適用されます。その IP アドレスから送信されるパケットには適用されません。

Publish と XPublish モード

Publish と XPublish モードでは、ARP オブジェクトは、外部デバイスに対してインタフェースでパブリッシュするために、IP アドレスと MAC アドレス間のアソシエーションを作成します。

MAC アドレスを指定しないと、関連付けられたイーサネットインタフェースの MAC アドレスが使用されます。

Publish と XPublish モードの違い

Publish と XPublish の違いを理解するためには、NetDefendOS が ARP クエリに応答する場合に、ARP レスポンスで返されたイーサネットフレームの中に 2 つの MAC アドレスが存在することを理解することが必要です。

1. 応答を送信するイーサネットインタフェースのイーサネットフレーム内の MAC アドレス。

2. このフレームに含まれている ARP レスポンス内の MAC アドレス。これは、(1) のイーサネットフレーム内の送信元 MAC アドレスと通常同じですが、必ずしも同じである必要はありません。

これらは ARP レスポンスを含むイーサネットフレームの以下の図に示されています。

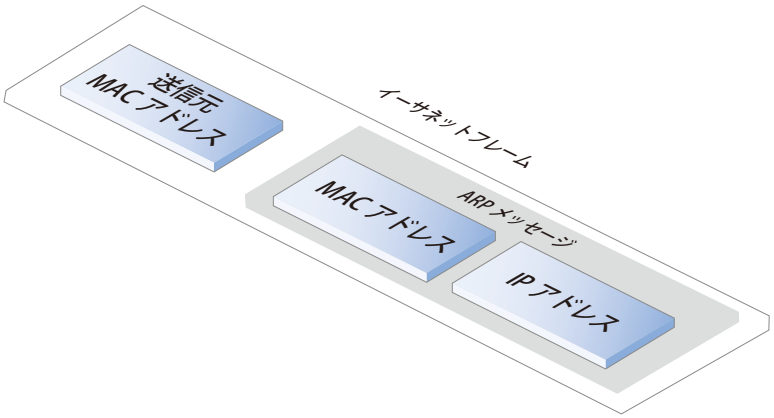


図 3-11　ARP パブリッシュイーサネットフレーム

Publish オプションは (1) のイーサネットフレームのアドレス用に、送信側インタフェースの本当の MAC アドレスを使用します。

まれに、いくつかのネットワークデバイスでは、応答内の両方の MAC アドレス（上記 1 と 2）が同じである必要があります。この場合、XPublish を使用して、応答内の両方の MAC アドレスをパブリッシュされた MAC アドレスになるように変更します。つまり、XPublish は ARP 応答の送信元アドレスを別のアドレスに置き換えます。

パブリッシュされた MAC アドレスが物理インタフェースの MAC アドレスと同じである場合、Publish と XPublish のどちらを選択しても違いはなく、結果は同じです。

ARP と Neighbor Discovery

IPv6 を使用した Neighbor 探索は IPv4 を使用した ARP と同等です。このため、NetDefendOS へのグラフィカルインタフェースでは ARP と Neighbor 探索は一緒の項目となっており、いずれを追加する場合も同じダイアログを使用します。Neighbor 探索に関する詳しい情報は、「3.2 IPv6 のサポート」を参照してください。

例題 3.32

ARP/ Neighbor Discovery オブジェクトを定義します。

「lan」インタフェースにおいて、IPv4 アドレス「192.168.10.15」とイーサネットアドレス「4b:86:f6:c5:a2:14」をスタティックにマッピングします。

CLI

```
DFL-xxxx:/> add ARPND Interface=lan IP=192.168.10.15 Mode=Static MACAddress=4b-86-f6-c5-a2-14
```

Web Interface

1. **Network > Interfaces and VPN > ARP/Neighbor Discovery > Add > ARP/Neighbor Discovery** の順にメニューをクリックします。

2. 以下を選択します。
   - Mode: Static
   - Interface: lan

3. 以下を入力します。
   - IP Address: 192.168.10.15
   - MAC: 4b-86-f6-c5-a2-14

4. 「OK」ボタンをクリックします。

3.5.4 Neighbor キャッシュ

ファイアウォールに直接接続されたデバイスに関する詳細情報を取得するために、キャッシュと呼ばれる機能を使用することができます。

- **Web インタフェースを使用する**
  Web インタフェースで **Status > SUB SYSTEMS > Neighbor Devices** の順にメニューをクリックし、キャッシュテーブルを表示します。
- **CLI を使用する**
  neighborcache コマンドを実行してキャッシュテーブルを表示します。
- **REST API**
  REST API を使用して、外部のコンピュータでソフトウェアを実行し JSON 形式のキャッシュコンテンツを取得します。「付録 I REAT API の使用方法」で詳しく説明します。

Neighbor キャッシュで表示される値

以下の値が Neighbor キャッシュから取得可能です。

項目	説明
Interface	これは外部デバイスに接続されたローカル NetDefendOS インタフェースです。
MAC Address	これは外部デバイスに接続された MAC アドレスです。ローカルコンフィグレーション内の最初のイーサネットアドレスオブジェクトの MAC アドレスとすることもできます。これには、デバイスと同じ MAC アドレスが含まれます。MAC アドレスの数字ではなく Ethernet Address オブジェクト名を表示するには、管理者は対象の MAC アドレスについてオブジェクトを作成しなければなりません。詳細は「3.1.3 イーサネットアドレス」を参照してください。
Vendor	通常、MAC アドレスに関連するベンダー名（会社名など）です。
IPv4 Address/IPv6 Address	外部デバイスの IPv4 または IPv6 アドレスです。
Authenticated User	デバイス接続時に NetDefendOS 認証が実行された場合、認証処理で使用されたユーザ名です。
DHCP Hostname	NetDefendOS が DHCP サーバとして IP アドレスを外部デバイスに割り当てた場合、この値が含まれます。ホスト名は、外部デバイスによって送信された、IP アドレスの DHCP リクエスト内の名前です。
Status	デバイスから（への）直近のトラフィックの有無によって、Active/Inactive どちらかの値となります。
Timeout	ステータスが「Inactive」の場合、最後のトラフィックが認識されてから経過した秒数となります。Web インタフェースでは、ステータスと共に分・秒の値で表示されます。

neighborcache CLI コマンドを使用する

上記の情報を表示するために、CLI で neighborcache コマンドを実行することができます。ただし、本コマンドですべての値を表示することはできません。

```
DFL-xxxx:/> neighborcache

Contents of Active Neighbor Cache [Active:1]
Idx Iface  HW Address        IP4 Address     State    Timeout Vendor
--- ------ ----------------- --------------- -------- ------- ------
1   wan    00-50-8B-E9-46-5E 203.0.113.5     Active   0       Mega Corp.
2   lan    40-45-D1-61-02-7B 192.168.188.1    Inactive 171954  D-Link
```

このデフォルトの表示では認証ユーザは表示されませんが、-users オプションを使用して表示することが可能です。

```
DFL-xxxx:/> neighborcache -users
```

同様に、-names オプションを使用すると DHCP ホスト名を表示することができます。

```
DFL-xxxx:/> neighborcache -names
```

3.5.5 アドバンスド ARP 設定

ここでは、ARP に関連するより詳しい設定について説明します。多くの場合、これらの設定を変更する必要はありませんが、いくつかの構成においては、修正が必要です。

すべての ARP アドバンスド設定の全リストは、「NetDefendOS CLI Reference」のオブジェクト名 ARPNDSettings にあります。

マルチキャストとブロードキャスト

マルチキャストとブロードキャストを含む ARP リクエストと ARP リプライは、ハードウェアレイヤのマルチキャストアドレスを使用する特定のロードバランシングと冗長デバイスを除き通常適切ではありません。

NetDefendOS の初期動作は、そのような ARP リクエストと ARP リプライの廃棄やログの出力を行うことです。この設定は **Network > Interfaces and VPN > ARP/Neighbor Discovery > Advanced Settings** の「ARP Multicast」および「ARP broadcast」で変更できます。

要求されていない ARP リプライ

対応する ARP リクエストが発行されていなくても、接続するネットワーク上のホストは、NetDefendOS に ARP リプライを送信することができます。これは Unsolicited ARP リプライ応答として知られています。ARP の仕様によると、受信者はこれらの ARP リプライのタイプを受け入れる必要があります。しかし、そのようなリプライは不正な接続の試みである可能性もあるため、NetDefendOS では、初期値ではそのようなリプライは廃棄して、ログに出力します。

この動作は、アドバンスド設定の「Unsolicited ARP Replies」設定を編集し、Accept に変更することで変更できます。

ARP リクエスト

ARP 仕様は、ホストが他のホストから受信した ARP リクエストのデータで ARP キャッシュを更新する必要があることを規定しています。しかし、この手順がローカル接続のハイジャックを容易にするため、NetDefendOS は通常これを許可しません。

RFC 826 仕様に準拠した動作にするためには、アドバンスド設定の「ARP Requests」を編集します。「ARP Requests」の値を「Drop（パケットを保存せずに廃棄）」に設定した場合でも、別のルールがリクエストを承認するように設定している場合、システムは、ARP リクエストにリプライします。

ARP キャッシュへの変更

取得した ARP 応答または ARP リクエストにより、ARP キャッシュ内のエントリが変更される場合もあります。この変更を許可した場合、ローカル接続のハイジャックを招く恐れがあります。一方で、変更を許可しない場合は、例えばネットワークアダプタが置き換えられた際に、古い ARP キャッシュエントリが期限切れになるまで新しいアドレスが許可されない状態になるといった問題が発生する可能性があります。

アドバンスド設定の「Static ARP Changes」によって、この動作を変更することができます。初期状態では、NetDefendOS は変更が行われることを許可していますが、すべての変更はログに出力されます。

ARP リプライまたは ARP リクエストの情報が ARP キャッシュ内のスタティックエントリと一致しない場合に、同様の問題が発生します。もちろん、この発生は決して許されません。しかし、アドバンスド設定「Static ARP changes」では、そのような状況をログに出力するかどうかを指定することができます。

送信元 IP 0.0.0.0

送信元 IP 0.0.0.0 を持つ ARP リクエストを処理することができるように、NetDefendOS を設定することができます。
そのような送信元 IP は、応答として決して有効ではありませんが、IP アドレスをまだ学習していないネットワークユニットは、ARP に「未指定の」送信者 IP に関する問い合わせをします。通常、これらの ARP リプライは、廃棄され、ログに出力されますが、アドバンスド設定の「ARP Query No Sender」設定を編集することで変更することができます。

イーサネットアドレスの一致

デフォルトでは、NetDefendOS は、イーサネットレベルにおける送信者アドレスが ARP データで報告されたイーサネットアドレスに適合していることが必要です。適合していない場合、そのパケットは廃棄され、ログが取得されます。その動作は、「ARP Match Ethernet Sender」設定を編集することで変更できます。

3.6 IP ルールセット

3.6.1 ルールセットの概要

詳細に IP ルールセットを検討する前に、NetDefendOS コンフィグレーションにおけるルールセットの基本的な概念について説明します。NetDefendOS セキュリティポリシーを定義する NetDefendOS のルールセットには以下の項目が含まれます。

• IP ポリシー

IP ルールセット内の IP Policy エントリは、ファイアウォールの通過を許可するトラフィックを決定するための主要な設定であり、アドレス変換の対象となるかどうかや、ALG やその他のサブシステムによるアプリケーションレベルでの処理についても定義します。ポリシーのネットワークフィルタに対しては、IPv4 または IPv6 アドレスを割り当てることが可能ですが、1 つのポリシー内で両方を設定することはできません。

IP Policy オブジェクトは異なる用法を持つ様々な形式があります。以下は利用可能なタイプです。

I. IP Policy - 一般的には IP ルールと同等であり、トラフィックに様々な幅のアクションを適用するようにトラフィックフィルタリングのオプションを提供します。

II. SLB Policy - サーバの負荷分散用のポリシーです。「11.3 サーバロードバランシング」で説明しています。

III. Stateless Policy - ステートレストラフィック用のポリシーであり、FwdFast のアクションを使用した IP Rule オブジェクトの代わりに使用することができます。詳しくは、「3.6.8 ステートレスポリシー」を参照してください。

IV. Multicast Policy - マルチキャストトラフィック用のポリシーであり、Multicast SAT のアクションを使用した IP Rule オブジェクトの代わりに使用することができます。詳しくは「4.8 マルチキャストルーティング」を参照してください。

IP Policy オブジェクトは、IP Rule オブジェクトによってバックグランドに実装され、1 つの IP Policy オブジェクトは複数の IP Rule に紐付けることができます。IP Policy オブジェクトは IP Rule オブジェクトよりも簡易的に利用することができるため、トラフィックフローの制御をする手段としてお勧めします。また、いくつかの NetDefendOS の新機能については、ポリシーのみで設定可能なものもあります。

• IP ルール

IP Rule オブジェクトは IP Policy オブジェクトの代替手段であり、IP Rule という構成要素に IP Policy オブジェクトが含まれる形となっています。IP Rule オブジェクトは、古い NetDefendOS バージョンとの互換性が必要とされる場合にのみ、使用される必要があります。

IP Rule の利用は無効化することが可能です（初期値は有効）。設定手順については「3.6.9 IP ルールの作成」を参照してください。

• Pipe ルール

トラフィックシェーピング実行のトリガとなるトラフィックを決定します。「11.1 トラフィックシェーピング」で説明します。

• ポリシーベースルーティングルール

このルールでは、トラフィックで使用されるルーティングテーブルを決定します。「4.3 ポリシーベースルーティング」で説明します。ルール内で設定するネットワークフィルタには IPv4 または IPv6 を指定できます（1 つのルールに両方指定することはできません）。

• 認証ルール

認証の実行をトリガするトラフィック（送信元ネットワーク / インタフェースのみ）を決定します。「第 9 章 ユーザ認証」で説明します。

ルールセットの基本的なフィルタリングプロパティ

管理者は、上記の NetDefendOS のルールセットを使用して、ファイアウォールを通過できるトラフィックの規定と、トラフィックの検証方法及び処理内容の設定を行います。

これらのルールセットのエントリは、適用するトラフィックタイプを決定するためのフィルタ条件の指定方法として、共通の項目を持っています。IP Policy オブジェクトなど、ルールセットの各エントリには、通常次のような必須のフィルタリング条件があります。

項目	説明
送信元インタフェース	ファイアウォールでパケットを受け取るインタフェースまたはインタフェースグループ。IPsec トンネルや VLAN インタフェースなどの論理インタフェースの場合もあります。any を指定するとすべてのインタフェースが含まれます。
送信元ネットワーク	パケットの送信元 IP アドレスを含むネットワーク。これは単一の IP アドレス、IP アドレスの範囲、またはネットワーク全体を表すことができるオブジェクトです。定義済みの all-nets オブジェクトですべての IPv4 アドレスを指定、または all-nets6 を使用してすべての IPv6 アドレスを指定することもできます。
送信先インタフェース	パケットがファイアウォールの送信元インタフェースまたはインタフェースグループ。送信元インタフェースと同様に、物理インタフェースまたは論理インタフェースどちらも指定することができます。any を指定するとすべてのインタフェースが含まれます。
送信先ネットワーク	パケットの送付先 IP アドレスが属するネットワーク。これは単一の IP アドレス、IP アドレスの範囲、またはネットワーク全体を表すことができるオブジェクトです。定義済みの all-nets オブジェクトですべての IPv4 アドレスを指定、または all-nets6 を使用してすべての IPv6 アドレスを指定することもできます。
サービス	対象となるプロトコルタイプを指定する Service オブジェクトです。定義済みの all_services を指定すると、すべてのプロトコルを意味します。 NetDefendOS は多くの定義済みサービスオブジェクトを提供しますが、管理者はカスタムサービスも作成できます。また、既存のサービスオブジェクトをサービスグループに集めることもできます。 詳細は「3.3 サービス」を参照してください。
Geolocation	IP ルールセットオブジェクトの IP Policy ファミリーでは、オプションの Geolocation Filter を使用することができます。このフィルタタイプでは、対応する地域に基づいた送信元／宛先 IP アドレスを指定します。本オプションが指定されていない場合、初期値ではすべての地域が指定されます。詳細は「3.6.3 Geolocation の使用」で説明します。

トラフィックフローのトリガとなるルールセットエントリについて、すべてのフィルタリング条件が論理的な AND 処理において一致しなければならないことに注意してください。一般的に、1 つのルールセットエントリの中でできる限り限定的なフィルタリング条件を設定し、想定するトラフィックのみがエントリのトリガとなるようにすることをお勧めします。これにより、安全性とシステムのパフォーマンス性が向上します。

セキュリティポリシーフィルタに使用される特別なオブジェクトと値

NetDefendOS ルールセットのフィルタリング条件を指定する場合、以下の定義済みオブジェクトや特別な値を使用することができます。

・ すべての IPv4 アドレスを指定

送信元 / 宛先ネットワークとして、アドレス帳の定義済みオブジェクトの all-nets を使用してすべての IPv4 アドレスを指定することができます。これは、IPv4 アドレス「0.0.0.0/0」と同等です。

・ すべての IPv6 アドレスを指定

送信元 / 宛先ネットワークとして、アドレス帳の定義済みオブジェクトの all-nets6 を使用してすべての IPv6 アドレスを指定することができます。これは、IPv6 アドレス「::/0」と同等です。1 つのルールセットエントリの中で IPv4 アドレスの all-nets と組み合わせて使用することはできません。

・ すべてのインタフェースを指定

送信元 / 宛先インタフェースとして、特別な値 any を使用することができます。すべてのインタフェースが一致することを意味します。

・ core インタフェース

宛先インタフェースを core とし指定することができます。core を指定した場合、ICMP Ping などのトラフィックが D-Link ファイアウォール自身に送信され、ファイアウォール自身で応答します。

NetDefendOS 自身で開始された新しい接続は、常に信頼された送信元であり初期値で許可されているため、明示的に IP ルールセットのエントリを設定する必要はありません。従って、core インタフェースは送信元インタフェースとして使用されません。信頼された NetDefendOS の接続には、IDP や Web コンテンツフィルタリングなどの NetDefendOS に必要とされる外部データベースへの通信も含まれています。

・ Service プロパティとしてすべてのプロトコルを指定

ルールセットエントリの Service プロパティは、すべての想定されるプロトコルを含む定義済みオブジェクト all_servies を指定することができます。

・ ローカルホスト IP アドレスを指定

定義済みのアドレスオブジェクト localhost を使用し、IPv4 ループバックアドレス 127.0.0.1 を指定することができます。IPv6 ループバックアドレス「：:1」は、定義済みのアドレス帳オブジェクト localhost6 を使用して指定することができます。

3.6.2 IP ポリシーの作成

IP ルールセットに含まれる IP Policy は、D-Link ファイアウォールで送受信されるトラフィックに対するセキュリティポリシーを課す方法として最も基本的な形式です。本セクションでは設定に IP Policy を追加する方法を説明します。

初期値の IP ルールセットは基本的にエントリが含まれない

NetDefendOS には main という名前の IP ルールセットがあります。NetDefendOS の初回起動時、IP ルールセットのエントリは設定れていないたため、すべてのトラフィックが破棄されます。トラフィックの通過を許可する（また、NetDefendOS が ICMP Ping リクエストに応答することを許可する）には、トラフィックを許可するために少なくとも 1 つの IP ルールセットのエントリ（通常は IP Policy オブジェクト）が存在する必要があります。

IP ルールの代わりに IP ポリシーを使用する

IP ポリシーは、他のより細かい IP ルールの上に位置するポリシーであり、IP ルールを使用する複雑性（特に ALG プロセスの設定における複雑性）を見えないようにしています。例えば、SAT 変換では 2 つ以上の IP ルールが必要となりますが、これは 1 つの IP ポリシーにより設定可能です。IP ルールはバックグラウンドで作成されますが、管理者は IP ポリシーオブジェクトのみを認識します。IP ルールは、古い NetDefendOS バージョンとの互換性を保つ必要がある場合にのみ、使用するべきです。

IP ポリシーを定義した際に作成された IP ルールを確認する必要がある場合は、次の CLI コマンドを使用します。

```
DFL-xxxx:/> rules
```

作成された各 IP ルールの詳細を確認するには、rule -verbose コマンドを使用できます。rules コマンドでは IP Rule オブジェクトのみを表示します。

IP ポリシーは特定の機能に対して使用する

一部の機能では IP Policy オブジェクトのみが使用可能で、IP ルールは設定できません。以下の項目が含まれます。

- トラフィックに対する Geolocation フィルタリング。オプションの 1 つとして、トラフィックの送信元 / 宛先となる世界の地域を指定することができます。
- 送信元 / 宛先ネットワークの FQDN Address オブジェクトを使用できます。詳細は「3.1.7 FQDN アドレスオブジェクト」を参照してください。
- DNS、IMAP ALG を使用できます。

IP ポリシーの作成

IP Policy オブジェクトには、以下の基本的なプロパティがあります。

- **Allow/Deny アクション**

IP ポリシーは特定のトラフィックタイプを許可または拒否します。Deny アクションは IP ルールの Drop アクションと同等です。

- **Source/Destination Interface/Network フィルタ**

このフィルタは IP ルールのフィルタと同様に、対象のトラフィックを特定します。

- **Geolocation**

このフィルタは、特定の定義済みの地域、または管理者が定義した特定の国のグループを識別する Geolocation Filter オブジェクトです。初期値は Everywhere（どの場所も除外しない）です。

- **Service**

ポリシーで使用するプロトコルのタイプを特定します。IP ポリシーで使用するオプションによっては、Protocol プロパティセットを持つサービスしか使用できません。該当するプロパティは後述します。

- **ポリシーオプション**

フィルタによって特定されたトラフィックは、以下に示す 1 つ以上のオプションの対象となります。

I. Logging - 有効または無効にします。

II. Anti-Virus - Anti-Virus ポリシーを選択できます。Protocol プロパティセットを含む Service オブジェクトを必要とします。

III. Web Content Filtering - 本オプションを有効にするには、Web Profile オブジェクトを作成し、ポリシーに関連付ける必要があります。さらに、Protocol プロパティを HTTP に設定した Service オブジェクトを使用しなければなりません。Web Profile オブジェクトでは、子供のオブジェクトとして定義された 1 つ以上の URL Filter オブジェクトを持つことができます。各 URL フィルタではブラックリストやホワイトリストとして URL または URL セット（ワイルドカードが許可されています）を指定できます。

IV. Application Control - アプリケーションコントロールは IP ポリシーで直接有効化することができます。すべてのタイプの Service オブジェクトを使用することができます。

V. File Control - 特定のファイルタイプをブロックまたは許可することができます。新しい File Control Profile オブジェクトを作成し、IP Policy オブジェクトに関連付けることで有効になります。ファイルコントロールは、HTTP、SMTP、POP3 および FTP プロトコルにだけ適用できます。Protocol プロパティが適切なターゲットのプロトコルに設定された Service オブジェクトを使用する必要があります。

VI. Advanced Actions - 拒否された接続に対する動作として Reject アクションを指定します。（acknowledgment が送信元ホストに送信されません。）

ALG オプションでは割り当てられた Protocol プロパティが必要

先に述べた通り、Protocol 値が正しく設定された Service オブジェクトが割り当てられている場合のみ、IP ポリシーで ALG を使用することができます。

例えば、IP Policy オブジェクトで Web Content Filtering (WCF) が有効化されている場合、割り当てられた Service オブジェクトの Protocol プロパティは HTTP に設定されている必要があります。適切に設定されていると、WCF を設定する Web Profile とポリシーとの紐づけが行われます。

アプリケーションコントロールは LAG を使用しないため、Service オブジェクトの Protocol プロパティを指定する必要がない IP ポリシーオプションの一つです。

トラフィックフローに対してルートの設定も必要となる

IP ポリシーによってインタフェース間のトラフィックが許可されている設定があったとしても、これらのインタフェースに対応する送信元と宛先インタフェース両方に対するルートがルーティングテーブルに存在する必要があることに注意しなければなりません。この内容については「3.6.4. IP ルールセットのプロセス」で説明します。

例題 3.33

DMZ への接続を許可するポリシーを設定する

この例題では、lan インタフェースのネットワーク lan_net から dmz インタフェースのネットワーク dmz_net までの、新しい HTTP/HTTP 接続が許可されます。どちらのネットワークもプライベート IP ネットワークと想定し、アドレス変換は行いません。
使用される Service オブジェクトは定義済みの http-all で、HTTP と HTTPS 両方のトラフィックを許可します。ここではトラフィックに対して ALG を使用しないため、Service オブジェクトの Protocol プロパティは HTTP に設定する必要はありません。
この例題では IP ポリシーの Source Translation を初期値の Auto にしておくことに注意してください。これにより、接続の送信元 / 宛先 IP アドレスがプライベート IP アドレスである場合、変換処理が実行されません。Auto 設定については別途「8.5 自動変換」XXX リンク更新 XXX で説明します。

CLI

```
DFL-xxxx:/> add IPPolicy Name=lan_to_dmz SourceInterface=lan SourceNetwork=lan_net DestinationInterface=dmz
            DestinationNetwork=dmz_net Service=http-all Action=Allow
```

Web Interface

1. **Policies > Firewalling > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name : lan_to_dmz
   - Action : Allow
   - Source Interface : lan
   - Source Network : lan_net
   - Destination Interface : dmz
   - Destination Network : dmz_net
   - Service : http-all
3. 「OK」ボタンをクリックします。

「Drop ALL」IP ルールセットエントリの作成

IP ルールセットにおけるどんな IP ルールまたは IP ポリシーにも一致しないトラフィックは、初期値で NetDefendOS が廃棄します。ただし、自動的に破棄されたトラフィックはログメッセージを生成しません。破棄された接続をログに出力するためには、すべての送信元 / 送信先ネットワーク / インタフェースへのトラフィックを破棄する明示的な IP ポリシーを定義し、IP ルールセットの最後の項目として置くことを推奨します。これは、「Drop-All」エントリとして言及されます。

注意 drop-all エントリ名にルールセットの名前を含める

複数の IP ルールセットを使用している場合があります。ログメッセージ内で簡単に識別できるように drop-all エントリの名前に IP ルールセットの名前を含めることをお勧めします。

例えば、ルールセット main における drop-all エントリに対しては「main_drop_all」などと名付けるべきです。

IP ルールセットエントリにおける IP アドレスは IPv4 または IPv6 とすることが可能

IP ルールセットエントリは、フィルタリングプロパティの送信元および送信先ネットワークとして IPv4 または IPv6 アドレスのいずれかをサポートしています。

ただし、送信元および送信先ネットワークの両方を IPv4 または IPv6 のいずれかに統一する必要があります。単一のルールセットエントリで IPv4 と IPv6 アドレスを組み合わせることはできません。このため、以下に示すように IPv6 を使用する場合、2 つの「Drop All」ルール（1 つは IPv4 用でもう 1 つは IPv6 用）が必要となります。

名称	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
DropAll	Drop	any	all-nets	any	all-nets	all_services
DropAll6	Drop	any	all-nets6	any	all-nets6	all_services

詳しくは、「3.2 IPv6 のサポート」を参照してください。

例題 3.34

「Drop All」IP ルールセットエントリの作成

この例題では、main IP ルールの最後に IP ポリシーを配置して、破棄された通信がログ出力されるように設定します。ログ出力は IP ポリシーで初期値で有効化されていますが、明確にするために例題の中では明示的に有効に設定しています。
拒否されたトラフィックに対しては変換処理が行われないため、IP ポリシーの Source Translation プロパティは初期値の Auto ままにしておくことができます。

CLI

```
DFL-xxxx:/> add IPPolicy Name=main_drop_all SourceInterface=any SourceNetwork=all-nets DestinationInterface=any
            DestinationNetwork=all-nets Service=all_services Action=Deny LogEnabled=Yes
```

Web Interface

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name : main_drop_all
   - Action : Deny
3. 以下を入力します。
   - Source Interface : any
   - Source Network : all-nets
   - Destination Interface : any
   - Destination Network : all-nets
   - Service : all_services
4. LOGGING & COMMENTS セクションで以下の設定をします。
   - Logging : ON
5. 「OK」ボタンをクリックします。

3.6.3 Geolocation の使用

NetDefendOS IP Policy オブジェクトでのみ利用可能である追加のトラフィックフィルタリングオプションが Geolocation です。この機能により、地理的な関連性によりトラフィックの送信元および / または送信先の IPv4 と IPv6 アドレスをフィルタリングできます。いくつかの IP アドレスは既知の地理的関連性を持たない可能性がありますが、この機能のターゲットとなります。

Geolocation 機能は NetDefendOS の基本的な機能の一部であり、この機能を使用するために特別なサブスクリプションは必要ありません。ここで使用される IP データベースは NetDefendOS に組み込まれており、NetDefendOS の新しいバージョンがインストールされると一緒に更新される可能性があります。

Geolocation の使用方法

geolocation 機能は以下の 2 つの方法で使用できます。

- 送信元 / 宛先 IP アドレスに Geolocation プロパティを設定し、一致するトラフィックを許可します。これは特定のエリアからのトラフィックを受け付けます。

- 送信元 / 宛先 IP アドレスに Geolocation プロパティを設定し、一致するトラフィックを破棄します。これは特定のエリアからのトラフィックを除外します。

Geographic エリアを選択する

IP Policy オブジェクトにフィルタとして選択されるエリアは、以下の 2 つのタイプのいずれかです。

- **定義済みのリージョン**

  NetDefendOS は広大な世界の地域の定義済みリストを提供します。これらの地域は以下の通りです。

  - Africa
  - Antartica
  - Asia
  - Europe
  - North America
  - Oceana
  - South America

  初期値では、どのフィルタも選択されていません。これは、すべての地域 (どこでも) が許可されていることを意味します。

- **管理者が定義した Geolocation フィルタオブジェクト**

  ターゲットの国を制御するために、管理者は、ターゲットとする 1 つ以上の国からなる Geolocation Filter オブジェクトを作成します。IP ポリシーの Geolocation プロパティの値としてこのオブジェクトを使用できます。

  Geolocation フィルタオブジェクトへの国の指定に加えて、または、国の代わりに、以下の 2 つのオプションをフィルタに加えることができます。

  i. Match Private Networks - これはプライベートネットワークに使用される IP アドレスを含みます。これは IPv4 ネットワーク 10.0.0.0/、172.16.0.0/12、192.168.0.0/16、および IPv6 ネットワーク fd00:: 8 を含みます。本オプションは、Geolocation とは直接関係がある訳ではなく、アドレス帳経由で実行され得ますが、利便性のために用意されています。

  ii. Match Unclassified Networks - これはパブリックである任意の IP アドレスにマッチしますが、既知の国との関係はありません。

Web インタフェースのフラグアイコンは、geolocation が設定されていることを示します。

Web インタフェースで表示される IP ルールセットのサマリには、geolocation が IP ポリシーに設定されていることを示すための個別の欄がありません。代わりに、Src Net と Dest Net 欄の IP ネットワーク値の右にフラグアイコンが表示されます。

例題 3.35

Geolocation フィルタを設定する

この例題では、架空の国である Hackerland から来るすべてのインターネットトラフィックを破棄する IP Policy オブジェクトを設定します。Hackerland だけを含む Geolocation Filte を最初に作成します。次に、送信元としてこのフィルタを使用する IP Policy オブジェクトを設定します。

さらに、IP ポリシーは国に関連付けられていない未知の IP アドレスから来るトラフィックを破棄します。

Hackerland は国の定義済みのリストに表示されません。ここでは例題の目的で使用しているだけであることに注意してください。

CLI

A. GeolocationFilter オブジェクトを作成する :

```
DFL-xxxx:/> add GeolocationFilter hackerland_filter Regions=HL MatchUnknown=true
```

B. 次に、このフィルタを使用する IP Policy オブジェクトを作成する :

```
DFL-xxxx:/> add IPPolicy Name=lan_to_dmztest SourceInterface=any SourceNetwork=all-nets DestinationInterface=any
            DestinationNetwork=all-nets Service=all_services Action=Deny Reject=No SourceGeoFilter=hackerland_filter
```

Web Interface

A. GeolocationFilter オブジェクトを作成する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: hackerland_filter
   - Selected リストに国 Hackerland を追加します。
   - Match unclassified networks を有効にします。
3. 「OK」ボタンをクリックします。

B. 次に、このフィルタを使用する IP Policy オブジェクトを作成する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: drop_hackerland
   - Action: Deny
   - Denied Behavior: Drop
   - Source Interface: any
   - Source Network: all-nets
   - Source Geolocation: hackerland_filter
   - Destination Interface: any
   - Destination Network: all-nets
   - Destination Geolocation: Anywhere
   - Service: all_services

3. 「OK」ボタンをクリックします。

3.6.4. IP ルールセットのプロセス

トラフィックフローには IP ルールセットエントリとルートが必要

NetDefendOS が初めて起動される時、IP ルールセットの初期値は通常空の状態であり、トラフィックフローを許可するためには、少なくとも 1 つの IP ルールセットエントリを追加する必要があります。また、IP ルールセットのエントリの追加以外にも以下の設定が必要です。

- パケットが宛先に到達するために、どのインタフェースでパケットが送信されるかを指定するルートが、NetDefendOS ルーティングテーブルに存在する必要があります。

  パケットを受信するインタフェース上で、トラフィックの送信元が見つかることを示す 2 番目のルートも必要です。

- トラフィックが送信元ネットワーク / インタフェースから宛先ネットワーク / インタフェースへ送信されることを許可する IP ルールセットのエントリ。

  通常、このエントリは IP Policy オブジェクトか、その変種（Stateless Policy など）です。あるいは、古い NetDefendOS バージョンとの互換性が必要となる場合は IP Rule を使用します。

インタフェースのネットワークアドレスオブジェクトが正確でなければならない

すべてのインタフェースに対して、main ルーティングテーブルに定義済みのルートが存在していることに注意してください。ただし、あるインタフェースに対する定義済みのネットワークアドレスオブジェクト（例えば wan_net など）は、そのインタフェース経由で送信される前に、正しくルートされるために適切な値が割り当てられている必要があります。

初期値の管理インタフェースには定義済みのネットワークがあり、IP アドレスオブジェクト（lan_net など）に対して割り当てられています。しかしながら、他のネットワークアドレスオブジェクトの初期値には 127.0.0.1（ループバックアドレス）が割り当てられており、トラフィックが IP ポリシーで送信できるようにネットワークが割り当てられなければなりません。

パケットフローの順序

これらのコンポーネントが使用される順番が重要です。はじめに既存のインタフェースを決定するためにルート検索が行われ、次に、NetDefendOS は、そのインタフェースからトラフィックが出て行くことを許可する IP ルールセットのエントリを検索します。ルールが存在しない場合、トラフィックは廃棄されます。

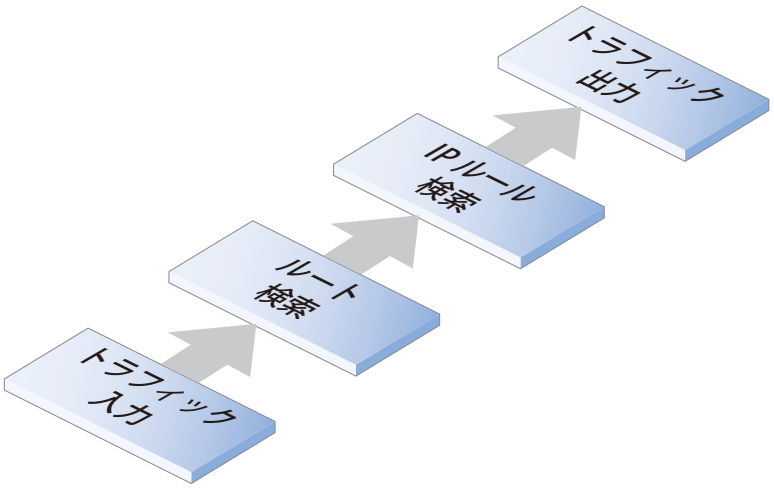


図 3-12　簡略化した NetDefendOS トラフィックフロー

このトラフィックフローに関する説明は、簡略化したものです。詳しくは、「1.3 NetDefendOS パケットフロー」を参照してください。

例えば、ルート検索の完了前に、NetDefendOS は、実際に送信元ネットワークからのトラフィックがそれを受信するインタフェースに到着していることをチェックします。これは、NetDefendOS がリバースルート検索を実行することで行われます。つまり、ルーティングテーブルを使用して、そのインタフェースにネットワークが検出されることを示すルートを検索します。

接続が双方向であり、それに関連する 1 組のルート（各方向に 1 つ）があれば、この 2 番目のルートは論理的に存在するはずです。

IP ルールセットのスキャン

D-Link ファイアウォールを通る新しい TCP/IP 接続を確立した時は、新しい接続のパラメータに合致するエントリが見つかるまで既存の IP ルールセットを上から下までスキャンします。最初に一致したエントリのアクションを実行します。

一致した IP ルールセットのエントリによって接続が許可されると、その新しい接続の確立作業を続けます。一致したエントリがステートフル（例えば IP ポリシーなど）である場合、新しい接続のエントリまたはステートが NetDefendOS の内部のステートテーブルに追加され、ファイアウォールを通る接続のオープン / アクティブな通信をモニタすることが可能になります。アクションが Deny（拒否）となれば、新しい接続は拒否されます。

注意 間違った順序のエントリは問題を起こすことがあります。

NetDefendOS は、最初に一致するエントリのために上から下まで IP ルールセットを検索するということを覚えておくことが重要です。IP ルールセットのエントリが無視されていると思われる場合、まず、対象のルールの上にある別のルールが始動していないことをチェックしてください。

ステートフルインスペクション

ステートフル IP ルールセットのエントリ（IP Policy オブジェクトなど）がトリガされた場合、その接続の後続のパケットは個別にルールセットに照らして評価する必要はありません。代わりに、ステートテーブルを高速にサーチして、各パケットが確立済みの接続に属しているかを判断します。

このアプローチは、ステートフルインスペクションとして知られていて、TCP などのステートフルプロトコルに適用されるだけではなく、「疑似接続」の概念を使用して、UDP や ICMP などのステートレスプロトコルにも適用されます。このアプローチは、IP ルールセットに対しての評価は接続の初期の段階で行われるだけであることを意味します。従って、IP ルールセットのサイズはスループット全体に対しほとんど影響を及ぼさないということになります。

ファーストマッチングルール

複数のルールセットのエントリが同じパラメータに一致する場合、全体のスキャンにおけるファーストマッチングルールが、接続をどう扱うかを決めるものとなります。

ノンマッチングトラフィック

Incoming パケットのうちルールセットのルールやステートテーブル上の既に開かれた接続のいずれにも一致しないパケットは、自動的に「Deny」アクション（ログ出力なし）で処理されます。上記の通り、一致しないトラフィックをログに出力するためには、ルールセットには最終的なルールセットのエントリとして、送信元 / 送信先ネットワーク「all-nets」と送信元 / 送信先インタフェース「all」を指定した「Deny」アクションを持つ「Drop-All」という明示的な IP ポリシーを用意しておくことをお勧めします。これにより、ログ出力は IP ルールに一致しないトラフィック用に有効にされます。

いくつかのアクションが TCP シーケンス番号を変更する

特定のネットワーク装置のタイプがあるいくつか状況では、TCP シーケンス番号は、データトラフィックがファイアウォールを横断する場合と同じにする必要があります。
そのため、Stateless Policy ルールセットのエントリ（FwdFast IP ルール）だけが TCP シーケンス番号を不変とすることを保証していることに注意してください。トラフィックが NetDefendOS を通じてフローするため、「NAT」などの他のアクションでは TCP シーケンス番号が変更されます。

ログへの出力

IP ルールセットのエントリが作成されると、初期値でログへの出力は有効になります。これは、エントリがトリガされる場合には常に、ログメッセージが生成されることを意味します。個々のルールセットエントリでログへの出力を無効にすることで、この動作を変更できます。

双方向接続

IP ルールセットを設定するときによくある間違いは、一方向ずつ２つのエントリを定義する、というものです。IP ルールセットのエントリがステートフル（IP Policy オブジェクトなど）である場合、通常、そのように設定する必要はありません。

この双方向フローの例外となるのは、Steteless Policy オブジェクト（FwdFast IP ルール）です。このルールが使用される場合、一方向のトラフィックフローのみが許可されます。双方向フローが必要な場合は、それぞれの方向に 1 つずつ、２つのステートレスエントリが必要です。

IDENT と IP ルールセットのエントリ

通常、IP ルールセットのエントリによってトラフィックが破棄される場合、送信元 IP に対しては何も応答が返されません。IDENT ユーザ登録名プロトコルに応じる場合など、拒否の回答をすることが必要となる例があります。そのような場合、IP Policy オブジェクトの Action に「Deny」を指定し、Deny Behavior に「Reject」を指定することができます（IP ルールのアクション「Reject」）。

3.6.5 複数の IP ルールセット

概要

NetDefendOS は、管理者がセキュリティポリシーを定義する場合に簡素化とより柔軟性を提供する複数の IP ルールセットを定義することを許可します。デフォルトの IP ルールセットは main として知られていて、NetDefendOS に常に存在しています。追加ルールセットは、必要に応じて管理者が定義し、名前をつけることができます。

複数の IP ルールセットの利点は以下の通りです。

- 管理者は、コンフィグレーションを理解しやすいように、1 つの大きな IP ルールセットを複数の、より小さく、より管理しやすいルールセットに細かく分けることができます。
- 1 つの名前付きの IP ルールセットをルーティングテーブルに関連付けすることができます。これは、各ルータで専用の IP ルールセットを関連付けることができるので、仮想ルーティングの実行をはるかに簡単にします。詳しくは「4.6 仮想ルーティング」を参照してください。
- 非常に大きいルールセットにおいて IP ルール検索速度を向上できます。大きいルールセットをいくつかの小さいセットに分解することで処理速度を向上します。Goto ルールは、特定のトラフィックタイプ用の新しいルールセットまでジャンプするのに使用され、Return ルールは、他のルールセットエントリが動作しないと、オリジナルのルールセットまでジャンプして戻るために使用されます。

新しい IP ルールセットが作成されると、IP ルールおよび / または IP ポリシーは通常の手順で追加することができます。

例題 3.36

IP ルールセットを作成する

この例題では、新しい IP ルールセットを dmz_rules という名前で作成します。このルールセットは後の例題でも使用されます。DMZ に関連するすべての IP ルールを含みます。

CLI

```
DFL-xxxx:/> add IPRuleSet dmz_rules
```

Web Interface

1. **Policies > Firewalling > Additional IP Rule Sets > Add > IP Rule Set** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: dmz_rules
3. 「OK」ボタンをクリックします。

Goto ルールと Return ルール

NetDefendOS は、異なる IP ルールセットにジャンプするルールと異なる IP ルールセットから戻ってくるルールの 2 つの特別なルールタイプを提供します。

- **Goto ルール**

  Goto ルールは、どんな IP ルールセットにも追加することができ、ルールセット内のどんな位置にも置くことができます。このルールには、送信元 / 送信先 インタフェース / ネットワークおよびサービスという通常のフィルタリングプロパティがあります。ルールセットのスキャンで一致が見つけられると、Goto ルールのアクションは、別のルールセットの先頭まで処理を移すという動作になります。

注意 Goto ルールは main ルールセットをターゲットにできない

Goto ルールはターゲットとしてルールセット main を使用しません。

- **Return ルール**

  Return ルールに遭遇すると、最後に実行された Goto ルールに続くルールセットエントリの位置に IP ルールセットのスキャンを戻します。特定の送信先 / 宛先 インタフェース / ネットワークおよびサービスの値で起動することができます。

注意 main ルールセットは Return ルールを含むことはできません。

NetDefendOS は IP ルールセット main に Return ルールを含めることを許可しません。また、Web インタフェースまたは CLI を使用した設定もできません。

複数のルールセットの検索処理

複数のルールセットが定義されると、それらが新しい接続のために処理される方法は以下の通りです。

- プライマリの main IP ルールセットは常に最初に送信元 / 送信先 インタフェース / ネットワークおよびサービスの一致を検索されます。
- main で起動するルールまたはポリシーが Goto ルールである時にだけ、ユーザ定義のルールセットはルールの検索に使用されます。Goto ルールは、管理者により定義された別の IP ルールセットを関連付ける必要があります。そして、トラフィックがその Goto ルールにマッチすると、ルールテーブル検索は新しいルールセットの先頭までジャンプします。
- 新しいルールセットの検索で一致を見つけられないと、接続は破棄されます。
- 新しいルールセットに一致が見つかると、一致するルールまたはポリシーが実行されます。これは別の Goto ルールであるかもしれません。その場合、ルール検索は別のルールセットの先頭にジャンプします。
- Return ルールに遭遇すると、スキャンは、前のルールセットの最後の Goto ルール直後にジャンプして戻り、再開されます。Goto ルールに遭遇せずに、また他のエントリも起動しないのであれば、スキャンは停止し、接続は破棄されます。

ループの回避

Goto ルールのシーケンスにより、スキャンがルールセット間でジャンプを繰り返すなどの無限ループをもたらすかもしれません。新しいコンフィグレーションが保存される時、NetDefendOS はそのようなロジックを検出します。潜在的にループを引き起こす可能性のあるロジックを検出すると、新しいコンフィグレーションは拒否されます。

ループ回避メカニズムは、速いコンフィグレーション展開を可能とするために効率的でなければなりません。そのため、正確かつ複雑なロジックにより欠陥を見つけるアルゴリズムを使用します。この場合、新しいコンフィグレーションが保存されるように、ルールのロジックを簡素化することが必要であるかもしれません。

簡単な複数のルールセットの例

以下の 2 個の簡単な IP ルールセットの表は、複数のルールセットの使用例を示します。main ルールセットには ExtraRules という管理者が定義したテーブルにジャンプする最初の Goto ルールがあります。

管理者が定義したルールセット ExtraRules は NAT と SAT ルールを含みます。どちらも起動しないと、最終的に Return ルールによりスキャンプロセスは Goto ルールに続く main 内のエントリに戻ります。この場合、それは main 内の 2 番目のエントリです。

mainIP ルールセット

#	Rule Type	Src Iface	Src Net	Dest Iface	Dest Net	Service
1	Goto ExtraRules	any	all-nets	core	172.16.40.0/24	all_services
2	Allow	any	192.168.0.0/24	core	172.16.0.0/16	all_services

ExtraRules IP ルールセット

#	Rule Type	Src Iface	Src Net	Dest Iface	Dest Net	Service
1	Allow/SAT	any	all-net	any	172.16.40.66	all_services
2	Allow/NAT	If2	176.16.0.0/16	any	all-nets	all_services
3	RETURN	If2	all-nets	any	all-nets	all_services

IP ルールセットの検索速度を向上する

ルールセット main が何千ものルールを含む時、ルールセット検索の速度は損なわれる可能性があり、これはファイアウォールの全体的な処理能力を下げてしまう可能性があります。代表的な症状は以下の通りです。

- ファイアウォールの CPU 負荷が連続して高い。
- （高い CPU 負荷の結果）Web インタフェースページのロード時間が異常に長くなる。

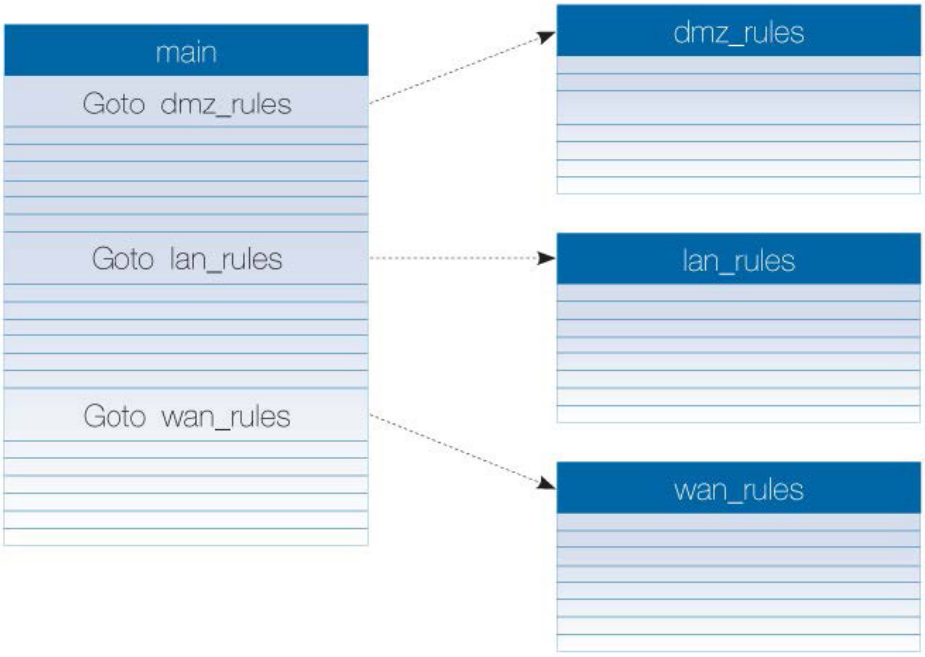
これらに対するソリューションは、大きいルールセットをいくつかの新しいルールセットに分割することです。通常、それぞれの新しいルールセットは特定のトラフィックタイプに関連するエントリを含みます。次に、少数の Goto ルールをルールセット main に追加して、それぞれを特定のトラフィックタイプに関連するルールセットに指定することができます。

例えば、IP ルールセット main において、Destination Network が dmznet、lannet、wannet のいずれかである数千のルールが含まれているとします。Destination Network に基づいたこれらのルールを分割して、dmz_rules、lan_rules および wan_rules という新しいルールセットに各グループを置くことが、はるかに効率的である場合があります。

3 つの Goto ルールが、これらの新しいルールセットを示すように main ルールセットに置かれます。

Goto rule set	Src Iface	Src Net	Dest Iface	Dest Net	Service
dmz_rules	any	all-nets	any	dmznet	all_services
lan_rules	any	all-nets	any	lannet	all_services
wan_rules	any	all-nets	any	wannet	all_services

新しい接続が宛先として dmz_net でオープンされると、NetDefendOS は最初に、main テーブルの検索を実行します。適切な Goto ルールが起動し、ルール検索は dmz_ip_rules と呼ばれるルールセットで継続します。以下の図は例題を示しています。



この例題ではルールを分割する方式として送信先ネットワークを使用しますが、インタフェースまたはサービスなどの別の要素を代わりに使用することもできます。

この手法は、マルチレベルのツリー構造を作成します。多量のデータを効率的に検索するための多くの状況で使用される技術です。ルールセットの最適なサイズは、個々の場合に応じて決定されます。とはいえ通常は、1,000 のエントリを超過するルールセットは許可しない方が良いでしょう。それ以上では、Goto ルールを使用するのが、ルールセット処理のスピードアップに役立ちます。

例題 3.37

Goto ルールを追加する

この例題では、ネットワーク dmz_net に行くすべてのトラフィックがルールセット dmz_rules を使用するように、Goto ルールを IP ルールセット main の終わりに追加します。IP ルールセット dmz_rules が既に作成されているものとします。

CLI

```
DFL-xxxx:/> add GotoRule SourceInterface=any SourceNetwork=all-nets DestinationInterface=any DestinationNetwork=dmz_net
            Service=all_services RuleSet=dmz_rules Name=goto_dmz
```

Web Interface

1. **Policies > Firewalling > Main IP Rules > Add > Goto Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: goto_dmz
   - RuleSet: dmz_rules
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: any
   - Destination Network: dmz_net
   - Service: all_services
3. 「OK」ボタンをクリックします。

Return ルールを追加する

前に述べたように、ルールセット main に Return ルールを追加することはできません。管理者が定義した IP ルールセットに追加できるだけです。フィルタリング基準を Return ルールに追加することはできますが、以下の例に示されているようにどんなトラフィックタイプも指定しないのが普通です。これは、Return ルールに遭遇すると、常に最後の Goto ルールが実行された直後に IP ルールセットのスキャンを戻すことを意味します。

例題 3.38

Return ルールを追加する

この例題では、Return ルールは管理者が定義した IP ルールセット dmz_rules の終わりに加えられます。これはすべてのトラフィックに適用されるため、Return ルールに遭遇すると、プロセスは、最後に実行された Goto ルールの直後のルールセットエントリに戻ります。

CLI

```
DFL-xxxx:/> cc IPRuleSet dmz_rules
```

ルールセットに Return ルールを追加します。

```
gw-world:/dmz_rules> add ReturnRule SourceInterface=any SourceNetwork=all-nets DestinationInterface=any
            DestinationNetwork=all-nets Service=all_services Name=return_dmz_to_main
```

初期値の CLI コンテキストに戻します。

```
DFL-xxxx:/main> cc
DFL-xxxx:/>
```

Web Interface

ルールセットになるように CLI コンテキストを変更します。

1. **Policies > Firewalling > Additional IP Rule Sets** の順にメニューをクリックします。
2. ルールセット dmz_rules を選択します。
3. **Add > Return Rule** を選択します。
4. 以下の情報を入力します。
   - Name: return_dmz_to_main
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: any
   - Destination Network: all-nets
   - Service: all_services
5. 「OK」ボタンをクリックします。

3.6.6 IP ルールセットフォルダ

IP ルールセットにおける大量のエントリ構成を整理するために、IP ルールセットフォルダを作成することができます。これらのフォルダはコンピュータのファイルシステム内のフォルダによく似ています。それらは、指定した名称で作成され、グループとして関連するすべてのエントリを含めるために使用されます。

フォルダを使用することで、管理者は簡単に IP ルールセットエントリを分割することができ、異なるフォルダにあるエントリに個別の特別なプロパティを与えることはありません。

NetDefendOS は、まるでそれらが IP ルールの一つのセットであるかのようにすべてのエントリを参照します。また、NetDefendOS はアドレス帳においてもフォルダ概念を使用します。そこでは、関連する IP アドレスオブジェクトが、管理者によって作成されたフォルダにグループ化されます。

3.6.7 構成オブジェクトグループ

NetDefendOS オブジェクトのグループを関連するコレクションに構成するのにフォルダの概念を使用することができます。これらのフォルダはコンピュータのファイルシステム内のフォルダの概念によく似ています。フォルダについては、「3.1.6 Address Book フォルダ」のアドレス帳に関連して説明します。また、これは IP ルールを体系化する場合に使用できます。

オブジェクトを構成するためのフォルダの代替方法として、構成オブジェクトグループを使用することができます。オブジェクトグループでは、NetDefendOS の GUI で表示する場合により簡単に関連性を理解してもらえるように、管理者が指定タイトル文字の下に構成オブジェクトを集めて、色分けすることができます。フォルダと異なり、それらは、個々のオブジェクトを見るために個別にフォルダを開く必要はありません。代わりに、すべてのグループ分けで全オブジェクトを直ちに見ることができます。

オブジェクトグループはアドレス帳オブジェクトで使用できるだけではなく、NetDefendOS オブジェクトがテーブルとして表示される多くの場合にも使用されます。また、テーブルの各行がオブジェクトのインスタンスを表示します。NetDefendOS アドレス帳における IP アドレスの分類や、IP ルールセットにおけるルールの体系化に最も一般的に使用されます。

注意 **オブジェクトグループは、コンフィグレーションの文書化を補助する**

オブジェクトグループは、NetDefendOS 構成のコンテンツを文書化する推奨方法です。

これは、初めてコンフィグレーションを参照する人に非常に役に立ちます。何百ものルールを含む IP ルールセットでは、オブジェクトグループによって、NetDefendOS 操作に関する特定のアスペクトに関連付けられたルールを迅速に識別することが可能になります。

オブジェクトグループと CLI

オブジェクトグループの表示機能は、コマンドラインインタフェース（CLI）とは関連がないことを意味しています。CLI を使用してオブジェクトグループを定義または編集することは不可能であり、それらは CLI の出力では表示されません。Web インタフェースを通じてすべてのグループ編集が行われる必要があります。次に、これについて説明します。

シンプルな例題

例として、内部ネットワークから Web サーフィンを許可する 2 つのルールを含む IP ルール「main」とその他のトラフィックすべてを捕捉してログ出力する 3 つ目の drop-all ルールについて考えてみます。

#	Name	Log	Src If	Src Net	Dest If	Dest Net
1	▶ lan-to-internet-http	✔	lan	lannet	wan1	al-nets
2	▶ lan-to-internet-dns	✔	lan	lannet	wan1	al-nets
3	■ drop-all	✔	any	all-nets	any	al-nets

注意 この例で使用される画面は、オブジェクトプロパティの最初の 2、3 個の欄だけを表示しています。

Web サーフィン用の 2 つの IP ルールにオブジェクトグループを作成します。これを以下の手順で行います。以下は、Main IP Rules 画面における設定例です。

1. 新しいグループに追加する最初のオブジェクトを選択して右クリックします。

2. メニューから「New Group」オプションを選択します。

3. グループには、タイトル行と唯一のメンバである IP ルールが含まれます。タイトル名は初期値で「new Group」となります。

#	Name	Log	Src If	Src Net	Dest If	Dest Net
(New Group)						
1	▶ lan-to-internet-http	✔	lan	lannet	wan1	al-nets
2	▶ lan-to-internet-dns	✔	lan	lannet	wan1	al-nets
3	■ drop-all	✔	any	all-nets	any	al-nets

また、初期カラーがグループ全体に割り当てられて、グループメンバにはインデントがつけられます。グループ内のオブジェクトは、全体のテーブルの位置を示すために同じインデックス番号を保持します。インデックスは、グループメンバシップによる影響を受けません。グループタイトル行は文字のラベルにすぎないため、インデックス番号は不要であり割り当てられていません。

グループプロパティの編集

グループのプロパティを変更するためには、グループタイトル行を右クリックしてメニューから「Edit」オプションを選択します。

2 つの機能を可能とするグループ編集ダイアログが表示されます。

- タイトルの指定
  グループのタイトルは、任意のテキストを設定することが可能であり、空行と新しい行を含むことができます。また、それがラベルとして使用されるので、グループ名がユニークである必要はありません。

- 表示カラーの変更
  どんなカラーもグループに選択することができます。カラーは定義済みの 16 個のカラーボックス、または 16 進数 RGB 値として入力したものから選択することができます。さらに、16 進数の入力が選択されると、フルスペクトラムカラーが表示され、マウスを使用してボックス内のカラーを選択することができます。

この例では、グループ名を「Web Surfing」に変更し、また、グループカラーも緑に変更します。変更後のグループ表示は以下の通りです。

#	Name	Log	Src If	Src Net	Dest If	Dest Net
Web Surfing						
1	▶ lan-to-internet-http	✔	lan	lan_net	wan1	all-nets
2	▶ lan-to-internet-dns	✔	lan	lan_net	wan1	all-nets
3	▶ drop-all	✔	any	all-nets	any	all-nets

追加オブジェクトの追加

新しいグループには通常 1 つのオブジェクトだけがあります。
グループのすぐ下にあるオブジェクトを右クリックし、「Join Preceding」オプションを選択すると、このグループに追加することができます。

画像例における 2 番目の IP ルールに対しこの操作を実行すると、以下の結果になります。

#	Name	Log	Src If	Src Net	Dest If	Dest Net
Web Surfing						
1	lan-to-internet-http	✔	lan	lan_net	wan1	all-nets
2	lan-to-internet-dns	✔	lan	lan_net	wan1	all-nets
3	drop-all	✔	any	all-nets	any	all-nets

グループにオブジェクトを追加するには、追加先のグループのすぐ下に位置するオブジェクトで「Join Preceding」を選択します。これは、次のセクションで詳しく説明しています。

オブジェクトの追加

オブジェクトの位置が、グループの上やグループの直下以外に位置している場合、下記手順が必要となります。

1. オブジェクトを右クリックして、「Move Up」オプションを選択します。
2. ターゲットグループのすぐ下の位置にくるようにインデックスを入力します。
3. オブジェクトが新しい位置に移動した後に再度オブジェクトを右クリックして「Join Preceding」オプションを選択します。

グループオブジェクトの移動

IP ルールなどのオブジェクトがグループに追加されると、移動処理のコンテキストは、そのグループになります。例えば、グループオブジェクトを右クリックし、「Move to Top」を選択すると、全体のテーブルの上部ではなく、グループの先頭にオブジェクトを移動させます。

グループの移動

グループは個別のオブジェクトと同様に移動できます。グループタイトル行を右クリックすることで、グループ全体を移動させるためのオプションメニューが表示されます。例えば、「Move to Up」オプションはテーブルの上部にグループ全体を移動します。

グループからの離脱

グループ内のオブジェクトで右クリックすると、「Leave Group」オプションメニューが表示されます。これを選択すると、グループからオブジェクトを削除し、そのグループの直下に場所を移動させます。

グループの削除

グループ名を右クリックすることで、「Ungroup」オプションが表示されます。これはグループを削除しますが、すべてのグループのメンバオブジェクトは残っています。グループタイトル行は表示されませんが、各メンバは普通のグループ化されていないカラーとインデントなしで表示されます。テーブル内の各オブジェクトのインデックス位置には影響はありません。

グループからメンバが削除され、グループメンバが残らない場合にも、グループは削除されます。グループに 1 つのメンバしかない場合に、このメンバがグループを離脱すると、グループはもう存在しなくなり、タイトル行はなくなります。

グループとフォルダ

フォルダを使用したオブジェクトの収集と、グループを使用したオブジェクトの収集を区別することが重要です。

どちらもオブジェクトのグループ化に使用されますが、フォルダはコンピュータのファイルシステムにおけるフォルダの概念と同様です。しかし、フォルダはグループの一部となることはできません。グループは関連する基本オブジェクトも一緒に収集しますが、フォルダはこのタイプとは違います。一方で、フォルダ内でグループを使用することは可能です。

NetDefendOS オブジェクトを最適にまとめるために、これらの機能をどのようにして最適に使用するかは管理者の設定次第です。

3.6.8 ステートレスポリシー

Stateless Policy は IP Rule と同等です。ステートレス接続を定義するのに両方の方式を使用できますが、Stateless Policy 方式を使用することをお勧めします。

ステートレス接続は、パケットが NetDefendOS のステートテーブルに接続の状態を設定されずに D-Link ファイアウォールを通過することを意味します。ステートフルインスペクションプロセスは迂回するので、ステートフル接続ほど安全ではありません。また、あらゆるパケットがルールセット全体に対してチェックされるので、トラフィック処理がより遅くなります。

一般的に、普通のステートフル接続と比べるとトラフィック処理が遅いため、FwdFast アクションがある Stateless Policy または IP ルールを使用することは推奨されません。しかし、特定のプロトコルがあるいくつかのシナリオではステートレス接続が必要な場合があります。

Stateless Policy と共に使用される Service オブジェクトの Protocol プロパティには何も設定する必要がないことに注意してください。Protocol プロパティは Stateless Policy では無視されます。

注意 初期値では、ログの出力は Stateless Policy で有効です。

他のポリシータイプと同様に、Stateless Policy オブジェクトのログへの出力が初期値で有効です。残念ながら、これは、ログメッセージがルールのトリガーとなる各パケットのために生成されることを意味します。これが通常望ましくないため、ポリシーへのログの出力を無効にする方がよいと言えます。

例題 3.39

ステートレスポリシーを作成する

この例題では、TCP パケットは内部ネットワーク lannet と dmznet ネットワーク間で送信されます。これは、実際の環境において、問題を引き起こすトラフィックタイプを考慮すると必要な設定となる場合があります。

FwdFast IP ルールと同様に、2 つの Stateless Policy オブジェクトがトラフィックフローの各方向に 1 つ必要です。カスタム Service オブジェクトを作成する代わりに、この例題では定義済みのオブジェクト all_tcp を使用します。

CLI

ステートレス TCP フローを lannet から dmznet まで許可する :

```
DFL-xxxx:/> add StatelessPolicy SourceInterface=lan SourceNetwork=lannet DestinationInterface=dmz
            DestinationNetwork=dmznet Service=all_tcp Name=stateless_lan_to_dmz Action=Allow
```

ステートレス TCP フローを dmznet から lannet まで許可する :

```
DFL-xxxx:/>  add StatelessPolicy SourceInterface=dmz SourceNetwork=dmznet DestinationInterface=lan
             DestinationNetwork=dmznet Service=all_tcp Name=stateless_dmz_to_lan Action=Allow
```

Web Interface

ステートレス TCP フローを lannet から dmznet まで許可する :

1. **Policies > Firewalling > Add > Stateless Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: stateless_lan_to_dmz
   - Action: Allow
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: dmz
   - Destination Network: dmznet
   - Service: all_tcp
3. 「OK」ボタンをクリックします。

ステートレス TCP フローを dmznet から lannet まで許可する :

1. **Policies > Firewalling > Add > Stateless Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: stateless_dmz_to_lan
   - Action: Allow
   - Source Interface: dmz
   - Source Network: dmznet
   - Destination Interface: lan
   - Destination Network: lannet
   - Service: all_tcp
3. 「OK」ボタンをクリックします。

3.6.9 IP ルールの作成

IP Rule では、IP Policy オブジェクトで作成したものと同じようなトラフィックフローポリシーを作成することができます。しかしながら、IP Rule は IP Policy と比較して複雑であり、古いバージョンの NetDefenOS との互換性で必要で必要な場合のみ使用します。

IP Rule オブジェクトは以下の 2 つの構成から成ります。
- ルールが対象とするターゲットのフィルタ条件
- トラフィックに対してルールが実行するアクション

IP ルールのフィルタ

IP ルールのフィルタ条件には以下の項目があります。
- 送信元インタフェース
- 送信元ネットワーク
- 宛先インタフェース
- 宛先ネットワーク
- サービス（トラフィックのプロトコルを識別）

IP ルールのアクション

対象トラフィックの一致により IP ルールが軌道した場合、次のいずれかのアクションが実行されます。

項目	説明
Allow	パケットの通過が許可されます。ルールは接続オープン時のみに適用されるため、「ステートテーブル」内のエントリで通信のオープンを記録します。この通信の残りのパケットは NetDefendOS の「ステートフルエンジン」を通じて通過します。
FwdFast	ステートテーブルにステートを設定せずに、パケットはファイアウォールを通過します。つまり、ステートフルインスペクションプロセスが迂回され、Allow や NAT ルールに比べて安全性は低くなります。すべてのルールセットに対して全パケットがチェックされるため、Allow ルールに比べてパケットの処理時間も遅くなります。 IP Rule オブジェクトを使用せずに、FwdFast 機能で Stateless Policy オブジェクトを使用して設定することができます。この内容については「3.6.8 ステートレスポリシー」で説明しています。
NAT	この機能は Allow ルールと似ていますが、Allow ルールに加えて動的な変換（NAT）を有効化されます。詳細は「第 8 章 アドレス変換」の「8.2 NAT（ダイナミックアドレス変換）」を参照してください。
SAT	NetDefenOS によりスタティックアドレス変換が実行されます。SAT ルールでは、ルールセットの Allow、NAT、FwdFast の IP Rule が一致する必要があります。詳細は「第 8 章 アドレス変換」の「8.4 SAT（スタティックアドレス変換）」を参照してください。
Drop	NetDefenOS により、直ちにパケットを破棄します。これは、送信者に応答を返す Reject とと比較して「丁寧ではない」バージョンのアクションです。攻撃者に攻撃の糸口を与えないように、通常、Drop を使用することが推奨されます。
Reject	Drop と似たような動作ですが、パケットが破棄されたことを送信元コンピュータに通知するために、TCP RST や ICMP Unreachable メッセージを返します。Drop IP ルールの「丁寧な」バージョンのアクションです。

例題 3.40

Allow IP ルールを作成する

この例題では、lannnet インタフェース上の lan ネットワークから、wan インタフェース上のすべてのネットワーク（all-nets）でオープンした HTTP 及び HTTPS 通信を許可するシンプルなルールを作成します。

CLI

```
DFL-xxxx:/> add IPRule SourceInterface=lan SourceNetwork=lannet DestinationInterface=wan
            DestinationNetwork=all-nets Service=http-all Action=Allow Name=lan_http
```

Web Interface

ステートレス TCP フローを lannet から dmznet まで許可する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name : lan_http
   - Action : Allow
   - Source Interface : lan
   - Source Network : lannet
   - Destination Interface : wan
   - Destination Network : all-nets
   - Service : http-all
3. 「OK」ボタンをクリックします。

activate 及び commit コマンドを実行後、設定の変更が保存されます。

IP Rule オブジェクトの使用を無効化する

IP Rule オブジェクトの使用を無効化することができます（初期値では有効です）。以下の例では、無効化する手順を示しています。IP Rule の使用を無効化した場合でも、コンフィグレーションの既存 IP ルールには影響ありません。既存の IP ルールは意図する機能を実行し、IP ルールセットの一覧に表示されたままとなります。ただし、新しい IP ルールを作成することはできなくなります。

例題 3.41

IP Rule オブジェクトの使用を無効化する

この例題では、コンフィグレーションに IP Rule を追加する機能を無効化します。

CLI

```
DFL-xxxx:/> set Settings MiscSettings AllowIPRules=No
```

Web Interface

1. **System > Advanced Settings >Misc. Settings** の順にメニューをクリックします。
2. Allow IPRules を無効にします。
3. 「OK」ボタンをクリックします。

3.7 アプリケーションコントロール

特定のアプリケーションに関連するトラフィックだけに適用するように IP ポリシーを設定できます。この種類の管理者の制御を必要とするかもしれないアプリケーションの例は、BitTorrent に関連するトラフィックです。アプリケーションタイプに基づいて IP ポリシーを適用することを NetDefendOS では Application Control と言います。

アプリケーションコントロールのサブシステムは、アプリケーションのシグネチャに関するデータベースを使用することで運用されます。それぞれのシグネチャは 1 つのタイプのアプリケーションに対応しています。全体のシグネチャデータベースは「NetDefendOS Application Control Signatures」というタイトルの別のドキュメントに記載されています。

アプリケーションコントロールは、サブスクリプションベースの機能で、アプリケーションコントロールが機能するようにサブスクリプションを購入している必要があります。詳細と、サブスクリプションが期限切れになった場合の動作については、「付録 A セキュリティ更新サービス」を参照してください。

アプリケーションコントロールを有効にする

アプリケーションコントロールは 2 つの方法で有効にできます。

- **IP Policy オブジェクトで使用するアプリケーションを直接指定します。**
  これは特定アプリケーションに関連しているデータフローを許可または拒否する基本的な方法です。これは簡単ですが、あまり柔軟性がないため、多くの場合アプリケーションをテストする時に使用されます。

- **IP Policy オブジェクトで使用するアプリケーションルールセットを関連付けます。**
  これは、アプリケーションコントロールを使用する上で推奨の方式であり、アプリケーションに関連しているデータフローを処理するより柔軟な方法を提供します。アプリケーションを扱う方法を定義する Application Rule Set を最初に作成し、次に、1 つ以上の Application Rule オブジェクトをそれに追加します。全体のルールセットは、IP Policy オブジェクトに関連付けられます。

アプリケーションコントロールを設定するこれらの 2 つの方式を、以降のセクションで説明します。

直接 IP ポリシーに関連付ける

以下の方法で直接アプリケーションコントロールを設定します。

- 特定の通信を対象とするフィルタパラメータのセットを指定し、IP Policy を作成します。
- Action に Allow を設定し、オプションで NAT の送信元アドレス変換を指定します。
- アプリケーションコントロールを有効にして、手動構成を使用するオプションを選択し、許可または拒否を行うアプリケーションを追加します。

  Deny オプションを選択しても、アプリケーションを 1 つも選択しないと、すべてが許可されます。Allow オプションを選択しても、アプリケーションを 1 つも選択しないと、何も許可されません。

例題 3.42

アプリケーションコントロールポリシーを指定する

この例題では *_groups シグネチャフィルタと一致する lan ネットワークから生じた接続を拒否する IP Policy を作成します。これらは、yahoo_groups や google_groups などのサイトへのアクセスを含んでいます。作成される IP ポリシーでは、初期値の送信元変換「Auto」が使用されます。これは、プライベート IP アドレスからパブリックアドレスへの通信に対して NAT 変換が実行されることを意味します。

CLI

まず、興味のあるアプリケーションのリストを作成するために、appcontrol コマンドを使用します。

```
DFL-xxxx:/> appcontrol -filter -name=*_groups -save_list
```

これはインデックス番号 1 を持つリストを作成します。その後リストは IP ポリシーに使用されます。

```
DFL-xxxx:/> add IPRule Action=Allow SourceInterface=lan SourceNetwork=lannet DestinationInterface=all
            DestinationNetwork=all-nets Service=all_services AppControl=Yes AC_AppAction=Deny AC_Applications=1
            Name=Allow_Comp
```

Web Interface

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 適切なルール名を指定します。ここでは allow_comp

3. 以下の情報を入力します。
   - Action: Allow
   - Service: all_services
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: all
   - Destination Network: all-nets

4. Application Control セクションで、次のように設定します。
- Application Control: ON
- Mode: Use Manual Configuration
- Application Action: Deny
- Add ボタンを使用して、アプリケーション定義から yahoo_groups および google_groups を選択します。

5. 「OK」ボタンをクリックします。

アプリケーションルールセットを使用する

前述の通り、アプリケーションをコントロールする推奨方法は、Application Rule Set オブジェクトを作成して、IP Rule または IP Policy オブジェクトにこれを関連させることです。

Application Rule Set オブジェクトには子供として 1 つ以上の Application Rule オブジェクトがあります。これらは、アプリケーション及びアプリケーションが NetDefendOS によって認識される時に行うアクションを定義しています。

アプリケーションルールセットには、Allow または Deny のどちらかの値を持っている Default Action プロパティがあります。Action が Allow に設定されると、ルールが明示的に拒否しない限り、すべてが許可されます。アクションが Deny に設定されると、ルールが明示的に許可しない限り、すべてが拒否されます。

アプリケーションルールセットを使用すると、特定のアプリケーションのデータを許可、または拒否するだけではなく、以下の追加コントロールも行うことができます。

- **認証設定**

  Allow アプリケーションルールでは、リクエストするクライアントが NetDefendOS に既に認証され、アプリケーションルール内に指定されているユーザ名の 1 つであるか、ルールに指定されているグループの 1 つに属していると、そのクライアントだけが接続を許可されます。さらに、特定のグループまたはユーザ名は、関連する IP ルールまたは IP ポリシーで使用されるソースネットワークアドレスオブジェクトに指定されるべきです。これは、本セクションの後で詳しく説明されます。

  Deny ルールでは、リクエストするクライアントが認証されていて、指定されているユーザ名の 1 つであるか、または指定されているグループの 1 つに属している場合、拒否されます。

  認証は、Identity Awareness を含む NetDefendOS Authentication ルールオブジェクトで利用可能なあらゆる方法を使用して実行されます。

  グループもユーザ名も Application Rule オブジェクトに指定されていない場合、認証は無視されます。

- **トラフィックシェーピング設定**

  定義済みの NetDefendOS Pipe オブジェクトはルールに関連付けできるため、pipe オブジェクトで指定された帯域幅の制限をデータフローの 1 方向または両方向に設定することができます。

  そのため、この機能により、帯域幅の制限を特定のアプリケーションや、（認証設定に関連して使用している場合は）そのアプリケーションを使用する特定のユーザまたはグループに適用することができます。

  Application Control Rule に Allow アクションがある場合にだけ、トラフィックシェーピングは関連します。

特定のグループまたはユーザ名にアプリケーションコントロールを適用する

時には、アプリケーションコントロールは、特定のユーザグループまたは特定の個人ユーザに適用される必要があります。以下を行うことで、これを実行できます。

- 関連する Application Rule オブジェクトの Authentication Settings プロパティに特定グループ、および / またはユーザ名のリストを指定します。

- 関連付けられる IP Rule または IP Policy の Source Network プロパティをアドレス帳の IP オブジェクトに設定する必要があります。以下のいずれかに当てはまります。
  i. アドレスオブジェクトは、プロパティ No defined credentials が有効化されています。
  ii. アドレスオブジェクトには User Auth Groups プロパティに定義された Application ルールと同じグループ、および / またはユーザ名があります。

例題 3.43

アプリケーションコントロールのルールセットを使用する

この例は、BitTorrent を使用したデータのアップロードおよびダウンロードの両方に対して、ユーザグループ rogue_users が使用する帯域を 0.25M ビットに制限します。以下の通りとします。

- グループ「rogue_users」におけるユーザのメンバシップは、認証プロセスで確立されます。RADIUS サーバを使用するか、または LDAP サーバに対する認証など他の手段を使用することによって行います。認証の手段については記載しません。
- Pipe オブジェクト「narrow_025_pipe」は、このデータフローを許可することを NetDefendOS に定義済みです。
- IP Policy オブジェクト「lan_to_wan_policy」は、保護された内部ネットワークからパブリックインターネットまでの接続を許可することを定義されています。
- IP ポリシー「lan_to_wan_policy」の Source Network プロパティは IPv4 アドレス帳オブジェクト「lan_users_net」に設定されています。

インターネットにアクセスするローカルネットワーク上のすべてのクライアントを認証しなければならないものとします。

CLI

BitTorrent 用のフィルタを作成するために「appcontrol」コマンドを使用します。これには UTP プロトコルも含めます。

```
DFL-xxxx:/> appcontrol -filter -application=bittorrent,utp -save_list
```

このフィルタリストは 3 番目に作成されたフィルタリストであり、リスト番号 3 が割り当てられるものとします。コマンドを使用するとすべてのフィルタを表示できます。

```
DFL-xxxx:/> appcontrol -show_lists
```

bt_app_list という名の ApplicationRuleSet を作成します。

```
DFL-xxxx:/> add Policy ApplicationRuleSet bt_app_list DefaultAction=Allow
```

CLI コンテキストを bt_app_list に変更します。

```
DFL-xxxx:/> cc Policy ApplicationRuleSet bt_app_list
DFL-xxxx:/bt_app_list>
```

ApplicationRule オブジェクトを追加します。

```
DFL-xxxx:/bt_app_list> add ApplicationRule Action=Allow AppFilter=3 UserAuthGroups=rogue_users
            ForwardChain=narrow_025_pipe ReturnChain=narrow_025_pipe Name=bt_app_rule
```

初期値の CLI コンテキストに戻します。

```
DFL-xxxx:/bt_app_list >  cc
DFL-xxxx:/>
```

この ApplicationRuleSet を IPPolicy に関連付けます。

```
DFL-xxxx:/> set IPPolicy lan_to_wan_policy AppControl=Yes AC_RuleSet=bt_app_list
```

最後に、アプリケーションルールと同じグループ名を持つ送信元ネットワークアドレスオブジェクト lan_to_wan_policy を設定します。

```
DFL-xxxx:/> set Address IP4Address lan_users_net UserAuthGroups=rogue_users
```

また、以下の通り、アプリケーションコントロールが機能するように許可することに注意してください。

```
DFL-xxxx:/> set Address IP4Address lan_users_net NoDefinedCredentials=Yes
```

Web Interface

まず、Application Rule Set を定義します。

1. **Policies > Firewalling > Application Rule Sets > Add > Application Rule Set** の順にメニューをクリックします。
2. 適切なリスト名を指定します。ここでは bt_app_list
3. Default Action を Allow に設定します。
4. 「OK」ボタンをクリックします。

次に、子供として Application Rule を定義します。

1. **Policies > Firewalling > Application Rule Sets > bt_app_list > Add > Application Rule** の順にメニューをクリックします。
2. ルール名を指定します。
3. Action に Allow を選択します。

4. Application Filter で Select Filter ボタンをクリックし、シグネチャの bittorrent と utp を追加します。（両方とも BitTorrent に必要です。）
5. Authentication Settings を選択し、グループ名 rogue_users を入力します。
6. Traffic Shaping Settings を選択して、Forward chain と Return chain の両方について、Selected リストに narrow_025_pipe を移動させます。
7. 「OK」ボタンをクリックします。

Application Rule Set を IP Policy に関連付けます。

1. **Policies > Firewalling > Main IP Rules > lan_to_wan_policy** の順にメニューをクリックします。
2. Application Control で以下の通り設定します。
   - Enable Application Control を ON に設定します。
   - Mode を Use Rule Set に設定します。
   - Application Rule Set を bt_app_list に設定します。
3. 「OK」ボタンをクリックします。

最後に、アプリケーションルールと同じ認証グループ名となるようにソースネットワークアドレスオブジェクト lan_to_wan_policy を設定します。

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。
2. lan_to_wan_policy を選択します。
3. User Auth Groups に rogue_users を入力します。
4. 「OK」ボタンをクリックします。

また、lan_to_wan_policy で No defined credentials を有効にすると、アプリケーションコントロールの動作も許可されることにご注意ください。

注意 BitTorrent は UTP を含む必要があります。

上記の例の通り、アプリケーションコントロールを BitTorrent をターゲットとして設定する時、2 つのシグネチャの bittorrent および utp を共に選択するべきです。

Strict HTTP 設定

アプリケーションコントロールが調べる多くのプロトコルは、HTTP プロトコル上で構築されます。HTTP 自身がアプリケーションコントロールによってブロックされている場合は、HTTP に構築されるプロトコルも同様にブロックされる可能性があります。この問題を解決するために、関連する Application Rule Set オブジェクトの Strict HTTP 設定を無効にすることができます。これにより、プロトコルタイプに対して決定を行う前に、アプリケーションコントロールは全体のプロトコル構造を評価します。

Maximum Unclassified Packets を変更する

NetDefendOS アプリケーションコントロールのサブシステムは、接続が分類不能かどうかを判断するまで接続中のデータフローを処理します。この判断をするために処理されるデータの最大量が、パケット数とバイト数の両方で NetDefendOS に指定されます。初期値では、これらの 2 つの値は以下の通りです。

- **Max Unclassified Packets:** 5
- **Max Unclassified Bytes:** 7500

これらの値のどちらかに到達すると、分類できないという判断をします。分類不可能として不正を示すフラグをつけられるプロトコルもあるので、管理者が処理されるデータの最大量を増やす必要がある場合には、以下の 2 つの方法のいずれかで値を変更することができます。

- NetDefendOS Advanced Settings でグローバルに変更できます。
- 現在のグローバル設定は、Application Rule Set オブジェクトの Use Custom Limits オプションを選択することで、ルールセットにあるすべてのルールに対して上書きされます。

アプリケーションコンテンツコントロール

ここまで、アプリケーションコントロールが BitTorrent などの特定のアプリケーションをターゲットとすることについて説明してきました。しかし、NetDefendOS は、ターゲットとするアプリケーションのコンテンツがトラフィックを許可するか、ブロックするか、あるいはログに出力するだけかを判断するアプリケーションコントロール内の更に詳細なレベルでフィルタリングを行うことができます。この機能はアプリケーションコンテンツコントロールと呼ばれます。

注意 アプリケーションコンテンツコントロールは CLI では設定できません。

アプリケーションコンテンツコントロールの設定機能を CLI では利用できません。Web インタフェースのみ、この機能の設定に使用されます。

アプリケーションコンテンツコントロールはアプリケーションルールセット内のアプリケーションルールオブジェクトで設定されます。ターゲットとするアプリケーションの特定のコンテンツを対象とするためにアプリケーションコンテンツコントロールを使用できます。この設定は、Facebook を対象とした例題で分かりやすく説明することができます。ルールは Facebook を対象とすることができ、特定のゲーム、アプリケーション、チャットまたはメッセージなど Facebook のコンテンツのタイプを対象とするようにアプリケーションコンテンツを使用できます。

深いコンテンツコントロールを使用しているルールセットに複数の IP ポリシーがあると、ルールセット内のより高いポリシーが低いものより先に起動する可能性があるため、すべてのポリシーが同じフィルタリングを実行する必要があるかもしれません。例えば、Chrome ブラウザだけが許可されている場合、アプリケーションコンテンツコントロールを使用しているすべての IP ポリシーは、HTTP user-agent エージェントが Chrome であるかどうかテストするべきです。

例題 3.44

アプリケーションコンテンツコントロール

この例題では、アプリケーションコンテンツコントロールを使用してアプリケーションルールが Chrome と Firefox ブラウザだけを許可する方法を示しています。

IP ポリシーと共に作成されたアプリケーションルールセットを関連させる手順は、例題に含まれませんが、前の例題と同じ手順に従います。

Web Interface

まず、Application Rule Set を定義する :

1. **Policies > Firewalling > Application Rule Sets > Add > Application Rule Set** の順にメニューをクリックします。
2. 適切なリスト名を指定します。ここでは browser_list
3. Default Action を Allow に設定します。
4. 「OK」ボタンをクリックします。

次に、このルールセットに Application Rule を定義する :

1. **Policies > Firewalling > Application Rule Sets > browser_list > Add > Application Rule** の順にメニューをクリックします。
2. Name に名前を入力します。
3. Action に Allow を選択します。
4. Application Filter の下で、Select filter を押します。
5. Search フィールドに http を入力します。
6. Matches specific applications を選択します。
7. Web ノードを開き、マッチするアプリケーションのリストから http を選択してください。
8. 「Select」ボタンを押して、フィルタダイアログをクローズします。

Application Content フィルタを定義する :

1. Content Control タブを選択します。
2. User Agent のアクションを Allow Selected に設定します。
3. 空白のフィールドに firefox、chrome を入力します。
4. 「OK」ボタンをクリックします。

最後に、前の例題に示されているように、関連するトラフィックで起動する適切な IP ポリシーにこの Application Rule Set を関連付けます。

先に説明した通り、前のルールが同じトラフィックに対して始動しない場合だけ、このポリシーとこのルールセットが始動します。

注意 文字列整合は、サブセットであり大文字と小文字を区別しません。

文字列整合をアプリケーションコンテンツコントロールに指定する場合、マッチング関数は、大文字と小文字を区別せず、常にサブセットは機能します。上の例題では、文字列 firefox を user_agent プロパティに指定します。agent フィールドが常にこの文字列を含んでいるため、Firefox のどのバージョンもトリガーとなります。

拡張ログ出力

アプリケーションコンテンツコントロールを使用する時、コンテンツ毎にログの出力を有効にすることができます。これは、ルールが特定の設定したコンテンツで始動する時に、固有のログメッセージが NetDefendOS によって生成されることを意味します。

例えば、アプリケーションコンテンツ内の user_agent がログ出力を有効にし、Firefox に Allow Selected という文字列を設定すると、Firefox ブラウザの使用が許可され、Firefox がルールを始動したことを示すログメッセージを生成します。文字列 firefox はログメッセージに含まれます。

アプリケーションコントロールへの拡張されたログ出力によって、生成されたログメッセージは、常に以下のイベントのいずれかになります。

- **application_content_allowed**
- **application_content_denied**
- **application_content**（アクションは Ignore でしたが、ログへの出力は Yes です。）

例題 3.45

ログへの出力を行うアプリケーションコンテンツコントロール

この例題では、アプリケーションコンテンツコントロールを使用して、Facebook へのアクセスは許可するが、Facebook の chat 機能は許可しない方法を示しています。ユーザが chat 機能を使用しようとする度に、ログイベントが生成されます。

IP ポリシーと共に作成されるアプリケーションルールセットを対応付けることは本例題に含まれませんが、前の例題と同様の手順に従います。

Web Interface

まず、Application Rule Set を定義する：

1. **Policies > Firewalling > Application Rule Sets > Add > Application Rule Set** の順にメニューをクリックします。
2. 適切なリスト名を指定します。ここでは facebook_list
3. Default Action を Allow に設定します。
4. 「OK」ボタンをクリックします。

次に、このルールセットに Application Rule を定義する：

1. **Policies > Firewalling > Application Rule Sets > facebook_list > Add > Application Rule** の順にメニューをクリックします。
2. Name で名前を入力します。
3. Action に Allow を選択します。
4. Application Filter の下で、Select filter を押して、フィルタダイアログを開きます。
5. Tag 下で Social Networking を選択します。
6. Matches specific applications を選択します。
7. Web ノードを開き、Facebook を選択します。
8. 「Select」ボタンを押して、フィルタダイアログをクローズします。

Application Content フィルタを定義する：

1. Content Control タブを選択します。
2. Chat では、Action には Deny、Log には Log を設定します。
3. 「OK」ボタンをクリックします。

最後に、前の例題に示されているように、関連するトラフィックで起動する適切な IP ポリシーにこの Application Rule Set を関連付けます。

データ漏洩がありうる

パケットの連続したストリームと特定のパケットを分析することにより行うアプリケーションコントロールは、アプリケーションを識別する前にシグネチャを使用して処理します。

これは、対象となるアプリケーションに属しているパケットすべてをとらえることは不可能であり、ブロックされたトラフィックが宛先に到着する場所にデータ漏洩が起こるのを避けられないことを意味します。しかし、IP ルールまたは IP ポリシーだけを使用する場合、トリガー接続のあらゆるパケットがブロックされ、少しのデータ漏洩もありません。

アプリケーションコントロールデータベースをブラウズする

CLI では、アプリケーションを定義するアプリケーションコントロールデータベースを検証するためにコマンド「appcontrol」を使用できます。パラメータを指定しないと、本コマンドはデータベースのサイズを表示します。例題は以下の通りです。

```
DFL-xxxx:/> appcontrol

Application library contents:
  842 application definitions.
  34 families.
  4 tags.
```

コマンドの後に Tab 補完を使用すると、すべての定義ファミリを表示します。例題は以下の通りです。

```
DFL-xxxx:/> appcontrol <tab>

antivirus/           file_transfer/     network_management/ thin_client/
application_service/ forum/             network_service/    tunneling/
audio_video/         game/              peer_to_peer/       unclassified/
authentication/      instant_messaging/ printer/            wap/
compression/         mail/              qosmos/             web/
database/            messenger/         routing/            webmail/
encrypted/           microsoft_office/  security_service/
erp/                 middleware/        telephony/
file_server/         music_player/      terminal/
```

これらのファミリは個々の定義から成ります。例えば、以下のコマンドを使用して、compression ファミリの 2 つの定義を参照してください。

```
DFL-xxxx:/> appcontrol compression

compression - Compression:

  ccp
  comp

2 application(s)
```

1 つの定義を参照するために、ファミリなしで個別の名前を使用できます。例えば、以下の通り、compression ファミリ内の comp の定義を表示します。

```
DFL-xxxx:/> appcontrol comp

comp - Compression

COMP protocol is used for data compression over PPP.

Family:     Compression
Risk Level: 1 - Very low risk
Tags:
Revision:   0
Enabled:    Yes
```

Tags と Risk Level は各定義に詳細を加えますが、定義階層の一部ではありません。Risk Level はこの特定のアプリケーションが引き起こす脅威の程度を示します。Tags はアプリケーションに関連するデータトラフィックに関する詳しい情報を提供します。例えば、High Bandwidth が代表的なタグです。

フィルタパラメータのいずれかを使用することで定義データベースを検索することができます。

- name
- family
- name
- risk
- tag

name パラメータは常に検索の上で 1 番速いことには間違いありませんが、ワイルドカードとしてアスタリスク「*」文字も使用できます。例題は以下の通りです。

```
DFL-xxxx:/> appcontrol -filter -name=* -family=webmail -risk=HIGH
```

先に説明した通り、-save_list オプションは、フィルタリストを保存して IP ルールや IP ポリシーと一緒に使用できるようにします。

フィルタを管理する

BitTorrent の設定について、上記のアプリケーションの例題で示した通り、CLI コマンド「appcontrol」は、CLI で ApplicationRule オブジェクトに使用される保存フィルタを作成するためにも使用することができます。例えば、以下は BitTorrent のために保存フィルタを作成します。

```
DFL-xxxx:/> appcontrol -filter -application=bittorrent,utp -save_list
```

-application パラメータは名前ごとに別のシグネチャを指定します。代わりに、「-name」パラメータを使用して、ワイルドカードを許可し、文字パターンの一致を検索しながらシグネチャ名を探す方法もあります。例えば以下のように指定することもできます。

```
DFL-xxxx:/> appcontrol -filter -name=bit* -save_list
```

プレフィックスの bit で始まる名前を持つすべてのシグネチャが選択されます。「-name」パラメータを使用して bittorrent と utp を選択するのは不可能です。以下の通りコマンドを使用してすべての保存フィルタを表示できます。

```
DFL-xxxx:/> appcontrol -filter -show_lists
```

すべての保存フィルタを削除するには、以下のコマンドを使用します。

```
DFL-xxxx:/> appcontrol -delete_lists=all
```

個別の保存フィルタは、-delete_lists= の後にフィルタ番号を指定することで削除されます。

すべてのシグネチャを選択する

管理者が、どのアプリケーションユーザがアクセスしているかを見つけるためには、すべてのシグネチャでアプリケーションコントロールを始動し、トラフィックをブロックする代わりに許可します。イベントが生成したログは検出されたアプリケーションを示します。

すべてのシグネチャを選択するには、Web インタフェースではチェックボックスを選択し、CLI では、ApplicationRuleSet オブジェクトにワイルドカードを使用します。アプリケーションコントロールを直接 IP ルールで使用する場合、CLI を使用できません。

シグネチャの継承

アプリケーションコントロールシグネチャには階層構造があり、許可も引き継がれることを覚えておくことが重要です。例えば http シグネチャです。管理者がすべての http トラフィックをブロックするアプリケーションコントロールを設定すると、facebook や dropbox などの http を使用するすべてのアプリケーションはブロックされます。

しかし、管理者が http シグネチャを許可するアプリケーションコントロールを設定すると、http を使用するすべてのアプリケーションが許可されます。例えば、DropBox のシグネチャは http シグネチャの子供であるため、http トラフィックを許可すると dropbox トラフィックも常に許可します。http を許可する一方で dropbox をブロックするのであれば、個別にブロックする必要があります。

リスクのガイドライン

以下は、各アプリケーションコントロールシグネチャのリスクパラメータが、管理者によってどのように参照されるべきかを示すガイドラインです。

プロパティ	内容
Risk Level 5	非常に高いリスク。特別な事情や要求が存在しない限り、このトラフィックをブロックすべきです。例えば、攻撃サイトとして知られる PHP-、CGI-、HTTPS- プロキシ。
Risk Level 4	高いリスク。このトラフィックを見直して、アクションをブロックまたは許可にするべきです。可能であれば Site-to-site トンネリングを使用するべきです。例えば、SSH、LDAP、Dropbox、RADIUS、類似のもの。
Risk Level 3	中間のリスク。このリスクレベルを持つシグネチャは、注意しないと、ネットワークセキュリティ、帯域幅利用、および会社の保全性に影響を与えます。例えば、Facebook や別のソーシャルネットワーク、Google Analytics と同様のアグリゲータ、P2P/ ファイル共有。
Risk Level 2	あまり高くないリスク。このリスクレベルを持つシグネチャは、ネットワークセキュリティ、そして / または、帯域幅利用に影響を与えます。例えば、ビデオストリーミングサイト、Java/ フラッシュゲームサイト。
Risk Level 1	低いリスク。ブロックする候補とできるシグネチャ。通常脅威ではありません。例えば、電子商取引サイト、ニュースポータル。

アプリケーションコントロールサブスクリプションの期限

既述のとおり、アプリケーションコントロールを使用するには購入したサブスクリプションが必要です。
サブスクリプションの期限が切れると、アプリケーションコントロールがどの IP Policy オブジェクトで設定されていても、以下の項目が起こります。

- サブスクリプション期限を示すコンソールメッセージが、システム起動や再構成の際に生成されます。
- アプリケーションコントロールは動作を継続し、NetDefendOS を通してトラフィックフローは送信され続けますが、トリガーが発生するとデータタイプは Unknown に設定されます。

  例えば、管理者が BitTorrent トラフィックを破棄するように設定しても、トラフィックを認識した後に Unknown トラフィックとして分類するため、もはや破棄は行われません。

- アプリケーションコントロールが起動する時はいつでも、ログメッセージ application_identified が生成されますが、トラフィックタイプは Unknown としてマークされます。同様に、タイプ Unknown は application_end ログメッセージにも現れます。
- さらに、ログメッセージ application_control_disabled が、アプリケーションコントロール起動時に生成されます。

Web インタフェースで **Status > Maintenance > License** の順にメニューをクリックしていくと、アプリケーションコントロールのサブスクリプションの現在の状態を参照できます。

3.8 スケジュール

いくつかのシナリオでは、どの機能を有効にするかだけではなく、いつ使用するかを制御することが必要です。

例えば、エンタープライズの IT ポリシーが、ある部署から外部への Web トラフィックは、業務時間内のみ許可するという規定であるかもしれません。また、特定の VPN 接続を使用した認証が、平日のみ許可される例もあるかもしれません。

NetDefenOS はこのタイムベースの要件に対し、以下のいずれかのコンフィグレーションオブジェクトにより対応することができます。
- Schedule Profile オブジェクト - シンプルなスケジュール機能です。
- Advanced Schedule Profile オブジェクト - より詳細なスケジュール機能を提供します。

いずれかのタイプのスケジュールを作成し、IP ルールセットエントリやトラフィックシェーピングルール、IDP ルール、ルーティングルールなどの様々な種類のコンフィグレーションオブジェクトの Schedule プロパティに割り当てることができます。割り当てたスケジュールにより、オブジェクトが有効 / 無効になる時間が決定されます。

重要 **システム日時は正確でなければならない**

スケジュールは正確な日付と時刻に依存するため、システム日付と時刻を正確に設定することが非常に重要です。これは、VPN トンネルの証明書の利用など他の機能に対しても重要です。
システム時刻が正しく設定されるように、時刻の自動同期機能を有効にすることをお勧めします。詳しくは、「2.2 システムの日時設定」を参照してください。

スケジュールプロファイル

Schedule Profileオブジェクトでは、スケジュールのシンプルなフォームを提供しています。各曜日で任意の時間帯を設定することが可能であり、開始・終了日も指定することができます。

Schedule Profile オブジェクトには以下のプロパティがあります。

項目	説明
Name	スケジュール名。これは、ユーザインタフェース表示や他のオブジェクトからスケジュールを参照する場合に使用されます。
スケジュール	スケジュールが適用される各曜日の時間です。最も近い時間になるように指定します。スケジュールは、1 週間の各曜日の各時間にチェックを入れるとアクティブになります。
Start Date	このスケジュールオブジェクトが開始する日です。指定しない場合、オブジェクトに割り当てられた後、すぐに適用されます。
End Date	このスケジュールオブジェクトが終了する日です。指定しない場合、スケジュールの終了日はありません。
Comments	オブジェクトの説明。

例題 3.46

タイムスケジュールされたセキュリティポリシーを設定する

ここでは、平日の就業時間のスケジュールオブジェクトを作成し、このオブジェクトを HTTP トラフィックを許可する IP ルールに割り当てます。

CLI

```
DFL-xxxx:/> add ScheduleProfile my_basic_schedule Mon=8-17 Tue=8-17 Wed=8-17 Thu=8-17 Fri=8-17 Sta-
            Date=2018-12-24
```

このスケジュールを使用する IP ポリシーを作成する :

```
DFL-xxxx:/> add IPPolicy Name=my_client_access_policy SourceInterface=lan SourceNetwork=lannet
            DestinationInterface=any DestinationNetwork=all-nets Service=http-all Action=Allow
            SourceAddressTranslation=NAT NATSourceAddressAction=OutgoingInterfaceIP Schedule=my_basic_schedule
```

コンフィグレーションの変更は、activate と commit コマンドを実行することで保存する必要があります。

Web Interface

スケジュールの作成

1. **Policies > Schedules > Add > Schedule Profile** の順にメニューをクリックします。

2. 名前とスケジュールを入力し、「OK」ボタンをクリックします。
   - Name : my_basic_schedule
   - Monday から Friday の 08-17 にチェックを入れます。

3. Start Date に 2018-12-24 を指定し、「Done」をクリックします。

IP ポリシーの作成

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。
   - Name : my_client_access_policy
   - Action : Allow

   FILTER
   - Service : http
   - Schedule : my_basic_schedule
   - Interface - Source : lan
   - Network - Source : lannet
   - Interface - Destination : any
   - Network - Destination : all-nets

   SOURCE TRANSLATION
   - Address Translation: NAT
   - Address Action: Outgoing Interface IP

詳細なスケジュールポリシー

dvanced Schedule Profile オブジェクトを使用すると、オブジェクトの配下に複数の Advanced Schedule Occurance オブジェクトを追加することができます。

これにより、Schedule Profile オブジェクトと比べて、より複雑なスケジュールを作成することができます。例えば Advanced Schedule Profile を使用した場合、複数の日を中断させず連続したものとして扱うことができます。
また、週単位の曜日による指定だけではなく、月単位のスケジューリングも可能です。

Advanced Schedule Profile には Name と Comments 以外のプロパティはありません。追加される Advanced Schedule Occurance オブジェクトに以下のプロパティが含まれます。

項目	説明
Start Time	スケジュールが開始する時刻（時、分）を指定します。
End Time	スケジュールが終了する時刻（時、分）を指定します。
Occurance	スケジュールの種類を指定します。Weekly（初期値）または Monthly から選択します。
Weekly	Occurance プロパティが Weekly に設定された場合、スケジュールの種類は週単位になります。
Monthky	Occurance プロパティが Monthly に設定された場合、スケジュールの種類は月単位になります。

例題 3.47

IP ポリシーに Advanced Schedule Profile を設定する

ここでは、内部クライアントからインターネットへの HTTP/HTTPS 通信によるトラフィックフローを許可する NAT を行う IP Policy に対して、Advanced Schedule Profile オブジェクトを設定します。月～金の 7:15-17:45 と、土日の 11:30-16:15 にアクティブになるようにします。

CLI

```
DFL-xxxx:/> add AdvancedScheduleProfile my_adv_schedule
DFL-xxxx:/> cc AdvancedScheduleProfile my_adv_schedule
DFL-xxxx:/my_adv_schedule> add AdvancedScheduleOccurrence StartTime=7:15 EndTime=17:45 Occurrence=Weekly Week-
            ly=1-5
```

2 つ目ののスケジュールを追加する :

```
DFL-xxxx:/> my_adv_schedule> add AdvancedScheduleOccurrence StartTime=11:30 EndTime=16:15 Occurrence=Weekly
            Weekly=6-7
DFL-xxxx:/> my_adv_schedule> cc
DFL-xxxx:/>
```

スケジュールを使用する IP ポリシーを作成する :

```
DFL-xxxx:/> add IPPolicy Name=http_during_office_hour SourceInterface=lan SourceNetwork=lannet
            DestinationInterface=any DestinationNetwork=all-nets Service=http-all Action=Allow
            SourceAddressTranslation=NAT NATSourceAddressAction=OutgoingInterfaceIP Schedule=my_adv_schedule
```

Web Interface

スケジュールの作成

1. **Policies > Firewalling > Schedules > Add > Advanced Schedule Profile** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。
   - Name: my_adv_schedule

3. Occurence タブを選択します。

4. **Add > Advanced Schedule Occurance** の順にメニューをクリックします。

5. 以下の情報を入力します。
   - Start Time : 7:15
   - End Time : 17:45
   - Occurance : Weekly
   - 有効化する曜日 : Monday-Friday

6. 「OK」をクリックして Occurrence 設定を閉じます。

2 つ目のスケジュールを追加する :

1. **Add > Advanced Schedule Occurance** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Start Time : 11:30
   - End Time : 16:15
   - Occurance : Weekly
   - Enable days : Saturday, Sunday

3. 「OK」をクリックして Occurance 設定を閉じます。

4. 「OK」をクリックしてスケジュール設定を終了します。

IP ポリシーを作成し、スケジュールに紐づける :

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name : me: http_during_office_hours
   - Action : Allow

3. FILTER セクションで以下の情報を入力します。
   - Source Interface : lan
   - Source Network : lannet
   - Destination Interface : any
   - Destination Network : all-nets
   - Service : http
   - Schedule : my_adv_schedule

4. SOURCE TRANSLATION セクションで以下の情報を入力します。
   - Address Translation : NAT
   - Address Action : Outgoing Interface IP

5. 「OK」をクリックします。

3.9 証明書

3.9.1 概要

X.509 規格

NetDefendOS は、ITU-T X.509 規格に準拠しているデジタル証明書をサポートしています。これは公開鍵暗号技術を持つ X.509 認証階層を使用して、鍵配布とエンティティ認証を行います。本ドキュメントにおける「証明書」とは、X.509 証明書を意味しています。

第三者に配布する場合、証明書は以下の 2 つの機能を実行します。
- 証明書のオーナは公開鍵を配布します。
- 証明書のオーナは ID を設定します。

証明書は、デジタル身分証明書として扱われます。公開鍵が所有者と考えられている人に本当に帰属するかどうかを立証するために公開鍵に識別子をリンクさせています。これを行うことで、受信者の名前とユーザ ID を持つ偽物の鍵を送る悪意のあるサードパーティによるデータ転送妨害を防ぎます。

証明書の内容

証明書は以下の項目で構成されています。
- 公開鍵
- 名前、ユーザ ID などのユーザの識別子
- デジタル署名は CA が検証した証明書に同封された情報を確認します。

上記の情報を結合することで、証明書は、信頼された機関による承認印を添付、連結されている識別子を持つ公開鍵となります。

NetDefendOS における認証書

証明書は Certificate オブジェクトとして NetDefendOS コンフィグレーションに保存されます。NetDefendOS には定義済みの証明書オブジェクトが常にあります。これは、ローカルな自己署名証明書 HTTPSAdminCert であり、HTTPS を使用した Web インタフェースのオープンセッションでブラウザに送信されます。また、SSL VPN でも使用されます。インストールされた証明書のリストは Web インタフェースまたは CLI で表示できます。

CLI を使用すると、コマンドは以下の通りとなります。

```
DFL-xxxx:/> show Certificate

    Name            Type   Comments
    --------------  -----  --------
    HTTPSAdminCert  Local  <empty>
```

HTTPSAdminCert は、HTTPS を使用した管理通信に使用される NetDefendOS のインストール済みの証明書です。この証明書は「self-signed（自己署名）」です。この証明書のプロパティを見るには、CLI コマンドを使用してください。

```
DFL-xxxx:/> show Certificate HTTPSAdminCert

Property          Value          Remarks
----------------- -------------- ---------
            Name: HTTPSAdminCert
            Type: Local
 CertificateData: (binary data)
      PrivateKey: (binary data)
       CRLChecks: Enforced
CRLDistPointList: <empty>
         PKAType: RSA            Read-only
            IsCA: No             Read-only
       Attribute: <empty>
        Comments: <empty>
```

注意 Certificates オブジェクトを CLI を使用して追加することはできません。

CLI では、証明書オブジェクトを作成するのに Add コマンドは使用されません。代わりに、証明書ファイルは、SCP を使用することで直接アップロードされ、アップロードにより直接オブジェクトが作成されます。また、Web インタフェースを使用してファイルをアップロードできます。

Certificate オブジェクトプロパティ

Certificate オブジェクトの主要なプロパティは以下の通りです。

- **Type**

Certificate オブジェクトの Type プロパティは以下の値の 1 つを取ることができます。

項目	説明
Local	これは、多くの証明書のタイプであり、証明書の公開鍵と秘密鍵の両方がファイアウォールに保存されることを意味します。 ローカル証明書では、署名付き、または署名なしとすることができます。それらは常に 2 個のファイルから成ります。ファイルタイプ .cer を持つ公開鍵ファイルとファイルタイプ .key を持つ秘密鍵ファイルです。
Remote	これは NetDefendOS のローカルにある公開鍵ファイルと CA サーバにある秘密鍵ファイルを持つリモート証明書のためのタイプです。多くの場合、証明書は、他の証明書を有効にするのに使用される CA 署名入りルート証明書です。 これらの証明書は「.cer」のファイルタイプを持つ 1 つの公開鍵ファイルだけから成ります。
Request	このタイプは現在、NetDefendOS では使用されません。

- **CRL Checks**

Certificate オブジェクトの CRL Checks プロパティは、証明書の CRL を NetDefendOS がチェックするかどうか、チェックを行うために CRL を検索できない場合の動作を決定します。設定可能なプロパティは以下の通りです。

項目	説明
Enforced	これは、初期値であり、証明書を認証に使用する前に、関連する CRL をチェックしなければならないことを意味します。CA サーバがオフラインである場合などに、関連 CRL を検索できないと、証明書は使用不能になり、認証は失敗します。 証明書が関連する CRL を持たないと、実施されたチェックは無視されます。NetDefendOS 管理接続に使用されるような自己署名入り証明書は、関連する CRL は存在しませんが、やはり初期値としてこの値が設定されています。
Conditional	いずれかの関連する CRL が利用可能であると、条件付きの CRL 検査が NetDefendOS によって実行されます。CA サーバがオフラインである場合などに、CRL がアクセスできなくても、証明書は使用されます。
Disabled	すべての CRL チェックを無効にします。証明書に関連している CRL があっても、その証明書は使用されます。

本セクションの後でさらに CRL について記載します。

- **CRL 配布ポイントリスト**

管理者は、CRL Distribution Point List コンフィグレーションオブジェクトに Certificate オブジェクトの CRL Distribution Point List プロパティを設定できます。これにより、CRL が有効であるかどうかをチェックする別の手段を提供します。詳しくは「3.9.3 CRL 配布ポイントリスト」を参照してください。

NetDefendOS に Certificates オブジェクトを作成する

Certificate コンフィグレーションオブジェクトは、NetDefendOS の論理的な証明書を定義するのに使用されます。そのようなオブジェクトが追加されると、関連する証明書ファイルのための入れ物として動作します。証明書ファイルは 2 つの方法のいずれかで証明書オブジェクトに関連付けられます。

- **外部証明書ファイルのインポート**

  管理者用ワークステーションのローカルなハードディスクに保存された証明書ファイルを NetDefendOS にインポートします。

- **自己署名証明書を作成する**

  Web インタフェースを使用して、NetDefendOS は自己署名証明書にファイルを作成できます。Web インタフェースでは、**Objects > Key Ring > Add > Certificate** の順にクリックしてメニューに行き、次に、新しい証明書のための Source オプションから Generate（RSA）を選択してください。これにより、以下のプロパティを自己署名証明書に指定することができます。

  i. 一般名

  ii. Certification Authority

  Certification Authority が有効であるなら、自己署名証明書は、他の証明書に署名して、CA ルート証明書として機能するために使用できることを意味します。

VPN トンネルを使った証明書

NetDefendOS においてよく使われている証明書は VPN トンネルを使ったものです。トンネルの両端で最も簡単で最も速くセキュリティを提供する方法は、事前共有鍵（Pre-shared Keys）を使う方法です。VPN ネットワークが成長するにつれ、事前共有鍵を使用する複雑さも増しています。証明書ははるかに大きいネットワークでセキュリティをよりよく管理する手段を提供します。

認証発行局（CA : Certification Authority）

認証発行局（CA : Certification Authority）は、他のエンティティに証明書を発行する信頼された機関です。CA は発行するすべての証明書をデジタルで署名します。証明書内の有効な CA 署名は証明書の保有者の識別子を検証し、証明書がどんなサードパーティによっても改ざんされていないことを保証します。

CA は発行するすべての証明書の情報が正しいことを確認する義務があります。さらに証明書の識別子が証明書の保有者の識別子に一致することも確認する必要があります。

ルート証明書とホスト証明書

証明書が認証に使用される場合、Host Certificate として参照されますが、NetDefendOS では時々 Gateway Certificate として参照されます。証明書は 2 個のファイル（公開鍵を含む「.cer」ファイルと秘密鍵を含む .key ファイル）から物理的に構成されています。両方のファイルを NetDefendOS にロードしなければなりません。

ホスト証明書が CA 署名付きであれば、CA 署名入りの Root Certificate を NetDefendOS にロードする必要があります。これは、CA の公開鍵を含む 1 つの「.cer」ファイルです。自己署名証明書には、対応するルート証明書はありません。

証明書チェーン

CA は他の CA に対しても証明書を発行します。CA はチェーンのような認証階層を形成します。最上位の CA はルート認証と呼ばれ、ルート CA が署名します。チェーン内の各証明書はチェーンのすぐ上にある証明書の CA が署名されます。しかし、ルート証明書は自身で署名（「自己署名」）されます。ルート証明書と最後の証明書間のチェーンにおける証明書は「Intermediate Certificate」（中間証明書）と呼ばれます。

証明書の経路は、ひとつの証明書から別の証明書へと証明書の経路を参照します。ホスト証明書の有効性を検証する場合、ホスト証明書から信頼されたルート証明書までのすべての経路はホスト証明書の有効性を立証する前に検証されている必要があります。このため、ルート証明書とホスト証明書の間のすべての中間証明書を NetDefendOS にロードする必要があります。

チェーンで結ばれた証明書は以下の NetDefendOS 機能でサポートされます。

- HTTPS を使用した Web インタフェースへのアクセス
- IPsec VPN
- SSL VPN
- TLS ALG

NetDefendOS では、証明書チェーンの最大の長さは 4 です。ローミングクライアントがある VPN シナリオでは、クライアントの証明書は証明書チェーンの末尾になります。

有効期間（Validity Time）

証明書は永遠に有効ではありません。各証明書には証明書の有効期間を示す 2 つの値があります。この有効期間が終了すると、その証明書は使用できなくなり、新しい証明書が発行される必要があります。

注意 システムの日付と時間は正確である必要があります。

証明書を使用する場合、NetDefendOS システムの日付と時間が正確に設定されていることを確認してください。証明書の問題（例 : VPN トンネル確立における問題）は不正確なシステム日付または時間により起こることがあります。

NetDefendOS の証明書キャッシュ

NetDefenOS はローカルメモリ内に Certificate Cache を保持することで、証明書が繰り返しアクセスされる場合の処理速度を向上します。NetDefenOS が再起動した場合のみ、このキャッシュが完全に削除・初期化されます。

そのため、証明書が追加・更新・削除された場合には NetDefenOS を再起動することが重要です。以下の CLI コマンドでシステムのシャットダウンを実行できます。

```
DFL-xxxx:/> shutdown
```

証明書失効リスト（CRL : Certificate Revocation List）

証明書失効リスト（CRL : Certificate Revocation List）は、有効期限以前にキャンセルされたすべてのデジタル証明書のリストです。通常、それらは、証明書がまだ有効であるかどうかを判断するためにアクセスされる外部サーバに保持されています。サーバから CRL をダウンロードし、NetDefendOS はリストに対して証明書の確認を実行します。ユーザ証明書の有効性を検証するこのような機能により、規模の大きいユーザコミュニティの管理において証明書セキュリティを簡素化することができます。

CRL は、すべての証明書ユーザがアクセスできるサーバ上に、LDAP または HTTP プロトコルを使用して、定期的に発行されます。失効にはいくつかの理由があります。1 つの理由は、証明書の鍵が何らかの方法で漏洩されたり、証明書の所有者が、会社を退職したなどでその証明書の使用による認証権限を失った場合です。理由が何であっても、サーバの CRL は更新され、複数の証明書の有効期間を変更することができます。

証明書には多くの場合 CRL Distribution Point（CDP）フィールドがあり、CRL がダウンロードされる 1 つ以上の URL を指定します。場合によっては、証明書にこのフィールドが含まれず、CRL の場所を手動で設定しなければならないかもしれません。NetDefendOS では、CRL Distribution Point List オブジェクトを指定し、コンフィグレーションの証明書にこれを関連付けることで設定します。詳しくは「3.9.3 CRL 配布ポイントリスト」を参照してください。

CA は、通常指定した間隔で、CRL をアップデートします。この間隔は CA の設定内容に依存します。一般的にこれは大体 1 時間から数日の間です。

NetDefendOS が特定の証明書に対して CRL をチェックするためには、外部の CA サーバにアクセスする必要があるかもしれません。このアクセスの許可に関する詳細は、「3.9.4 CA サーバアクセス」を参照してください。

証明書の信頼性

証明書を使用する場合、ファイアウォールは所定の CA によって署名された証明書を持つ相手を信頼します。認証を受諾する前に、以下の手順が証明書の有効性を検証するために行われます。

- 信頼できるルート CA までの認証経路を作成します。
- 認証経路内のすべての証明書の署名を検証します。
- 無効とされている証明書がないことを検証するために、各証明書の CRL を取得します。

ID リスト

証明書のシグネチャの検証に加えて、接続する IPsec クライアントを認証する場合に、NetDefendOS は ID リストオブジェクトも使用できます。ID リストは特定の IPsec トンネルを通してアクセスを許可されるすべての ID を含んでいます。ID は IKE ネゴシエーションの間、ピアによって送信され、このリモート ID に対して一致するトンネルが見つかった場合、クライアントが送信した証明書がその ID を含むかどうかを確認するためにチェックすることによって認証が実行されます。

証明書を持つ IPsec ID の使用については、「10.3.18 証明書を使用した ID リスト」を参照してください。

ルート証明書の再利用

NetDefendOS では、ルート証明書は VPN トンネル間で再利用されるグローバルな実体と見なされるべきです。1 つのルート証明書は NetDefendOS の 1 つの VPN トンネルに関連付けられてはいますが、同じそのルート証明書は他の様々な VPN トンネルでも再利用することが可能です。

他の考慮事項

証明書を使用する場合、下記要素にも留意しておく必要があります。

- 証明書失効リスト（CRL: Certificate Revocation List）を使用していると、CRL 配布点はパブリック DNS サーバを使用して IP アドレスに解決すべき FQDN（例 : caserver.example.com）として定義されます。そのため、この FQDN を解決できる少なくとも 1 つの DNS サーバを NetDefendOS に定義する必要があります。

  証明書に CRL 配布ポイントを含めることができますが、NetDefendOS は代替手段として CRL 配布ポイントを証明書に関連付ける機能を提供します。詳しくは「3.9.3 CRL 配布ポイントリスト」を参照してください。

- ホスト証明書ファイルとルート証明書ファイルを混在しないようにします。ルート証明書として NetDefendOS でホスト証明書を使用することはできませんが、意図せず、ルート証明書としてホスト証明書を使用することがありえます。

- ホスト証明書にはファイルタイプの「.key」および「.cer」を持つ 2 つの関連ファイルがあります。NetDefendOS がそれらを使用できるように、これらのファイル名は同じにする必要があります。例えば、証明書が「my_cert」の場合、ファイルは「my_cert.key」と「my_cert.cer」です。

3.9.2 証明書のアップロードと使用

証明書ファイルのアップロード

以下の 2 つの方法のいずれかで証明書ファイルを NetDefendOS にアップロードできます。

- Secure Copy（SCP）を使用したアップロード。
- Web インタフェースを使用したアップロード。

SCP アップロード

以下のコマンドラインは、代表的な SCP ユーティリティが、管理 IP アドレス 192.168.3.1 を持つファイアウォールに、「cert-1.cer」および「cert-1.key」という名称の 2 個のファイルから成る証明書をアップロードする方法を示します。

```
scp C:\cert-1.cer admin@192.168.3.1:certificate/my_cert
```

```
scp C:\cert-1.key admin@192.168.3.1:certificate/my_cert
```

NetDefendOS の証明書オブジェクト名は「my_cert」です。このオブジェクト名がコンフィグレーションの他のオブジェクトから参照されます。

証明書のアップロードの際、新しいオブジェクトによる更新を伴うため、全ての証明書アップロードの後にコンフィグの保存を行う必要があります。

グラフィカルインタフェースのアップロード

この例題では、Web インタフェースで証明書ファイルのインポートを示しています。

先に述べたように、証明書タイプによってアップロードするファイルは 1 つまたは 2 つになります。

- **ローカル証明書**
  これらの証明書は、ファイルタイプ .cer を持つ公開鍵ファイルとファイルタイプ「.key」を持つ秘密鍵ファイルから構成されます。

- **リモート証明書**
  Remote Certificate は CA によって発行され、ファイルタイプ「.cer」を持つ 1 つのファイル（公開鍵）で構成されます。秘密鍵は CA サーバに保持されます。NetDefendOS アップロード手順はこの 1 つのファイルをアップロードするものです。

例題 3.48

Web インタフェースで、証明書をアップロードする

この例題では、管理者用 PC のディスクに保存された 1 個以上の証明書ファイルをアップロードします。

Web Interface

1. **Objects > Key Ring > Add > Certificate** の順にメニューをクリックします。
2. 適切な証明書名を指定します。例 : my_cert
3. Source として Upload（初期値）を選択します。
4. Certificate ファイル選択を使用して、ローカルの公開鍵「.cer」ファイルを選択します。
5. 証明書がローカルである場合、Private Key ファイル選択を使用して、秘密鍵証明書ファイルを選択します。
6. 「OK」ボタンをクリックします。

アップロードした証明書を使用する

証明書が 1 度アップロードされると、それらは非揮発性 NetDefendOS メモリに保存されます。証明書を使用するには、明示的に NetDefendOS オブジェクトに関連付ける必要があります。例えば、証明書を使用する IPsec トンネルオブジェクトに Gateway および Root 証明書を割り当てなければなりません。

例題 3.49

証明書と IPsec トンネルを関連付ける

インポートした証明書を IPsec トンネルに関連付けします。

Web Interface

1. **Network > Interfaces and VPN > IPsec** の順にメニューをクリックします。
2. IPsec トンネルのプロパティを選択します。
3. Authentication を選択します。
4. Authentication Method で Certificate を選択します。
5. 正しい Gateway 証明書と Root 証明書を選択します。
6. 「OK」ボタンをクリックします。

3.9.3 CRL 配布ポイントリスト

NetDefendOS により管理者は 1 つ以上の NetDefendOS CRL Distribution Point List（CDPL）オブジェクトを定義できます。各リストは 1 つ以上のエントリで構成されます。サーバの URL を指定する各エントリは、証明書有効性を検証する Certificate Revocation List（CRL）を NetDefendOS に提供できます。

NetDefendOS で CDPL を使用するために、以下の手順を行います。

- 証明書を NetDefendOS にロードします。
- CRL 配布ポイントリストを定義します。
- 証明書に CRL Distribution Point List を関連付けます。

アソシエーションが 1 度証明書と CDPL の間で作成されると、その証明書のすべての CRL 検索が関連付けられた CDPL のエントリを使用して行われます。関連リストの最初のエントリがまず試行され、それが失敗すると 2 番目というように試行されます。証明書が自身に組み込まれた CDPL を持っているかどうかは関係ありません。NetDefendOS 内の関連する CDPL が常に使用されます。

証明書チェーンの場合は、チェーンの先頭の証明書だけを NetDefendOS で定義された CDPL に関連付ける必要があります。この CDPL は、チェーンにおけるトップレベルの証明書または低いレベルにあるどんな証明書に組み込まれたどんな CDPL より高い優先度を持ちます。

証明書に組み込まれたあらゆる CRL の代わりに管理者が定義した CDPL を使用することによって、利用可能な CA サーバへ確実にアクセスすることができます。

例題 3.50

CRL 配布ポイントリスト

この例題では、CDPL オブジェクト my_cdpl を作成して、1 つの URL http://crls.example.com を持つ証明書 my_cert に関連付けます。my_cert が既に NetDefendOS にアップロードされているものとします。

証明書の CRL checks プロパティは Enforced の初期値のままにします。これは、http://crls.example.com サーバから取得にしたリストに対して CRL チェックが常に行われることを意味します。

CLI

A. 配布ポイントリストを設定する :

最初に、配布ポイントリストを追加します。

```
DFL-xxxx:/> add CRLDistPointList my_cdpl
```

次に、対象の配布ポイントリストに CLI コンテキストを変更します。

```
DFL-xxxx:/> cc CRLDistPointList my_cdpl
```

その後、リストに配布ポイントを追加します。

```
DFL-xxxx:/my_cdpl> add CRLDistPoint URL=http://crls.example.com
```

最後に、CLI コンテキストを初期状態に戻します。

```
DFL-xxxx:/my_cdpl> cc
DFL-xxxx:/>
```

B. 証明書に配布ポイントリストを関連付ける :

```
DFL-xxxx:/> set Certificate my_cert CRLDistPointList=my_cdpl
```

Web Interface

A. 配布ポイントリストを設定する :

1. **Objects > CRL Distribution Point Lists** の順にメニューをクリックします。
2. **Add > CRL Distribution Point List** を選択します。
3. Name に my_cdpl を入力します。
4. CRL Distribution Points タブを選択します。
5. 「Add」を選択します。
6. URL に http://crls.example.com を入力します。
7. 「OK」ボタンをクリックして、配布ポイントを保存します。
8. 「OK」ボタンをクリックして、配布ポイントリストを保存します。

B. 証明書に配布ポイントリストを関連付ける :

1. **Objects > Key Ring** の順にメニューをクリックします。
2. 証明書 my_cert を選択します。
3. Manual CRL dist. points プロパティを my_cdpl に設定します。
4. 「OK」ボタンをクリックします。

3.9.4 CA サーバアクセス

概要

個別の認証局（CA）のサーバにアクセスすることで証明書の確認を行うことができます。IPsec トンネルの両側ではトンネルセットアップ時のネゴシエーションで互いの証明書を交換し、どちらかが受信した証明書を確認しようとするかもしれません。

証明書には確認する CA サーバを指定する URL（CRL 配布ポイント）があり、サーバアクセスは、HTTP 応答による HTTPGET リクエストを使用することで実行されます。（この URL は、正しくは FQDN（Fully Qualified Domain Name）と呼ばれます。）

証明書が配布ポイントを持たない場合、個別に NetDefendOS で CRL Distribution Point List オブジェクトを指定して、コンフィグレーション内の証明書にこれを関連させることで定義できます。詳しくは「3.9.3 CRL 配布ポイントリスト」を参照してください。

CA サーバタイプ

2 つのタイプの CA サーバがあります。

- **商用の証明書を発行する会社の 1 つで動作するコマーシャル CA サーバ**
  これらはパブリックインターネット上でアクセス可能で、それらの FQDN はパブリックインターネットの DNS サーバシステムを通じて解決されます。

- **同じ組織が設定する VPN トンネルで動作するプライベート CA サーバ**
  プライベートサーバの IP アドレスは、明示的に登録しない限り、パブリックの DNS システムに知られることはありません。さらに、内部の DNS サーバに登録しない限り、内部のネットワークに知られることはありません。

アクセスへの配慮すべき事項

CA サーバアクセスが成功するように、以下の注意事項について考慮されるべきです。

- VPN トンネルのいずれか一端が CA サーバに検証リクエストを送信する可能性があります。
- 証明書の検証リクエストが発行されるためには、まず証明書の CA サーバの FQDN が IP アドレスに解決される必要があります。

以下のシナリオが考えられます。

1. CA サーバは、D-Link ファイアウォールの背後のプライベートサーバであり、トンネルは、NetDefendOS が送信した証明書を有効にしようとしないクライアントではなくパブリックインターネット上に確立されます。

この場合、プライベートサーバの IP アドレスは、FQDN が解決されるようにプライベート DNS サーバに登録される必要があります。また、このプライベート DNS サーバは、NetDefendOS が検証リクエストを発行する場合に見つけられるように NetDefendOS に設定される必要があります。これは、また、トンネルがパブリックインターネットを使用せず、完全に内部に設定されている場合の設定となります。

2. CA サーバは、パブリックインターネットにセットアップされたトンネル設定と、NetDefendOS から受信した証明書を有効にしようとするクライアントを持つプライベートサーバです。この場合、以下を行う必要があります。

a. プライベート DNS サーバは、NetDefendOS がクライアントからの証明書を検証するプライベート CA サーバを置くことができるように設定される必要があります。

b. D-Link ファイアウォールの外部 IP アドレスは、クライアントに送信された証明書のプライベート CA サーバの FQDN 参照が解決できるように、パブリック DNS システムに登録される必要があります。例えば、NetDefendOS は、ca.example.com という FQDN を持つクライアントに証明書を送信するかもしれません。クライアントが、これをパブリック DNS システム経由でファイアウォールのパブリック外部 IP アドレスに解決する必要があります。

トンネルの一方が、多数のクライアントではなく別のファイアウォールである場合は、同じ手順に従います。

3. CA サーバはパブリックインターネット上の商用サーバです。これは最も簡単なケースで、パブリック DNS サーバのアドレス設定が FQDN を解決します。唯一必要なのは、NetDefendOS が、受信する証明書内の FQDN を解決するために少なくとも一つのパブリック DNS サーバのアドレス設定を持つ必要があることです。

- HTTP PUT リクエストを、検証リクエストソース（ファイアウォールまたはクライアントのいずれか一方）から CA サーバに送信し、HTTP リプライを受信する可能性があります。リクエストがファイアウォールを通過する場合、NetDefendOS の IP ルールセット内の適切なエントリが、本トラフィックの通過を許可するように定義される必要があります。

NetDefenOS 自身が CA サーバにリクエストを発行している場合、IP ルールセットのエントリは必要ありません。NetDefendOS が行うアクションは初期値で信頼されています。また、これは NetDefendOS が発行した DNS 解決リクエストに適用される一般的なルールです。

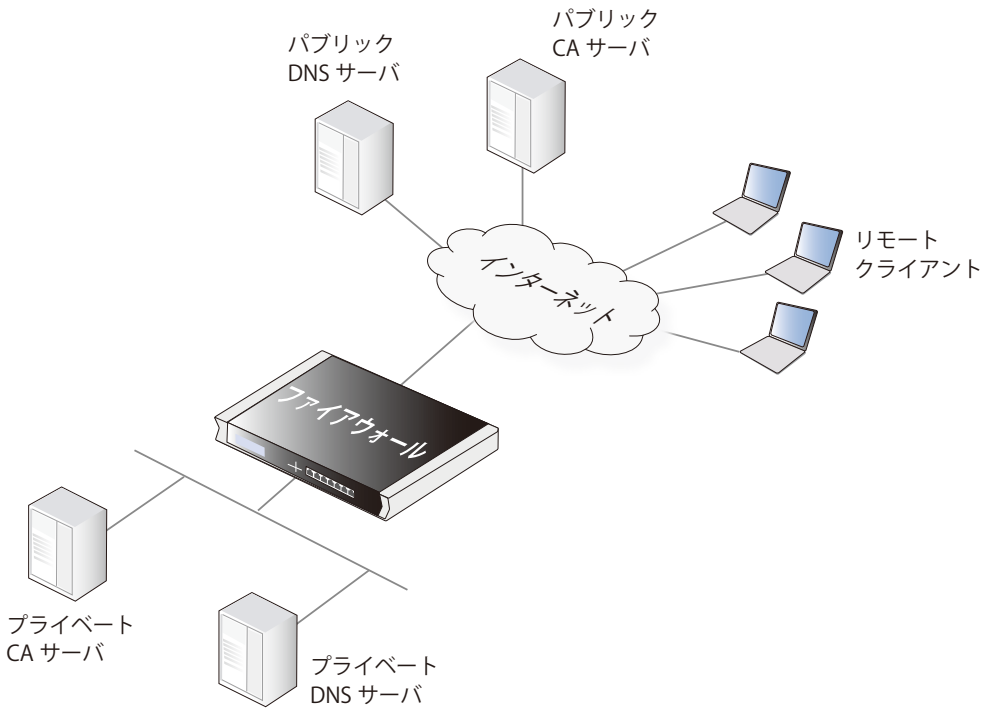


図 3-13　証明書検証コンポーネント

クライアントによる CA サーバアクセス

D-Link ファイアウォールに接続するローミングクライアントを持つ VPN トンネルでは、VPN クライアントソフトウェアにより CA サーバにアクセスする必要があります。すべての VPN クライアントソフトウェアがこのアクセスを必要とするというわけではありません。Vista の前のマイクロソフトクライアントでは、CA サーバリクエストは全く送信されません。Microsoft Vista では、検証はオプションであり、初期値で無効になっています。他のマイクロソフト以外のクライアントは動作方法に違いがありますが、大部分が証明書の有効化を試みます。

プライベート CA サーバの場所

プライベート CA サーバの位置を決める最も簡単なソリューションは、ファイアウォールの保護のない側にサーバを置くことです。しかし、これはセキュリティの観点からお勧めしません。内部（できれば DMZ）で、NetDefendOS がアクセスをコントロールする場所にサーバを置くほうがより望ましいと言えます。

以前に説明した通り、プライベート CA サーバのアドレスは、インターネットから来る証明書の検証リクエストのためにパブリック DNS サーバを通して解決される必要があります。証明書クエリが D-Link ファイアウォールのみから到来し、CA サーバがファイアウォールの内側にある場合は、これらのリクエストを解決できるように、NetDefendOS に内部の DNS サーバの IP アドレスを設定する必要があります。

検証を無効にする

以下のトラブルシューティングセクションで説明するように、証明書を有効にするリクエストを無効にすることによって CA サーバアクセスの問題を特定することができます。証明書オブジェクトの CRL checks オプションで NetDefendOS から CA サーバにアクセスする試みを無効にすることができます。これは、CA サーバの違反者リストに対するチェックが無効となり、サーバへのアクセスが試みられないことを意味します。

3.9.5 Windows CA サーバ要求の作成

CA サーバまたは CA 会社に証明書を要求するために最適な方法は、よく知られ事前に定義された形式での証明書の要求を含む CA Certificate Request ファイルを送信することです。

NetDefendOS の Web インタフェース（WebUI）は、現在、NetDefendOS が必要とする「.cer」および「.key」ファイルの生成用に CA サーバに送信する証明書のリクエストを生成する機能をサポートしていません。

しかし、以下の手順を使用して、手動で Windows CA サーバに必要なファイルを作成することができます。

- Windows CA サーバにゲートウェイ証明書を作成し、「.pfx」形式のファイルとしてそれをエクスポートします。
- 「.pfx」ファイルを「.pem」形式に変換します。
- 「.pem」ファイルの関連部分を取り出して、必要な「.cer」と「.key」ファイルを作成します。

詳しい手順は以下の通りです。

1. Windows CA サーバにゲートウェイ証明書を作成し、ローカルな NetDefendOS 管理ワークステーションのディスクに「.pfx」形式のファイルとしてそれをエクスポートします。
2. 次に、ローカルの「.pfx」ファイルを「.pem」ファイルに変換します。

   これは、コンソールのコマンドラインを使用した OpenSSL ユーティリティで行います。

   ```
   > openssl pkcs12 -in gateway.pfx -out gateway.pem -nodes
   ```

   このコマンドラインの例では、CA サーバからエクスポートされたファイルが gateway.pfx であり、OpenSSL プログラムが同じローカルディレクトリにあるものとします。

   オリジナルの「gateway.pfx」ファイルには CA ルート証明書、パーソナル証明書、および秘密鍵証明書の 3 通の証明書が含まれています。「gateway.pem」ファイルは、これらを含んでおり、テキストエディタでカット & ペーストすることができます。

注意 ここでは、OpenSSL は通信ユーティリティという通常の役割として使用されるのではなく、変換ユーティリティとして使用されています。

3. Windows™ のメモ帳などのテキストエディタで 2 つの空のテキストファイルを作成します。同じファイル名を指定し、拡張子は一方のファイルに「.cer」を、もう片方には「.key」を使用します。例えば、gateway.cer と gateway.key です。

4. テキストエディタを起動し、ダウンロードした「.pem」ファイルを開いて以下の行の場所を見つけてください。

   ```
   -----BEGIN RSA PRIVATE KEY-----
   ```

5. BEGIN を含む行から以下の行までのすべての行を選択して、システムのクリップボードにコピーします。

   ```
   -----END RSA PRIVATE KEY-----
   ```

6. コピーされたテキストを「.key」ファイルに貼り付けて保存します。

7. 「.pem」ファイルを開いて以下の行で始まる場所を見つけてください。

```
-----BEGIN CERTIFICATE-----
```

BEGIN を含む行から以下の行までのすべての行を選択して、システムのクリップボードにコピーします。

```
-----END CERTIFICATE-----
```

8. 今度は、コピーされたテキストを「.cer」ファイルに貼り付けて保存します。

保存した「.key」と「.cer」ファイルを NetDefendOS にアップロードします。

3.10 DNS 設定

DNS 概要

DNS サーバは完全修飾ドメイン名（FQDN）を対応する数値 IP アドレスに変換することができます。FQDN は、インターネットの DNS ツリー階層構造において、あるノードの固有の立場を指定するドメイン名で、サブドメイン名、ホスト名等をすべて省略せずに記述した形式のドメイン名です。FQDN 解決では、FQDN は変更せずに実際の物理的な IP アドレスを変更することができます。

Uniform Resource Locator（URL）は、FQDN にはないアクセスプロトコルを含んでいるという点で、FQDN とは異なっています。例えば、www ページのためのプロトコルは「http//:」で明示されます。

FQDN は、NetDefendOS の設定で、IP アドレスが不明な場合や、スタティック IP アドレスの代わりに DNS を利用する方がわかりやすい場合など、多くの局面で使用されています。

NetDefendOS を使用した DNS

NetDefendOS は、DNS 解決を行うために、最大 3 つの IPv4 および（または）IPv6 DNS サーバの利用が設定できる DNS クライアントを実装しています。これらはプライマリサーバ、セカンダリサーバ、およびターシャリサーバと呼ばれます。DNS が機能するためには、少なくともプライマリサーバを定義する必要があります。常にバックアップができるように少なくとも 2 つのサーバ（プライマリとセカンダリ）を定義することをお勧めします。

DNS の名前解決を必要とする機能

NetDefendOS の以下のモジュールが動作するためには、少なくとも一つの DNS サーバが定義されていることが必要です。

- Automatic time synchronization（自動時間同期）
- CA 自己署名証明書のために外部の認証発行局のサーバへアクセスする
- アンチウィルスや IDP など外部サーバへのアクセスを必要とする UTM の機能
- FQDN アドレスオブジェクト解決

例題 3.51

DNS サーバを設定する

ここでは、NetDefendOS クライアントが IPv4 アドレス 10.0.0.1 および 10.0.0.2 をそれぞれ持つプライマリとセカンダリの DNS サーバを使用する方法を説明します。

CLI

```
DFL-xxxx:/> set DNS DNSServer1=10.0.0.1 DNSServer2=10.0.0.2
```

Web Interface

1. **System > Device > DNS** の順にメニューをクリックします。

2. DNS サーバの設定を行い、「OK」ボタンをクリックします。

< 入力例 >

- Primary Server : 10.0.0.1
- Secondary Server : 10.0.0.2

3. 「OK」ボタンをクリックします。

自動 DNS アドレス指定

外部の DHCP サーバに接続するインタフェースに対して DHCP（IPv4 用）または DHCPv6（IPv6 アドレス用）を有効にすることで、DNS アドレスを割り当てることも可能です。ISP を経由してインターネットにアクセスして、ISP の DHCP サーバから必要なすべてのアドレスを受信する場合に、この方式がよく使用されます。

インタフェース上で DHCP 経由で受信した DNS アドレスは、スタティックな DNS アドレスが設定されていない場合、システム全体の NetDefendOS DNS サーバとなります。しかし、スタティックな DNS アドレスを手動で設定すると、そのインタフェースの DHCP を通じて受信された DNS サーバアドレスは無視されます。また、既に手動で設定されている DNS アドレスは影響を受けません。

DHCP を使用した DNS アドレスの設定については、「5.2 IPv4 DHCP クライアント」および「5.6.1 DHCPv6 クライアント」で詳しく説明します。

DNS ルックアップと IP ルールセット

NetDefendOS 自身が DNS サーバ要求を生成する場合、接続が成功するように IP ルールセットのエントリを定義する必要はありません。これは NetDefendOS が開始する接続は信頼されると見なされるためです。例えば、NetDefendOS が、証明書の妥当性を証明するために CA サーバにアクセスし、最初に証明書の FQDN を IP アドレスに解決する場合などです。

ダイナミック DNS と HTTP Poster

NetDefendOS が提供する DNS 機能は、本製品の外部 IP アドレスが変更されると明示的に DNS サーバに通知することができます。これは、ダイナミック DNS（DDNS）として時々参照され、本製品が変更できる外部 IP アドレスを持つ場合に有効です。

ダイナミック DNS は、またトンネルの両端がダイナミック IP アドレスを持っている IPsec VPN シナリオで有効です。トンネルの片側にだけにダイナミックなアドレスがある場合、IPsec Tunnel オブジェクトの Auto Establish プロパティはこの問題を解決できます。

Web マネージャの **Network > Network Services** 画面で、いくつかのダイナミック DNS サービスを定義します。HTTP Poster クライアントオブジェクトは以下の特性を持つダイナミック DNS クライアントです。

- 複数の HTTP Poster オブジェクトをそれぞれ異なる URL と異なるオプション設定を使用して定義できます。
- 初期値では、HTTP Poster オブジェクトは定義した URL に HTTP GET リクエストを送信します。いくつかのサーバが HTTP POST 要求を必要とします。これを実行するためには、オプション「HTTP Post the Values」を有効にする必要があります。これは、認証パラメータが URL で送信されている場合に通常必要とされます。
- 初期値では、HTTP Poster は NetDefendOS の再構成後にサーバ要求を自動的には送信しません。オプションの「Repost on each reconfiguration.」を有効にすることで、この動作を変更できます。例外的に、インタフェース上で新しいローカル IP アドレスを取得した後の再構成後、DNS サーバに接続します。NetDefendOS は通常、再構成後リポスティング前に 20 秒間（定義済み）待機します。
- Repost Delay の初期値は 1200 秒（20 分）です。これは変更できます。定義済みの DynDNS クライアントには 30 日の再取得時間が定義済みであり、これを変更することはできません。

HTTP Poster と定義済みのネーム DNS サーバの違いは、HTTP Poster はあらゆる URL の送信に使用できる点です。ネームサービスは、その特定サービスに必要とされる URL を簡単に正しい書式にするために便利です。例えば、dyndns.org サービス用の http://URL は以下の通りです。

```
myuid:mypwd@members.dyndns.org/nic/update?hostname=mydns.dyndns.org
```

これは、HTTP Poster を使用して送信することができます。または、URL は、DynDNS オプションを使用することや dyndns.org に必要な情報のみ入力することで NetDefendOS によって自動的にフォーマットされます。

HTTP Poster 応答の要件

HTTP Poster から応答が返ってくるには、以下の要件を満たしている必要があります。

- HTTP ヘッダに応答コード 200 が含まれ有効であること。
- 応答の本体に何らかのテキストが含まれ空ではないこと。このテキストはステータスメッセージの中で使用されます。

HTTP Poster の失敗

NetDefenOS により HTTP Poster の失敗が検出されると、連続的に長くなる間隔で処理を試行を続けます。初期間隔は 60 秒で、試行を繰り返すたびに 2 倍になっていきます。間隔が 24 時間に到達すると、それ以上倍にはならず、同じ間隔で成功するまで試行を継続します。

HTTP Poster は成功または失敗のログメッセージを生成します。CLI コンソールコマンド「httpposter」を使用して、NetDefenOS の送信内容やサーバの応答内容を確認することにより、問題のトラブルシューティングに役立てることができます。

NetDefendOS が何を送信しているのか、およびサーバが何を返しているのかを表示することによって障害調査するために CLI コンソールコマンドの「httpposter」を使用することができます。

```
DFL-xxxx:/> httpposter
```

注意 高頻度のサーバクエリは問題を起こします。

ダイナミック DNS サービスは、短い期間にわたって頻繁に繰り返されたログインの試みに敏感であり、過度の要求を送る送信元の IP アドレスをブラックリストに掲載します。従って、あまりにも頻繁にこれらのサーバに問い合わせを行うことをお勧めしません。頻繁に問い合わせを行うと、サービスは応答しなくなる可能性があります。

以下のコマンドで個々のサーバに Repost を実行します。

```
DFL-xxxx:/> httpposter -repost=<index>
```

<index> は Poster のリストにあるオブジェクトの位置を示します。例えば、リストで 2 番目の Repost を実行します。

```
DFL-xxxx:/> httpposter -repost=2
```

HTTP Poster の他の用途

HTTP Poster はダイナミック DNS 以外の目的に使用される可能性があります。NetDefendOS が HTTP GET または POST メッセージを特定の URL に送信するという処理を行いたい場合は、本機能を使用することができます。

第 4 章 ルーティング

この章では、NetDefendOS において IP ルーティングを設定する方法について記述します。

- 「4.1 概要」
- 「4.2 スタティックルーティング」
- 「4.3 ポリシーベースルーティング」
- 「4.4 ルートロードバランス」
- 「4.5 Active-Active セットアップ」
- 「4.6 仮想ルーティング」
- 「4.7 OSPF」
- 「4.8 マルチキャストルーティング」
- 「4.9 透過モード」

4.1 概要

IP ルーティングは、NetDefendOS における基本機能のひとつです。システムを通過するどの IP パケットも、時間内にいくつかの地点で少なくとも１つの経路決定が必要であり、NetDefendOS が期待通りに機能するためにはルーティングの適切な設定がきわめて重要です。

NetDefendOS は、以下のルーティングメカニズムのタイプを持っています。

- スタティックルーティング
- ダイナミックルーティング

NetDefendOS は、フェイルオーバ機能で経路とリンクの冗長性を達成するためにルートモニタリングもサポートしています。

4.2 スタティックルーティング

ルーティングの最も基本的な形式は、スタティックルーティングとして知られています。ルーティングテーブルのほとんどのエントリが NetDefendOS システムのスタティックなコンフィグレーションにあるため、「static」という用語が使用されます。通常、それらは長期間のシステム運用では変更はされません。

スタティックルーティングは、アドレスがほぼ固定していて、接続しているネットワークが少数に限定されている、より小規模のネットワーク構成で使用するのが最もふさわしいと言えます。しかし、大規模なネットワークやネットワークトポロジが複雑である場合には、スタティックルーティングテーブルを手動で管理する作業は、手間がかかるため問題となります。従ってそのようなケースでは、ダイナミックルーティングが使用されるべきです。

NetDefendOS のダイナミックルーティング機能に関する詳しい情報は、「4.7 OSPF」を参照してください。しかし、ご使用のネットワークにダイナミックルーティングの実行を選択したとしても、スタティックルーティングの原理と、NetDefendOS 内で実行される方法についても理解する必要があります。

4.2.1 NetDefenOS のスタティックルーティング

IP ルーティングは、多くの中継ネットワークデバイスを経由して送信元からの最終送信先まで IP パケットを送信するために使用される TCP/IP ネットワーク内の基本的なメカニズムであり、これらのデバイスは、パケットの宛先をルーティングするタスクを実行するため、よくルータと呼ばれます。各ルータでは、一つ以上のルーティングテーブルがルートのリストを持っており、次にパケットを送信する場所を検索するためにこれらを参照します。

一つのルートを構成する項目については、次に記述します。

ルートを構成する項目

NetDefendOS の Route オブジェクトは Routing Table に追加することができます。Route オブジェクトには以下のプロパティがあります。

項目	説明
Interface	送信先ネットワークに到達するようにパケットを転送するインタフェース。つまり、送信先 IP レンジが直接またはルータを経由して接続するインタフェース。 インタフェースは、ファイアウォールの物理インタフェース、または VPN トンネル（トンネルは NetDefendOS によって物理インタフェースのように扱われます）です。
Network	これは、このルートが到達する送信先ネットワーク IP アドレスの範囲です。ルーティングテーブルから選ばれたルートは、検索された IP アドレスを含む送信先 IP アドレス範囲を持つルートです。そのように一致するルートが 2 つ以上ある場合、選ばれるルートは、最も小さな IP アドレス範囲を持つものです。 通常、送信先ネットワーク all-nets は、ISP 経由でインターネットへアクセスするためのルートで使用されます。
Gateway	送信先ネットワークへの経路に存在するネクストルータであるゲートウェイの IP アドレス。これはオプションです。送信先ネットワークが直接インタフェースに接続される場合には、これは必要ありません。 ファイアウォールと送信先ネットワークの間にルータがある場合、ゲートウェイ IP を指定する必要があります。 例えば、ルートが ISP 経由でインターネットにアクセスするためのものであれば、ISP のゲートウェイルータのパブリック IPv4 アドレスを指定します。
Local IP Address	本項目は通常指定する必要はありません。指定された場合、NetDefendOS はこのアドレスに送信された ARP クエリに応答します。以下の特別なセクションで、本項目についてさらに詳しく説明します。 Local IP Address と Gateway は互いに排他的であり、どちらか一方を指定してください。
Metric	これは、ルートに割り当てられたメトリック値であり、代替ルート間の比較を行う場合の重み付けとして使用されます。2 つのルートは同等で、異なるメトリック値を持つ場合、最も低いメトリック値を持つルートが選択されます。 また、メトリック値は「Route Failover」と「Route Load Balancing」によっても使用されます。 詳しくは、「4.4 ルートロードバランス」と「4.2.3 ルートフェイルオーバ」を参照してください。
Forward Broadcast Traffic	初期値（無効）ではブロードキャストトラフィックは破棄されます。

典型的なルーティングのシナリオ

以下の図は、典型的なルーティングのシナリオを示しています。

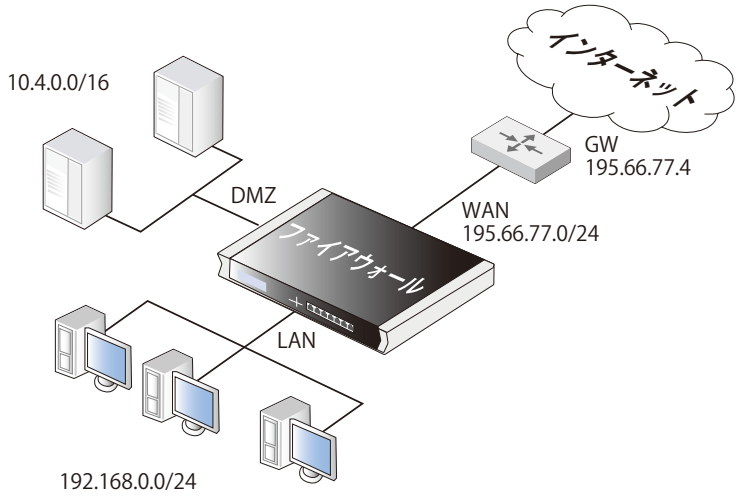


図 4-1　典型的なルーティング

上の図では、LAN インタフェースはネットワーク 192.168.0.0/24 に関連付けられ、DMZ インタフェースはネットワーク 10.4.0.0/16 に関連づけられています。WAN インタフェースはネットワーク 195.66.77.0/24 に関連付けられ、インターネットへの ISP ゲートウェイのアドレスは 195.66.77.4 です。

これに関連するルーティングテーブルは以下の通りです。

経路 #	インタフェース	送信先	ゲートウェイ
1	lan	192.168.0.0/24	
2	dmz	10.4.0.0/16	
3	wan	195.66.77.0/24	
4	wan	all-nets	195.66.77.4

上記のルーティングテーブルは以下の情報を提供します。

経路 #	説明
1	192.168.0.0/24 ネットワーク上のホストに向かうすべてのパケットは、lan インタフェース上に送信される必要があります。ゲートウェイが経路エントリには指定されていないため、ホストは lan インタフェースから直接到達可能なネットワークセグメント上に置かれているものとします。
2	10.4.0.0/16 ネットワーク情報ホストに向かうすべてのパケットは、dmz インタフェースに送信されます。さらに、この経路には、ゲートウェイは指定されません。
3	195.66.77.0/24 ネットワークのホストに向かうすべてのパケットは、wan インタフェースに送信されます。ゲートウェイはホストに到達するために必要とされません。
4	すべてのホスト（all-nets ネットワークはすべてのホストと一致します。）に向かうすべてのパケットは、wan インタフェースと IP アドレス 195.66.77.4 を持つゲートウェイに送信されます。その後、ゲートウェイはパケットが次に送信される場所を検出するために、ルーティングテーブルを調べます。 送信先 all-nets を持つ経路は、経路が設定されていないすべてのパケットに応じるデフォルトルートとして参照されます。通常、このルートはインターネットに接続するインタフェースを指定します。

狭い範囲のルーティングテーブルが選択される

ルーティングテーブルが評価される場合、経路の順番は重要ではありません。通常、関連するルーティングテーブルのすべての経路が評価され、最も特定的なルートが使用されます。つまり、 2 つの経路が重複する送信先ネットワークを持っている場合、より狭いネットワークが、広いものより優先して評価されます。この動作は最初に一致するルールが使用される IP ルールセットとは対照的です。

上の例では、送信先 IP アドレス 192.168.0.4 を持つパケットは、理論上ははじめの経路と最後の経路に一致します。しかし、はじめの経路エントリは、より範囲が特定された一致であるため、評価は終了し、パケットはそのエントリに従って送られます。

単一のホストのための複数の経路（1 つの IP アドレスのルート）が一致した場合、ルートの選択は任意のものとなります。コンフィグレーションに変更がないと、毎回同じルートが選出されます。

一致するアドレス範囲を持ち、同じ範囲の大きさである場合は、低いメトリック値を持つルートが選ばれます（メトリックのプロパティの説明で説明した通りです）。

ルーティングテーブルの順番は重要ではありませんが、実行時の読みやすさのために、狭い範囲のルートを最初に配置し、デフォルトの all-nets を最後に配置することをお勧めします。

ルートインデックスは表示用に使用される

ルーティングテーブルが管理インタフェースで一覧表示される際、各ルートにインデックス番号が割り当てられ、このインデックス番号はルートを設定する場合に使用することができます。このインデックス値は固定ではなく、テーブル表示用に NetDefendOS によって割り当てられているということに注意してください。手動でインデックス番号を変更することも可能ですが、テーブルにおける位置を一時的に変更するだけです。システムの再起動によってルーティングテーブルが完全に再構成され、インデックス番号も新しく割り振られます。NetDefendOS によって自動的に作成されたルートについても同様です。

ローカルな IP アドレスパラメータ

Local IP Address パラメータの正しい使用法はわかりにくいため、説明を補足します。

通常、lan などの物理インタフェースが単一のネットワークに接続しており、インタフェースとネットワークが同じネットワークにあります。ネットワークが物理インタフェースに割り当てられており、接続するネットワークのクライアントは ARP クエリを経由して自動的に D-Link ファイアウォールを見つけることができると言えます。クライアントと NetDefendOS インタフェースが同じネットワークの構成要素であるため、ARP は動作します。

スイッチを通じて、同じ物理ネットワークに対し、その物理インタフェースの IP アドレスを含まない新しいネットワーク範囲でセカンドネットワークが追加されるかもしれません。このネットワークは、物理インタフェースに割り当てられていないとみなされます。ARP がクライアントとインタフェースの間で機能しないため、このセカンドネットワークのクライアントは、ファイアウォールと通信できません。

この問題を解決するために、NetDefendOS に以下の項目を持つ新しいルートを追加します。

項目	説明
Interface	セカンドネットワークを見つけるインタフェース。
Network	セカンドネットワークの IP アドレス範囲。
Local IP Address	セカンドネットワークの IP 範囲内のアドレス。

セカンドネットワーククライアントのデフォルトゲートウェイが、上のルートの「Local IP Address」と同じ値に設定される場合、クライアントはインタフェースとの通信に成功します。IP アドレスがクライアントのデフォルトゲートウェイと Local IP Address に対して同じ値である限り、セカンドネットワークで選ばれた IP アドレスは重要ではありません。

Local IP Address を持つルートを加えることにより、ファイアウォールは Local IP Address を持つゲートウェイとして動作して、インタフェースがその IP アドレスを持つように ARP クエリへの応答と送信を行います。

以下の図は、この機能を使用するシナリオを示しています。ネットワーク 10.1.1.0/24 は 10.1.1.1 のネットワークに IP アドレスを持っている物理インタフェースに割り当てられています。スイッチ経由でセカンドネットワーク 10.2.2.0/24 をインタフェースに割り当てる場合、インタフェースの IP アドレスがそれに属さないため、割り当てられません。

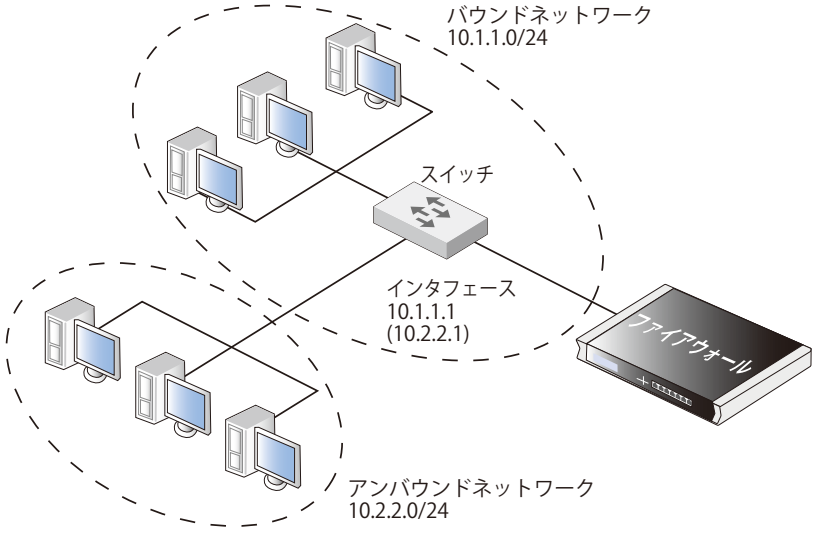


図 4-2　アンバウンドネットワークとローカル IP アドレスを使用する

Local IP Address10.2.2.1 を持つセカンドネットワークに NetDefendOS ルートを追加することによって、インタフェースは 10.2.2.0/24 ネットワークからの ARP リクエストに応答します。また、このセカンドネットワークのクライアントは、ファイアウォールに到達するためにデフォルトゲートウェイを 10.2.2.1 に設定する必要があります。

本機能は、通常、ネットワークをインタフェースに追加しても、ネットワークの既存の IP アドレスを変更することが望ましくない場合に使用されます。異なるネットワーク同士が相互通信においてトラフィック制御なしに接続することになるため、セキュリティの見地から、このような設定を行うことは重大なリスクを負います。そのため、この機能を使用する前に十分に注意するべきです。

すべてのトラフィックは、２つの関連するルートを持つ必要があります。

NetDefendOS におけるルーティングを理解しようとする場合に、直感的には理解できないこととして、すべてのトラフィックには関連する 2 つのルートが必要であるという事実があります。ルートは、接続において送信先ネットワークのために定義されるだけではなく、送信元ネットワークにも定義される必要があります。

送信元ネットワークを定義するルートは、単に送信元ネットワークが特定のインタフェースで見つけられることを表しています。新しい接続がオープンされる場合、NetDefendOS は、このルートを検索するリバースルート検索と呼ばれるチェックを実行します。送信元のネットワークルートはルーティングを実行するためには使用されませんが、代わりに送信元ネットワークが到達するインタフェース上に見つけられることをチェックします。チェックが失敗すると、Default Access Rule エラーメッセージが生成されます。

ICMP ping リクエストなど Core（NetDefendOS 自身）に向かうトラフィックでさえ、関連する 2 つのルートを持つこのルールに従う必要があります。この場合、ルートのうちの 1 つのインタフェースが Core として指定されます。

4.2.2 スタティックルーティングの設定

このセクションでは、ルーティングが NetDefendOS で実行される方法とスタティックルーティングを設定する方法を記載します。

NetDefendOS は、複数のルーティングテーブルをサポートしています。デフォルトテーブル main は、定義済みで NetDefendOS に常に存在します。しかし、管理者は代替ルーティングを提供するために追加で完全に別々のルーティングテーブルを定義できます。

追加で、ユーザ定義のルーティングテーブルを 2 つの方法で使用できます。

- 「仮想ルーティング」を特定のルーティングテーブルを持つインタフェースに関連付けます。これは、1 つの NetDefendOS インストールが複数の仮想システムとして動作するように有効にします。これらのシステムの通信は Loopback インタフェースで行われます。「4.6 仮想ルーティング」と「3.4.9 ループバックインタフェース」を参照してください。
- どのルーティングテーブルが、どのトラフィックタイプに対処するかを判断する「ポリシーベースルーティングルール」を定義することができます。「4.3 ポリシーベースルーティング」を参照してください。

経路検索メカニズム

NetDefendOS における経路検索メカニズムは、他のルータ製品の動作方法といくつかわずかな違いがあります。多くのルータでは、IP パケットがコンテキストなしで送信され（フォワーディングがステートレス）、ルータによって受信されたすべての IP パケットに対してルーティングテーブルが検索されます。しかし、NetDefendOS では、state-awareness（状態認識）でパケットを送信するため、ルート検索プロセスは NetDefendOS のステートフルインスペクションメカニズムに集約されます。

どのインタフェースが IP パケットを受信しても、受信パケットが属するオープン済みの接続があるかどうかを参照するために接続テーブルを調べます。既存の接続が検出される場合、接続テーブルのエントリにはパケットを送信する場所に関する情報があるため、ルーティングテーブルで索引を行う必要はありません。これは、従来のルーティングテーブル索引よりはるかに効率的であり、NetDefendOS の高い送信性能の 1 つの理由であると言えます。

確立した接続を検出できないと、ルーティングテーブルを調べます。様々なポリシールール（例：IP ルールセット）の評価を行う前に経路検索が実際に行われることを理解することが重要です。そのため、NetDefendOS によって接続の許可 / 拒否が決定される時には、宛先インタフェースを認識していることになります。この設計はセキュリティポリシーでよりきめ細かく制御を考慮しています。

NetDefendOS の経路表示

NetDefendOS は、他の多くのシステムと比較して、経路の説明方法が若干異なりますが、こちらの方が理解しやすく、エラーの発生を減らします。

他の多くの製品はルーティングテーブルにおいて特定のインタフェースを使用せずに、代わりにインタフェースの IP アドレスを指定します。以下のルーティングテーブルは、Microsoft Windows™ ワークステーションの形式です。

```
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...00 13 d4 51 8d dd ...... Intel(R) PRO/1000 CT Network
0x20004 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
===========================================================================
===========================================================================
Active Routes:
Network Destination                 Netmask      Gateway    Interface Metric
                    0.0.0.0         0.0.0.0  192.168.0.1 192.168.0.10     20
                   10.0.0.0       255.0.0.0   10.4.2.143   10.4.2.143      1
                 10.4.2.143 255.255.255.255    127.0.0.1    127.0.0.1     50
              10.255.255.255 255.255.255.255   10.4.2.143   10.4.2.143     50
                85.11.194.33 255.255.255.255  192.168.0.1 192.168.0.10     20
                   127.0.0.0       255.0.0.0    127.0.0.1    127.0.0.1      1
                 192.168.0.0   255.255.255.0 192.168.0.10 192.168.0.10     20
                192.168.0.10 255.255.255.255    127.0.0.1    127.0.0.1     20
               192.168.0.255 255.255.255.255 192.168.0.10 192.168.0.10     20
                   224.0.0.0       240.0.0.0   10.4.2.143   10.4.2.143     50
                   224.0.0.0       240.0.0.0 192.168.0.10 192.168.0.10     20
             255.255.255.255 255.255.255.255   10.4.2.143   10.4.2.143      1
             255.255.255.255 255.255.255.255 192.168.0.10 192.168.0.10      1
Default Gateway: 192.168.0.1
===========================================================================
Persistent Routes:
None
```

NetDefendOS において対応するルーティングテーブルは、これに似ています。

```
Flags Network         Iface Gateway       Local IP Metric
----- --------------- ----- ------------- -------- -------
      192.168.0.0/24  lan                         20
          10.0.0.0/8  wan                          1
           0.0.0.0/0  wan   192.168.0.1           20
```

NetDefendOS ルート定義の利点

NetDefendOS のルート定義の方法により、ルーティング情報の閲覧と理解がより簡単になります。

さらに NetDefendOS の方法を使用する利点は、管理者が以下の通り直接特定のルートにゲートウェイを指定できるということです。

- 個別のルートには、ゲートウェイ IP アドレスを定義する必要はありません。
- ゲートウェイ IP アドレスを含み、別のインタフェースにトラフィックを送るルートがあっても、それは重要ではありません。

混合のサブネットを指定可能

また、ルート定義に対する NetDefendOS を使用する利点は、従来のサブネットマスクで連携されない送信先に経路を指定できるということです。例えば、宛先アドレス範囲 192.168.0.5-192.168.0.17 に 1 つの経路、IP アドレス 192.168.0.18-192.168.0.254 に対して別の経路を指定することが可能です。そのため、NetDefendOS は非常に複雑なネットワークトポロジにおけるルーティングタスクに最適です。

ルーティングテーブルの表示

管理者が最初に設定したルーティングテーブルには、生存期間中、自動的にルートの追加、削除、および変更が行われ、これらの変更はルーティングテーブルの内容を表示する際に示されることに注意することが重要です。

これらのルーティングテーブルの変更は、様々な理由で起こります。例えば、OSPF を使用したダイナミックルーティングが有効な場合、ルーティングテーブルは、OSPF ネットワークにおいて他の OSPF ルータと通信することによって学習した新しいルートでポピュレートされます。 また、ルートフェイルオーバなどのイベントは時間の経過に伴ってルーティングテーブルの内容の変更を引き起こすことがあります。

例題 4.1

ルーティングテーブルを表示する

ここでは、アクティブルーティングテーブルをはじめ設定したルーティングテーブルの内容を表示する方法を説明します。

CLI

ルーティングテーブルのコンテンツを参照する方法：

```
DFL-xxxx:/> cc RoutingTable main

DFL-xxxx:/main> show

Route/

   #  Interface  Network                  Gateway                    Local IP
   -  ---------  -------------------------  -------------------------  --------
   1  wan        InterfaceAddresses/wannet  <empty>                    <empty>
   2  wan        all-nets                   InterfaceAddresses/wan1_gw  <empty>
   3  dmz        InterfaceAddresses/dmznet  <empty>                    <empty>
   4  lan        InterfaceAddresses/lannet  <empty>                    <empty>

SwitchRoute

   (Empty)
```

CLI コンテキストを初期値に戻す：

```
DFL-xxxx:/main> cc
DFL-xxxx:/>
```

アクティブルーティングテーブルを参照する方法：

```
DFL-xxxx:/> routes

Flags Network          Iface Gateway       Local IP Metric
----- ---------------- ----- ------------- -------- ------
      192.168.0.0/24   lan                         0
      213.124.165.0/24 wan                         0
      0.0.0.0/0        wan   213.124.165.1         0
```

Web Interface

設定したルーティングテーブルを参照する方法:

1. **Network > Routing > Routing Tables** の順にメニューをクリックします。
2. 「main」ルーティングテーブルを選択します。
3. 設定した経路の一覧が表示されます。

アクティブルーティングテーブルを参照する方法:

1. メニューバーの「Status」を開き、ツリーメニューから「Routes」を選択します。
2. メイン画面にアクティブなルーティングテーブルが表示されます。

注意 コンテキストの変更には CLI コマンド「cc」が必要です。

上の CLI の例では、個別のルートを操作する前に、まず「cc」コマンド（カテゴリの変更：change category、またはコンテキストの変更：change context）を使用して特定のルーティングテーブル名を選択することが必要でした。

デフォルトスタティックルートは、各インタフェースに自動的に追加される

D-Link ファイアウォールを初めて起動する場合、NetDefendOS は、各物理インタフェースの main ルーティングテーブルに自動的にルートを追加します。これらのルートは、アドレス帳のデフォルト IP アドレスオブジェクトに割り当てられ、この IP オブジェクトは、アドレスをトラフィックが流れるように適切な範囲に変更する必要があります。

注意 デフォルトルートのメトリック は 100 です。

自動的に物理インタフェースに作成されたデフォルトルートに割り当てられたメトリックは、通常 100 です。

これらの自動的に追加されたルートは、ルーティングテーブルから手動で削除することはできません。代わりに、インタフェースのプロパティを選択し、アドバンスドオプションの「Automatically add a route for this interface using the given network」を無効にします。無効にすることにより、起動時に自動的に追加されたすべてのルートを削除します。本オプションには、自動的に追加されたルートを削除する以外に他の目的はありません。

all-nets 経路

定義するべき最も重要なルートは、通常、インターネットアクセスを提供する ISP と通信する all-nets へのルートです。NetDefendOS セットアップウィザードを使用すると、このルートもまた自動的に追加されます。

物理インタフェースに対し、インターネットへの接続に使用するように設定するオプションも存在します。Web マネージャでは、イーサネットインタフェースプロパティの「Advanced settings」のオプション「Automatically add a default route for this interface using the given default gateway.」で指定します。

本オプションを選択する場合、適切な all-nets ルートが自動的にインタフェースの main ルーティングテーブルに追加されます。

例題 4.2

main テーブルにルートを追加する

この例題は all-nets ルートを main ルーティングテーブルに追加する方法を示しています。このルートは wan インタフェースに接続する ISP 用のもので、ルートのゲートウェイである IP アドレス isp_gw_ip を持つルータを経由して ISP にアクセスします。

CLI

コンテキストをルーティングテーブルに変更する

```
DFL-xxxx:/> cc RoutingTable main
```

ルートの追加

```
DFL-xxxx:/main> add Route Interface=wan Network=all-nets Gateway=isp_gw_ip
```

初期値の CLI コンテキストに戻す

```
DFL-xxxx:/main> cc
DFL-xxxx:/>
```

Web Interface

1. **Network > Routing > Routing Tables** の順にメニューをクリックします。
2. 「main」ルーティングテーブルをクリックし、「Add」から「Route IPv4」を選択します。
3. 以下の通り入力し、「OK」ボタンをクリックします。
   - Interface: wan
   - Network:all-nets
   - Gateway: isp_gw_ip

ルートは IPv4 または IPv6 アドレスを含むことが可能

単一ルートは、IPv4 または IPv6 アドレスのいずれかを含むことができますが、両方を含むことはできません。IPv4 または IPv6 アドレスを使用するルートを同じルーティングテーブルに混ぜることができます。本機能に関する詳しい情報は、「3.2 IPv6 のサポート」を参照してください。

core 経路

NetDefendOS は、core 経路を持つアクティブなルーティングテーブルを自動的に作成します。これらの経路は、NetDefendOS が NetDefendOS 自身に到達するトラフィックを送信する方法を理解するために存在します。そのようなトラフィックの良い例は、イーサネットインタフェースに送信された ICMP Ping メッセージに対し、NetDefendOS が処理を行いその ping メッセージに応答するケースです。

システムには各イーサネットインタフェースに追加される経路がひとつあります。例えば、lan と wan という名前で、IPv4 アドレスがそれぞれ 192.168.0.10 と 193.55.66.77 の 2 つのインタフェースは、以下の経路に帰着します。

経路 #	インタフェース	送信先	ゲートウェイ
1	core	192.168.0.10	
2	core	193.55.66.77	

基本的には、送信先アドレスがインタフェース IP のひとつであるパケットを NetDefendOS が受信する場合、パケットは core インタフェースに送信されます。これは、システム自身によって処理されるということです。

経路 #	インタフェース	送信先	ゲートウェイ
1	core	224.0.0.0/4	

アクティブなルーティングテーブルを表示する際に core ルートを含むようにするためには、すべてのルートが表示されるようにオプションを明確に指定する必要があります。以下のルーティングコマンド例に表示します。

例題 4.3

core 経路を表示する

ここでは、アクティブなルーティングテーブル内の core 経路を表示する方法を説明します。

CLI

```
DFL-xxxx:/> routes -all
Flags Network           Iface Gateway         Local IP  Metric
----- ---------------- ----- -------------- --------- ------
      127.0.0.1         core  (Shared IP)               0
      192.168.0.1       core  (Iface IP)                0
      213.124.165.181   core  (Iface IP)                0
      127.0.3.1         core  (Iface IP)                0
      127.0.4.1         core  (Iface IP)                0
      192.168.0.0/24    lan                             0
      213.124.165.0/24  wan                             0
      224.0.0.0/4       core  (Iface IP)                0
      0.0.0.0/0         wan   213.124.165.1             0
```

Web Interface

1. Web インタフェースで core 経路を参照するためには、メニューバーの「Status」を開き、ツリーメニューから「Routes」を選択します。
2. 「Show all routes」にチェックをし、「Apply」ボタンをクリックします。
3. メイン画面に core 経路を含むアクティブなルーティングテーブルが表示されます。

「routes」コマンドからの出力を理解する

CLI 経路コマンドの出力に関する詳しい情報については、個別の「CLI Reference Guide」を参照してください。

4.2.3 ルートフェイルオーバ

概要

D-Link ファイアウォールは可用性と接続性が重要であるミッションクリティカルな位置にたびたび配置されます。例えばインターネットへのアクセスに依存する会社では、1 つのインターネットサービスプロバイダ（ISP）を通じた外部インターネットへの単一の接続に失敗すると、作業に多大な混乱を引き起こします。

そのため、セカンダリインターネットサービスプロバイダ（ISP）を使用して、バックアップのインターネット接続を持つのが非常に一般的です。2 つのサービスプロバイダへの接続は、多くの場合、一方の障害時には、回避策として異なるルートを使用します。

複数の ISP などを使用したシナリオを容易にするために、NetDefendOS は、経路エラーによりトラフィックが自動的に別の代替経路に引き継がれるフェイルオーバ機能を提供します。NetDefendOS は、経路の可用性をモニタするルートモニタを使用することで経路フェイルオーバを実行し、エラーが発生すると、トラフィックを代替経路に切り換えます。

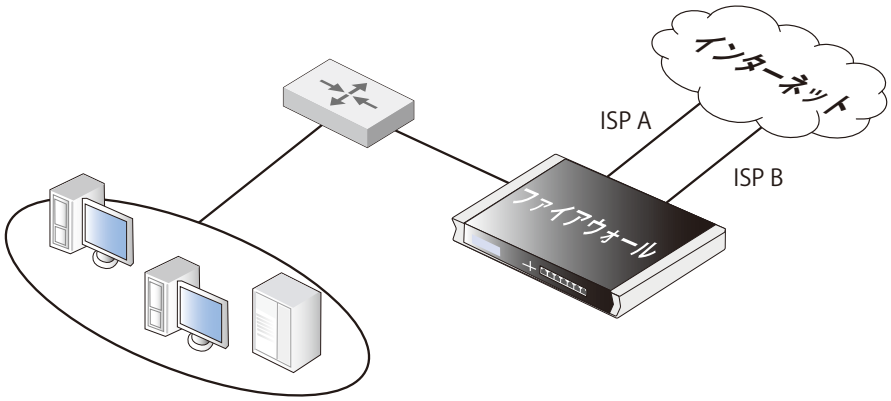


図 4-3　IPS アクセスのためのルートフェイルオーバのシナリオ

ルートフェイルオーバの設定

ルートフェイルオーバを設定するために、ルートモニタリング機能を有効にする必要があります。そして、これはルートごとを基本にして有効にされるオプションです。優先されるバックアップ経路でシナリオ内の経路フェイルオーバ機能を有効にするためには、優先される経路のルートモニタリング機能を有効とします。しかし、バックアップ経路では、通常フェイルオーバするための経路を持たないため有効にする必要はありません。ルートモニタリングが経路に有効な場合、以下のモニタリング方式から一つの方式を選択する必要があります。

- インタフェースリンクステータス
  NetDefendOS は、経路に指定されているインタフェースのリンクステータスをモニタします。インタフェースの稼働中、経路は正常であると診断されます。本方式は、インタフェースが物理的に割り当てられ、ケーブル接続が予想通りに動作していることをモニタするために適しています。リンクステータスのどのような変化も直ちに通知されるため、本方式はエラーに対して最速で応答することができます。

- ゲートウェイモニタリング
  指定のゲートウェイが経路のネクストホップとして指定される場合、そのゲートウェイへのアクセス可否は定期的な ARP リクエストを送信することによってモニタできます。ゲートウェイがこれらのリクエストに応じる間、経路が正しく機能していると見なされます。

- ホストモニタリング
  最初の 2 つのオプションは、D-Link ファイアウォールに対してローカルなコンポーネントがアクセス可能かをチェックします。これらの代替手段は、指名された 1 つ以上のリモートホストがアクセス可能かをモニタすることです。これらのホストには既知の高可用性があり、それらをポーリングすることで、ローカルなファイアウォールからのトラフィックがそれらに到達しているかどうかを示すことができます。また、ホストモニタリングは、リモートホストに到達する際にネットワーク遅延を測り、遅延が管理者が指定したしきい値を超過すると、代替経路にフェイルオーバを開始する方法を提供します。

自動的に追加されたルートには再定義が必要

自動的に追加されたルートでルートモニタリングを有効にできないことに注意することが重要です。例えば、初期のスタートアップで NetDefendOS が物理インタフェースに作成するルートは、自動的に追加されるルートです。これらのルートでモニタリングを有効にすることができない理由は自動的に作成されたルートが NetDefendOS 構成内で特別なステータスを持っており、別に扱われるためです。

ルートモニタリングが自動的に作成されたルートで必要である場合、そのルートを最初に削除し、新しいルートとして手動で再作成する必要があります。そうすることで、新しいルートにモニタリングを有効にすることができます。

ルートメトリックの設定

経路を指定する場合、管理者は手動で経路のメトリックを設定する必要があります。メトリックは、経路が宛先に到達する手段としてどれくらい適切かを示す整数の値です。2 つの経路が同じ宛先に到達する手段を提供する場合、NetDefendOS は、データを送信するために最も低いメトリック値を持つ経路を選択します。2 つの経路が同じメトリック値を持っていると、ルーティングテーブルではじめに検出したで経路を選択します。
プライマリの優先される経路は、より低い値のメトリック値（例：10）を持ち、セカンダリのフェイルオーバルートは高いメトリック値（例：20）を持っています。

複数のフェイルオーバルート

複数のフェイルオーバルートを指定することができます。例えば、プライマリルートには、 1 つだけの経路の代わりのフェイルオーバルートとして追加の 2 つのルートを持つことができます。この場合、メトリックは 3 つの経路のそれぞれで異なるようにするべきです。プライマリルートに「10」、はじめのフェイルオーバルートに「20」および 2 番目のフェイルオーバルートに「30」。はじめの 2 つの経路はルーティングテーブルでルートモニタリングを有効にしますが、最も高いメトリック値を持つ最後の 1 つの経路はフェイルオーバする経路がないためルートモニタリングを有効にする必要はありません。

フェイルオーバ処理

モニタリングによって経路が有効でないとみなされた場合、NetDefendOS はその経路を無効にするようにを印を付け、既存または新規接続のためにルートフェイルオーバを起動します。既に確立した接続では、ルート索引で次に合致する経路を探し、新しい経路を使用した接続に切り替わります。新しい接続のためには、ルート検索は無効な経路を無視し、次に最適な経路を代わりに使用します。

以下のテーブルは宛先として「all-net」を持ち、2 つの異なるゲートウェイを使用する 2 つのデフォルトルートを定義します。はじめのプライマリルートは、最も低いメトリック値を持ち、ルートモニタは有効となっています。2 番目の代替ルートに対するルートモニタは、フェイルオーバルートを持たないため意味がありません。

経路 #	インタフェース	送信先	ゲートウェイ	メトリック	モニタリング
1	wan	all-nets	195.66.77.1	10	On
2	wan	all-nets	193.54.68.1	20	Off

新しい接続がインターネットのホストに対して確立されようとしている場合、経路索引は最も低いメトリック値を持つ経路を選択するという結果になります。次に、プライマリ WAN ルータが故障すると、これを NetDefendOS が検知し、はじめの経路は無効になります。結果として、新しい検索索引が実行され、はじめの経路が無効にされるようにマークされている状態で、2 番目の経路が選択されます。

経路の再有効化

経路が無効にされても、NetDefendOS は、その経路のステータスチェックを続けます。経路が再び利用可能になると、再度その経路は有効にされて既存の接続は自動的に元の経路に戻ります。

経路インタフェースのグループ化

ルートモニタリングを使用する場合、別のルートへのフェイルオーバがルーティングインタフェースを変更するかどうかをチェックすることが重要です。これが起こりうる場合、ポリシーと既存接続が維持されることを保証するためにいくつかの予防措置を採る必要があります。
問題を例示するために、以下の設定について検討します。
はじめに、wan インタフェースを経由してインターネットに到達するすべての HTTP トラフィックに NAT を行う IP ルールセットのエントリがあります。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	パラメータ
Allow/NAT	lan	lannet	wan	all-nets	http

その結果、ルーティングテーブルは以下のデフォルトルートを含みます。

インタフェース	送信先	ゲートウェイ	メトリック	モニタリング
wan	all-nets	195.66.77.1	10	Off

セカンダリルートがバックアップ用の DSL 接続に追加され、ルートモニタはこれに対して有効とされます。更新されたルーティングテーブルは以下のようになります。

経路 #	インタフェース	送信先	ゲートウェイ	メトリック	モニタリング
1	wan	all-nets	195.66.77.1	10	On
2	dsl	all-nets	193.54.68.1	20	Off

ルートモニタリングがバックアップのフェイルオーバルートではなく、はじめのルートに対して有効となることに注意してください。

選択された wan 経路が正常である限り、すべてが予想通りに動作します。また、ルートモニタが機能しているので、wan ルートがエラーになると、セカンダリルートが有効となります。

しかし、この設定にはいくつかの問題点があります。ルートフェイルオーバが発生すると、その時デフォルトルートは dsl インタフェースを使用します。次に、新しい HTTP 接続が確立される場合、ルート索引は、dsl の宛先インタフェースで行われます。その後、IP ルールが評価されますが、オリジナルの NAT IP ポリシーは、宛先インタフェースが wan であると見なし、新しい接続はルールセットによって破棄されます。
また、さらに、宛先インタフェースの変更の結果、NAT ルールに一致する既存の接続はすべて破棄されます。明らかに、これは望ましくない結果です。

この問題を解決するために、フェイルオーバ先となり得る宛先インタフェースはインタフェースグループにグループ化して、接続がインタフェース間で移動されるように Security/Transport Equivalent オプションをグループに対して有効にするべきです。そして、ポリシー設定時に、インタフェースグループを宛先インタフェースとして使用します。インタフェースグループに関する詳しい情報は、「3.4.10 インタフェースグループ」を参照してください。

Gratuitous ARP Generation

初期状態では、ルートフェイルオーバが発生すると、NetDefendOS は Gratuitous ARP リクエストを生成します。これはルート変更があったことを周囲のシステムに通知するためです。この動作は **Network > Routing > Routing Settings** の「Gratuitous ARP on Fail」で制御することができます。

4.2.4 ルートフェイルオーバのためのホストモニタリング

概要

ルートの保全をモニタリングする、より柔軟で設定しやすい方法を提供するために、NetDefendOS はホストモニタリングを実行する追加機能を提供します。本機能は、特定のルートが利用可能であることをチェックするために 1 台以上の外部ホストシステムが定期的にポーリングを行うものです。

ホストモニタリングには 2 つの利点があります。

- 複雑なネットワークトポロジでは、外部ホストへのアクセス性をチェックすることがより信頼性を高めます。ローカルスイッチとのリンクをモニタリングするだけでは、内部ネットワークの別の部分にある問題を提示することはできません。
- ホストモニタリングは、インターネット応答回数の許容可能な QoS レベルの設定を補助するために使用されます。インターネットアクセスは機能しても、応答待ち時間が既存のルートを使用することを受け入れられなかった場合に、ルートフェイルオーバを起動することが望ましいと言えます。

ホストモニタリングの有効化

Route オブジェクトのプロパティとして、ホストモニタリングを有効にし、1 つのルートでモニタリング用に複数のホストを関連付けることができます。複数の複数のホストをモニタリングすることにより、リモートホスト自身がダウンしているのではなく、ローカルネットワーク内に問題が存在するということを、より確実性を持って確認することができます。

ホストモニタリングに関連して、ルートには以下の項目があります。

項目	説明
Grace Period（猶予期間）	D-LInk ファイアウォールの起動後または再構成後、モニタリング開始する前に NetDefendOS が待機する時間です。この待ち時間によって、ファイアウォールがオンラインになった際に、全てのネットワークリンクにおいて初期化が実行されるようにします。
Minimum Number of Hosts Reachable（到達可能なホストの最小数）	全てのホストまたは指定したホストが利用不可の場合、ルートがエラーであるとみなされます。All または Specific を選択します。Specific を選択した場合、Minimum Reachable Hosts を選択します。
Minimum Reachable Hosts	アクセス可能なホスト数がこの値を下回ると、ルートがエラーであるとみなされます。

ホストの指定

ホストモニタリングに指定された各ホストのために、設定の必要がある多くのプロパティがあります。

項目	説明
Method	ホストがポーリングされる方法を選択します。 • ICMP - ICMP「Ping」のポーリング。これには IP アドレスを指定します。 • TCP - TCP 接続が確立され、ホストから切断されます。これには IP アドレスを指定します。 • HTTP - URL を使用する通常の HTTP サーバリクエストです。有効なレスポンスのはじめ（またはすべて）の文字列で URL を指定します。指定しないと、サーバからのすべての応答が有効になります。
IP Address	ICMP または TCP オプションを使用する場合のホストの IP アドレス。
Port	TCP オプションを使用する場合のポーリング用ポート番号。
Source IP Selection	外向きのパケットモニタリングのための送信元 IP を指定できます。初期値では、送信側インタフェースの IP アドレス（Automatic オプション）が使用されますが、このプロパティを Manual に設定して、IP アドレスを指定することで設定できます。
Polling Interval	ポーリングの試みの間隔（ミリ秒）。初期値は 10,000ms で、設定可能な最小値は 100ms です。
Sample	Percentage Loss と Average Latency を計算するためにサンプルとして使用されたポーリング実行数。この値は 1 未満にはできません。
Max Poll Fails	失敗するポーリングの試みの最大許容数。この数を超えると、未到達状態と見なされます。
Max Average Latency	ポーリングリクエストと応答の間で許容できる最大時間（ミリ秒）。このしきい値を超過すると、ホストは未到達状態と見なされます。Average Latency は、ホストからの応答時間を平均化することによって計算されます。ポーリングに対する応答を受信しないと、平均化計算には含まれません。

Reachability Required オプション

Reachability Required オプションは、ホストに対して有効な重要なオプションです。これを選択する場合、そのルートが機能していると見なされるために、ホストは、アクセス可能であると判断される必要があります。他のホストがアクセス可能であっても、このオプションが設定されたホストについてはアクセス可能であることが必須となります。

複数のホストがホストモニタリングに指定される場合には、1 つ以上のホストで Reachability Required を有効することが可能です。NetDefendOS が、このオプションが有効であるホストが 1 台でも未到達であると判断すると、ルートフェイルオーバが開始されます。

HTTP パラメータ

HTTP ポーリングが選択される場合、さらに 2 つのパラメータを入力することができます。

項目	説明
Request URL	リクエストされる URL。
Expected Response	URL の問い合わせから戻ってくると予想されるテキスト。 特定のレスポンステキストのテストは、アプリケーションがオフラインであるかどうかをテストすることができます。例えば、サーバからの Web ページの「Database OK」などのテキストによる応答が、指定データベースが操作可能であることを示している一方で、その応答がない場合は、サーバの操作はできても、アプリケーションはオフラインである可能性を示しています。

外部ルートが指定されていない場合の既知の問題

インターネット ISP に接続している場合、通常、外部ネットワークのルートを指定する必要があります。この外部ルートは、D-Link ファイアウォールと ISP の間に存在するネットワークが、どのインタフェースで見つけることができるかを指定するものです。all-nets ルートだけが ISP のゲートウェイに指定されると、接続する装置によっては、ルートフェイルオーバは予想通りに機能しないかもしれません。

この問題はめったに起こりませんが、これは、無効なルートに到着する ARP クエリが無視されるために起こるものです。

4.2.5 ルートフェイルオーバのアドバンスド設定

以下の NetDefendOS アドバンス設定はルートフェイルオーバに使用することができます。Web インタフェースの **Network > Routing > Routing Settings** で設定することができます。

項目	説明
Iface poll interval	インタフェースエラーのポーリング間隔（ミリ秒）。 初期値 : 500
ARP poll interval	ホストの ARP 検索間隔（ミリ秒）。これは個別のルートで変わる可能性があります。 初期値 : 1000
Ping poll interval	Ping をホストに送信する間隔（ミリ秒）。 初期値 : 1000
Grace time	起動または再構成からモニタリング開始までの長さ（秒）。 初期値 : 30
Consecutive fails	ルートが無効であるとしてマークされるまでに発生する連続失敗数。 初期値 : 5
Consecutive success	ルートが有効であるとしてマークされるまで発生する連続成功数。 初期値 : 5
Gratuitous ARP on fail	HA フェイルオーバ時、インターネットインタフェースや IP アドレスの変更をホストに通知するために Gratuitous ARP を送信します。 初期値 : Enabled
Gratuitous Proxy ARP On Fail	フェイルオーバ時、ARP キャッシュ内のプロキシ ARP ホストのインタフェースイーサネットアドレスの変更についてホストに通知するために Gratuitous ARP パケットを送信します。 初期値 : Disabled

4.2.6 プロキシ ARP

概要

「3.5 ARP」で説明した通り、ARP プロトコルは、イーサネットネットワーク上のノードの IP アドレスと MAC アドレスをマッピングする手助けをします。

しかし、イーサネットが動作するネットワークが D-Link ファイアウォールのようなルーティングデバイスにより 2 つのセグメントに分割されているという状況では、NetDefendOS 自身がプロキシ ARP を使用することで D-Link ファイアウォールの反対側にあるネットワークへの ARP リクエストに応じることができます。

イーサネットネットワークを分割して、その間のトラフィックを制御できるようにすることは、プロキシ ARP 機能の一般的な利用法です。それに加えて、NetDefendOS ルールセットは異なるネットワーク間を通過するトラフィックにセキュリティポリシーを課すために使用されます。

典型的なシナリオ

典型的なプロキシ ARP のシナリオの例として、2 つのサブネットワークに分割されたネットワークでそれぞれ D-Link ファイアウォールが配置されているシナリオについて考えてみます。

例えば、あるサブネットにあるホスト A は、ARP リクエストを送信して、別のサブネットワークにあるホスト B の IP アドレスに対応する MAC アドレスを検出します。プロキシ ARP 機能を設定すると、NetDefendOS がホスト B の代わりに、この ARP リクエストに応答します。NetDefendOS は、ターゲットホストであるようなふりをして、応答の代わりに自身の MAC アドレスを送信します。応答を受信後、ホスト A は、ホスト B にデータを転送する NetDefendOS に直接データを送信します。処理中に、NetDefendOS は構成されたルールセットに対してトラフィックのチェックを行います。

プロキシ ARP の設定

プロキシ ARP の設定は、ルーティングテーブル内のルートにオプションを指定することによって行われます。「net_1」と「net_2」と呼ばれる 2 つの部分に分割されたネットワークがあるものとします。

ネットワーク「net_1」はインタフェース「if1」に接続し、ネットワークネット「net_2」はインタフェース「if2」に接続しています。NetDefendOS には、「net_1」が「if1」で検出されることを設定したルートがあります。これを「route_1」と呼びます。

「route_1」に対して、このネットワークがインタフェース「if2」にプロキシ ARP を実行するべきであるというオプションを指定することができます。「net_1」内の IP アドレスを検索している「if2」に接続する「net_2」ホストが発行する ARP リクエストは、NetDefendOS から肯定的な応答を取得します。つまり、NetDefendOS は「net_1」アドレスが「if2」で検出されるふりをして、「net_1」にデータトラフィックを送信します。

同様にパブリッシュされているルートと ARP プロキシのミラーリングが存在するように、「net_2」がインタフェース「if1」でパブリッシュされます。

経路 #	ネットワークインタフェース	プロキシ ARP	パブリッシュされたプロキシ ARP
1	net_1	if1	if2
2	net_2	if2	if1

このように、サブネットワークの完全分離がありますが、ホストはこれを認識しません。ルートは相互にミラーイメージであるペアですが、プロキシ ARP がこのようにペアリングに使用される必要はありません。

ホストがローカルネットワークの外側の IP アドレスに対する ARP リクエストを持っていると、このリクエストはそのホストに設定されたゲートウェイに送信されることを覚えておいてください。例題の全体を以下で図示しています。

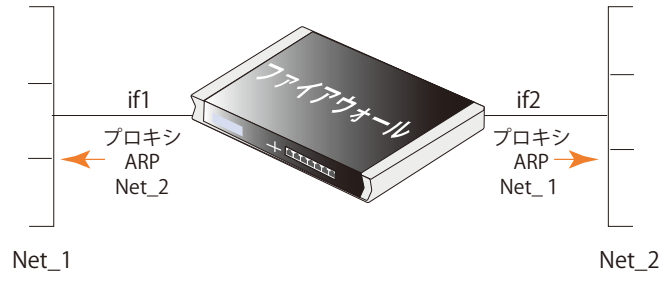


図 4-4　プロキシ ARP の例

代替策としての透過モード

透過モードはイーサネットネットワークを分割する別の推奨される方法です。設定は管理者が適切な switch ルートを定義するだけでよいので、プロキシ ARP を使用するよりも簡単です。switch ルートの使用については、「4.9 透過モード」を参照してください。HA クラスタでは、switch ルートは使用できません。

プロキシ ARP は、通常、スタティックルーティングに依存しており、このルーティングではインタフェース上のネットワーク位置が固定されています。透過モードは、インタフェース位置が変更され得るネットワークにより適しています。

プロキシ ARP と高可用性クラスタ

HA クラスタでは、switch ルートが使用できないため、透過モードがオプションとして選択できません。一方で、プロキシ ARP は HA と一緒に動作することが可能であるため、これがクラスタ環境で透過モード機能を実装する唯一の方法となります。

参照 どんなインタフェースもプロキシ ARP を利用できるというわけではありません。

イーサネットと VLAN インタフェース上でのみプロキシ ARP は有効です。ARP が関係しないため、プロキシ ARP は他のタイプの NetDefendOS インタフェースに関連しません。

自動的に追加されたルート

プロキシ ARP は、自動的に追加されたルートで有効とすることはできません。例えば、NetDefendOS が物理インタフェースに初期のスタートアップで作成するルートは、自動的に追加されるルートです。これらのルートでモニタリングを有効にすることができない理由は、自動的に作成されたルートが NetDefendOS 構成内で特別なステータスを持っており、別に扱われるためです。

プロキシ ARP が自動的に作成されたルートで必要である場合、そのルートを最初に削除し、新しいルートとして手動で再作成する必要があります。そうすることで、新しいルートにプロキシ ARP を有効にすることができます。

4.2.7 ブロードキャストパケットの転送

ブロードキャストパケットは、ネットワークで最も大きい値の IP アドレスを持っているパケットであり、関連する MAC アドレス FF:FF:FF:FF:FF:FF を持っています。例えば、ネットワーク 192.168.1.0/24 のブロードキャストパケットには、IPv4 アドレス 192.168.1.255 があります。

初期値では、NetDefendOS はインタフェースに到着するそのようなすべてのブロードキャストパケットを破棄します。いくつかの状況では、特に透過モードを使用する場合、トラフィックを送信するべきかどうかを判断するために経路検索および IP ルールセットのエントリを適用することによって、NetDefendOS がトラフィックを他のインタフェースに転送することが望ましいと言えます。

ブロードキャストパケットの転送の有効化

ブロードキャストパケットの転送を有効にするためには、管理者は以下の手順を実行する必要があります。

- Route オブジェクトの Forward Broadcast Traffic プロパティを有効にします（CLI では BroadcastFwd プロパティ）。パケットの送信元と宛先インタフェースの両方のルートでいつも有効にする必要があります。
- 非透過モードのトラフィックのみに対しては、ブロードキャストの転送が行われるように、グローバル IP 設定の Direct Broadcast を有効にする必要があります。設定値は初期値で DropLog であり、ブロードキャストパケットを送信するためには Ignore または Log を設定する必要があります。

ブロードキャストパケットの転送を有効にしている場合でも、NetDefendOS はブロードキャスト IPv4 アドレスが FF:FF:FF:FF:FF:FF の MAC アドレスにマッチすることを確認するため、インタフェースに到着するブロードキャストパケットのチェックを行います。マッチしないパケットは破棄されます。

ブロードキャスト転送の際にアドレス変換を使用する

ブロードキャスト転送されたトラフィックにアドレス変換を使用する場合、以下の項目について注意するべきです。

- **SAT**
  SAT 変換は、適切な場合、ブロードキャストパケットに対して行われます。SAT 変換を使用すると、宛先アドレスは通常ブロードキャストアドレスとなります。
- **NAT**
  透過モードは、ブロードキャストパケットに NAT 変換を使用できません。NAT IP ポリシーに出会うと、パケットは破棄されて、ログメッセージが生成されます。

  非透過モードルーティングではブロードキャストパケットに NAT を使用できます。これはいくつかのまれなネットワークシナリオに適切であるかもしれません。

透過モードのブロードキャスト転送は常にステートレスである

透過モードにあるとき、ブロードキャストパケットが NetDefendOS によって常にステートレスで送信されることに注意することが重要です。言い換えれば、アクション Allow を持つ IP ルールセットのエントリが、透過モードのブロードキャストパケットのフローを許可している場合であっても、エントリがステートレスポリシー（FwdFast IP ルール）に設定されているかのようにパケットを送信します。

ステートレス送信を実施する理由は、パケットが複数のインタフェースで複製されて、転送される必要があるかもしれないからです。ブロードキャストパケットが複製されない非透過ルートといった通常のルートでは、通常の Allow ルールやポリシーを使用し、トラフィックをステートフルに処理することができます。ステートフルルール / ポリシーには、パケットの多くが同じ送信元から来る場合、ブロードキャストパケットを処理する際にハードウェアリソースの使用が少ないという利点があります。

ブロードキャストパケットに対してのみ起動する IP ポリシー

ブロードキャストパケットに対してのみトリガされる IP ポリシーを作成する場合、送信先ネットワークプロパティがブロードキャスト IP アドレスとなるように設定する必要があります。しかし、送信先ネットワークはブロードキャストアドレスが所属するネットワークであるべきです。例えば、IPv4 ネットワーク 10.0.0.0/8 のためのブロードキャストパケットは、アドレス 10.255.255.255（ネットワークで最も大きい値の IP アドレス）を持ちます。そのため、これらのパケットをターゲットとする IP ポリシーでは送信元ネットワークプロパティは 10.0.0.0/8 で、送信先ネットワークプロパティは 10.255.255.255 に設定されるべきです。

ブロードキャストパケットのログメッセージ

（switch ルートを使用した）透過モードにある場合、ログメッセージは IP ルールセットのエントリのトリガとなるブロードキャストパケットに対してのみ生成されます。生成できるメッセージは以下の 2 つだけです。

- **allow_broadcast**
  このログメッセージは、ブロードキャストパケットが、透過モードでアクション Allow を持つ IP ルールセットのエントリのトリガとなる度に生成されます。まるで、ルールにアクション FwdFast（またはポリシーは Stateless Policy）があるかのように、パケットがステートレスに送信されたことを示します。このタイプの代表的なログメッセージは以下に類似しています。

```
prio=Notice id=06000016 rev=1 event=allow_broadcast
action=stateless_fwd rule=a recvif=If3 srcip=192.168.100.25
destip=192.168.100.255 ipproto=UDP ipdatalen=58 srcport=137
destport=137 udptotlen=58
```

ブロードキャストパケットが送信されるあらゆるインタフェースについて、このイベントメッセージが生成されることに注意するべきです。例えば、透過モードを使用した同じネットワークにインタフェースの if1、if2、および if3 がすべて定義されると、ネットワークのブロードキャストパケットは、2 回ポリシーのトリガとなり、2 つのログメッセージを生成する可能性があります。これはブロードキャストパケットが 1 つのインタフェースに到着して、他の 2 つのインタフェースへの転送が必要となるためです。

トリガとなる IP ポリシーに対するログメッセージを無効にすることで、複数のログメッセージをすべてオフにできます。

- **broadcast_nat**
  ブロードキャストパケットが透過モードの NAT IP ポリシーのトリガとなり、破棄されたときに生成されます。このタイプの代表的なログメッセージは以下に類似しています。

```
prio=Notice id=06000014 rev=1 event=broadcast_nat action=drop rule=a
recvif=If3 srcip=192.168.100.25 destip=192.168.100.255 ipproto=UDP
ipdatalen=58 srcport=137 destport=137 udptotlen=58
```

NAT ルールのトリガとなるブロードキャストパケットは、オプションでログメッセージが生成されると共に警告なしで破棄されます。これは TransparentBroadcastNAT と呼ばれるグローバル設定によって制御されます。この設定の初期値は DropLog です。ログメッセージが生成されない場合でも Drop に設定されるべきです。

例題 4.4

ルートにおけるブロードキャスト転送を有効にする

この例題では、main ルーティングテーブルの 3 番目のルートである定義済みルートへのブロードキャストパケットの転送を有効にする方法を示しています。

CLI

まず、非透過モードのトラフィックに対するブロードキャスト転送をグローバルに有効にします。

```
DFL-xxxx:/> set Settings IPSettings DirectedBroadcasts=Log
```

次に、関連ルートへのブロードキャスト転送を有効にします。コンテキストを main ルーティングテーブルに変更します。

```
DFL-xxxx:/> cc RoutingTable main
```

Foward Broadcast Traffic オプションを有効にします。

```
DFL-xxxx:/main> set Route 3 BroadcastFwd=Yes
```

初期値の CLI コンテキストに戻します。

```
DFL-xxxx:/main> cc
DFL-xxxx:/>
```

Web Interface

まず、非透過モードのトラフィックに対するブロードキャスト転送をグローバルに有効にします。

1. **System > Advanced Settings > IP Settings** の順にメニューをクリックします。
2. Directed Broadcasts を Log に設定します。
3. 「OK」ボタンをクリックします。

次に、関連ルートへのブロードキャスト転送を有効にします。

1. **Network > Routing > Routing Tables > main** の順にメニューをクリックします。
2. 設定対象のルートを選択します。
3. Forward Broadcast Traffic オプションを有効にします。
4. 「OK」ボタンをクリックします。

4.3 ポリシーベースルーティング

概要

ポリシーベースルーティング（PBR:Policy Based Routing）は、既述した標準のルーティングに対する拡張機能です。指定した基準に従って異なるルーティングテーブルを使用することにより、管理者にとって有意義で柔軟なルーティング決定ポリシーを提供します。

通常のルーティングは、スタティックな経路または動的ルーティングプロトコルから取得した送信先 IP アドレス情報に従って、パケットを転送します。例えば、OSPF を使用して、パケットに対して選択された経路は、SPF 計算から取得した最小コスト（最短コスト）経路です。ポリシーベースルーティングでは、特定のトラフィックパラメータに基づいてトラフィックの経路を決定できます。

ポリシーベースルーティングでは以下のことが可能です。

- 送信元ベースのルーティング
  トラフィックの送信元に基づいて、異なるルーティングテーブルが選択されます。インターネットサービス提供のために 1 つ以上の ISP を使用する場合、ポリシーベースルーティングは、異なる経路を経由して、さまざまなユーザグループから生成されるトラフィックの経路を決めることができます。例えば、あるアドレス範囲のトラフィックは 1 つ目の ISP を経由し、別のアドレス範囲のトラフィックは 2 つ目の ISP を経由するなどの場合です。

- サービスベースのルーティング
  サービスに基づいて、異なるルーティングテーブルが選択されます。ポリシーベースルーティングは、Web キャッシュなどの透過プロキシを通じて、HTTP など特定のプロトコルの経路を決めることができます。1 つの ISP ですべての HTTP トラフィックを扱うよう、複数の特定サービスを 1 つの特定の ISP に経由させることもできます。

- ユーザベースのルーティング
  ユーザ ID やユーザの所属するグループに基づいて、異なるルーティングテーブルが選択されます。すべてのユーザが共通のアクティブなバックボーンを共有しながらも、さまざまな ISP に申し込みを行い、異なる ISP を使用するような、プロバイダから独立したメトロポリタンエリアネットワークにおいて、これは特に便利です。

PBR コンポーネント

NetDefendOS におけるポリシベースルーティングは、以下の 2 つのコンポーネントを使用して実行されます。

- 追加のルーティングテーブル
  標準の初期 main ルーティングテーブルに加え、ユーザ定義の 1 つ以上の代替ルーティングテーブルが作成されます。

- ルーティングルール
  どのルーティングテーブルをトラフィックに使用するかを決定する、1 つ以上のルーティングルールが作成されます。

  ルーティングルールがないと、main ルーティングテーブルが初期値です。しかし、ルールを使用せずに特定のインタフェースのためのデフォルトテーブルとして明示的に代替のルーティングテーブルを割り当てることもできます。

ルーティングテーブル

NetDefendOS は、標準として、main と呼ばれる 1 つのデフォルトルーティングテーブルを持っています。main テーブルに加え、ポリシーベースルーティングのために 1 つ以上の追加ルーティングテーブルを定義できます。（これらは、代替のルーティングテーブルと呼ばれることもあります。）

代替ルーティングテーブルには、各テーブルについて定義された追加のプロパティが並ぶ以外は、main と同様の経路説明情報が含まれています。Ordering プロパティは、main テーブルと共に代替テーブルを使用して、経路検索を行う方法を規定します。これは以下でさらに説明します。

注意 テーブル数はモデルによって制限されます。

作成できるルーティングテーブルの最大数は D-Link ハードウエアモデルのタイプによって制限されます。

例題 4.5

ルーティングテーブルの作成

MyPBRTable と呼ばれる新しいルーティングテーブルを作成し、Ordering プロパティセットを First に設定します。

CLI

ルーティングテーブルの追加

```
DFL-xxxx:/> add RoutingTable MyPBRTable Ordering=First
```

Web Interface

ルーティングテーブルの追加

1. **Network > Routing > Routing Tables** の順にメニューをクリックします。

2. 「Add」から「Routing Table」を選択します。

3. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : MyPBRTable
- Ordering から 1 つを選択します。
  - First - 指定されたルーティングテーブルがはじめに参照されます。この検索に失敗すると、検索は main ルーティングテーブルで継続します。
  - Default - main ルーティングテーブルははじめに参照されます。唯一の一致がデフォルト経路（all-nets）であれば、指定されたルーティングテーブルが参照されます。指定されているルーティングテーブルの検索に失敗すると、全体が失敗したと見なされます。
  - Only - 指定されているルーティングテーブルだけを参照します。この検索に失敗すると、検索は main ルーティングテーブルで継続しません。

4. 「Remove Interface IP Routes」が有効になると、core インタフェースへのルート（NetDefendOS 自身へのルート）であるデフォルトのインタフェースルートは削除されます。

例題 4.6

ルートの追加

ルーティングテーブル MyPBRTable の定義後に、テーブルにルートを追加できます。ネットワーク my_network に対するルートが lan インタフェースに定義されているものとします。

CLI

コンテキストをルーティングテーブルに変更する

```
DFL-xxxx:/> cc RoutingTable MyPBRTable
```

ルートの追加

```
DFL-xxxx:/> add Route Interface=lan Network=my_network
```

Web Interface

1. **Network > Routing > Routing Tables > MyPBRTable** の順にメニューをクリックします。

2. 「Add」から「Route IPv4」を選択します。

3. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Interface : lan
- Network : my_network
- Gateway : ゲートウェイルータは 1 つあるものとします。
- Local IP Address : ここで指定した IP アドレスは、対応するインタフェースで自動的にパブリッシュされます。また、このアドレスは ARP クエリ内で送信元アドレスとして使用されます。アドレスを指定しないと、ファイアウォールのインタフェース IP アドレスが使用されます。
- Metric : このルートに対するメトリックを指定します。（主としてルートフェイルオーバのシナリオで使用されます。）

ルーティングルール

ルーティングルールセットにおけるルールは、選択するルーティングテーブルを決定します。ルーティングルールには、IP ルールセットのエントリに使用されるものと同様に多くのフィルタリングプロパティがあります。ルールは、指定した送信元 / 送信先インタフェースと送信元 / 送信先ネットワークを組み合わせて、サービスタイプ（例 :HTTP）によって起動されます。

ルーティングルールを検索中、はじめに一致したルールが実行されます。

例題 4.7

ルーティングルールの作成

この例では、my_routing_rule と言う名称のルーティングルールを作成します。ネットワーク my_network に到達するすべての http トラフィック用にルーティングテーブル MyPBRTable を選択します。

CLI

```
DFL-xxxx:/> add RoutingRule Service=http SourceInterface=any SourceNetwork=all-nets DestinationInterface=any
            DestinationNetwork=my_network ForwardRoutingTable=MyPBRTable ReturnRoutingTable=MyPBRTable
            Name=my_routing_rule
```

Web Interface

1. **Network > Routing > Static Routes > Policy-based Routing Rules** の順にメニューをクリックします。
2. 「Add」から「Routing Rule」を選択します。
3. 以下の情報を入力し、「OK」ボタンをクリックします。
   - Name : my_routing_rule
   - Service : http
   - SourceInterface : any
   - SourceNetwork : all-nets
   - DestinationInterface : any
   - DestinationNetwork : my_network
   - ForwardRoutingTable : MyPBRTable
   - ReturnRoutingTable : MyPBRTable
4. 「Remove Interface IP Routes」プロパティが有効になっていると、core インタフェースへのルート（NetDefendOS 自身へのルート）であるデフォルトのインタフェースルートは削除されます。

ルーティングルールは IPv4 または IPv6 アドレスを使用可能

ルーティングルールは、ルールのフィルタリングプロパティの送信元および送信先ネットワークとして IPv4 または IPv6 アドレスのいずれかをサポートしています。

しかし、送信元および送信先ネットワークの両方を IPv4 または IPv6 のいずれかにする必要があります。単一のルールで IPv4 と IPv6 アドレスを組み合わせることはできません。

詳しくは、「3.2 IPv6 のサポート」を参照してください。

フォワードルーティングテーブルとリターンルーティングテーブルを別にできます。

多くの場合、フォワードおよびリターントラフィック用へのルーティングテーブルは同じテーブルとなります。しかし、異なる値を持つことが有利である場合があります。

以下の例では、2つのISPに接続されたインタフェースwan1とwan2、およびlf1インタフェース上の保護されたネットワークlf1_netの設定を持つファイアウォールを示しています。以下に示す 2 つのルーティングテーブル、main ルーティングテーブルおよび isp2 ルーティングテーブルがあります。

main ルーティングテーブル

インデックス #	インタフェース	ネットワーク	ゲートウェイ
1	lf1	lf1_net	
2	wan1	all_nets	isp1_ip

isp2 ルーティングテーブル

インデックス #	インタフェース	送信先	ゲートウェイ
1	wan2	all_nets	isp2_ip

wan2 を通過するトラフィックが lf1_net にアクセスする場合、ルーティングルールは以下のように構成される必要があります。

送信元 インタフェース	送信元 ネットワーク	送信先 インタフェース	送信先 ネットワーク	送信 ルーティングテーブル	送信 ルーティングテーブル
wan2	all-nets	any	lf1_net	main	isp2

本ルールにより、wan2 テーブルを通過する送信トラフィックは main ルーティングテーブルで lf1_net に対するルートを検出できます。リターントラフィックは、接続の開始者に到達できるように isp2 テーブルを使用します。
また、本例では、おそらく lf1_net がプライベート IP ネットワークとなるため、いくつかのアドレス変換を持つ必要があります。
簡略化のために、それは省略しています。

明示的インタフェース / ルーティングテーブルアソシエーション

サービスにかかわらず特定の送信元インタフェースからのトラフィックに特定のルーティングテーブルが常に使用される場合、インタフェースの R ルーティングテーブルのメンバシッププロパティを使用して、特定のテーブルに送信元インタフェースを明示的に関連付けることができます。

明示的な関連付けのこの方式が異なる点は、管理者がルックアップを適用する HTTP などのサービスを指定できないということです。ルーティングルールでは、特定のサービスとインタフェース / ネットワークフィルタを選択することもできるため、ルーティングテーブル選択に対してきめの細かいアプローチが可能となります。

ルーティングテーブルの選択処理

新しい接続に関わるパケットが最初に到着した時、次の処理手順で使用するルーティングテーブルを決定します。

1. ルーティングルールが最初に調べられます。これを実行するには、main ルーティングテーブルで常に実行される初期の経路検索を使用して、パケットの宛先インタフェースを決定する必要があります。そのため、送信先ネットワークに一致が見つけられることが重要です。これを確実にするために、明示的ではないが、一致するすべてをとらえることができるデフォルト all-nets ルートを少なくとも持つことをお勧めします。

2. ここではじめて、パケットの送信元 / 送信先インタフェースおよびネットワークとサービスとが一致するルーティングルールについて、検索が実行されます。一致するルールが見つかると、次に、使用するルーティングテーブルを決定します。ルーティングルールが見つからない場合は、main テーブルが使用されます。

3. マッチしているルーティングルールが全く見つからないと、受信しているインタフェースが特定のルーティングテーブルのメンバであるかどうか参照するためにチェックが行われます。インタフェースがルーティングテーブルのメンバシッププロパティを通じて、特定のルーティングテーブルに関連すると、そのルーティングテーブルが使用されることが決定します。メンバシップが見つからない場合は、main テーブルが使用されます。

4. 正しいルーティングテーブルが決定されたら、受信するインタフェースに送信元IPアドレスが実際に存在するかどうかのチェックが行われます。まずアクセスルールを検査し、このチェックを行うことができるかどうかを確認します。本機能の詳細については、「7.1 アクセスルール」を参照してください。アクセスルールがないか、または、ルールと一致するアドレスが見つからない場合は、送信元 IP アドレスを用いて、先に選択したルーティングテーブル内のリバース検索が実行されます。チェックが失敗すると、デフォルトのアクセスルールログエラーメッセージが生成されます。

5. この時点で、選択したルーティングテーブルを使用して、実際の経路検索が実行され、パケットの送信先インタフェースが検索されます。ここで、実際に行われる検索の方法を規定するためにルーティングテーブルの Ordering プロパティが使用されることに注意してください。オプションについては次のセクションで説明します。仮想システムを実装するためには、プロパティは Only に設定されるべきです。

6. 接続はその後、通常の IP ルールセットの対象となります。SAT が発生すると、アドレス変換が実行されます。使用するルーティングテーブルは、アドレス変換より前に決定されますが、実際の経路検索は、変更されたアドレス上で実行されます。（すべてのルール検索に使用された送信先インタフェースを検索するための元の経路検索は、変換されていない元のアドレスで実行されたことに注意してください。）

7. IP ルールセットで許可されると、NetDefendOS のステートテーブルで新しい接続が開始され、この接続を介してパケットが送信されます。

配列パラメータ

新しい接続用のルーティングテーブルが選択され、そのテーブルが代替ルーティングテーブルであった場合、そのテーブルに関連する配列（Ordering）パラメータを用いて、その代替テーブルを main テーブルとどのように組み合わせて適切な経路を検索するのかを決定します。3 種類のオプションが利用できます。

1. Default
   デフォルトの動作では、はじめに main テーブル内のルートが検索されます。一致する経路が見つからないか、または、デフォルトの経路（送信先 all-nets の経路）が見つかった場合、代替テーブル内で一致経路の検索が行われます。代替テーブルで一致が見つからない場合は、main テーブルのデフォルト経路が使用されます。

2. First
   最初に代替テーブル内で接続の経路を検索します。一致する経路が見つからない場合は、main テーブルが検索されます。main テーブルで一致する経路が見つかった場合は、デフォルトの all-nets 経路が、代替テーブルでの一致としてカウントされます。

3. Only
   このオプションでは、代替テーブル以外の他のテーブルの存在が無視されるため、代替テーブルだけが検索に使用されます。このオプションを適用する例として、1 つのルーティングテーブルを 1 セットのインタフェース専用に用いる方法を管理者に提供することが挙げられます。ルーティングテーブルを 1 セットのインタフェース専用にできるので、仮想システムを作成する時には Only オプションを使用します。

main テーブルと代替テーブル両方に一致がある場合、はじめの 2 つのオプションは、代替テーブルと main テーブルを組み合わせて 1 つの経路を割り当てる方法であると見なせます。

注意 main テーブル内に「all-nets」経路を必ず置いてください。

ポリシーベースルーティング設定の際によく見られる誤りは、main ルーティングテーブルにデフォルトの all-nets ルートが存在しないことです。受信しているインタフェースが特定のルーティングテーブルのメンバではない限り、マッチするルートが 1 つも main にないと、トラフィックは破棄されます。これは前述の「ルーティングテーブルの選択処理」で、より詳しく説明しています。

例題 4.8

複数の ISP を使用したポリシーベースルーティング

この例題は、ポリシーベースルーティングの一般的な使用例として、複数の ISP のシナリオを示しています。

本シナリオは、以下の条件を想定しています。

- 各 ISP は、そのネットワーク範囲からユーザにひとつの IPv4 ネットワークを付与します。ここでは「ISP A」に所属する「10.10.10.0/24」と「ISP B」に所属する「20.20.20.0/24」を使用した 2 つの ISP についてのシナリオを想定しています。ISP ゲートウェイは、それぞれ「10.10.10.1」と「20.20.20.1」です。
- 簡便化のために、このシナリオのすべてのアドレスは、パブリックアドレスとしています。
- これは ISP ゲートウェイと D-Link ファイアウォールの間に明確なルーティングサブネットがない「drop-in」のシナリオです。

プロバイダと関係しないネットワークにクライアントは ISP の一つに所属する IP アドレスを一つ持っているかもしれません。単一の組織のシナリオでは、パブリックにアクセス可能なサーバが、それぞれ異なる ISP から提供される 2 つの IP アドレスで構成されます。これらシナリオの差異は、ポリシールーティングにおいては重要ではありません。

一つの組織では、複数の ISP 経由のインターネット接続が、通常 BGP プロトコルによって適切に処理されるため、異なる IP スパンやポリシールールについて考慮する必要はありません。しかしながら、ポリシーベースルーティングが必要となる場合もあります。

ここでは「ISP A」を使用するためにメインルーティングテーブルを設定し、「ISP B」のデフォルトゲートウェイを使用する「r2」という名前のルーティングテーブルを追加します。

メインルーティングテーブルのコンテンツ：

インタフェース	ネットワーク	ゲートウェイ	プロキシ ARP
lan1	10.10.10.0/24		wan1
lan1	20.20.20.0/24		wan2
wan1	10.10.10.1/32		lan1
wan2	20.20.20.1/32		lan1
wan1	all-nets	10.10.10.1	

「r2」という名前のポリシーベースルーティングテーブルのコンテンツ：

インタフェース	ネットワーク	ゲートウェイ
wan2	all-nets	20.20.20.1

テーブル「r2」は Ordering パラメータが「Default」に設定されています。これはメインルーティング検索がデフォルトルート（all-nets）に一致するかどうかだけが調査されることを意味します。

ポリシーベースルーティングポリシーのコンテンツ：

送信元インタフェース	送信元範囲	送信先インタフェース	送信先範囲	サービス	フォワード PBR	リターン PBR
lan1	10.10.10.0/24	wan1	all-nets	all_services	r2	r2
wan2	all-nets	lan1	20.20.20.0/24	all_services	r2	r2

この例題のシナリオを設定する方法：

Web Interface

1. 上記の通り、メインルーティングテーブル内の経路リストで検出される経路を追加します。

2. 「r2」という名前のテーブルを作成し、「Ordering」が「Default」に設定されていることを確認します。

3. 上記の通り、ルーティングテーブル「r2」内の経路リストで検出される経路を追加します。

4. リストに従って 2 つの PBR ルーティングルールを追加します。
- **Network > Routing > Policy-based Routing Rules > Add > Routing Rule** の順にメニューをクリックします。
- リストに示されている情報を設定します。
- この手順を繰り返して次のルールを追加します。

参照 上記例題のルーティングルールは、内向き / 外向き接続両方に追加されます。

4.4 ルートロードバランス

概要

NetDefendOS は、Route Load Balancing（RLB）を実行するためのオプションを提供します。これは、定義済みである多くの配布のアルゴリズムに基づいて複数の代替経路にトラフィックを送信する機能です。

本機能の目的は、以下の通りです。

- ポリシードリブン型でインタフェース間のトラフィックを分散します。
- 複数のインターネットリンクを同時利用している場合に負荷分散を行い、ネットワークが一つの ISP に依存しないようにします。
- 異なる物理インタフェースに設定される複数の VPN トンネルを経由したトラフィックの負荷分散を可能にします。

RLB の有効化

RLBは、ルーティングテーブルベースで有効化されます。これは、RLBインスタンスオブジェクトを作成することで行われます。このオブジェクトでは、ルーティングテーブルと RLB アルゴリズム 2 つのパラメータを指定します。テーブルは、1 つのインスタンスオブジェクトだけと関連します。

以下のリストにあるアルゴリズムの 1 つを RLB インスタンスオブジェクトに指定できます。

項目	説明
Round Robin	一致するルートは、次に一致するルートへと順々に向かうことによって、等しく使用されます。
Destination	これは、ラウンドロビンと似たアルゴリズムですが、同じ送信先 IP アドレスが同じルートを取得するように送信先 IP を提供します。アルゴリズムは常に ALG に関連して使用されます。
Spillover	特定のインタフェースのトラフィック制限が指定時間に連続して超過する場合、次のルートを使用します。

重要 ALG と共に宛先を使用する必要があります。

NetDefendOS ALG の対象となるトラフィックに Destination アルゴリズムを使用しなければなりません。Round Robin または Spillover を ALG と組み合わせて使用すると、その動作が予測通りにならない可能性があります。

RLB の無効化

ルーティングテーブルのインスタンスオブジェクトを削除すると、そのテーブルに対する RLB をオフにするという影響があります。

RLB 操作

RLB インスタンスオブジェクトを通じて RLB がルーティングテーブルに有効にされる場合、処理の手順は以下の通りです。

1. ルーティングテーブルでルート検索が行われ、一致するすべてのルートがリストに集められます。リスト内のルートは、正確に同じ IP アドレス範囲をカバーしている必要があります。以下に詳しく要件について説明します。
2. ルート検索が一致するルートを 1 つだけ検出した場合、そのルートが使用され、バランシングは行われません。
3. 一致するルートを 2 つ以上検出すると、RLB がルートの選択のために使用されます。これは、テーブルの RLB インスタンスオブジェクトから選択されたアルゴリズムに従って行われます。

- **Round Robin（ラウンドロビン）**
  ルートのメトリックが同じであれば、連続したルートは、「ラウンドロビン」型で一致するルートから選択されます。これにより、ルート検索は、一致するルートで同じメトリックを持つものに均等に広げて行われます。一致するルートが違うメトリックを持つ場合、すべてのメトリックの相対的な値に従って、より低いメトリック値を持つルートが選択されます。以下でさらに詳しく説明します。

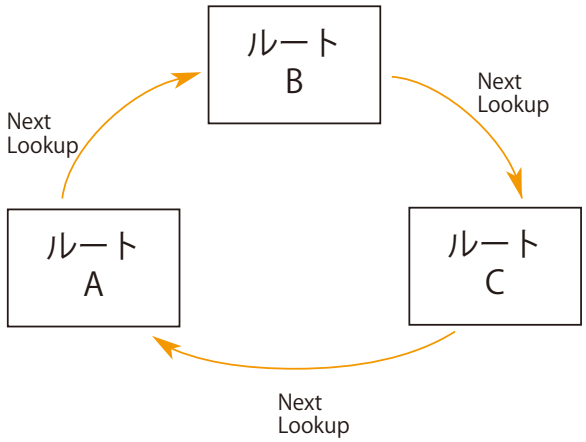


図 4-5　RLB ラウンドロビンアルゴリズム

- **Destination**
  これはラウンドロビンと似ていますが、経路検索において固有の送信先 IP アドレスが常に同じルートを取得するための「stickiness」を提供します。特定の宛先のアプリケーションが同じ送信元 IP アドレスから送信されるすべてのトラフィックを見ることができるという点が重要です。

- **Spillover（スピルオーバ）**
  前述のアルゴリズムと異なり、スピルオーバを使用すると、はじめに一致するルートのインタフェースは、ルートのインタフェースの Spillover Limits が Hold-time（秒）を継続して超過するまで繰り返し使用されます。

  指定時間を継続して超過すると、次の一致するルートが選択されます。インタフェースの Spillover Limits は、インタフェースに対して Hold-time（秒）（初期値は 30（秒））と共に RLB Algorithm Settings で設定されます。

  元のルートのインタフェースを通過するトラフィックが、Hold-time（秒）間に継続的に Spillover Limits を下回ると、ルート索引は元のルートとその関連インタフェースに復帰します。

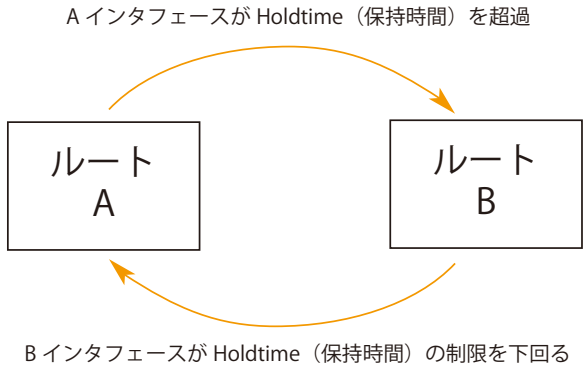


図 4-6　RLB スピルオーバアルゴリズム

Spillover Limits は、内向き及び外向きトラフィックに対して別々に設定することができます。両方が指定されている時は、Hold-time の期間にどちらかの設定を継続的に超過した場合に、次の一致ルートが選択されます。Mbps などの制限の単位を選択することができます。

ラウンドロビンを使用したルートメトリックの使用

個別のルートは、関連するメトリックとメトリックの初期値である 0 を持っています。

ラウンドロビンと関連する Destination アルゴリズムを使用して、より低いメトリックを持つルートに向かうバイパスを作成するように、メトリック値は一致するルートに対して異なる値で設定することができます。より低いメトリックを持つルートは、より高いメトリックを持つものより頻繁に選択され、その使用の割合は、一致しているルートのメトリック間の相対的な違いに基づきます。

2 つの ISP があるシナリオで、トラフィックの大半が ISP の 1 つを通過することが要件である場合、RLB を有効にし、対象の ISP へのルートに対して、低いメトリック値を設定することで、この要件を満たすことが可能です。他の ISP へのルートに対しては、相対的に高い値のメトリックを設定します。

スピルオーバでルートメトリックを使用する

スピルオーバアルゴリズムを使用する場合、メトリック及び代替ルートの選択方法に関して多くのポイントに注意するべきです。

- ルートメトリックは常に設定する必要があります。
  スピルオーバでは、NetDefendOS は常に、一致するルートリストで最も低いメトリックを持つルートを選択します。アルゴリズムは、同じメトリックを持つルートで使用されることを意図していないため、管理者はスピルオーバが適用されるすべてのルートに異なるメトリックを設定するべきです。
  メトリックは、選択ルートのインタフェーストラフィックの制限値が超過した後に、次にどのルートが選択されるべきかという明確な配列を決めるものです。

- 多くの代替ルートを持つことができます。
  インタフェース制限と、異なるメトリックを持つ複数の代替ルートを設定することができます。最も低いメトリックを持つルートは、始めに選択され、そのルートのインタフェース制限値が超過すると、次に低いメトリック値を持つルートが選択されます。

  また、新しいルートのインタフェース制限値も超過していると、次に低いメトリックを持つルートというように選択されます。
  そして、より低いメトリック値を持つルートが、そのインタフェースの Hold-time（秒）を下回ると、その選択ルートに復帰します。

- 代替ルートがないと、ルートは変更されません。
  スピルオーバ制限に到達し、すべての代替ルートも制限に達すると、ルートは変更されません。

一致する IP 範囲の要件

上記説明の通り、RLB がルーティングテーブルから一致するルートの一覧を作成する場合、選択するルートは同じ範囲を持つ必要があります。それらの範囲が正確に同じでないと、ルート間のバランシングは行われません。

例えば、1 つの一致するルートが IP 範囲 10.4.16.0/24 を持ち、次に一致するルートのアドレス範囲 IP10.4.16.0/16（10.4.16.0/24 を含む範囲）であると、RLB は、これらのルート間では行われません。範囲が正確に同じでないため、RLB はルートを異なるものとして扱います。

ルート検索は、検索に使用される宛先 IP アドレスに一致する最も狭い範囲を持つルートを選択することにご注意ください。上記の例では、10.4.16.0/24 のアドレス範囲は 10.4.16.0/16 よりも狭いため、両方の範囲を含む 10.4.16.0/24 の方が選択されます。

RLB リセット

すべての RLB アルゴリズムが初期状態にリセットするケースとして、以下の 2 つの原因があります。

- NetDefendOS の再構成後である。
- 高可用性フェイルオーバ後である。

これらの場合の両方において、選択ルートはアルゴリズムが操作を開始した時に選択されたものに戻ります。

RLB の制限

別の代替ルートの選択が行われるのは、経路検索が行われた時のみであり、検索されたルーティングテーブルで使用されるアルゴリズム及びアルゴリズムのステートに基づいているということに留意してください。

RLB は、各検索に関連するデータトラフィックの量を知ることができません。RLB の目的は、各検索が、想定するトラフィック量を送信する接続に関連するという前提で代替ルートに渡りルート検索を広げられることです。

RLB シナリオ

以下の図は、RLB が使用される典型的なシナリオを示しています。D-Link ファイアウォールの LAN インタフェース経由で接続するネットワークにクライアントのグループがあり、これらはインターネットにアクセスしています。

インターネットアクセスは、2 つの ISP から利用可能です。そのゲートウェイ GW1 GW2 は、ファイアウォールインタフェースの WAN1 と WAN2 に接続しています。RLB は、2 つの ISP 間の接続のバランスをとるために使用されます。

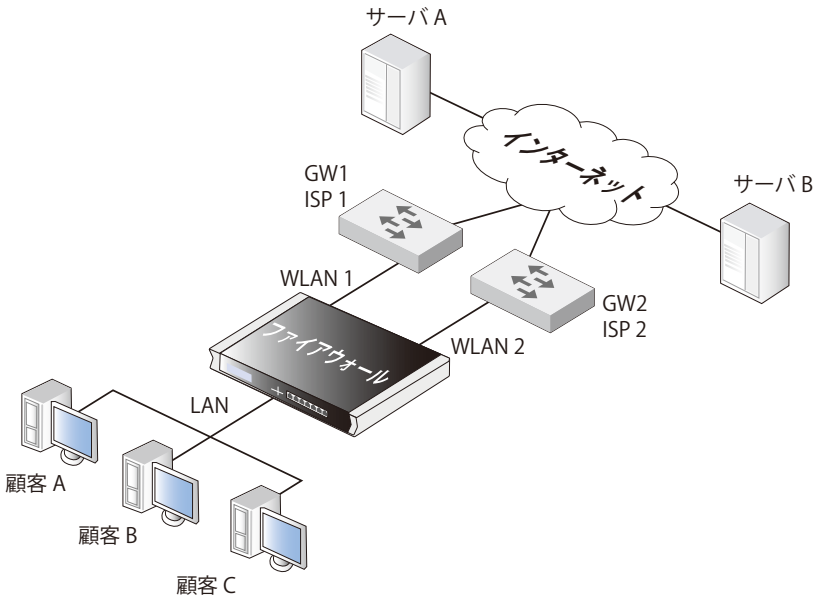


図 4-7　ルートロードバランシングのシナリオ

初めに以下の通り、ルーティングテーブル main にこれら 2 つの ISP へのルートを定義する必要があります。

経路 No.	インタフェース	送信先	ゲートウェイ	メトリック
1	wan1	all-nets	GW1	100
2	wan2	all-nets	GW2	100

この例ではスピルオーバのアルゴリズムを使用しないので、両方のルートへのルーティングメトリックは同じにします。ここでは、100 の値が選択されています。

Destination RLB アルゴリズムを使用することによって、クライアントが同じルートと同じ送信元 IP アドレスを使用することで特定のサーバとの通信を保証します。NAT がクライアント通信に使用されている場合、サーバが見る IP アドレスは、WAN1 か WAN2 となります。

すべてのトラフィックは、フローが行われるためにルートと Allow IP ルールセットのエントリの両方を必要とします。以下のルールは、トラフィックが ISP にフローすることを許可して、インタフェースの WAN1 と WAN2 の外部 IP アドレスを使用してトラフィックを NAT 変換します。

ルール No.	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
1	Allow/NAT	lan	lannet	WAN1	all-nets	all_services
1	Allow/NAT	lan	lannet	WAN2	all-nets	all_services

上記の IP ルールセットのエントリではサービス「all_services」が使用されていますが、より限定的となるように、特定のプロトコルをカバーする特定のサービスまたはサービスグループに指定するべきです。

例題 4.9

RLB を設定する

この例では、上述の RLB シナリオの詳細について実行しています。必要とされる IP アドレス帳オブジェクトは既に定義されているものとします。IP オブジェクトの WAN1 と WAN2 は 2 つの ISP に接続するインタフェースを表し、IP オブジェクトの GW1 と GW2 は 2 つの ISP のゲートウェイの IP アドレスを表します。

1. ルーティングテーブル main にルートを設定します。
2. RLB インスタンスオブジェクトを作成します。

Route Load Balancing Instance オブジェクトが作成され、スティッキー接続を行うために Destination アルゴリズムが選択されます。そのため、サーバはいつもクライアントからの同じ送信元 IP アドレス（WAN1 または WAN2）を参照します。

CLI

```
DFL-xxxx:/> add RouteBalancingInstance main Algorithm=Destination
```

Web Interface

1. Web インタフェースで RLB を設定するためには、**Network > Routing > Instances > Add > Route Balancing Instance** の順にメニューをクリックします。

2. 以下の通り入力し、「OK」ボタンをクリックします。
   - Routing Table : main
   - Algorithm : Destination

3. トラフィックのフローを許可する IP ルールセットのエントリを作成します。
   最終的にトラフィックのフローを許可する IP ルールセットのエントリを追加する必要があります。これに関する詳細な手順はここには含まれていませんが、作成済みのルールは上で説明したパターンに従います。

VPN トンネルを使用した RLB

RLB を VPN と共に使用する場合、多くの問題を克服する必要があります。

2 つの IPsec トンネル間でトラフィックのバランスをとるのに RLB を使用する場合に生じる課題は、NetDefendOS における 2 つの IPsec トンネルへのリモートエンドポイントが異なる必要があるということです。このソリューションは以下の通りです。

- それぞれのトンネルが別の ISP を経由して接続されている 2 つのトンネルを使用します。RLB は、2 つのトンネルに標準として適用されます。

  この場合、2 番目のトンネルを機能させるためには、セカンダリの ISP インタフェースに向けたルーティングテーブル main に、セカンダリ ISP ゲートウェイと共に 1 つのホストルートを追加する必要があります。

  このソリューションには、1 つの ISP リンクがエラーになった場合に冗長性を提供する利点があります。

- IPsec ベースのトンネルと、異なるプロトコルを使用する別のトンネルと共に VPN を使用します。

  例えば両方のトンネルを IPsec で接続する必要がある場合、GRE トンネルで IPsec を覆うことができます。つまり、IPsec トンネルは GRE トンネルが制御します。GRE は暗号化を行わないと簡単なトンネリングプロトコルであるため、それに伴う負荷オーバヘッドは最小となります。GRE に関する詳しい情報は、「3.4.7 GRE トンネル」を参照してください。

4.5 Active-Active セットアップ

概要

NetDefendOS には、Active-Active 構成を作成する機能があり、D-Link ファイアウォールを複数配置することにより、ロードバランシングと冗長性を持つ通信を行うことが可能です。下記の図では、内部のクライアントとインターネット間の接続を示しています。

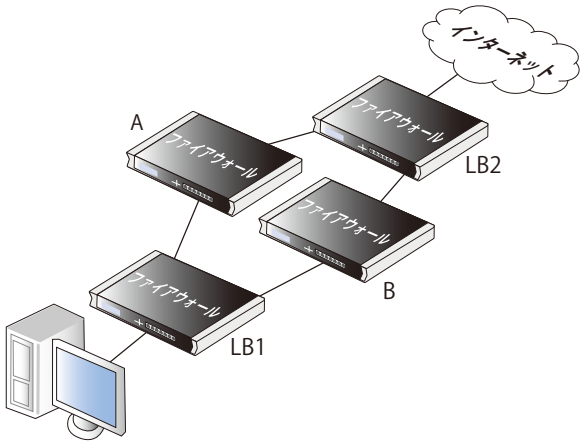


図 4-8　Acitve-Active 構成

ここで、4 つの異なる D-Link ファイアウォールが配置されているものとします。ロードバランシング機能により、ファイアウォール A と B の間で、ファイアウォール「LB1」と「LB2」が内部と外部の通信負荷を分散しています。さらに、ルートフェイルオーバ機能により、A と B の冗長性が保たれています。

セットアップ手順の概要

以下に、複数のファイアウォールを使用したセットアップ手順の概要を示します。4 台すべてが同じハードウェアモデルであり、それぞれで if1、if2、if3 のイーサネットインタフェースが設定されているものとします。

1. ファイアウォール「LB1」の設定

LB1 は、ファイアウォール A と B の間でクライアントからインターネットへの通信の負荷分散を行います。インターネット側から来る通信は、通常通り扱われます。

LB1 のインタフェース名と IP アドレスは以下の図の通りです。

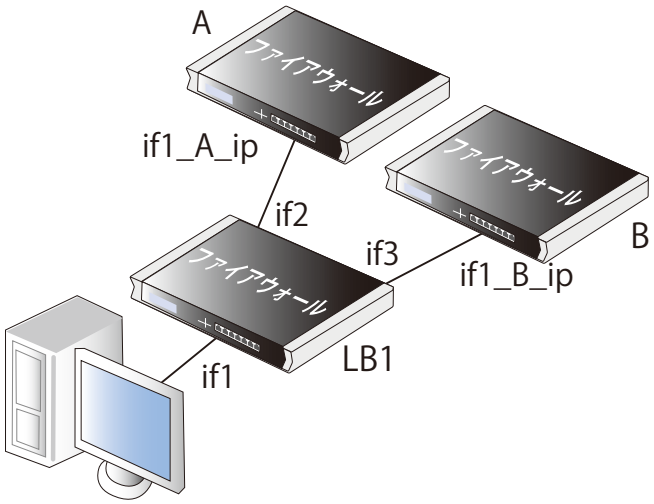


図 4-9　Acitve-Active のロードバランシング

- アドレス帳に、ファイアウォール A と B 上のインタフェースに接続する IP アドレスオブジェクトを作成します。ここでは if1_ip_A と if1_ip_B とします。

- main ルーティングテーブル上にルートを追加します。このルートのネットワークを all-nets、インタフェースを if2、ゲートウェイアドレスを if1_ip_A とします。これがファイアウォール A への経路となります。

- ルートの設定方法については「4.2.2 スタティックルーティングの設定」を参照してください。

- 新しく追加したルートで Monitor プロパティを有効化し、Monitor Interface Link Status プロパティと Monitor Gateway using ARP プロパティも有効化します。これにより、ファイアウォール A の応答がなくなった場合にルートが無効化されます。
- ルートモニタリングについては「4.2.3 ルートフェイルオーバ」を参照してください。

- main ルーティングテーブルにもう 1 つルートを作成します。このルートのネットワークを all-nets、インタフェースを if3、ゲートウェイアドレスを if1_ip_B とします。これがファイアウォール B への経路となります。

- この 2 番目のルートの Monitor プロパティも有効化されているようにしてください。併せて、Monitor Interface Link Status プロパティと Monitor Gateway using ARP プロパティも有効化します。これにより、ファイアウォール B の応答がなくなった場合にルートが無効化されます。

- main ルーティングテーブルに対し、適切な分散方式で Route Balancing Instance を作成します。この方式は Round Robin または Destination とします。Destination 方式を指定すると、同じ送信先 IP アドレスへのクライアント通信が同じインタフェースを介してルーティングされるようになります（ファイアウォール A または B からも同様）。
- ルートバランシングインスタンスの設定については「4.4 ルートロードバランス」を参照してください。

- 多くの場合、さらに追加の 2 つのルートとして、インタフェース if2 に対してアドレス if1_ip_A、インタフェース if3 に対してアドレス if1_ip_B のルーティングを行うルートを作成しておくことが推奨されます。ICMP を使用した Ping ではこのような設定が必要となります。これらのルートを設定しない場合、ファイアウォール A と B へ向かうすべての通信に対してルートロードバランシングが適用されます。

- LB1 用に作成されたすべてのルートは、以下の通りです。

ネットワーク	インタフェース	ゲートウェイ
all-nets	if2	if1_A_ip
all-nets	if3	if1_B_ip
if1_A_ip	if2	
if1_B_ip	if3	

2. ファイアウォール「LB2」の設定
LB2 は、ファイアウォール A と B の間でインターネットからクライアントへの通信の負荷分散を行います。クライアント側から来る通信は、通常通り扱われます。
セットアップ手順は LB1 と同じですが、方向が逆になります。

3. ファイアウォール A と B の設定
A と B に対しては、通常のコンフィグレーションと同様に、トラフィックに対して IP ルールセットやほかのポリシーが設定されます。イーサネットインタフェースの IP アドレス以外はお互いに同じ設定となります。

注意 AHA を使用してフォールトトレランスを改善する。

上記の例では、ファイアウォール LB1 と LB2 がセットアップにおける潜在的な単一障害点を示しています。しかしながら、両方またはどちらか片方を NetDefendOS の HA クラスタとすることでこれを回避します。

4.6 仮想ルーティング

4.6.1 概要

仮想ルーティングは、NetDefendOS 内で、自身のルーティングテーブルに、論理的に独立した仮想システムを作成できる NetDefendOS の機能です。これらのシステムは物理的に分かれている D-Link ファイアウォールのように動作することができ、OSPF を使用したダイナミックルーティングを含め、別々のファイアウォールで可能な機能のほぼ全部を行うことができます。仮想システムは仮想ルータと呼ばれることもあります。

仮想ルーティングの作成に関連する NetDefendOS のコンポーネントは以下の通りです。

- 各仮想システム用の独立したルーティングテーブル。
- インタフェース IP アドレスを特定のルーティングテーブル経由で到達可能にする 1 インタフェースごとのポリシーベースルーティングテーブルのメンバシップ。特定のルーティングテーブルにインタフェースをリンクすることで、明示的にこの連携を作ることができます。
- 必要に応じて、仮想システム間の通信にループバックインタフェースのペアを使用できます。(「3.4.9 ループバックインタフェース」を参照してください。)

特定のインタフェースに特定のルーティングテーブルを関連させる 2 つの方法があります。

- **Routing Rules を使用する**
  特定のインタフェースのすべてのトラフィックが特定のルーティングテーブルの対象となるように Routing Rules を定義することができます。

- **インタフェースにルーティングテーブルを指定する**
  特定のルーティングテーブルに直接インタフェースを関連させることができます。インタフェースのルーティングテーブルのメンバシップとしてこれは知られています。本オプションはインタフェースの virtual routing オプションの一部です。

  これは仮想ルータを実装するために推奨される方法です。インタフェースを物理インタフェース、または仮想 LAN (VLAN) とすることができます。

ルーティングテーブルが確実に経路検索処理で他のどのテーブルも使用しないためには、テーブルの Ordering パラメータを Only に設定するべきです。詳しくは、「4.3 ポリシーベースルーティング」で説明しています。

4.6.2 簡単なシナリオ

2つの外部のISP（ISP1およびISP2）に接続された1つのD-Linkファイアウォールを考えてみます。ISP1は部門A用に内部ネットワークにインターネット接続を提供して、物理インタフェースIf1を経由してD-Linkファイアウォールに接続します。

ISP2は部門B用に内部ネットワークにインターネット接続を提供して、物理インタフェースIf2を経由して接続します。管理目的のために、D-Linkファイアウォールを2台の仮想システム（各ISPあたり1つ）に分割することに決めます。

2つの専用のルーティングテーブルを作成します。pbr1は、ISP1と部門Aのトラフィックを処理するために作成されます。pbr2は、ISP2と部門Bのトラフィックを処理するために作成されます。以下の図はこの仕組みについて説明しています。

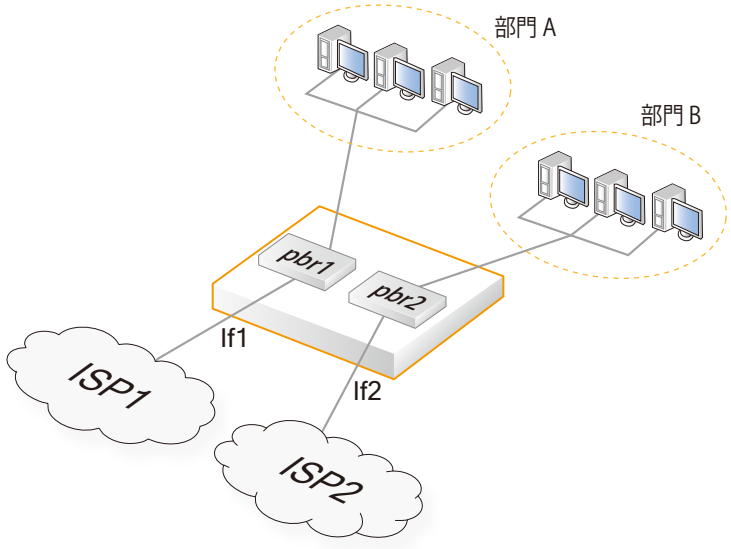


図4-10　仮想ルーティング

管理者がこれをNetDefendOSに設定すると、インタフェースIf1は、ルーティングテーブルpbr2ではなく、pbr1のメンバになります。言い換えれば、If1は明示的にpbr1に関連付けられます。逆に、インタフェースIf2は、pbr1ではなく、pbr2のメンバになります。どのルーティングテーブルが使用されるかを判断するのは、このインタフェースメンバシップで、これは2つのトラフィックのセットを完全に分けたままにします。

参照 専用のルーティングテーブルを作成するのが最善である

mainルーティングテーブルを2つのルーティングテーブルの1つとして使用することができます。しかし、通常、新しいものを作る代わりに、データトラフィックのそれぞれの分かれた部分に適切な名称を持つ専用ルーティングテーブルを作る方がよりよく、明確です。

プライベートIPアドレスの再利用

異なるインタフェースで別々のルーティングテーブルを使用する利点は、異なる仮想システムで内部のプライベートIPアドレス範囲を再利用できることです。例えば、部門Aと部門Bはともに内部ネットワーク192.168.0.0/24を使用できます。

完全に分かれたルーティングテーブルで経路検索をするため、競合が全くありません。

VPNトンネルはインタフェースである

VPNトンネルもまたNetDefendOSのインタフェースであると考えると、物理インタフェースと同様に自身のルーティングテーブルに関連付けることができます。

これは、NetDefendOS内部で互いからVPNトンネルを論理的に分けることができることを意味します。

ループバックインタフェースを使用する

このシンプルな例では、仮想システム間の通信という要件がなかったため、ループバックインタフェースは使用されませんでした。例えば、部門Aは部門Bと通信する必要はありません。それらの間に通信が必要であるなら、これを許可するために適切なループバックインタフェースのペアを定義する必要があります。

ループバックインタフェースを定義すると、そのインタフェースに送信されたすべてのトラフィックが自動的に別のインタフェースで受信されるものとして現れます。

4.6.3 ルーティングルールの欠点

ルーティングルールを使用すると、仮想ルーティングの問題の多くを解決できますが、複雑な構成となり、使いにくくなる可能性があります。
ともに同じ IP 範囲を使用して、2 つの組織にファイアウォールとして使用される 1 つの D-Link ファイアウォールを考えてみます。

この場合、以下の通り、2 つの異なるルーティングテーブルが 1 つずつ各組織に使用されます。

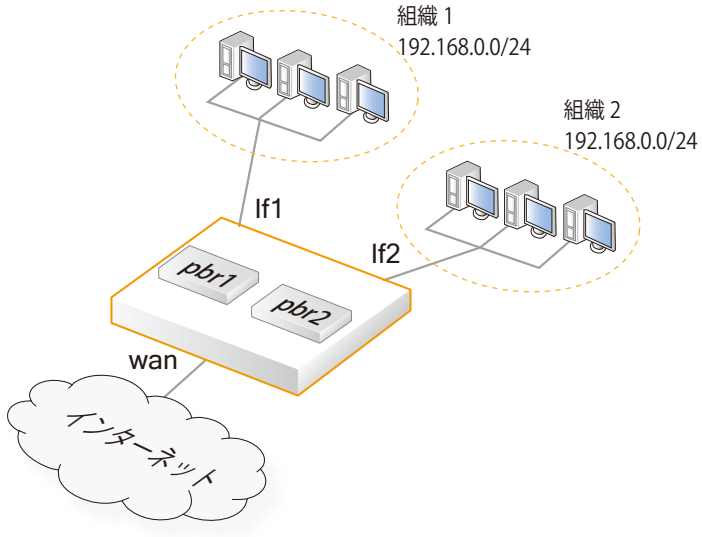


図 4-11　ルーティングルールの欠点

2 のルーティングテーブル pbr1 と pbr2 はこのシナリオのために最初に定義されます。内容を以下に表示します。

ルーティングテーブル pbr1

経路 #	インタフェース	ネットワーク	ゲートウェイ
1	wan	all-nets	wan_gw
2	lf1	192.168.0.0/24	

ルーティングテーブル pbr2

経路 #	インタフェース	ネットワーク	ゲートウェイ
1	wan	all-nets	wan_gw
2	lf2	192.168.0.0/24	

各ネットワークから、およびインターネットからトラフィックを取得するのは簡単です。外向きトラフィックのみを考えた場合は、2 つのルーティングルールオブジェクトのみを必要とします。各組織がパブリック IPv4 を保持し、各ネットワーク上のサーバにマッピングされているとします。その場合、外向きトラフィックは、内向きトラフィックと同様に下記の 4 つのルーティングルールで処理されます。

ルート #	名前	送信元インタフェース	送信元ネットワーク	送信先ネットワーク	Fwd Table	Ret Table
1	org1-in	wan	all-nets	pubip-org1	pbr1	pbr1
2	org1-out	lf1	all-nets	all-nets	pbr1	pbr1
3	org2-in	wan	all-nets	pubip-org2	pbr2	pbr2
4	org2-out	lf2	all-nets	all-nets	pbr2	pbr2

2 つの組織が互いに通信する必要がなければ、これは正常に動作します。通信する必要があると、以下の 2 つの追加ルーティングルールが必要であり、上の 4 つのテーブルより前におかれます。

ルート #	名前	送信元インタフェース	送信元ネットワーク	送信先ネットワーク	Fwd Table	Ret Table
1	org1-org2	lf11	all-nets	pubip-org2	pbr1	pbr2
2	org2-org1	lf2	all-nets	pubip-org1	pbr2	pbr1

2 つの組織では、2 つのルーティングルールがあれば、それら組織間の通信を許可するのに十分です。しかし、3 つの組織の場合、6 つが必要となります。4 つでは 12 個必要となります。5 つでは 20 個必要となります。これは、all-to-all マッピングで 30、42、56 個のルールというように増えていき、すぐに管理者のタスクでは制御が難しくなります。

仮想ルーティングの利点

ルーティングルールの代わりにインタフェースのルーティングテーブルのメンバシップを使用することで、ルーティングルールに必要とされる all-to-all マッピングを削除することができます。これは、以下の図のルータのシンボルで表される 3 台の仮想システムを作成することによって、複雑さを軽減させます。

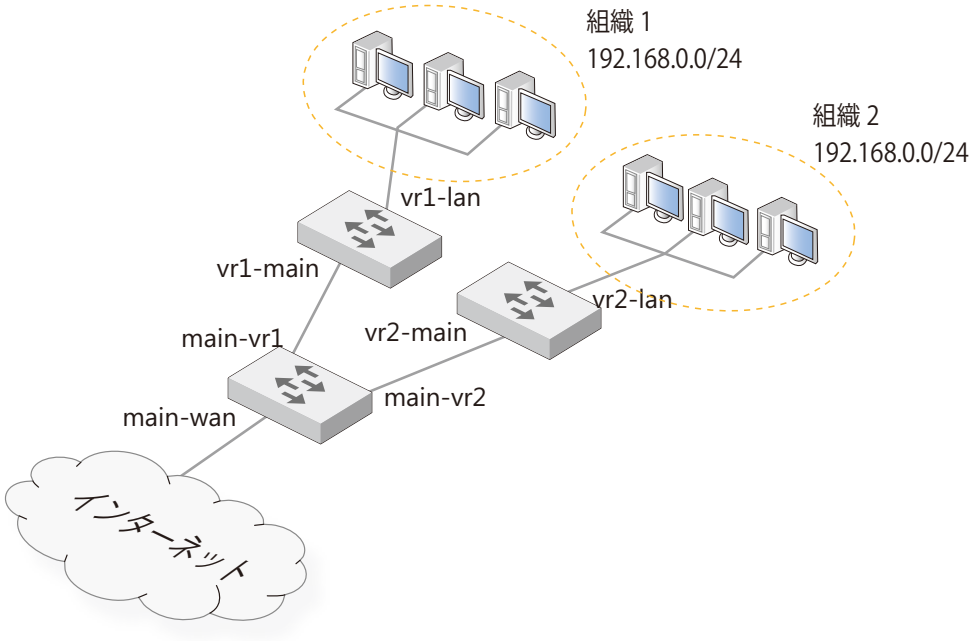


図 4-12　仮想ルーティングの利点

ここで、各組織は自身の仮想システムを取得します。これらは、ループバックインタフェースのペアを使用して、main ルーティングテーブルに接続します。ルーティングテーブルには、以下のエントリがあります。

ルーティングテーブル main

経路 #	インタフェース	ネットワーク	ゲートウェイ
1	main-wan	all-nets	wan_gw
2	main-vs1	pubip-vs1	
3	main-vs2	pubip-vs2	

ルーティングテーブル vs1

経路 #	インタフェース	ネットワーク	ゲートウェイ
1	vs1-main	all-nets	
2	vs1-lan	192.168.0.0/24	

ルーティングテーブル vs2

経路 #	インタフェース	ネットワーク	ゲートウェイ
1	vs2-main	all-nets	
2	vs2-lan	192.168.0.0/24	

イーサネットインタフェース

インタフェース #	名前	IP アドレス	ルーティングテーブル
1	main-wan	ip_main-wan	main
2	vs1-lan	192.168.0.1	vs1
3	vs2-lan	192.168.0.254	vs2

ループバックインタフェース

#	名前	IP アドレス	ループ先	ルーティングテーブル
1	main-vs1	ip_main-wan	vs1-main	main
2	vs1-main	pubip-vs1	main-vs1	vs1
3	main-vs2	ip_main-wan	vs2-main	main
4	vs2-main	pubip-vs2	main-vs2	vs2

1 組の仮想システム間の接続には、1 組のループバックインタフェースが必要です。 各システムあたり 1 つです。トラフィックは main-vs1 を通じて送信されると、vs1-main に到着します。トラフィックは vs1-main を通じて送信されると、main-vs1 が受信します。これはまさに、お互いに対応する 2 台のファイアウォールと 2 つのインタフェース、及びそれらの間の通信と同じようなものです。

ルーティングテーブルのメンバシップ設定は、接続がインタフェースまで到達すると、インタフェースがメンバであるルーティングテーブルに従って送信されるということを意味します。

また、仮想システムの内部インタフェースの IPv4 アドレスが異なる点について注意してください。インタフェースごとにルーティングテーブルメンバシップが使用されなかったとすると、両方の IP アドレスのための core ルートは、vs2（たとえそれは使用可能であるべきでも）で使用不能な 192.168.0.1 と vs1 で使用不能な 192.168.0.254 に至る両方のルーティングテーブルに追加されます。インタフェースごとのルーティングテーブルメンバシップで、1 台の仮想システムに所属するインタフェース IP アドレスが、他の仮想システムを妨害することはありません。また、ループバックインタフェースも必要ではありません。

main-vs1 と main-vs2 インタフェースの IPv4 アドレスは外部インタフェースの IP アドレスと同じです。それらは 127.0.0.1 などの何か意味のないものに設定されているかもしれません。ループバックインタフェースが raw IP インタフェース（ARP プロトコルはそれらに使用されない）であるため、通常のルーティングがまだ動作しています。しかし、それらの IP アドレスは内部から traceroute を使用してユーザに可視化されます。また、問題は、ping やログ出力など、ファイアウォール自身から内部ネットワークに生成されるトラフィックの存在です。そのようなトラフィックは、多くの場合、main ルーティングテーブルに従って送信され、main ルーティングテーブルで最も近いインタフェースの IP アドレスから提供されます。

4.6.4 仮想ルーティングが使用する IP ルールセット

複数の IP ルールセットを作成する NetDefendOS 機能を使用して、個別のルールセットに異なる仮想システムの IP ルールセットを分割できます。（この機能に関する詳細は「3.6.5 複数の IP ルールセット」を参照してください。）

異なる仮想システムのために IP ルールセットのエントリを分ける必要はありません。それらは 1 つの IP ルールセットに一緒に常駐できます。これを行う利点は、数台の仮想システムにわたる「共有される」または「グローバルな」IP ポリシーを定義できることです。例えば、「worm」攻撃に対して、対抗手段がおかれるまでは、worm が使用すると知られているポートへの全通信を破棄することが望ましいかもしれません。ルールセットの先頭におかれる 1 つの Drop エントリが、すべての仮想システムのためにこれを処理することができます。前のセクションの例を使用して、以下のような IP ルールセットを設定することができます。

インタフェースグループ

#	名前	インタフェース
1	main-vsifs	main-vs1, main-vs2
2	main-ifs	main-wan, main-vsifs
3	vs1-ifs	vs1-main, vs1-lan
4	vs2-ifs	vs2-main, vs2-lan

IP ルールセットのエントリ

#	名前	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
「main」仮想システムの IP ルール							
1	main-allowall	Allow	main-ifs	all-nets	Any	all-nets	all_services
「vs1」仮想システムの IP ルールセットエントリ							
2	vs1-http-in	Allow/SAT	vs1-ifs	all-nets	pubip-vs1	all-nets	http（Destination が 192.168.0.5）
3	vs1-http-in	Allow	vs1-main	all-nets	Any	pubip-vs1	http
4	vs1-out	Allow/NAT	vs1-int	all-nets	Any	all-nets	all_services
「vs2」仮想システムの IP ルールセットエントリ							
5	vs2-smtp-in	Allow/SAT	vs2-main	all-nets	Any	pubip-vs2	all_services
6	vs2-smtp-in	Allow	vs2-main	all-nets	Any	pubip-vs2	smtp
7	vs2-http-out	Allow/NAT	vs2-int	192.168.0.4	vs2-main	all-nets	http

SAT ルールが、同じ物理ユニットに接続する多くの組織があることを考慮に入れる必要はないことに注意してください。それらの間には、直接接続は全くありません。main ルーティングテーブルに接続する同じインタフェースを通じてすべてが到着します。仮想ルーティングなしでこれを行うと、NAT ルールは、他の組織から来るトラフィックに対して Allow ルールに先行しなければなりません。そのようなルールは、それぞれの組織のセキュリティポリシーに従うようにしなければならないことに注意してください。それらの問題は仮想ルーティングで解決されます。

送信元インタフェースフィルタは非常に特定的です。そのようなルールであってもトリガされるため、Any は送信元インタフェースとして使用されません。例えば、vs1-http ルールが送信元インタフェースとして Any を使用すると何が起こるか考えてみます。pubip-vs1 に向かうパケットが、main-ext で受信されるとすぐに、それらはトリガーとなります。宛先アドレスは 192.168.0.5 に書き直されて、main ルーティングテーブルを使用して通過します。main ルーティングテーブルは、192.168.0.5 に何をするべきかわからず、D-Link ファイアウォールの外のデフォルトゲートウェイにトラフィックを戻します。

この例題に示されているのと同じ命名体系を使用していれば、送信元インタフェースが正しいことを素早く確認できます。main システムに関するすべてのルールには、「main-」で始まる送信元インタフェースがあります。vs1 システムに関するすべてのルールには、「vs1-」で始まる送信元インタフェースがあります。

しかし、宛先インタフェースフィルタは送信元インタフェースがフィルタするのと同様に特定的である必要はありません。対象となる宛先は、使用するルーティングテーブルによって制限されます。vs1 テーブルだけが vs1- インタフェースに通じるルートを持っているのであれば、Any フィルタは「同じ仮想システムの他のインタフェースを通る」ことを意味するだけです。とはいえ、より限定的な宛先インタフェースを設定することにより、コンフィグレーションのエラー発生場所をフィルタする場合に役立つ可能性もあります。この例題では、ルール 1 は main-ifs を、ルール 4 は vs1-main を使用するかもしれません。しかし、1 つの宛先 IP アドレスにしか関係しないという点で、SAT とそれに対応する Allow ルールは既にかなり限定的なものになっています。

4.6.5 複数の IP ルールセット

1 つのルールセットに異なる仮想システムのための全 IP ルールを持つ代わりのアプローチは、複数の IP ルールのセットを利用することです。

IP ルールセットのすべてのスキャンが main ルールセットで始まりますが、main にエントリを定義することは可能です。このエントリのアクションを「Goto」に設定してスキャンが別の名前付きルールセットに続くようにします。必要に応じて、これらの付加的なルールセットを定義することができます。そして、各仮想システムとその対応するルーティングテーブルのためにそれぞれルールセットを作成することができます。

このサブジェクトに関する詳細は、「3.6.5 複数の IP ルールセット」を参照してください。

4.6.6 トラブルシューティング

仮想ルーティングを設定する場合、以下の手順が様々な問題に関する障害調査の役に立ちます。

- 送信元インタフェースフィルタが正しいことを確認してください。
- すべてのインタフェースとトンネルタイプに対して、インタフェース PBR テーブルのメンバシップをダブルチェックしてください。
- 異なる仮想システムからソースへの「ping <string> -pbr=<pbrtable>」を使用してください。
- 「ping <string> -srcif=<srcif>」を使用して、ルールセットをテストします。これは、ping が特定のインタフェースで特定の IP アドレスから受信されたことをシミュレーションします。
- 「arpsnoop <ifacenames> -v」を使用して、ARP 解決に関する詳細な情報を取得します。
- 「route <pbrtable> -all」を使用して、「core」ルートを含む特定のテーブル内の全ルートエントリを参照します。
- 「route -lookup <ipaddr> <pbrtable>」を使用して、特定の IP アドレスが、特定の仮想システムで予測される方向に送られることを確認します。（ヒント :「-lookup」は「-l」に省略できます。）
- 「conn -show -verbose」を使用して、接続のオープンに関する詳細な情報を参照します。接続の両端が表示されます。: アドレス変換の前後。また、送信と返信方向に使用されるルーティングテーブルも表示されます。
- ログへの出力を有効にして、ログをご確認ください。各仮想システムでは、別々のルール決定を行い、別々の接続が確立します。

4.7 OSPF

NetDefendOS は OSPF（Open Shortest Path First）アーキテクチャを使用して、ダイナミックルーティングと呼ばれる機能を実行します。

ここでは一般的にダイナミックルーティングが何か、そしてそれはどのように実行するのかをはじめに記載します。次に、OSPF によるダイナミックルーティングと、簡易的な OSPF ネットワークの構築方法について説明します。

4.7.1 ダイナミックルーティング

ここでは、詳細に OSPF を見る前に、OSPF の一般的なダイナミックルーティングの概念と提供するダイナミックルーティングのタイプについて説明します。また、OSPF のダイナミックルーティングにおける重要な概念を紹介します。

スタティックルーティングとの違い

ダイナミックルーティングは、ファイアウォールなどのルーティングデバイスがネットワークトポロジの変更に自動的に対応するという点でスタティックルーティングとは異なります。

ダイナミックルーティングは、はじめに直接接続するすべてのネットワークについて学習し、次にどのネットワークに接続しているかを指定している詳しいルート情報を他の接続ルータから取得します。このルーティング情報のすべてが処理されて、ローカル接続およびリモート接続する宛先のために最適なルートをローカルルーティングテーブルに追加します。

ダイナミックルーティングは、ルーティング更新にダイナミックに応じますが、ルーティングループなどの特定の問題に、より影響されやすいという欠点もあります。一般的には、以下に示す 2 つのタイプのアルゴリズムのうち 1 つが、ダイナミックルーティングメカニズムを実行するために使用されます。

- 距離ベクトル (DV) アルゴリズム
- Link State(LS) アルゴリズム

最適な経路を決定し、他のルータと更新情報を共有する方法は、使用されるアルゴリズムのタイプに依存します。2 つのアルゴリズムタイプについては次に説明します。

距離ベクトルアルゴリズム（DV : Distance Vector）

距離ベクトル（DV）アルゴリズムは、分配型の方法で最適な経路を計算する分散型のルーティングアルゴリズムです。各ルータは自身が持つリンクのコストを計算して、その経路情報を隣接ルータとだけ共有します。各ルータは、反復的な計算と隣接ルータとの情報交換よって宛先までの最短コスト経路を決定します。

RIP（Routing Information Protocol）は、ルータ情報交換用の既知の DV アルゴリズムであり、通常の更新メッセージの送信とルーティングテーブル内のルーティング変更の反映を行います。パス決定は中間ルータ (または「ホップ」として知られている) の数であるパスの「長さ」に基づいています。

自身のルーティングテーブルを更新した後、変更を通知するために、ルータはすぐに隣接ルータに全ルーティングテーブルの送信を開始します。

Link State アルゴリズム

DV アルゴリズムとは異なり、Link State（LS）アルゴリズムは、ルータが全ネットワークのトポロジを表すルーティングテーブルを保持することができます。各ルータはネットワークのすべてのルータに接続されるリンクとリンクコストをブロードキャストします。ルータは、ブロードキャストを受信すると、LS アルゴリズムを動作させ、ルータ自身の最短コスト経路設定を計算します。Link State のどんな変更もネットワークの至る所に送信されるため、すべてのルータが、同じルーティングテーブル情報を保持しており、ネットワークに矛盾がなくなります。

Link State アルゴリズムの利点

グローバルな Link State 情報はネットワークの至る所で保持されているため、OSPF で使用されているような LS アルゴリズムは高いレベルの設定制御と拡張性を提供します。変更すると、他のルータに更新情報についてブロードキャストを行います。これは、ルーティングループをより速く収束し、発生の可能性も低くします。さらに、OSPF は階層の中で動作できますが、RIP には、サブネットワークアドレス指定に関する情報はありません。

OSPF ソリューション

OSPF（Open Shortest Path First）は、広く使用される LS アルゴリズムを基本とするプロトコルです。ダイナミックルーティングは、OSPF を使用して NetDefendOS で使用されます。

OSPF が有効なルータは、はじめに直接接続するルータとサブネットを識別して、次に他のすべてのルータに情報をブロードキャストします。各ルータは受信した情報を使用して、OSPF が学習したルートをルーティングテーブルに追加します。

より規模の大きな構成においても、ルーティングテーブルで、各 OSPF ルータは指定された宛先に通じるネットワークとルータを識別できるため、最適なルートを識別できます。OSPF を使用するルータは、他のルータに対して、全体のルーティングテーブルをブロードキャストする代わりに、ルートの変更を通知するための更新のみをブロードキャストします。

OSPF は、ホップ、帯域、ロード、遅延、その他を含む経路決定のための各種メトリックに依存します。パラメータが詳細に調整できるため、OSPF は、ルーティングプロセスに対して高いレベルの制御を提供します。

簡単な OSPF シナリオ

以下に示した簡単なネットワークトポロジは OSPF が実行できることをまとめた例題です。ここでは、2 つの D-Link ファイアウォール A と B が同じ OSPF エリアにあるように接続および設定されています。エリアに関する概念は後で説明します。

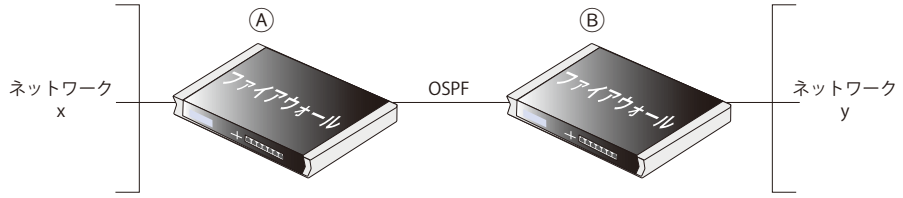


図 4-13　簡単な OSPF シナリオ

OSPF により、トラフィックがネットワーク Y に到達するためにはファイアウォール B に送信されなければならないことを、ファイアウォール A が認識しています。手動でこのルーティング情報を A のルーティングテーブルに挿入しなければならない代わりに、OSPF によって、B のルーティングテーブル情報を自動的に A と共有することができます。

同様に、ファイアウォール B は OSPF によって自動的にネットワーク X がファイアウォール A に接続されていることを認知するようになります。

OSPF の下では、このルーティング情報交換は完全に自動化されています。

OSPF はルートの冗長化を提供する

上のシナリオを使用して、C という 3 つめのファイアウォールを追加する場合、OSPF を通じて、3 つのファイアウォールがそれぞれ、自分以外のファイアウォールに接続されているネットワークを認識しているということになります。このシナリオについては、以下で図と共に説明します。

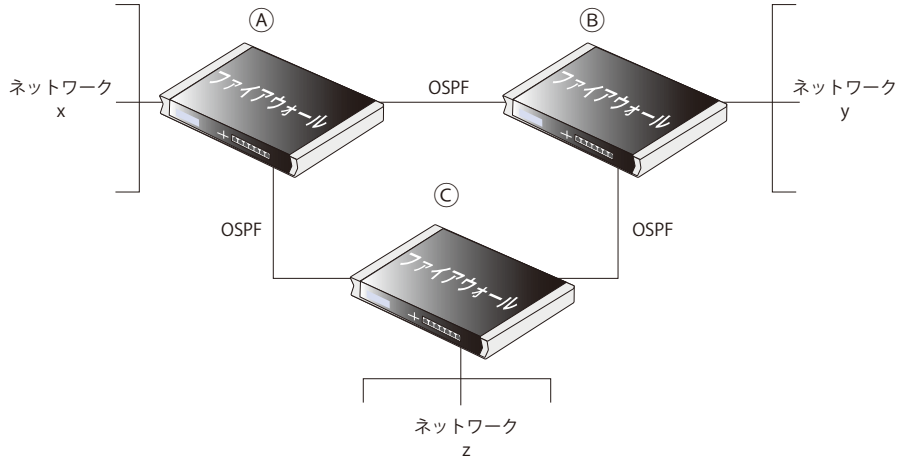


図 4-14　ルートの冗長化を提供する OSPF

さらに、今、2 つのファイアウォール間にルート冗長性を持っています。例えば、A と C の間の直接のリンクに失敗した場合、OSPF は、直ちに両方のファイアウォールにファイアウォール B を経由した代替経路があることを知らせることができます。

例えば、ネットワーク X からネットワーク Z に行く予定のトラフィックは、ファイアウォール B を通じて自動的に送信されます。管理者の観点から、直接接続されたネットワークのためのルートだけが、各ファイアウォールで構成される必要があります。トラフィックが目的地に到達するために他のいくつかのファイアウォールを通過する必要があっても、OSPF は、他のファイアウォールに接続されたネットワークを見つけるために自動的に必要なルーティング情報を提供します。

注意 リング型トポロジはいつも代替経路を提供します。

OSPF を実装するネットワークのトポロジを設計する場合、リング型で D-Link ファイアウォールを配置することで、各ファイアウォールは接続可能な 2 つのルートを持つことができます。1 つのファイアウォール間の接続に失敗しても、迂回経路がいつも存在しています。

ルーティングメトリック

ダイナミックルーティングと OSPF について議論する際に、ルーティングメトリックを理解することが重要です。

ここでは簡単に説明します。ルーティングメトリック（コスト）は、ルーティングアルゴリズムが送信先への最適なルートを計算するために使う基準です。ルーティングプロトコルは、ネットワークをまたぐリンクを評価するため、および最適な経路を決定するために 1 つ以上のメトリックを使用します。使用される主なメトリックは以下の通りです。

項目	説明
経路長	各リンクに関連するコストの合計です。このメトリックに一般的に使用される値は、ホップカウントと呼ばれ、送信元から送信先にパケットが移動するために通過しなければならないルーティングデバイス（ルータ / ファイアウォール）の数を示しています。
帯域	「Mbps」で示されるトラフィック容量です。
ロード	ルータの使用率。使用率は CPU 利用率とスループットで評価されます。
遅延	遅延は、送信元から送信先までのパケットの移動にかかる時間。その時間は、経路に関係する多くの要因（例えば帯域、ロード、および経路長）に依存します。

4.7.2 OSPF 概念

概要

OSPF は、Internet Engineering Task Force（IETF）によって IP ネットワークのために開発されたプロトコルです。NetDefendOS の実行は、RFC 2328 ベースで、RFC 1583 に対する互換性を持っています。

OSPF は、IP パケットヘッダに含まれる宛先 IP アドレスのみに基づいて IP パケットをルーティングすることによって動作します。IP アドレスは「そのまま」転送されます。つまり、自律システム (AS) を通過する際、他のプロトコルヘッダによってカプセル化されません。

自律システム

自律システム（AS: Autonomous System）は、一般的な管理者が制御する単一で明確に定義されたルーティングポリシーが設定された、単一ネットワークまたはネットワークグループを示しています。それは様々な OSPF の構成部分を説明するツリー構造の最上位を形成します。

NetDefendOS では、AS は OSPF ルータオブジェクトに対応しています。OSPF を設定する場合、最初に、これを定義する必要があります。多くのシナリオでは、1 つの OSPF ルータのみを定義する必要があり、OSPF ネットワークにかかわる各 D-Link ファイアウォールで個別に定義する必要があります。NetDefendOS オブジェクトについては、「4.7.3.1 OSPF Router Process」で詳しく説明しています。

OSPF はダイナミックルーティングプロトコルで、（ルータインタフェースエラーのような）AS 内のトポロジの変更を直ちに検出し、送信先への経路として、ループのない新しいルートを計算します。

Link-State ルーティング

OSPF は、同じエリア内の他のすべてのルータに Link-State Advertisement(LSA) を送信する Link-State ルーティング（LS）を形成します。各ルータは AS トポロジについて記述する Link-State データベースとして知られるデータベースを保持しています。このデータベースを使用して、各ルータは自身をルートとして他のルータへの最短経路のツリーを構築します。この最短経路ツリーが自律システム（AS）内の各送信先への経路を提供します。

Authentication

必要に応じ、全ての OSPF プロトコル交換について認証を行うことができます。これは、正しい認証を持つルータだけが AS に参加できることを意味します。また、異なる認証体系を使用することが可能であり、NetDefendOS では体系は「パスフレーズ」または「MD5 ダイジェスト」のいずれかとなります。各 AS には個別の認証方法を設定することが可能です。

OSPF エリア

OSPF エリアは自律システム（AS）内にあるグループ化されたネットワークとホストで構成されます。エリア内にあるルータは、内部ルータと呼ばれ、内部ルータ上のすべてのインタフェースがそのエリア内のネットワークに直接接続します。

エリアのトポロジは、残りの AS から隠されます。情報が隠されることによって、交換されるルーティングトラフィック量を低減します。また、エリア内のルーティングが、そのエリアの所有するトポロジによってのみ決定され、不正なルーティングデータから、そのエリアを保護します。エリアは IP でサブネット化されているネットワークを汎用化したものです。

NetDefendOS では、エリアは、OSPF エリアオブジェクトによって定義されて、OSPF ルータオブジェクトが定義する AS に追加されます。AS 内に 1 つ以上のエリアが存在できるため、単一の OSPF ルータに複数の OSPF エリアオブジェクトを加えることができます。多くの場合、1 つで十分であり、どれが OSPF ネットワークの一部になるかを各 D-Link ファイアウォールに定義するべきです。

NetDefendOS オブジェクトについては、「4.7.3.2 OSPF Area」で詳しく説明しています。

OSPF エリアのコンポーネント

エリアに関連する OSPF コンポーネントのサマリは、以下で詳しく説明します。

項目	説明
ABR	1 個以上のエリアにインタフェースを持つルータを、エリア境界ルータ（ABR: Area Border Router）と呼び、これらは、AS が持つインタフェースのいずれかに接続している各エリアのために、個別のトポロジデータベースを保持しています。
ASBR	別の AS 内のルータとルーティング情報を交換するルータは、自律システム境界ルータ（ASBR: Autonomous System Boundary Routers）と呼ばれています。ASBR は学習した経路を AS 経由で外部に通知します。
バックボーンエリア	すべての OSPF ネットワークは、少なくともバックボーンエリア（ID が 0 のエリア）を持つことが必要です。これは、他のすべてのエリアが接続されるべきであるエリアで、バックボーンが設定されることにより、ルーティング情報が接続エリア間に配布されるようになります。エリアがバックボーンエリアに直接接続されていない場合、接続のためには仮想リンクが必要です。 OSPF ネットワークは、バックボーンを発端として設計されるべきです。
スタブエリア	スタブエリアは AS 経由または AS への外部通知がフラッドされないエリアです。エリアがスタブエリアとして設定されると、ルータは自動的にデフォルト経路を通知するため、スタブエリア内のルータは、エリアの外側の送信先に到達できます。
トランジットエリア	トランジットエリアは、バックボーンエリアに直接接続しないエリアからトラフィックを通過させるために使用されます。

代表ルータ（DS: Designated Router）

各 OSPF ブロードキャストネットワークには、代表ルータ（DR）とバックアップ代表ルータ（BDR）があります。ルータが OSPF Hello メッセージを使用して、すべてのルータに通知された優先順に基づいてネットワークの DR と BDR を選出します。ネットワーク上に既に DR がある場合、ルータはそれ自身のルータプライオリティにかかわらず、それを受け入れます。

NetDefendOS では、DR と BDR は自動的に割り当てられます。

Neighbor

同じエリア内にあるルータが、そのエリアで Neighbor になります。Neighbor は、Hello メッセージによって選出されます。これらは、IP マルチキャストを使用して各インタフェースから定期的に送信されます。
ルータは、Neighbor の Hello メッセージ内のリストに自身を見つけると、すぐに Neighbor になります。こうして、2 つの通信方法が保証されます。

以下の通り隣接状態が定義されます。

項目	説明
Down	これは、隣接関係の初期の状態です。
Init	Hello パケットが Neighbor から受信され、その中にファイアウォールのルータ ID を含んでいない場合、Neighbor は Init state 内に置かれます。当該 Neighbor が Hello メッセージを受信すると、すぐに送信ルータのルータ ID を知り、それを含む Hello メッセージを送信します。Neighbor の状態は、2-Way 状態に変化します。
2-Way	この状態では、ルータと Neighbor 間の通信は 2 方向になります。ポイントツーポイントとポイントツーマルチポイント OSPF インタフェースでは、状態は Full に変更されます。ブロードキャストインタフェースでは、DR/BDR だけが Neighbor を持つ Full state になり、残りのすべての Neighbor は 2-Way 状態のままになります。
ExStart	Adjacency（隣接関係）を構築する準備をします。
Exchange	ルータは Data Descriptor（DD）を交換します。
Loading	ルータは LSA を交換します。
Full	これは、ルータと DR/BDR 間の Adjacency（隣接関係）における通常の状態です。

アグリゲーション

OSPF アグリゲーションは、ルーティングテーブル内で共通のアドレスを持つ経路グループを一つのエントリに結合するために使用されます。これは、通常ルーティングテーブルを最小にするために使用されます。

NetDefendOS で本機能を設定するためには、「4.7.3.5 OSPF Aggregate」を参照してください。

仮想リンク

仮想リンクは以下のシナリオで使用されます。

A. バックボーンエリアに直接接続していないエリアをリンクする。

B. 独立したバックボーンエリアの場合、バックボーンをリンクする。

次に、2 つの用途について説明します。

A. バックボーンに直接接続しないエリアをリンクする

バックボーンは、通常他の全エリアの中心にある必要がありますが、エリアがバックボーンエリアへの接続が物理的に困難な場合に仮想リンクが使用されます。この仮想リンクは、そのエリアにバックボーンエリアに対する論理的な経路を提供します。さらにこの仮想リンクは、ABR の一つをバックボーンエリアに接続した状態で、一つの共用エリア上にある 2 つの ABR 間で確立します。以下の例題では、2 つのルータが同じエリア（エリア 1）に接続されていますが、それらのうちの「fw1」だけが、バックボーンエリアに物理的に接続しています。

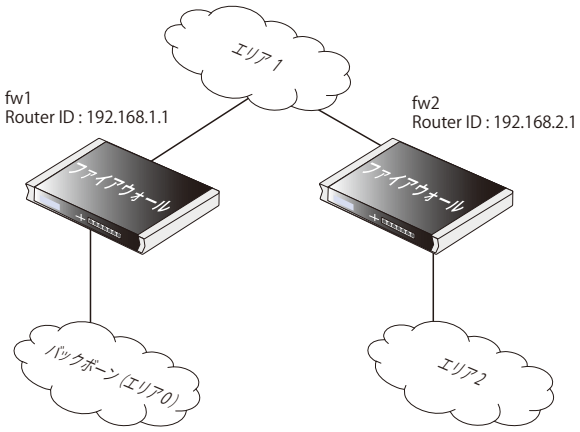


図 4-15　仮想リンクの例題 1

上記の例題では、仮想リンクはエリア 1 上の「fw1」と「fw2」の間で行われ、エリア 1 がトランジットエリアとして使用されます。この設定で、ルータ ID だけ設定される必要があります。図は、fw2 がルータ ID 192.168.1.1 を持つ fw1 に仮想リンクを持つ必要があります。そして、逆もまた同様です。これらの仮想リンクは、エリア 1 で設定される必要があります。

B. 独立したバックボーンエリアの場合、バックボーンをリンクする

OSPF は仮想リンクを使用して分割されているバックボーンをリンクすることができます。仮想リンクは、各サイドから、間にある共通のエリアを持つようにバックボーンに接する 2 つの独立した ABR 間に設定されます。

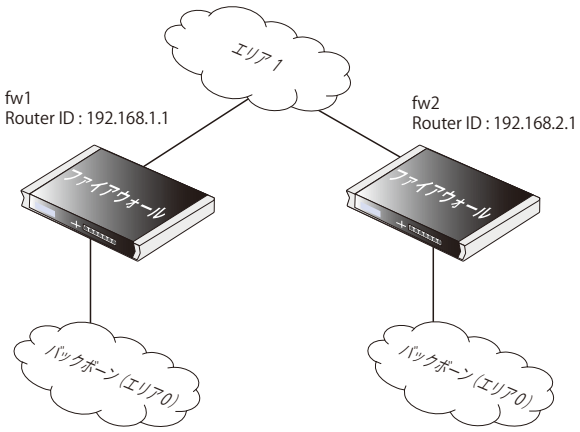


図 4-16　仮想リンクの例題 2

仮想リンクは、トランジットエリアに使用されるのと同様に、エリア上の「fw1」と「fw2」の間に設定します。この構成ではルータ ID のみを設定する必要があり、上記の例で示すように、fw2 は、ルータ ID 192.168.1.1 を持つ fw1 への仮想リンクを持つ必要があります。その逆も同様です。これらの仮想リンクは、エリア 1 に設定されます。

本機能については「4.7.3.6 OSPF VLink」を参照してください。

OSPF 高可用性サポート

OSPF の可用性サポートには、注意すべき制限事項がいくつかあります。

HA クラスタのアクティブおよびアクティブでない部分の両方ともが独立した OSPF プロセスを動作させます。ただし、アクティブでない部分はルーティングの推奨される選択にはなりません。HA マスタとスレーブはお互いに隣接関係を形成せず、ブロードキャストネットワーク上で DR/BDR になることを許可されません。これは、ルータプライオリティが 0 に設定されることで行われます。

D-Link ファイアウォールは、OSPF HA 機能が正しく動作するために、ファイアウォールに接続する全エリアに少なくとも 1 つの Neighbor を持つブロードキャストインタフェースを持つ必要があります。本質的に、HA クラスタのアクティブでない部分は link-stat データベースを取得するために Neighbor が必要です。

さらに、他の Neighbor を持たない同じブロードキャストネットワークに HA クラスタをおくことはできないことに注意してください（ルータプライオリティ 0 のためお互いに Adjacency を形成しない）。その代わりに、シナリオによってはそれらの間にポイントツーポイントリンクを設定することは可能かもしれません。HA ファイアウォールに仮想リンクを設定する場合、特別な配慮が必要です。HA ファイアウォールへのリンクを設定するエンドポイントには 3 個の独立したリンクを設定する必要があります。 2 つは共有され、1 つはファイアウォールのマスタ ID、もうひとつはスレーブルータ ID です。

NetDefendOS で OSPF を使用する

NetDefendOS で OSPF を使用する場合、シナリオでは、2 つ以上の D-Link ファイアウォールを何らかの方法で一緒に接続させます。OSPF によって、宛先用のルーティングテーブルにルートを持たなくても、これらのファイアウォールのどれかが、別のファイアウォールに接続する送信先ネットワークに正しくトラフィックを送信します。

OSPF セットアップの特徴は、接続されたファイアウォールがルーティングテーブルの情報を共有することであり、これにより、ファイアウォールのインタフェースに到達したトラフィックが自動的にルートされ、正しい宛先ネットワークへ紐づけられた他のゲートウェイのインタフェースへ出ていくことができます。

別の重要な面は、ファイアウォールが相互間の接続をモニタし、1 つが利用可能であれば代替接続によってトラフィックを送信するということです。そのため、ネットワークトポロジは、フォールトトレラントであるように設定することができます。2 つのファイアウォール間の接続に失敗すると、宛先に到達するいずれかの代替経路が使用されます。

4.7.3 OSPF コンポーネント

ここでは OSPF ルーティングのために設定する必要がある NetDefendOS オブジェクトについて記載します。これらのオブジェクトを定義することで OSPF ネットワークを作成します。オブジェクトは、OSPF ネットワークの一部分である各 D-Link ファイアウォールに定義され、同じネットワークを表す必要があります。

以下の図は、NetDefendOS OSPF オブジェクト間の関係です。

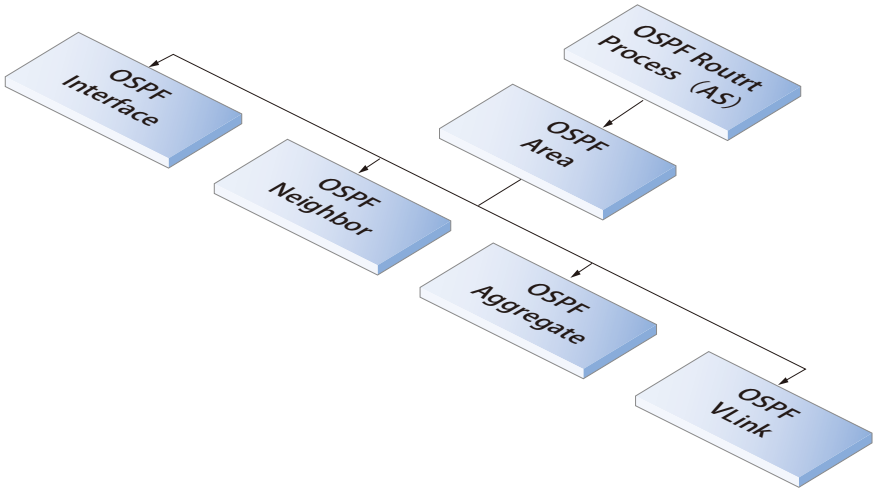


図 4-17　NetDefendOS OSPF オブジェクト

4.7.3.1 OSPF Router Process

このオブジェクトは OSPF ネットワークの最上位である自律システム（AS）を定義しています。OSPF ネットワークの一部となる各ファイアウォール上で、同様の Router Process オブジェクトが定義される必要があります。

General

項目	説明
Name	OSPF AS 名を指定します。
Router ID	AS でルータを識別するのに使用される IP アドレスを指定します。Router ID が設定されないと、ファイアウォールは OSPF AS に参加するすべてのインタフェースで最も高い IP アドレスを基に Router ID を計算します。
Private Router ID	これは、HA クラスタに使用されますが、クラスタではなく、このファイアウォールのための ID です。 注意 HA クラスタで OSPF が動作している場合、共有されている Router ID と同様にプライベートマスタおよびプライベートスレーブ Router ID も必要です。
Reference Bandwidth	ルートのためのデフォルトインタフェースコストを計算する場合、使用される参照帯域幅を設定します。OSPF インタフェースでメトリックを指定する代わりに帯域幅が使用される場合、コストは、以下の式を使用することで計算されます。 コスト = 参照帯域幅 / 帯域幅
RFC1583 の互換性	D-Link ファイアウォールが RFC 1583 のみをサポートするルータから構成される環境で使用される場合に有効です。

Debug

debug オプションは、追加の OSPF ログイベントの生成を有効にすることで、トラブルシューティングツールを提供します。詳しくは、「4.7.7 OSPF トラブルシューティング」で説明します。

Authentication

OSPF 認証の主要な目的は、正しい OSPF ルータプロセスがお互いにやり取りできるようにすることです。それゆえに、多くの場合、複数の OSPF の AS がある時に使用されます。OSPF には以下の認証オプションがあります。

項目	説明
No Authentication	OSPF プロトコルの交換に認証は使用されません。
Passphrase	シンプルなパスワードが、すべての OSPF プロトコル交換を認証するのに使用されます。
MD5 Digest	MD5 認証は ID と 128 ビットのキーで構成されます。MD5 ダイジェストを使用する場合、指定したキーは 128 ビットの MD5 ダイジェストを生成するために使用されます。 これは、OSPF パケットが暗号化されることを意味しません。OSPF トラフィックを暗号化する必要がある場合、それらを VPN を使用して送信する必要があります。例えば IPsec を使用して送信します。IPsec トンネルを通じた OSPF パケットの送信については、「4.7.5 OSPF の設定」でより詳しく説明されています。

注意 認証はすべてのルータで同じである必要があります。

パスフレーズまたは MD5 認証が OSPF に設定される場合、パスフレーズまたは認証キーは AS 内のすべての OSPF ルータで同じにする必要があります。つまり、すべてのファイアウォールに OSPF 認証方法をコピーする必要があります。

Advanced

項目	説明
Time Settings	
SPF Hold Time	SPF 計算の最短時間間隔（秒）を指定します。初期値は 10（秒）です。0 の値は、遅延が全くないことを意味します。しかし、SPF は潜在的に CPU が要求する処理であり、大きいネットワークではそれを頻繁に実行するのがよい考えとは言えないことに注意してください。
SPF Delay Time	OSPF がトポロジ変更を受信してから SPF 計算を開始する時間までの遅延時間（秒）を指定します。初期値は 5（秒）です。0 の値は、遅延が全くないことを意味します。しかし、SPF は潜在的に CPU が要求する処理であり、大きいネットワークではそれを頻繁に実行するのがよい考えとは言えないことに注意してください。
LSA Group Pacing	OSPF LSA がグループに収集されて、更新される間隔（秒）を指定します。 1 つずつ実行する代わりに、多くの LSA をグループ化して同時に処理することがより適しています。
Routes Holdtime	OSPF エントリの再構成または HA フェイルオーバ後に、ルーティングテーブルが変更されずに保持される時間（秒）を指定します。
Memory	
Memory Max Usage	OSPF AS 処理が使用を許可される RAM の最大量（キロバイト）。値が指定されないと初期値では 1% の内蔵 RAM を使用します。0 は、OSPF AS 処理がファイアウォールで利用可能なすべての RAM の使用を許可します。

4.7.3.2 OSPF Area

AS は、エリアと呼ばれる小さい部分に分割されます。ここでは、エリアの設定方法について説明します。エリアは OSPF インタフェース、Neighbor、アグリゲーション、および仮想リンクを収集します。

OSPF エリアは OSPF ルータプロセスの子であり、単一のルータプロセスの下に多くのエリアオブジェクトを定義することができます。多くのシンプルなネットワークシナリオでは、1 つのエリアで十分です。ルータプロセスオブジェクトのように、OSPF ネットワークの一部となるすべてのファイアウォール上で同様のエリアオブジェクトが定義される必要があります。

General

項目	説明
Name	OSPF 名を指定します。
Area ID	エリア ID を指定します。 0.0.0.0 が指定される場合、これはバックボーンエリアとなります。バックボーンエリアはひとつのみ設定することが可能であり、AS の中心部分となります。異なるエリアで交換されるルーティング情報は、通常バックボーンエリアを通過します。
Area is Stub Area	エリアがスタブエリアにある場合、このオプションを有効にします。
Become a default router for stub area ("Summarize")	ファイアウォールがスタブエリアに対するデフォルトルータになるべきであるかどうかの設定、およびメトリック値を設定することが可能です。

Import Filters

インポートフィルタは、(main ルーティングテーブルやポリシーベースのルーティングテーブルのような) いずれかの外部ソースまたは OSPF エリア内部から OSPF AS にインポートされるものをフィルタするために使用されます。

項目	説明
External	外部のルーティングソースからこの OSPF エリアにインポートすることが可能なネットワークアドレスを指定します。
Interarea	OSPF エリア内の他のルータからインポートすることが可能なネットワークアドレスを指定します。

4.7.3.3 OSPF Interfaces

ここでは OSPF インタフェースオブジェクトを構成する方法を説明します。OSPF インタフェースオブジェクトは OSPF エリア配下の構成要素です。エリアと異なり、それらは OSPF ネットワークにおける各ファイアウォール上で同じではありません。OSPF インタフェースオブジェクトの目的は、OSPF ネットワークの一部となる特定のインタフェースを表すことです。

注意 OSPF インタフェースでは異なるインタフェースタイプを使用できます。

これが最も一般的な用法ですが、OSPF インタフェースがいつも物理インタフェースに対応するわけではないことに注意してください。VLAN などの他のタイプのインタフェースが、代わりに OSPF インタフェースに関連付けられます。

General

項目	説明
Interface	この OSPF インタフェースに使用されるファイアウォール上のインタフェースを指定します。
Network	この OSPF インタフェースの IPv4 ネットワークアドレスを指定します。指定しないと、基本的な NetDefendOS インタフェースに割り当てられたネットワークをデフォルトとします。 このネットワークは、自動的に OSPF AS にエクスポートされるため、ダイナミックルーティングルールを必要としません。
Interface Type	以下のいずれかに設定できます。 • Auto - インタフェースタイプを自動的に検出しようとします。これは、物理インタフェースに使用されます。 • Broadcast - ブロードキャストインタフェースタイプはレイヤ 2 ブロードキャスト / マルチキャスト機能を持つインタフェースです。ブロードキャスト / マルチキャストネットワークの典型的な例は通常の物理イーサネットインタフェースです。 ブロードキャストが使用される場合、OSPF は IP マルチキャストアドレス 224.0.0.5 に OSPF Hello パケットを送信します。それらのパケットは、ネットワーク上の他のルータすべてでリッスンされます。そのため、近接するルータの検出のための OSPF Neighbor オブジェクトの設定は必要ありません。 • Point-to-point - ポイントツーポイントは、2 つのルータ (つまり、2 つのファイアウォール) だけにかかわる直接のリンクに使用されます。この典型的な例は、2 つのファイアウォール間に OSPF トラフィックを転送するために使用される VPN トンネルです。そのようなリンクの Neighbor アドレスは、OSPF Neighbor オブジェクトを定義することで設定されます。 VPN トンネルの使用については、「4.7.5 OSPF の設定」でより詳しく説明されています。 • Point-to-multipoint - ポイントツーマルチポイントインタフェースタイプは、ポイントツーポイントネットワークをまとめたものであり、ここには OSI レイヤ 2 ブロードキャスト / マルチキャスト機能を持たないリンクに 1 つ以上のルータがあります。
Metric	OSPF インタフェースに対するメトリックを指定します。これはこのインタフェースにパケットを送信する「コスト」を表しています。このコストはインタフェースの帯域幅に反比例します。
Bandwidth	メトリックを指定しない場合は代わりに帯域幅が指定されます。帯域幅がわかる場合には、直接メトリックの代わりにこれを指定できます。

Authentication

すべての OSPF プロトコル交換はシンプルなパスワードまたは MD5 暗号ハッシュを使用して認証されます。「Use Default for Router Process」を有効にすると、ルータプロセスのプロパティに設定されている値が使用されます。

これを有効にしない場合、以下のオプションの設定が使用可能です。

- No authentication
- Passphrase
- MD5 Digest

Advanced

項目	説明
Passive	他の OSPF ルータと接続するためにインタフェースが OSPF ルータプロセスに使用されていない限り、本オプションを有効とするべきです。Web インタフェースでは、オプションは No OSPF routers connected to this interface ("Passive") と呼ばれます。 有効であると、OSPF トラフィックはインタフェースで全く生成されません。
Hello Interval	インタフェースに送信される Hello パケットの間隔（秒）を指定します。
Router Dead Interval	この間に Neighbor から Hello パケットを受信しないと、その Neighbor ルータが操作から離脱していると見なされます。
RXMT Interval	このインタフェースの Neighbor に LSA の再送を行う間隔（秒）を指定します。
InfTrans Interval	インタフェースに推定される送信遅延を指定します。この値はルータを通じて LSA パケットを送信するためにかかる最大値を示しています。
Wait Interval	インタフェースが利用可能になってから、DR および BDR 選出までの時間（秒）を指定します。この値は、利用できる Hello Interval より高くする必要があります。
Router Priority	ルータ優先度を指定します。高い数値ほどこのルータが DR または BDR になる機会が増加します。0 が指定されると、このルータは DR/BDR 選出への資格がなくなります。 注意 HA クラスタは、ルータ優先度としていつも 0 を持っているため DR または BDR として使用できません。

ネットワークに接続するインタフェースで OSPF を実行せずに、OSPF ルータのプロセスにネットワークを含める必要がある場合もあります。これは、Passive オプションを有効にすることで行われます。: No OSPF routers connected to this interface ("Passive")

これは OSPF ルータのプロセスにスタティックルートをインポートするのにダイナミックルーティングポリシーを使用する代わりとなります。

「Ignore received OSPF MTU restrictions」が有効になると、OSPF MTU の不一致が許可されます。

プロミスキャスモード

OSPF が機能するために、OSPF インタフェースでもあるイーサネットインタフェースはプロミスキャスモードで動作する必要があります。このモードは、イーサネットインタフェースの MAC アドレスにマッチしない宛先 MAC アドレスを持つトラフィックが NetDefendOS に送信されても、インタフェースによって破棄されないことを意味します。NetDefendOS はプロミスキャスモードを自動的に有効にさせます。管理者はこれについて心配する必要はありません。

管理者が、CLI コマンド ifstat<ifname> を入力すると、Receive Mode 状況の行は、モードが変更されたことを示すため、Normal の代わりに隣に Promiscuous と表示します。詳しくは「3.4.2 イーサネットインタフェース」を参照してください。

4.7.3.4 OSPF Neighbor

いくつかのシナリオでは、ファイアウォールに隣接する OSPF ルータは、明示的に定義される必要があります。例えば、物理インタフェース間に接続がない場合です。

これを使用する最も一般的な状況は、VPN トンネルが 2 つの Neighbor を接続するのに使用される場合で、OSPF 接続がトンネルを経由して作成される必要があることを NetDefendOS に通知する必要があります。IPsec トンネルを使用した VPN タイプの使用については、「4.7.5 OSPF の設定」でより詳しく説明されています。

NetDefendOS OSPF Neighbor オブジェクトは OSPF エリア内に作成され、各オブジェクトには以下の項目があります。

項目	説明
Interface	Neighbor が位置する OSPF インタフェースを指定します。
IP Address	このルータに接続している Neighbor OSPF インタフェースの IP アドレスです。VPN トンネルでは、これはトンネルのリモートエンドの IP アドレスになります。
Metric	この Neighbor に対するメトリックを指定します。

4.7.3.5 OSPF Aggregate

これは、ルーティングテーブル内で共通のアドレスを持つ経路グループを一つのエントリに結合するために使用されます。アグリゲーションには以下の利点があります。

アドバタイズ（通知）されると、アグリゲーションによりファイアウォール内のルーティングテーブルのサイズが減少します。（主要な機能）
- アドバタイズされないと、アグリゲーションにより結合されたネットワークは非表示となります。
- OSPF が関連するトラフィックが減少します。

NetDefendOS での設定

NetDefendOS OSPF Aggregate オブジェクトは OSPF エリア内に作成され、各オブジェクトには、以下の項目があります。

項目	説明
Network	より小さいルータから構成されるネットワーク。
Advertise	アグリゲーションを通知するべきかどうかを指定します。

使用例

多くのシンプルな OSPF シナリオでは、OSPF Aggreegate オブジェクトは必要ありません。OSPF アグリゲーションは、D-Link ファイアウォールが Area Border Router（ABR）として動作し、2 つ以上の OSPF エリアとリンクしている場合にのみ使用されます。
以下の図では、アグリゲーションが使用される典型的な例を示しています。

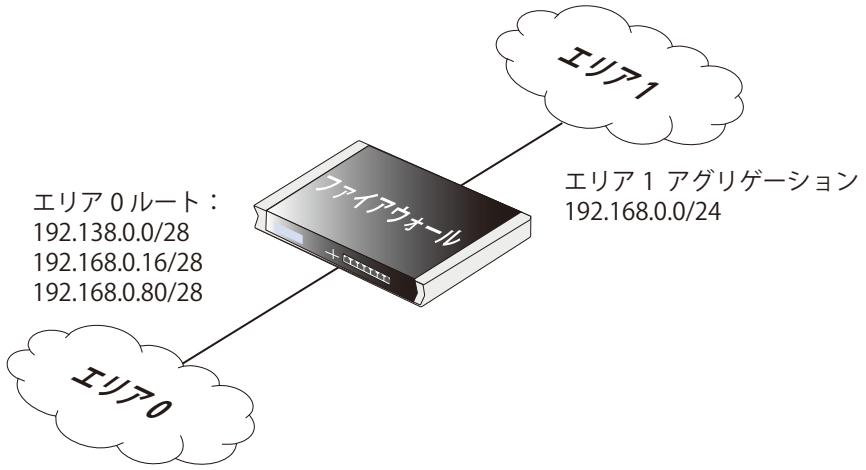


図 4-18　OSPF ルートアグリゲーション例

ここでは、ネットワーク 192.168.0.0/24 に対する OSPF Aggreegate オブジェクトの設定により、エリア 0 の 3 つのルートが 1 つに集約されています。

4.7.3.6 OSPF VLink

OSPF AS 内のすべてのエリアが物理的にバックボーンエリア（ID が 0 のエリア）に接続される必要がありますが、それができない場合もあります。この場合、仮想リンク（VLink）を使用し、バックボーンではないエリアを経由してバックボーンに接続します。

NetDefendOS OSPF VLink オブジェクトは OSPF エリア内に作成され、各オブジェクトには、以下の項目があります。

General

項目	説明
Name	仮想リンク名。
Link to router ID	仮想リンクの別サイドにあるルータの Router ID。

Authentication

項目	説明
Use Default for Router Process	AS プロパティ画面で設定された値を使用します。

注意　分割されているバックボーンのリンク

バックボーンエリアが分割されている場合、仮想リンクは別々の部分を接続するのに使用されます。

多くのシンプルなシナリオの場合、OSPF Vlink オブジェクトは必要ではありません。

4.7.4 Dynamic Routing Rules（ダイナミックルーティングルール）

本セクションはダイナミックルーティングルールを検証します。これらのルールは、ローカルなルーティングテーブルからどのルートを OSPF AS にエクスポートすることができるか、どれを AS からローカルなルーティングテーブルにインポートできるかを決定します。

4.7.4.1 概要

OSPF 設定手順の最後にダイナミックルーティングルールを作成する

OSPF 構造の作成後に行う最後の手順は、通常、各ファイアウォールにダイナミックルーティングルールを作成することです。これにより、OSPF AS がリモートファイアウォールから送信するルーティング情報をローカルなルーティングテーブルに追加します。

ダイナミックルーティングルールを OSPF のコンテキスト内で論じますが、他のコンテキストにも使用されます。

ダイナミックルーティングルールの理由

ダイナミックルーティング環境では、ルーティング交換に参加する範囲を規定することがルータにとって重要です。受信したすべてのルーティング情報を許容し、信頼することはできないため、ルーティングテーブルの一部を他のルータにパブリッシュすることを避けることが非常に重要です。

このため、ダイナミックルーティングルールは、ルーティング情報のフローを制限するために使用されます。

ダイナミックルーティングポリシールールは、ルートの開始地点、到達点、メトリックなどに従ってスタティックに設定または OSPF が学習した経路をフィルタします。一致した経路はアクションによって制御され、OSPF プロセスにエクスポートされるか、1 つ以上のルーティングテーブルに追加されます。

OSPF と共に使用

ダイナミックなルーティングルールは、以下を実行するのに OSPF と共に使用されます。

- ルートを OSPF AS からローカルルーティングテーブルにインポートすることを許可します。
- ルートをローカルルーティングテーブルから OSPF AS にエクスポートすることを許可します。
- ある OSPF AS から別の OSPF AS にエクスポートすることを許可します。

注意 非常に大規模なネットワークを除き、非同期システムを結合する上記 3 番目の使用法を行うことはあまりありません。

OSPF には少なくともインポートルールが必要です

初期値では、NetDefendOS はどのルートのインポートもエクスポートもしません。OSPF が機能するためには、Import ルールとなるダイナミックルーティングルールを少なくとも 1 つ定義する必要であることを覚えておいてください。

この Import ルールは、ローカルな OSPF Router Process オブジェクトを指定します。これにより OSPF AS で利用可能にされた外部ルートを、ローカルなルーティングテーブルにインポートすることができます。

フィルタを指定する

ダイナミックルーティングルールによりフィルタは到達したネットワークに基づいてインポートするルートを狭めることができます。多くの場合、「Or is within」オプションに all-nets を指定して、フィルタ条件をなしにする必要があります。

いつ「Export」ルールを使用するか

Import ルールは、OSPF AS からルートをインポートするのに必要ですが、エクスポートについては必要ではありません。OSPF インタフェースオブジェクトの一部分であるネットワークへのルートのエクスポートは自動です。

OSPF AS へのルートを明示的にエクスポートするためには、ダイナミックルーティング export ルールを作成する必要があります。

ダイナミックルーティングルールオブジェクト

以下の図は NetDefendOS ダイナミックルーティングルールオブジェクト間の関係を示しています。

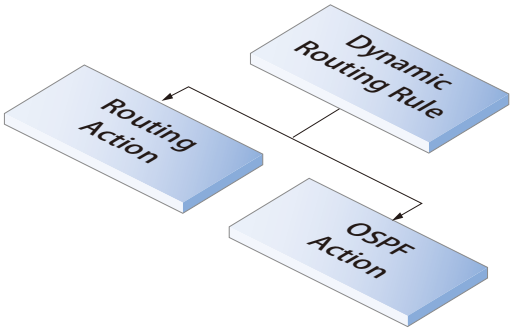


図 4-19　ダイナミックルーティングルールオブジェクト

4.7.4.2 Dynamic Routing Rule（ダイナミックルーティングルール）

ダイナミックルーティングルールを定義します。

General

項目	説明
Name	ルール名を指定します。
From OSPF Process	ルーティングテーブルまたは別の AS へインポートするルートのインポート元の OSPF AS（OSPF ルータプロセス）を指定します。
From Routing Table	OSPF AS へインポートする、または他のルーティングテーブルへコピーするルートのインポート元のルーティングテーブルを指定します。
Destination interface	ルールが、一致するべき宛先インタフェースを指定します。

Destination Network

項目	説明
Exactly Matches	正確に一致する必要があるインタフェースを指定します。
Or is within	送信先ネットワークとしておかれているネットワークを指定します。

More Parameters

項目	説明
Next Hop	このルールに始動されるネクストホップ（つまり、ルータ）を指定します。
Metric Range	ルータのメトリックが含まれる範囲を指定します。
Router ID	ルールが Router ID でフィルタされるべきかどうかを指定します。
OSPF Route Type	ルールが OSPF Router Type でフィルタされるべきかどうかを指定します。
OSPF Tag Range	ルータに関するタグが含まれる範囲を指定します。

4.7.4.3 OSPF Actions

本オブジェクトは OSPF のアクションを定義します。

General

項目	説明
Export to process	ルートの変更がどの OSPF AS にインポートされるべきであるかを指定します。
Forward	必要な場合、送信する IP を指定します。
Tag	このルートにタグを指定します。このタグはフィルタリングのために他のルータに使用されます。
Route Type	外部ルートタイプの種類を指定します。OSPF が、外部経路をタイプ 1 の OSPF ルートとして見なす場合に 1 を指定します。タイプ 2 は最も重要なルートコストです。
Offset Metric	インポートしたルートのメトリックを増加させます。
Limit Metric To	これらのルートへのメトリックを最小値と最大値で制限します。ルートは指定されるより高いまたは低い値を持っていると、指定した値に設定されます。

4.7.4.4 Routing Actions

ルーティングアクションは、ルーティングが 1 つ以上のローカルなルーティングテーブルへの変更を操作およびエクスポートするために使用されます。

項目	説明
Destination	OSPF AS へのルートの変更がどのルーティングテーブルにインポートされるべきであるかを指定します。
Offset Metric	この値によってメトリックを増加させます。
Offset Metric Type 2	この値によって Type 2 ルータのメトリックを増加させます。
Limit Metric Range To	これらのルートへのメトリックを最小値と最大値で制限します。ルートは指定されるより高い値を持っていると、指定した値に設定されます。
Allow Override of Static Route	スタティックルートの上書きを許可します。
Allow Overwrite of Default Route	デフォルトルートの上書きを許可します。

4.7.5 OSPF の設定

OSPF の設定は、OSPF が非常に多くの設定を提供するために複雑に見えるかもしれません。しかし、多くの場合、最小限の NetDefendOS オブジェクトを使用した簡単な OSPF ソリューションが必要であり、設定はわかりやすいと言えます。

先に説明した、2 台のみの D-Link ファイアウォールを使用した簡単なシナリオを見てみましょう。

この例では、ルーティングテーブルでルートを共有できるように、OSPF を使用して 2 つの D-Link ファイアウォールを接続します。両方とも単一の OSPF AS の部分である単一の OSPF エリア内にあります。これらの OSPF 概念になじみがない場合、詳しくは以前のセクションの説明を参照してください。

これらのファイアウォールの 1 つだけで開始する場合、NetDefendOS の設定手順は以下の通りとなります。

1. OSPF Router オブジェクトを作成します。
NetDefendOS OSPF Router プロセスオブジェクトを作成します。これは、OSPF 階層の最上位である OSPF 自律システム (AS) を定義しています。適切な名前をオブジェクトに指定します。これは NetDefendOS によって自動的に割り当てられるので、Router ID は空白のままにできます。

2. OSPF エリアを OSPF ルータに追加します。
前の手順で作成済みの OSPF Router プロセス内に、新しい OSPF エリアオブジェクトを追加します。適切な名前を割り当て、Area ID に値「0.0.0.0」を使用します。AS は複数エリアを持つことができますが、多くの場合 1 つだけが必要とされます。ID 0.0.0.0 により、このエリアが AS の中心となるバックボーンエリアであることを識別できます。

3. OSPF エリアに OSPF インタフェースを追加します。
前の手順で作成された OSPF エリアに、エリアの一部である各物理インタフェースに対する新しい OSPF エリアオブジェクトを追加します。OSPF インタフェースオブジェクトは、プロパティに以下のパラメータを指定する必要があります。

- Interface - OSPF エリアの一部になる物理インタフェース。

- Network - そのエリアの一部になるインタフェースのネットワーク。

  これは明示的に指定する必要はなく、指定しない場合、物理インタフェースに割り当てられたネットワークが使用されます。例えば、「lan」がインタフェースであれば、「lannet」がデフォルトネットワークになります。

- Interface Type - これは通常「Auto」であり、正しいタイプが自動的に選ばれます。

- 物理インタフェースが別の OSPF ルータ（OSPF ルータとして動作するほかの D-Link ファイアウォール）に直接接続していない場合、「Advanced」オプション「No OSPF routers connected to this interface ("Passive")」を有効にする必要があります。例えば、インタフェースがクライアントのネットワークだけに関連付けられる場合、オプションを有効とします。

  物理インタフェースが、OSPF ルータとして設定される別のファイアウォールに接続する場合には、このオプションを無効にする必要があります。

4. Dynamic Routing Rule（ダイナミックルーティングルール）を追加します。
最後に、OSPF ネットワークを展開するためにダイナミックルーティングルールを定義する必要があります。これには以下の 2 つの手順を実施する必要があります。

- ダイナミックルーティングポリシールールオブジェクトを追加します。このルールは、定義済みの OSPF ルータプロセスオブジェクトが選択されるようにオプション「From OSPF Process」を有効にする Import ルールであるべきです。OSPF AS からすべてのルートをインポートする場合に行います。

  さらに、送信先ネットワーク用の設定として、オプションの「Or is within」フィルタパラメータが「all-nets」となるように設定する必要があります。送信先ネットワークにより狭いフィルタも使用できますが、この場合ではすべてのネットワークに設定を行います。

- 追加されたダイナミックルーティングポリシールール内に Routing Action オブジェクトを追加します。ここで、OSPF からルーティング情報を受信する「Selected」リストにルーティングテーブルを追加します。

  典型的な例は、「main」というルーティングテーブルです。

OSPF Interface オブジェクトでは、自動的にエクスポートが行われるため、ローカルなルーティングテーブルを AS にエクスポートするダイナミックルーティングポリシールールを持つ必要はありません。

例外はルートがゲートウェイ（つまり、ルータホップ）を伴うかどうかということです。この場合、明示的にルートをエクスポートする必要があります。最も頻繁に起こり得るケースは、ゲートウェイが ISP のルータである外部のインターネットへの「all-nets」ルートの場合です。設定手順を以下で説明します。

5. 「all-nets」にダイナミックルーティングルールを追加します。
オプションで、Dynamic Routing Rule は、OSPF インタフェースルート以外の何らかのルートがエクスポートされる場合に定義される必要があります。これには以下の手順があります。

- ダイナミックルーティングポリシールールオブジェクトを追加します。このルールは、「From Routing Table」オプションを有効にして「Selected」リストに main テーブルを指定した Export ルールである必要があります。

  さらに、送信先ネットワーク用の設定として、オプションの「Or is within」フィルタパラメータが「all-nets」となるように設定する必要があります。これは、すべてのルートがエクスポートされることを意味します。

- 追加されたダイナミックルーティングポリシールール内に OSPF Action オブジェクトを追加します。ここで、Export to process オプションに OSPF router プロセス（OSPF AS）を設定します。

6. もう片方のファイアウォールにこれらの手順を繰り返します。
今度は、OSPF AS とエリアの一部になるもう片方のファイアウォールに対し、手順 1 ～ 5 を繰り返します。OSPF Router と OSPF Area オブジェクトは互いに同一とします。OSPF インタフェースオブジェクトは、どのインタフェースとネットワークが OSPF システムに含まれるかによって異なります。

2 つ以上のファイアウォールが同じ OSPF エリアの一部となる場合、それらのすべてが同様に構成されるべきです。

OSPF ルーティング情報交換は自動的に開始する

新しい構成が上記の手順で作成されて、展開されている場合、OSPF は自動的に始まりルーティング情報の交換を開始します。OSPF がダイナミックな分散システムであるため、個別のファイアウォールの構成が展開される順番は重要ではありません。

物理リンクが 2 つの異なるファイアウォール上にある 2 つのインタフェース間で確立され、それらのインタフェースが OSPF Router プロセスオブジェクトによって構成されると、OSPF はルーティング情報の交換を開始します。

OSPF 設定の確認

OSPF の動作とルーティング情報の交換をチェックすることができます。

ルーティングテーブルを検証することによって、それらの情報を確認します。OSPF を経由してルーティングテーブルにインポートされたルートは、ルートの説明文の左に「O」という文字を使用して示されます。例えば、routes コマンドを使用すると以下の出力結果となります。

```
DFL-xxxx:/> routes
Flags Network            Iface          Gateway         Local IP        Metric
----- ------------------ -------------- --------------- --------------- ------
      192.168.1.0/24     lan                                            0
      172.16.0.0/16      wan                                            0
O     192.168.2.0/24     wan            172.16.2.1                      1
```

ここで、192.168.2.0/24 のルートは OSPF 経由でインポートされており、172.16.2.1 のゲートウェイを持つ WAN インタフェースでそのネットワークを見つけることができます。この場合は、ゲートウェイはトラフィックが送信される D-Link ファイアウォールです。ファイアウォールは送信先ネットワークには接続されていない可能性もありますが、OSPF によって最適なルートであると判断されています。

また、CLI コマンドの「ospf」は、OSPF ステータスを示すために使用されます。このコマンドのオプションについては、「CLI Reference Guide」で詳しく説明しています。

VPN トンネルを通じてトラフィックを OSPF に送る

OSPF Router プロセスオブジェクトを使用して構成される 2 つのファイアウォール間のリンクは安全ではない場合があります。例えば、インターネット上です。

この場合、 2 つのファイアウォール間に VPN トンネルを設定し、OSPF 情報の交換のためにこのトンネルの使用を OSPF に通知することでリンクを保護します。次に、設定する方法を説明します。トンネルの実装方法として IPsec が選択されたものとします。

この設定を作成するためには、以下の追加手順と上記の通常の OSPF の手順を実行する必要があります。

1. IPsec をセットアップします。
最初に、2 つのファイアウォール A と B の間に通常の方法で IPsec トンネルを設定します。IPsec の設定オプションは「10.2 VPN クイックスタートガイド」で記載されています。

これにより、NetDefendOS で OSPF を構成した際に、IPsec トンネルは他のインタフェースと同様に扱われます。

2. ランダムな内部 IP アドレスを選択します。
各ファイアウォールに対し、内部 IPv4 アドレス（プライベートアドレス）を使用してランダムな IP ネットワークを選択する必要があります。例えば、ファイアウォール A のために、ネットワーク 192.168.55.0/24 を使用できます。

このネットワークは、OSPF セットアップ時の利便性のために使用されて、本当の物理ネットワークには関連付けされません。

3. OSPF インタフェースをトンネルに定義する
インタフェースパラメータに IPsec トンネルを持つ NetDefendOS OSPF インタフェースオブジェクトを定義します。Type パラメータをポイントツーポイントに、Network パラメータに前の手順で選択した 192.168.55.0/24 を指定します。

OSPF インタフェースによって、ネットワーク 192.168.55.0/24 の範囲に向かう OSPF 関連のすべて接続が、IPsec トンネルに送信されるべきであることが認識されます。

4. OSPF Neighbor を定義する
次に、隣接する OSPF ルータを検出する方法を OSPF に明示的に通知する必要があります。NetDefendOS OSPF Neighbor オブジェクトを定義することで、これを設定します。これは IPsec トンネル（インタフェースのように扱われます）のペアとトンネルの他方の端にあるルータの IP アドレスから構成されます。

ルータの IPv4 アドレスには、ネットワーク 192.168.55.0/24 からいずれか 1 つの IP アドレスを使用します。（例 : 192.168.55.1）

OSPF がセットアップされる際、NetDefendOS はこの OSPF Neighbor オブジェクトを見て、IPv4 アドレス 192.168.55.1 へ OSPF メッセージを送ろうとします。前の手順で定義された OSPF インタフェースオブジェクトは、この IP アドレスへの OSPF の関連するトラフィックが IPsec トンネルに送信されるべきであることを NetDefendOS に通知します。

5. トンネルのエンドポイントの Local IP を設定する
ファイアウォール A の設定を終了するために、ファイアウォール B における IPsec トンネル設定に 2 つの変更が行われる必要があります。以下の通りです。

- IPsec トンネルプロパティでは、トンネルへの Local Network は、「all-nets」に設定される必要があります。この設定は、トンネルに許可されるトラフィックのためのフィルタとして動作します。また、「all-nets」はトンネルへのすべてのトラフィックを許可します。

- IPsec プロパティのルーティングセクションでは、「Specify address manually」オプションが有効にされる必要があり、この説明における例の IPv4 アドレス 192.168.55.1 が入力される必要があります 。（CLI では、OriginatorType は manual に設定されており、OriginatorIP は 192.168.55.1 です。）これにより、トンネルのエンドポイントの IP が 192.168.55.1 に設定され、この送信元 IP を持つファイアウォール A にすべての OSPF トラフィックが送信されるようになります。

この設定を行うことで、ファイアウォール A から「core」ルートに OSPF トラフィックが到来します。つまり、トラフィックは NetDefendOS に向かいます。

6. もう片方のファイアウォールに手順を繰り返します。
今まで行ったことは、OSPF トラフィックが A から B までフローすることへの許可です。同じ IPsec トンネルを使用するファイアウォール B に対しても、ミラーイメージとして上記と同じ手順を実施する必要があります。ファイアウォール A、B 両方の OSPF 設定において、同様のランダムな内部 IP ネットワークを使用する必要があります。

注意 OSPF でないトラフィックもトンネルを使用できます。

VPN トンネルは OSPF トラフィックをはじめ、他のタイプのトラフィックも送信することができます。トンネルを OSPF トラフィック専用にする必要はありません。

4.7.6 OSPF の例

このセクションは以下で例証される簡単な OSPF シナリオについて詳細な設定手順を通じて説明します。

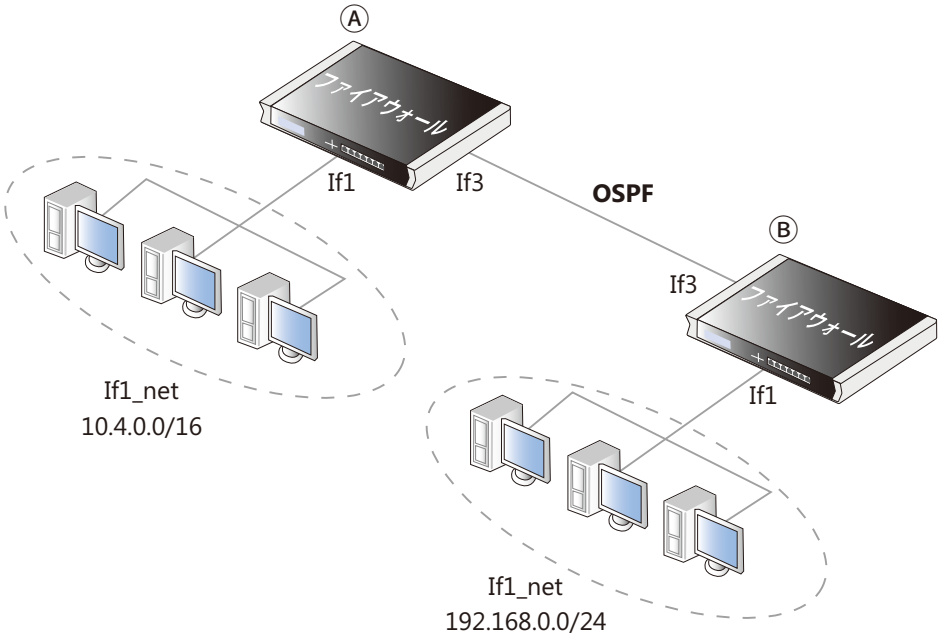


図 4-20　OSPF の例

ここに、A と B と呼ばれる 2 つの同じ D-Link ファイアウォールが、If3 インタフェースを介して接続されています。それぞれが If1 インタフェースに接続するホストのネットワークを持っています。片方の If1_net は IPv4 ネットワーク 10.4.0.0/16 で、もう一方の If1_net は IPv4 ネットワーク 192.168.0.0/24 です。

目標は、自動的にルーティング情報を交換して、10.4.0.0/16 ネットワークと 192.168.0.0/24 ネットワークの間で正しくトラフィックを送れるように両方のファイアウォールに OSPF を設定することです。そのようなトラフィックフローを許可するために必要とされる IP ルールセットのエントリは、この例には含まれていません。

例題 4.10

OSPF Router Process を作成する

まず、両方のファイアウォールで Autonomous System（AS）を定義する必要があります。

ファイアウォール A に、OSPF Router Process オブジェクトを作成します。オブジェクト名を as_0 と仮定します。

CLI

```
DFL-xxxx:/> add OSPFProcess as_0
```

Web Interface

1. **Network** > **Routing** > **OSPF** > **Add** > **OSPF Router Process** の順にメニューをクリックします。
2. プロセス名（ここでは as_0）を入力します。
3. 「OK」ボタンをクリックします。

次に、同じ OSPF Router Process 名 as_0 を使用して、ファイアウォール B に対しても同様の手順を実施します。

例題 4.11

OSPF エリアを追加する

OSPF Area オブジェクトをファイアウォール A の OSPF Router Process オブジェクト「as_0」に追加します。このエリアは、OSPF のバックボーンエリアであり、ID 0.0.0.0 を持っています。エリアオブジェクト名を area_0 であると仮定します。

CLI

まず、上記で作成された OSPFProcess オブジェクトになるように CLI コンテキストを変更します。

```
DFL-xxxx:/> cc OSPFProcess as_0
```

エリアを追加します。

```
DFL-xxxx:/as_0> add OSPFArea area_0 AreaID=0.0.0.0
```

以下のコマンドを使用すると、この新しい OSPFArea オブジェクトが表示されます。

```
DFL-xxxx:/as_0>  show

OSPFArea/
Name Area ID Comments
---- ------- --------
! area_1 0.0.0.0 <empty>
```

Web Interface

1. **Network > Routing > OSPF** の順にメニューをクリックします。
2. ルーティングプロセス「as_0」を選択します。
3. **Add > OSPF Area** の順にメニューをクリックします。
4. エリアプロパティ :
   - エリア名 (ここでは area_0) を入力します。
   - Area ID を 0.0.0.0 に指定します。
5. 「OK」ボタンをクリックします。

次に、同じ OSPF Area 名 area_0 を使用して、ファイアウォール B に対してこれを繰り返します。

例題 4.12

OSPF インタフェースオブジェクトを追加する

ファイアウォール A に、OSPF エリア「area_0」の一部である各物理インタフェースに対する新しい OSPF Interface オブジェクトを追加します。

CLI

コンテキストは、前述の例題のまま、OSPFProcess「as_0」であると仮定します。今度は、先ほど作成された OSPFArea になるようにコンテキストを変更します。

```
DFL-xxxx:/as_0> cc OSPFArea area_0
```

次に、OSPFInterface オブジェクトを追加します。

```
DFL-xxxx:/as_0/area_0> add OSPFInterface If1 Passive=Yes
```

Passive オプションが有効であることは、このインタフェースが別の OSPF ルータに接続されないことを意味します。最後に、デフォルトの CLI コンテキストに戻します。

```
DFL-xxxx:/as_0/area_0> cc
DFL-xxxx:/>
```

Web Interface

1. **Network > Routing > OSPF > as_0 > area_0 > OSPF Interfaces** の順にメニューをクリックします。
2. **Add > OSPF Interface** の順にメニューをクリックします。
3. インタフェースを選択します。ここでは If1 を選択します。
4. Advanced タブを選択します。
5. No OSPF routers connected to this interface (“Passive”) を選択します。
6. 「OK」ボタンをクリックします。

インタフェースのみを選択すると、ネットワークの初期値はそのインタフェースに割り当てられたネットワークとなります。ここでは If1_net となります。

この手順を、OSPF エリアの一部になるすべてのインタフェースに繰り返します。この場合、インタフェース If3 を OSPFInterface として追加する必要あります。しかし、このインタフェースは別のルータに接続されるので、Passive プロパティは初期値の有効のままとするべきです。

ファイアウォール B を同様にセットする必要があります。

例題 4.13

ルートを OSPF AS からルーティングテーブルにインポートする

この例題では、OSPF を使用して受信されたルートは、main ルーティングテーブルに追加されます。これを行うためには、Dynamic Routing Policy Rule を最初に作成する必要があります。この例題では、ルールは ImportOSPFRoutes と呼ばれます。

ルールには、ルートがどの OSPF AS からインポートされるべきであるかを指定しなければなりません。この例題では、先の例題で設定された OSPF AS「as_0」が使用されます。

ルーティングトポロジによっては、Destination interface/Destination Network フィルタを使用して特定のルートをインポートするのが望ましいかもしれませんが、このシナリオでは、all-nets ネットワークオブジェクトにあるすべてのルートが許可されます。手順は、最初にファイアウォール A で実行されます。

CLI

```
DFL-xxxx:/> add DynamicRoutingRule OSPFProcess=as_0 Name=ImportOSPFRoutes DestinationNetworkIn=all-nets
```

Web Interface

1. **Network** > **Routing** > **Routing Rules** > **Add** > **Dynamic Routing Policy Rule** の順にメニューをクリックします。
2. 適切なルール名を入力します。例 : ImportOSPFRoutes
3. 「From OSPF Process」オプションを選択します。
4. 「as_0」を「Available」から「Selected」に移動します。
5. DESTINATION NETWORK の「...Or is within」フィルタオプションで「all-nets」を選択します。
6. 「OK」ボタンをクリックします。

今度は、ルートをルーティングテーブルにインポートするダイナミックルーティングアクションを作成します。ルートが追加される宛先ルーティングテーブルは「main」です。

CLI

まず、CLI コンテキストをインポートのために追加された DynamicRoutingRule になるように変更します。

```
DFL-xxxx:/> cc DynamicRoutingRule ImportOSPFRoutes
```

次に、DynamicRoutingRuleAddRoute オブジェクトを追加します。

```
DFL-xxxx:/1(ImportOSPFRoutes)> add DynamicRoutingRuleAddRoute Destination=main
```

Web Interface

1. **Network** > **Routing** > **Routing Rules** の順にクリックします。
2. 定義済みの ImportOSPFRoutes をクリックします。
3. **Routing Action** > **Add** > **DynamicRoutingRuleAddRoute** の順にメニューをクリックします。
4. ルーティングテーブル「main」を「Available」から「Selected」に移動します。
5. 「OK」ボタンをクリックします。

同じ手順をファイアウォール B のために繰り返す必要があります。

例題 4.14

ルートを OSPF AS にインポートする

この例題では、main ルーティングテーブルからのルートを OSPF AS「as_0」にエクスポートします。ルートが自動的にエクスポートされないので、これを明示的に行う必要があります。

例外となるケースは、OSPF インタフェースネットワークのためのルートであり、これは自動的にエクスポートされます。（この例題では If1_net と If3_net）

最初にファイアウォール A に対しこの手順を実施します。

最初に新しいダイナミックルーティングポリシールールを追加します。

CLI

```
DFL-xxxx:/> add DynamicRoutingRule OSPFProcess=as_0 Name=ExportDefRoute DestinationNetworkIn=all-nets
            DestinationInterface=If3 From=RTable RoutingTable=main
```

Web Interface

1. **Network > Routing > Routing Rules > Add > Dynamic Routing Policy Rule** の順にメニューをクリックします。
2. ルール名を指定します。例 :ExportAllNets
3. 「 From Routing Table」オプションを選択します。
4. 「main」ルーティングテーブルを「Selected」リストに移動します。
5. DESTINATION NETWORK の「...Or is within」フィルタで「all-nets」を選択します。
6. 「OK」ボタンをクリックします。

次に、指定した OSPF AS にフィルタされたルートをエクスポートする OSPF アクションを作成します。

CLI

まず、CLI コンテキストをエクスポートのために追加された DynamicRoutingRule になるように変更します。

```
DFL-xxxx:/> cc DynamicRoutingRule ExportDefRoute
```

次に、DynamicRoutingRuleExportOSPF オブジェクトを追加します。

```
DFL-xxxx:/2(ExportDefRoute)> add DynamicRoutingRuleExportOSPF ExportToProcess=as_0
```

Web Interface

1. **Network > Routing > Routing Rules** の順にクリックします。
2. 定義済みの ExportAllNets をクリックします。
3. **OSPF Actions > Add > DynamicRoutingRuleExportOSPF** の順にメニューをクリックします。
4. 「Export to process」に「as0」を選択します。
5. 「OK」ボタンをクリックします。

同じ手続きをファイアウォール B のために繰り返す必要があります。

4.7.7 OSPF トラブルシューティング

OSPF に関する問題を障害調査する 2 つの特別な方法があります。

- 追加の OSPF ログイベントメッセージ
- OSPF CLI コマンド

これらを、以下で説明します。

追加の OSPF ログイベントメッセージ

初期値では、さまざまな基本のログイベントメッセージが NetDefendOS の OSPF 操作で生成されます。例えば、NetDefendOS 下で実行される OSPFProcess オブジェクトが my_ospf_proc という名前である場合、通常のログ生成は CLI コマンドで次のように有効にします。

```
DFL-xxxx:/> set OSPFProcess my_ospf_proc LogEnabled=Yes
```

これは初期設定であり、上のコマンドは例題用です。

以下のプロパティを有効にすると、障害調査やモニタを目的とした、追加 OSPF ログメッセージを提供することができます。

プロパティ	説明
DebugPacket	一般的なパケット解析イベントをログに出力します。
DebugHello	Hello パケットをログに出力します。
DebugDDesc	Database Description パケットをログに出力します。
DebugExchange	パケット交換をログに出力します。
DebugLSA	LSA イベントをログに出力します。
DebugSPF	SPF 計算イベントをログに出力します。
DebugRoute	ルーティングテーブルの操作イベントをログに出力します。

これらのプロパティに以下の値の 1 つを割り当てることができます。

値	説明
Off	ログに出力しません。
Low	すべてのアクションをログに出力します。
Medium	すべてのアクションにさらに詳細を加えてログに出力します。
High	最も詳細にすべてをログに出力します。

注意 高いレベルの設定ほど大量のデータを生成します。

High 設定を使用すると、小規模の AS に接続するだけの場合にもファイアウォールは多くの情報をログに出力します。「Advanced Setting」の「Log Send Per Sec Limit」を変更することが必要であるかもしれません。

例題 4.15

OSPF デバッグログイベントを有効にします。

この例題では、DebugHello と DebugRoute ログイベントを OSPFProcess「my_ospf_proc」で有効にします。

CLI

```
DFL-xxxx:/> set OSPFProcess my_ospf_proc DebugHello=Low DebugRoute=High
```

Web Interface

1. **Network** > **Routing** > **OSPF** > **my_ospf_proc** の順にメニューをクリックします。
2. Edit this object をクリックします。
3. Debug オプションを選択します。
4. 以下の情報を入力します。
   - Hello Packets: Low
   - Routing TableManipulation: High
5. 「OK」ボタンをクリックします。

OSPF CLI コマンド

CLI コマンド ospf は、リアルタイムに OSPF の動作を検証する様々なオプションを提供します。

CLI コンソールで一般的な OSPF のアクティビティを参照するために、「-snoop」オプションを使用できます。

```
DFL-xxxx:/> ospf -snoop=on
```

通常、ファイアウォールのために定義される OSPFProcess は 1 つだけであるため、コマンドで明示的にオブジェクトを指定する必要はありません。スヌーピングプロセスは以下のようにオフにされます。

```
DFL-xxxx:/> ospf -snoop=off
```

異なる OSPF コンポーネントのいずれかの状態をスナップショットにとって表示できます。例えば、OSPFInterface オブジェクトとして ospf_If1 という名前が設定されている場合、以下のコマンドを使用して、このオブジェクトに関する詳細を参照することができます。

```
DFL-xxxx:/> ospf -iface ospf_If1
```

エリア、Neighbor、ルート、および LSA のために同様のスナップショットを表示できます。

また、OSPF インタフェース操作を選択的に停止および再開できます。例えば、OSPFInterface「ospf_If1」を停止する CLI コマンドは以下の通りです。

```
DFL-xxxx:/> ospf -ifacedown ospf_If1
```

同じインタフェースを再開します。

```
DFL-xxxx:/> ospf -ifaceup ospf_If1
```

機能している OSPFRouteProcess を完全に止めることもできます。例えば、コンフィグレーションには定義済みの 1 つの OSPFRouteProcess オブジェクトだけがあるものと仮定した場合に、それを停止する CLI コマンドは以下の通りです。

```
DFL-xxxx:/> ospf -execute=stop
```

停止している OSPFRouteProcess を開始します。

```
DFL-xxxx:/> ospf -execute=start
```

1 つのコマンドで停止し、次に開始します。

```
DFL-xxxx:/> ospf -execute=restart
```

「ospf」コマンドのオプションは個別の「NetDefendOS CLI Reference Guide」に詳細に記載されています。

4.8 マルチキャストルーティング

4.8.1 概要

マルチキャスト問題

テレビ会議やビデオ放送など一部のインターネット通信では、単一のクライアントやホストが複数の受信者に同じパケットを送信する必要があります。これは、送信者が異なる受信 IP アドレスにパケットを複製するか、または、インターネットを介してパケットをブロードキャストすることによって実現されます。こうしたソリューションは、送信者のリソースやネットワーク帯域幅が大量に浪費されるため、好ましいとはいえません。また、適切なソリューションで受信者数を増やせることも必要です。

マルチキャストルーティングのソリューション

マルチキャストルーティングは、ネットワークルータ自体によってこの問題を解決し、最適な経路を介してグループ内のすべてのメンバにパケットを複製および転送します。

マルチキャストルーティングを有効にする IETF 標準は以下の通りです。

1. マルチキャストトラフィックのために予約されるクラス D の IPv4 アドレススペース。各マルチキャスト IP アドレスは、受信者の任意のグループを表します。

2. インターネットグループメンバシッププロトコル（IGMP : Internet Group Membership Protocol）により、受信者は特定のマルチキャストグループのメンバであることをネットワークに知らせることができます。

3. プロトコル独立マルチキャスト（PIM : Protocol Independent Multicast）は、マルチキャストパケットに最適な経路を決定するためのルーティングプロトコルの集合です。

基本的な原則

マルチキャストルーティングは、関係する受信者が IGMP プロトコルを用いてマルチキャストのためのグループに参加するという原理で機能します。この時、PIM ルータはこれらマルチキャストグループのすべてのメンバにパケットを複製および転送でき、それによりパケットフローのための分散ツリーを作成します。PIM は新しいネットワーク情報を入手するのではなく、OSPF などの既存のプロトコルから得られるルーティング情報を使用して最適な経路を決定します。

リバースパスフォワーディング（RPF : Reverse Path Forwarding）

マルチキャストルーティングプロセスの中でも重要なのは、リバース経路転送のメカニズムです。ユニキャストトラフィックでは、ルータはパケットの送信先だけを考慮します。マルチキャストでは、パケットの送信元から離れた下流の経路でパケットを転送するため、ルータはパケットの送信元についても考慮します。この方法は、分散ツリーでのループを防ぐために採用されます。

正しいインタフェースにルーティングする

初期値では、マルチキャストパケットは NetDefendOS によって core インタフェース（つまり、NetDefendOS 自身）へルーティングされます。正しいインタフェースへの転送を実行するため、Multicast Policy オブジェクトが IP ルールセットに設定されます。後述する例題で説明します。

プロミスキャスモード

IP ルールセットのエントリがマルチキャストパケットの宛先 IP アドレスに適用するルールセットに存在していると、そのイーサネットインタフェースは、マルチキャストパケットを受信するために、自動的に受信モード設定をプロミスキャスにします。プロミスキャスモードは、イーサネットインタフェースの MAC アドレスにマッチしない宛先 MAC アドレスを持つトラフィックが NetDefendOS に送信されても、インタフェースによって破棄されないことを意味します。NetDefendOS によってプロミスキャスモードが自動的に有効にされます。管理者はこれについて心配する必要はありません。

マルチキャストのみに関しては、プロミスキャスモードの使用は Ethernet オブジェクトのプロパティ Receive Multicast Traffic で初期値の Auto を指定することで明示的に制御することが可能です。このプロパティを Off に設定すると、マルチキャスト送信機能は動作できません。

管理者が、CLI コマンド「ifstat<ifname>」を入力すると、Receive Mode ステータスの行では、モードが変更されたことを示すため、Normal の代わりに Promiscuous と表示します。詳しくは「3.4.2 イーサネットインタフェース」を参照してください。

4.8.2 マルチキャストポリシーを使用してマルチキャストを転送する

Multicast Policy を使用して、複数のインタフェースを介したパケットの複製および転送を行います。この機能によって、NetDefendOS のマルチキャスト転送が実行され、マルチキャストパケットが複数インタフェースに送信されます。このルールは通常のルーティングテーブルを変更するため、Multicast Policy によって複製されるべきパケットは、core インタフェースにルーティングされる必要があります。

初期値では、マルチキャスト IP 範囲 224.0.0.0/4 は常に core インタフェースにルーティングされるため、ルーティングテーブルに手動で追加する必要はありません。指定した各出力インタフェースは、送信先アドレスのスタティックアドレス変換で個別に構成できます。「Interface/Net Tuple」ダイアログボックスの「Interface」フィールドは、「IPAddress」フィールドが設定されている場合は、空白のままで問題ありません。この場合、出力インタフェースは指定した IP アドレス上の経路検索によって決定されます。

Multicast Policy は、2 つのモードのいずれかで動作します。

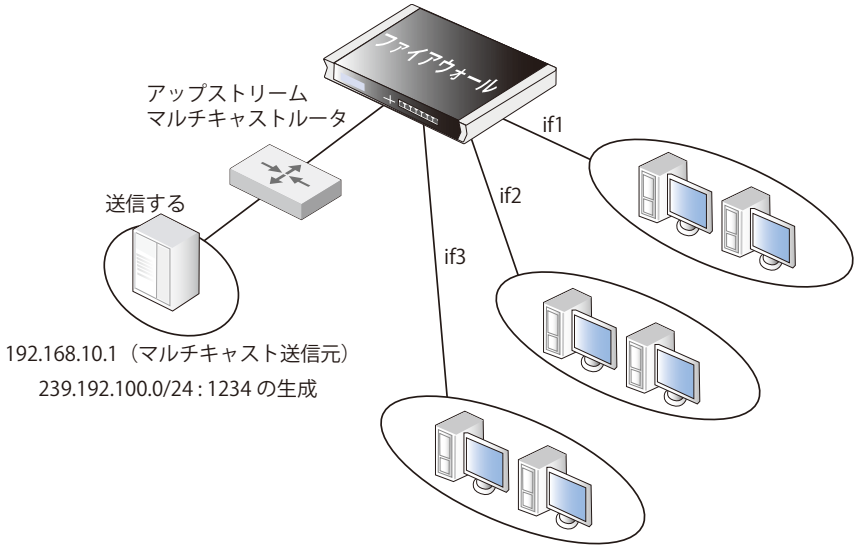
- IGMP を使用する
  指定したインタフェースでマルチキャストパケットが転送される前に、Multicast Policy で指定されたトラフィックフローが、IGMP を用いてホストからリクエストされます。これは、NetDefendOS のデフォルトの動作です。

- IGMP を使用しない
  トラフィックフローは、IGMP から推論されることなく、指定したインタフェースに従って直接転送されます。

例題 4.16

アドレス変換をしないマルチキャスト転送

この例では、マルチキャスト転送を IGMP と一緒に設定する方法について説明します。マルチキャストの送信者は 192.168.10.1 で、マルチキャストストリーム 239.192.10.0/24:1234 を生成します。これらのマルチキャストストリームは、インタフェース if1、if2、if3 を通じて、インタフェース wan から転送されます。一部のホストが IGMP プロトコルを用いてストリームをリクエストした場合のみストリームが転送されます。マルチキャストグループを転送するために Multicast Policy オブジェクトが作成されます。すべてのグループで IP アドレス 192.168.10.1 を持つ同じ送信者が設定され、これは wan インタフェースの後方に配置されています。



すべてのグループが wan インタフェース下のどこかに置かれている同じ IP アドレス 192.168.10.1 に送信元を持っています。

インタフェース配下のクライアントが IGMP を使用してグループをリクエストした場合、そのクライアントからの外向きインタフェースに対してのみマルチキャストグループが転送されるべきです。以下の手順を実施してマルチキャストトラフィックを転送するように設定します。

IGMP は個別に設定されます。IGMP の設定については、「IGMP ルールの設定 - アドレス変換をする場合」を参照してください。他の IP ルールセットのエントリを使用する場合と同様に設定します。

Web Interface

A. マルチキャストに対するカスタム Service オブジェクトを作成します。

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: my_multicast_service
- Type: UDP
- Destination: 1234

3. 「OK」ボタンをクリックします。

B. Multicast Policy オブジェクトを作成します。

1. **Policies > Firewalling > Main IP Rules > Add > Multicast Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: my_multicast_policy
- Source Interface: wan
- Source Network: 192.168.10.1
- Destination Interface: core
- Destination Network: 239.192.10.0/24
- Service: my_multicast_service

3. DESTINATION TRANSLATION セクションで、出力インタフェースの if1、if2、および if3 に 1 つずつエントリを追加します。各インタフェースにおいて、宛先のアドレス変換を行わないため「IPAddress」フィールドを空白のままにします。

4. 以下のオプションを有効にします。
- Require IGMP

5. 「OK」ボタンをクリックします。

CLI を使用して Multicast Policy を作成する

CLI を通してマルチキャストポリシーを作成するためには、以下の手順を行います。

Multicast Policy を作成する CLI コマンドは以下の通りです。

```
DFL-xxxx:/> add IPRule SourceNetwork=<srcnet> SourceInterface=<srcif>
DestinationInterface=<srcif> DestinationNetwork=<destnet> Action=MultiplexSAT
Service=<service> MultiplexArgument={outif1,ip1},{outif2;ip2},{outif3;ip3}...
```

2 つの値 {outif; ip} は、出力インタフェースと（グループのアドレス変換が必要な場合）IP アドレスの組み合わせを表します。

例えば、マルチキャストグループ 239.192.100.50 の多重化が出力インタフェースの if2 と if3 で必要とされる場合、ルールを作成するコマンドは以下の通りです。

```
DFL-xxxx:/> add IPRule SourceNetwork=<srcnet> SourceInterface=<if1>
DestinationInterface=core DestinationNetwork=239.192.100.50
Action=MultiplexSAT Service=<service> MultiplexArgument={if2;},{if3;}
```

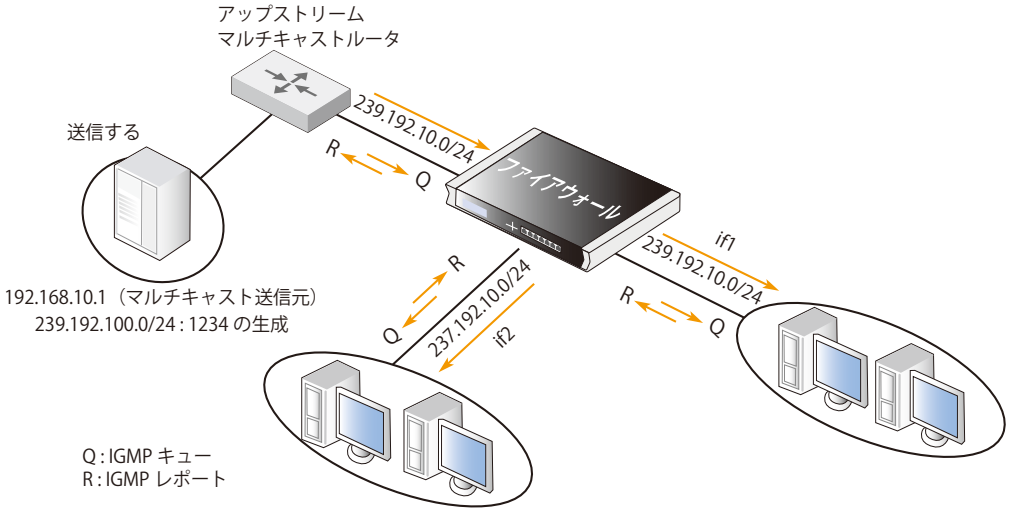
239.192.100.50 がマルチキャストグループであるため、宛先インタフェースは core となります。239.192.100.50 のアドレス変換は追加されていませんが、例えば if2 でアドレス変換が必要な場合、最終的な引数は以下の通りとなります。

```
MultiplexArgument={if2;<new_ip_address>},{if3;}
```

例題 4.17

マルチキャスト転送 - アドレス変換のシナリオ

この例は例題 4.16 を基本としていますが、ここでは、マルチキャストグループを変換します。マルチキャストストリーム 239.192.10.0/24 が if2 インタフェースを通じて転送される時、マルチキャストグループは 237.192.10.0/24 に変換されます。



インタフェース if1 を通じて転送する時には、アドレス変換は行われません。

Web Interface

A. multicast_service と呼ばれるマルチキャストに対するカスタムサービスを作成します。

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の通り入力し、「OK」ボタンをクリックします。
- Name : multicast_service
- Type : UDP
- Destination : 1234

B. マルチキャストポリシーを作成します。

1. **Policies > Firewalling >Main IP Rules > Add > Multicast Policy** の順にメニューをクリックします。

2. 以下の通り入力し、「OK」ボタンをクリックします。

General
- Name : my_multicast_sat
- Service : multicast_service

Address Filter
- Source Interface : wan1
- Source Network : 192.168.10.1
- Destination Interface : core
- Destination Network : 239.192.10.0/24

3. DESTINATION TRANSLATION セクションで、出力インタフェースの「if1」および「if2」を追加します。インタフェース「if1」の「IP Address」は空白のままとし、宛先のアドレス変換のためにインタフェース「if2」の「IP Address」フィールドには 237.192.10.0 を設定します。

4. オプションを有効にします。: Require IGMP

5. 「OK」ボタンをクリックします。

この例題における IGMP 設定については、「IGMP ルールの設定 - アドレス変換をする場合」を参照してください。

4.8.3 IGMP 設定

ホストとルータ間を通信する IGMP は、2 つのカテゴリに分類できます。

- **IGMP レポート**
  ホストが新しいマルチキャストグループに加入したい時、または現在のマルチキャスト加入を変更したい時、レポートがホストからルータへ送信されます。
- **IGMP クエリ**
  クエリは、一部のホストがまだ受信を希望するストリームが閉じないようにするために、ホストからルータへ送信される IGMP メッセージです。

通常、IGMP を機能させるためには両方のルールタイプを指定する必要がありますが、以下の 2 つの例外があります。

- マルチキャストソースがルータに直接接続されているネットワークに置かれている場合、クエリのルールは必要とされません。
- 隣接するルータが D-Link ファイアウォールにマルチキャストストリームを送付するようスタティックに設定されている場合、IGMP クエリも指定される必要はありません。

NetDefendOS は、2 つの IGMP 動作モード（スヌープモードとプロキシモード）をサポートしています。これらの 2 つのモードの操作は以下の図に示されています。

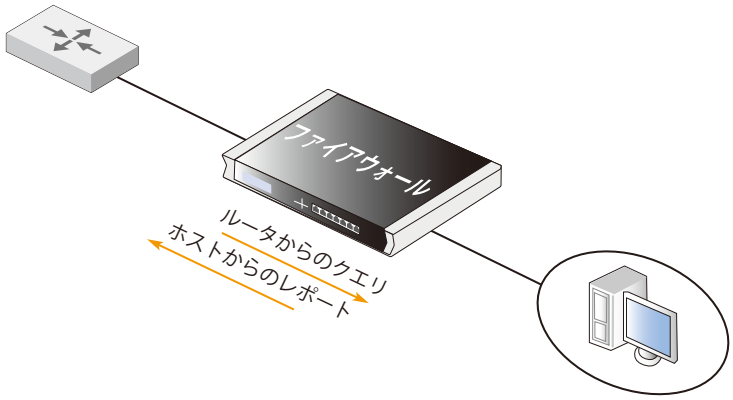


図 4-21　マルチキャストスヌープ

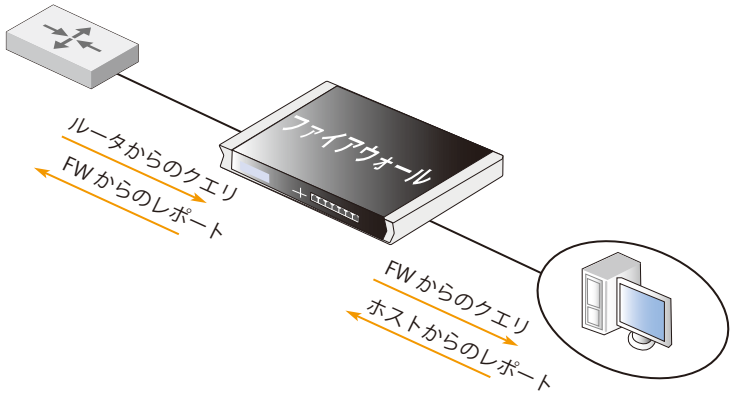


図 4-22　マルチキャストプロキシ

スヌープモードでは、ホストと他の IGMP ルータの間で D-Link ファイアウォールが透過的に動作します。この場合、IGMP クエリは送信されません。他のルータとホスト間でのみ、クエリとレポートを転送します。プロキシモードでは、ファイアウォールはクライアントに対して IGMP ルータとして動作し、積極的にクエリを送信します。上流ルータに対しては通常のホストとして動作し、クライアントの代わりにマルチキャストグループに加入します。

IGMP ルールの設定 - アドレス変換をしない場合

この例題では、アドレス変換を使用しない上記のシナリオ基づき、IGMP を設定する上で必要な IGMP ルールについて説明します。ルータは上流ルータに対してホストとして動作することが求められるため、プロキシモードで IGMP を実行するよう設定します。

例題 4.18

IGMP- アドレス変換をしない場合

以下の例題では、インタフェース if1、if2、if3 を含むインタフェースグループ IfGrpClients が設定済みであることが必要です。上流 IGMP ルータの IP アドレスは、UpstreamRouterIP と呼ばれます。

2 つのルールが必要です。1 つ目は、インタフェース if1、if2、if3 の背後のクライアントが、マルチキャストグループ 239.192.10.0/24 に参加することを許可するレポートルールです。2 つ目は、クライアントがリクエストしたマルチキャストグループについて、上流ルータが問い合わせすることを許可するクエリルールです。これら 2 つのルールを作成するには、以下の手順を実行する必要があります。

Web Interface

A. はじめに IGMP ルールを作成します。

1. **Network > Routing > IGMP Rules > Add > IGMP Rule** の順にメニューをクリックします。

2. 以下の通り入力し、「OK」ボタンをクリックします。

General

- Name : ルールに適する名前。例 : Report
- Type : Report (client->server)
- Action : Proxy
- Relay interface : wan1（これはリレーインタフェースです。）

Address Filter

- Source Interface : IfGrpClients
- Source Network : if1net、if2net、if3net
- Destination Interface : core
- Destination Network : Auto
- Multicast Source : 192.168.10.1
- Multicast Group : 239.192.10.0/24

B. 2 つ目の IGMP ルールを作成します。

1. **Network > Routing > IGMP Rules > Add > IGMP Rule** の順にメニューをクリックします。

2. 以下の通り入力し、「OK」ボタンをクリックします。

General

- Name : ルールに適する名前。例 : Queries
- Type : Query（server->client）
- Action : Proxy
- Relay interface : IfGrpClients（これはリレーインタフェースです。）

Address Filter

- Source Interface : wan1
- Source Network : UpstreamRouterIp
- Destination Interface : core
- Destination Network : Auto
- Multicast Source : 192.168.10.1
- Multicast Group : 239.192.10.0/24

IGMP ルールの設定 - アドレス変換をする場合

以下の例題では、上記の「マルチキャスト転送 - アドレス変換のシナリオ」で説明したシナリオに基づき、IGMP を設定するために必要な IGMP ルールについて説明します。クライアントインタフェースごとに、2 つの IGMP レポートルールが必要です。インタフェース if1 は、アドレス変換を使用せず、if2 はマルチキャストグループを 237.192.10.0/24 に変換します。また、if1 に対する 2 つのクエリルール（変換されたアドレスおよびインタフェース向けに 1 つと元のアドレス向けに 1 つ）が必要です。

レポートルールとクエリルールを対で作成する例題を 2 つ示します。上流マルチキャストルータは、UpstreamRouterIP という名前の IP を使用します。

例題 4.19

if1 の設定

アドレス変換を使用しない if1 向けにレポートとクエリのルールのペアを作成するには、以下の手順を実行する必要があります。

Web Interface

A はじめに IGMP ルールを作成します。

1. **Network > Routing > IGMP Rules > Add > IGMP Rule** の順にメニューをクリックします。

2. 以下の通り入力し、「OK」ボタンをクリックします。

General

- Name : ルールに適する名前。例 : Reports_if1
- Type : Report (client->server)
- Action : Proxy
- Relay interface : wan1（これはリレーインタフェースです。）

Address Filter

- Source Interface : if1
- Source Network : if1net
- Destination Interface : core
- Destination Network : Auto
- Multicast Source : 192.168.10.1
- Multicast Group : 239.192.10.0/24

B. 2 つ目の IGMP ルールを作成します。

1. **RNetwork > Routing > IGMP Rules > Add > IGMP Rule** の順にメニューをクリックします。

2. 以下の通り入力し、「OK」ボタンをクリックします。

General

- Name : Queries_if1
- Type : Query (server->client)
- Action : Proxy
- Output Interface : if1（これはリレーインタフェースです。）

Address Filter

- Source Interface : wan1
- Source Network : UpstreamRouterip
- Destination Interface : core
- Destination Network : Auto
- Multicast Source : 192.168.10.1
- Multicast Group : 239.192.10.0/24

例題 4.20

if2 の設定 - グループ変換

アドレス変換を使用する if2 向けにレポートとクエリのルールのペアを作成するには、以下の手順を実行する必要があります。

グループは変換されているため、IGMP レポートには変換された IP アドレスが含まれており、クエリには元の IP アドレスが含まれることに注意してください。

Web Interface

A. はじめに IGMP ルールを作成します。

1. **Network > Routing > IGMP Rules > Add > IGMP Rule** の順にメニューをクリックします。

2. 以下の通り入力し、「OK」ボタンをクリックします。

General

- Name : ルールに適する名前。例 : Reports_if2
- Type : Report (client->server)
- Action : Proxy
- Relay interface : wan1（これはリレーインタフェースです。）

Address Filter

- Source Interface : if2
- Source Network : if2net
- Destination Interface : core
- Destination Network : Auto
- Multicast Source : 192.168.10.1
- Multicast Group : 239.192.10.0/24

B. 2 つ目の IGMP ルールを作成します。

1. **Network > Routing > IGMP Rules > Add > IGMP Rule** の順にメニューをクリックします。

2. 以下の通り入力し、「OK」ボタンをクリックします。

General

- Name : ルールに適する名前。例 : Queries_if2
- Type : Query (server->client)
- Action : Proxy
- Relay interface : if2（これはリレーインタフェースです。）

Address Filter

- 送信元インタフェース : wan1
- Source Network : UpstreamRouterip
- Destination Interface : core
- Destination Network : Auto
- Multicast Source : 192.168.10.1
- Multicast Group : 239.192.10.0/24

IGMP 拡張設定

明示的な IGMP 設定を持たない全てのインタフェースに適用可能な、グローバルの IGMP 拡張設定が多数あります。

4.8.4 IGMP 拡張設定

Web インタフェースの **Network > Routing > Advanced Multicast Settings** で、以下の IGMP の高度な設定を確認できます。

項目	説明
Auto Add Multicast Core Route	本設定は、マルチキャスト IP アドレス範囲 224.0.0.0/4 に対するすべてのルーティングテーブルに core ルートを自動的に追加します。設定を無効にすると、デフォルトルートに従って、マルチキャストパケットは送信されます。 初期値 : Enabled（有効）
IGMP Before Rules	IGMP トラフィックについて、通常の IP ルールセットを迂回し、IGMP ルールセットを参照します。 初期値 : Enabled（有効）
IGMP React To Own Queries	ファイアウォールは、自身から生成されたクエリも含め、クエリに対して常に IGMP Membership レポートで応答する必要があります。優先的な IGMP 設定を持たないインタフェースのグローバル設定。 初期値 : Disabled（無効）
IGMP Lowest Compatible Version	これより低いバージョンを持つ IGMP メッセージは、ログに出力され、無視されます。優先的な IGMP 設定を持たないインタフェースのグローバル設定。 初期値 : IGMPv1
IGMP Router Version	IGMP 設定を持たないインタフェースでグローバルに使用される IGMP プロトコルバージョン。同じネットワークで問い合わせをする複数の IGMP ルータは、同じ IGMP バージョンを使用する必要があります。優先的な IGMP 設定を持たないインタフェースのグローバル設定。 初期値 : IGMPv3
IGMP Last Member Query Interval	ホストが「グループ」、または「グループと送信元」の指定クエリに対して応答を送信するまでの最大時間（ミリ秒）。重要な IGMP 設定を持たないインタフェースのグローバル設定。 初期値 : 5,000
IGMP Max Total Requests	1 秒間に処理する IGMP メッセージの最大のグローバルな数。 初期値 : 1,000
IGMP Max Interface Requests	1 インタフェースおよび 1 秒あたりの最大リクエスト数。優先的な IGMP 設定を持たないインタフェースのグローバル設定。 初期値 : 100
IGMP Query Interval	IGMP ステートを更新するために、デバイスに送信される General クエリの間隔（ミリ秒）。優先的な IGMP 設定を持たないインタフェースのグローバル設定。初期値 : 125,000
IGMP Query Response Interval	ホストがクエリに対して応答を送信するまでの最大時間（ミリ秒）。優先的な IGMP 設定を持たないインタフェースのグローバル設定。初期値 : 10,000
IGMP Robustness Variable	IGMPRobustnessVariable-1 パケット損失に対する強度です。優先的な IGMP 設定を持たないインタフェースのグローバル設定。初期値 : 2
IGMP Startup Query Count	ファイアウォールは、起動時に IGMPStartupQueryInterval の間隔で、IGMP Startup Query Count General クエリを送信します。優先的な IGMP 設定を持たないインタフェースのグローバル設定。初期値 : 2
IGMP Startup Query Interval	起動段階で使用される General クエリの間隔（ミリ秒）。優先的な IGMP 設定を持たないインタフェースのグローバル設定。初期値 : 30,000
IGMP Unsolicated Report Interval	最初の Membership レポートの繰り返し時間（ミリ秒）。優先的な IGMP 設定を持たないインタフェースのグローバル設定。 初期値 : 1,000

4.8.5 GRE を使用したマルチキャストトンネル

GRE トンネルを通じて 2 つの D-Link ファイアウォール間の NetDefendOS のマルチキャストをトンネルできます。2 つのファイアウォールをリンクする GER トンネルでは、マルチキャストサーバは一方のファイアウォールの背後にあり、クライアントは他方のファイアウォールの背後にあります。

セットアップの問題

マルチキャストのトンネリングで注意すべき問題は以下の通りです。

- マルチキャストサーバが 1 より高い TTL でストリームを送信していることを確認してください。（初期値では VLC は TTL=1 を使用します。）
- IGMP を使用する時には、送信先ネットワークが all-nets に設定されていないことを確認してください。all-nets に設定されていると、マルチプレックスルールは正しいインタフェースにストリームを送りません。
- Multicast Policy ルールセットはサーバが背後にあるファイアウォールとクライアントが背後にあるファイアウォールの両方に設定される必要があります。（つまり、トンネル終端）

トンネル設定の概要

以下のコンポーネントがクライアントとサーバの両側で必要です。

- GRE トンネルオブジェクトのリモートネットワークについて、サーバ側ではクライアントネットワーク、クライアント側ではサーバネットワークとなるように設定します。
- GRE トンネルを通じてもう一方のネットワークにまとめられたルートマルチキャストトラフィックを送るようにルートを設定します。
- 両側に Multicast Policy を設定します。
- Multicast Policy オブジェクトで Require IGMP オプションを有効にします。
- マルチキャストトラフィックに IGMP ルールオブジェクトを設定します。

設定例

以下の図はマルチキャストトンネルの例題です。

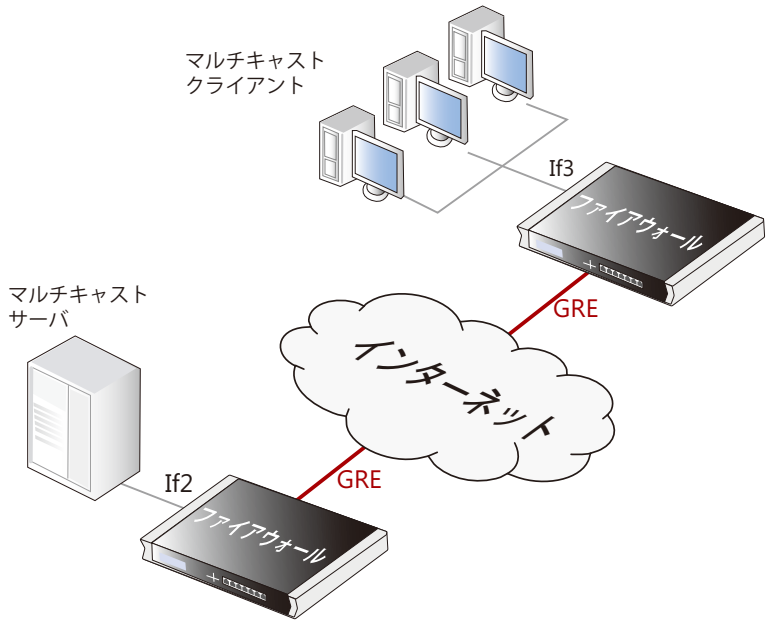


図 4-23　GRE を使用したマルチキャストトンネル

トンネルの両側にある IPv4 アドレス帳オブジェクト mc_group は、同じマルチキャスト IPv4 範囲にあります。例えば 239.100.100.0/24 です。

A. サーバ側のコンフィグレーション設定

サーバ側コンフィグレーションでは、クライアントネットワークは IPv4 アドレス帳オブジェクト client_net、ローカルな内部トンネルエンドポイントは If2_ip であるものとします。（サーバは If2 インタフェースにあります。）GRE トンネル gre_to_clients が設定され、リモートネットワークは、アドレス帳オブジェクト client_net です。

GRE トンネル

名前	IP アドレス	リモートエンドポイント	リモートネットワーク
gre_to_clients	If2_ip	client_interface_ip	client_net

ルート

上の GRE オブジェクトで自動的にルートを追加するオプションが有効であれば、以下のルートが NetDefendOS によって main ルーティングテーブルに追加されます。

ネットワーク	インタフェース
client_net	gre_to_clients

サービス

名前	タイプ	送信先ポート
mc_stream	udp	1234

IP ルールセットのエントリ

アクション	送信元 インタフェース	送信元 ネットワーク	送信先 インタフェース	送信先 ネットワーク	サービス	Multiplex インタフェース
Multicast Policy	If2	If2_net	core	mc_group	mc_stream	gre_to_clients
IP Policy	If2	If2_net	core	mc_group	mc_stream	

IGMP ルール

タイプ	アクション	送信元 インタフェース	送信元 ネットワーク	マルチキャスト グループ	マルチキャスト サービス	リレー インタフェース
Query	Proxy	If2	If2_net	mc_group	all-nets	gre_to_clients
Report	Proxy	gre_clients	all-nets	all-nets	all-nets	If2

B. クライアント側のコンフィグレーション設定

クライアント側コンフィグレーションでは、サーバネットワークは IPv4 アドレス帳オブジェクト server_net、ローカルな内部トンネルエンドポイントは If3_ip であるものとします。（クライアントは If3 インタフェースにあります。）GRE トンネル gre_to_server が設定され、リモートネットワークは、アドレス帳オブジェクト server_net です。

GRE トンネル

名前	IP アドレス	リモートエンドポイント	リモートネットワーク
gre_to_server	If3_ip	server_interface_ip	server_net

ルート

上の GRE オブジェクトで自動的にルートを追加するオプションが有効であれば、以下のルートが NetDefendOS によって main ルーティングテーブルに追加されます。

ネットワーク	インタフェース
server_net	gre_to_server

サービス

名前	タイプ	送信先ポート
mc_stream	udp	1234

IP ルールセットのエントリ

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス	Multiplexインタフェース
Multicast Policy	gre_to_server	server_net	core	mc_group	mc_stream	lf3
IP Policy	gre_to_server	server_net	core	mc_group	mc_stream	

IGMP ルール

タイプ	アクション	送信元インタフェース	送信元ネットワーク	マルチキャストグループ	マルチキャストサービス	リレーインタフェース
Report	Proxy	lf3	lf3_net	mc_group	all-nets	gre_to_server
Query	Proxy	gre_to_server	all-nets	all-nets	all-nets	lf3

4.9 透過モード

4.9.1 透過モードの概要

透過モードの動作方法

NetDefendOS 透過モード機能により、ネットワークの再構成をせずに、また、D-Link ファイアウォールの存在を認識するホストを必要とせずに、ファイアウォールをネットワーク内に配置することができます。すべての NetDefendOS 機能は、そのポイントを通じて流れるトラフィックをモニタリングおよび管理するために使用されます。NetDefendOS は各サービス（例：HTTP）や指定した方向に対し、アクセスの許可 / 拒否を行うことができます。許可されているサービスにアクセスしている限り、ユーザはファイアウォールの存在に気づくことはありません。

従って、ネットワークセキュリティと制御は、透過モードで動作している D-Link ファイアウォールの配置で顕著に強化されますが、既存のユーザとホストへの影響は最小になります。

注意 HA は透過モードをサポートしません。

switch ルートには状態の同期がないため、NetDefendOS の高可用性クラスタでは透過モードです。ループ回避は全く機能しません。これらの理由で、HA クラスタで透過モードを設定するべきではありません。

switch ルート

透過モードは、ルーティングテーブルの標準ルートの代わりに switch ルートを指定することで有効にされます。通常、switch ルートは、all-nets ネットワークが特定のインタフェースで見つけられることを示しています。NetDefendOS は、接続するイーサネットネットワークで ARP メッセージ交換を使用し、どのホスト IP アドレスがそのインタフェースに位置しているかを識別し、情報を取得します。詳しくは、以下で説明します。同じインタフェースには、通常の non-switch ルートが存在するべきではありません。

特別な条件下では、swich ルートが all-nets ではなく指定されたネットワーク範囲を持つことがあります。これは、ネットワークが 2 つのインタフェースに分割される場合に起こり得ることですが、管理者は、どのユーザがどのインタフェースにいるかは正確にはわかりません。

ブロードキャストパケットの送信

初期値では、ブロードキャストパケットは透過モードで送信されません。switch ルートでプロパティ「Forward Broadcast Traffic」を有効にすることによって、転送を有効にする必要があります。また、送信元と宛先インタフェースの両方のルートでこれを行う必要があります。これは「4.2.7 ブロードキャストパケットの転送」でより詳しく説明されています。

注意 IPv6 は switch ルートでサポートされません。

IPv6 は通常の NetDefendOS ルートでサポートされますが、switch ルートではサポートされません。これは、透過モードで IPv6 を使用できないことを意味します。

使用のシナリオ

透過モードの使用例は以下の通りです。

- ユーザ間のセキュリティの実現
  セキュリティを向上する透過モード機能の典型的な例が、各部署を別の部署から保護することが必要である会社の環境です。財務部は営業部のサーバ上で制限されているサービス（例 HTTP）にだけアクセスを要求するかもしれませんし、同時に営業部が財務部のネットワーク上で制限されているアプリケーションに同じくアクセスを要求するかもしれません。2 つの部署の物理的なネットワークの間に 1 台の D-Link ファイアウォールを配置することにより、透過的かつ制御されたアクセスを実現します。

- インターネットアクセスを制御する
  外部インターネットと、内部ネットワーク内の公開 IPv4 アドレス範囲との間のトラフィックを許可する構成を想定します。透過モードは、これらの IP アドレスに許可されるサービスの種類や方向を制御することができます。例えば、そのような状況で許可されたサービスは、インターネットへの HTTP アクセスかもしれません。詳しくは「4.9.2 インターネットアクセスを有効にする」を参照してください。

ルーティングモードとの比較

D-Link ファイアウォールは、以下の 2 つのモードのいずれかで動作していると想定することができます。

- non-switch ルートを使用したルーティングモード
- switch ルートを使用した透過モード

non-switch ルートでは、ファイアウォールはレイヤ 3 ルータの全機能を実行します。そのため、最初にファイアウォールがネットワークに置かれる時、またはトポロジの変化がある時には、ルーティングテーブルが新しいレイアウトに適合しているかどうか、ルーティング設定を徹底的にチェックする必要があります。IP 設定の再構成が、定義済みのルータと保護されたサーバに必要である可能性があります。
ルーティングへの完全な制御が必要とされる場合に本モードは適しています。

switch ルートでは、D-Link ファイアウォールは透過モードで動作し、OSI レイヤ 2 スイッチに似ています。IP またはイーサネットレベルでは送信元または送信先情報を変更せずに、IP パケットを調査して正しいインタフェースに透過的に送信します。これは、NetDefendOS が接続するホスト MAC アドレスの情報を取得することで行われます。そして、ファイアウォールのいずれか一方にある物理イーサネットネットワークは単一の論理 IP ネットワークであるかのように動作します。
（「付録 D OSI 参照モデル」を参照してください。）

従来のルーティングに加え、透過モードには 2 つの長所があります。

- ユーザは、IP アドレス（固定 IP アドレスと仮定）を変更しないで、「plug-n-play」形式で 1 つのインタフェースから別のインタフェースまで移動できます。ユーザは、ルートを変更せずに以前と同じサービス（例 : HTTP、FTP）を受けることができます。
- 同じネットワークアドレス範囲が複数のインタフェースに存在することができます。

注意 透過モードとルーティングモードを結合する。

透過モードとルーティングモードは、単一の D-Link ファイアウォールで一緒に動作できます。2 つのタイプを同じインタフェースに対して結合できませんが、標準の non-switch ルートと共に switch ルートを定義できます。インタフェースはどちらかのモードで動作します。

さらに、そうでない透過トラフィックにアドレス変換を適用することによってハイブリッドケースを作成することもできます。

透過モードの実行

透過モードでは、NetDefendOS は ARP トランザクションが D-Link ファイアウォールを通過することを許可して、この ARP トラフィックから IP アドレス、物理アドレスおよびインタフェース間の関連を判断します。NetDefendOS は IP パケットを正しいレシーバにリレーするため、このアドレス情報を記憶します。ARP 処理中、エンドポイントのいずれも、ファイアウォールの存在に気づくことはありません。

通信の最初には、ホストは ARP リクエストをブロードキャストすることによって、ターゲットホストの物理アドレスを知ろうとします。NetDefendOS がこの ARP リクエストを受け取ると、内部で ARP Transaction State に入り、既に ARP リクエストを受信したインタフェースを除くすべてのスイッチ経路が、設定されたインタフェースに APR リクエストをブロードキャストします。NetDefendOS は設定したタイムアウト期間以内に送信先から ARP リプライを受け取ると、ARP Transaction State エントリに蓄積された情報を使用して ARP 処理リクエストの送信元にリプライを転送します。

APR 処理中、NetDefendOS はリクエストとリプライの両方の送信元アドレス情報を学習します。NetDefendOS では、この情報を蓄積するために 2 つのテーブルが維持されています。それらは、CAM（Content Addressable Memory）テーブルとレイヤ 3 キャッシュと呼ばれています。CAM テーブルは、対象のインタフェース上で有効な MAC アドレス情報を追跡し、レイヤ 3 キャッシュは MAC アドレスとインタフェースに IP アドレスをマップします。レイヤ 3 キャッシュは IP トラフィックのみに使われ、レイヤ 3 キャッシュのエントリはルーティングテーブルにホストのエントリとして登録されます。

個々の IP パケットは D-Link ファイアウォールを通過する時に、送信先への経路を検索します。パケットの経路がスイッチの経路かルーティングテーブルのレイヤ 3 キャッシュエントリと一致すると、NetDefendOS はそのパケットを透過的に扱うようになります。送信先インタフェースと MAC アドレスが経路上で有効であれば、NetDefendOS は送信先にパケットを転送するのに必要な情報を持っています。経路が Switch ルートであれば、送信先を特定する情報はないので、ファイアウォールはネットワークのどこに送信先があるかを探す必要があります。NetDefendOS によって、ICMP（ping）と同様に ARP が送信され、探索が行われます。NetDefendOS は、Switch ルートで指定されたインタフェース上の宛先に対する元の IP パケットの最初の送信者としてふるまいます。ARP リプライを受け取ると、NetDefendOS は CAM テーブルとレイヤ 3 キャッシュを更新し、送信先にパケットを転送します。

CAM テーブルかレイヤ 3 キャッシュがいっぱいになると、テーブルは自動的に一部を消去します。NetDefendOS は、ARP と ICMP を送信する探索メカニズムを使って、消去された送信先を再度探索します。

透過モードの有効化

NetDefendOS の透過モードを有効にするためには、以下の手順が必要です。

1. 透過となるインタフェースは、はじめにインタフェースグループオブジェクトに集めておく必要があります。ホストがグループ内のインタフェースを自由に移動可能である場合、それらのインタフェースは Security transport equivalent としてをマークされます。

2. switch ルートは、適切なルーティングテーブルとそれに関連しているインタフェースグループで作成されます。グループ内のインタフェースに対する既存の non-switch は、ルーティングテーブルから削除する必要があります。

   switch ルートのネットワークパラメータに、all-nets を指定するか、または代わりにインタフェース間で透過である IP アドレス範囲を指定します。後者のオプションについては、以下に詳しく説明します。

3. 希望するトラフィックが透過モードで動作するインタフェース間に流れるように IP ルールセットに適切な IP ルールを作成します。

   透過モードのトラフィックフローに対し、最初に何も制限をかけない場合、以下の単一の IP ルールを追加することが可能ですが、より制限された IP ルールをお勧めします。

アクション	送信元インタフェース	送信元ネットワーク	インタフェース	送信先ネットワーク	サービス
Allow	any	all-nets	any	all-nets	all_services

ネットワークパラメータの制限

NetDefendOS は ARP トラフィックをリッスンし、IP アドレスが存在するインタフェースを検出して、ホストルートをルーティングテーブルに継続的に追加します。名前が示す通り、単一のホストルートはただ一つの IP アドレスに対してルートを指定します。従って、多くの接続がホストに行われた場合、これらのルート数は非常に多くなります。

ネットワークパラメータに対して all-nets の代わりにネットワークまたは IP アドレスを指定する主な利点は、NetDefendOS が自動的に生成するルート数が明らかに少なくなることです。指定したネットワークまたはアドレス内に該当 IP アドレスが存在する場合、ホストのルートが 1 つだけ追加されます。追加されるルート数を減らすことで、ルート検索の処理オーバヘッドを減少させることができます。

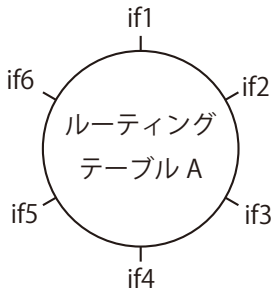
管理者がネットワークトポロジに関して把握している場合にだけ、ネットワークまたはアドレス範囲の指定はできます。

複数の switch ルートの接続

上記の設定手順は、一つの switch ルートに関連する一つのインタフェースグループにすべてのインタフェースを置くこと示しています。

1 つの switch ルートへの代替手段は、インタフェースグループを使用しないで、各インタフェースに個別の switch ルートを使用することですが、最終的な結果は同じです。一つのルーティングテーブルに定義されている全ての switch ルートが、NetDefendOS によって共に接続され、インタフェースがどのように switch ルートに関連付けられても、それらの間に透過性はあります。

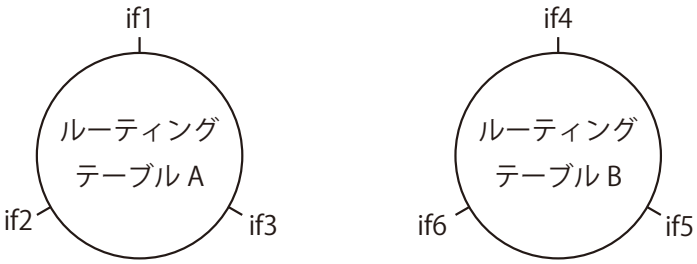
例えば、if6 へのインタフェース if1 がルーティングテーブル A の switch ルートにあると、結果として起こる相互接続は以下の通りです。



ただし、switch ルートをこのように相互接続することができるのは、すべてのインタフェースが同じルーティングテーブルに関連する場合です。そうでない状況については次に説明します。

独立した透過モードのネットワークを作成する

2つのルーティングテーブルAとBがあり、テーブルAのswitchルートにインタフェースif1、if2、およびif3、テーブルBのswitchルートにインタフェースif4、if5、およびif6がある場合、相互接続は以下の図の通りです。



上の図は、一つのルーティングテーブルにおけるswitchルートの相互接続を、別のルーティングテーブルにおけるswitchルートの相互接続から完全に分離する方法を示しています。このように異なるルーティングテーブルを使用することによって、2つの独立した透過モードネットワークを作成できます。

インタフェースに使用されるルーティングテーブルは、各インタフェースのルーティングテーブルメンバシップパラメータで決定されます。個別の透過モードのネットワークを実装するためには、インタフェースでルーティングテーブルのメンバシップをリセットする必要があります。

初期値では、各インタフェースは、すべてのルーティングテーブルのメンバシップとなるように設定されています。さらに、初期値では、1つのmainルーティングテーブルが通常存在しており、追加ルーティングテーブルが定義されると、インタフェースのMembershipをそのテーブルに追加することができます。

VLANを使用した透過モード

透過モードが一つのVLAN上にあるすべてのホストとユーザに設定されていると、上で説明した通り、複数のルーティングテーブルを使用する技術を適用することができます。各VLAN用に専用のルーティングテーブルを定義し、その後、VLANインタフェースを参照するルーティングテーブルでswitchルートを定義します。これを行う理由は、ARPリクエストをVLANが定義されるインタフェースに制限するためです。
これについて、さらに詳しく説明するために、「if1」と「if2」という2つの物理インタフェースに定義されるVLAN vlan5を想定します。両方の物理インタフェースには透過モードで操作するように定義されたswitchルートがあります。同じVLAN IDを持つ2つのVLANインタフェースを2つの物理インタフェースに定義し、これらを「vlan5_if1」と「vlan5_if2」と呼びます。

VLANが透過モードで動作するためには、オーダリング設定を持つルーティングテーブルを作成します。これには以下の2つのswitchルートが含まれます。

ネットワーク	インタフェース
all-nets	vlan5_if1
all-nets	vlan5_if2

各エントリを作成する代わりに、上のルーティングテーブルでインタフェースグループを使用できます。

他のnon-switchedルートは、そのようなルートに従うトラフィックはVLAN IDで不正にタグ付けされているため、このルーティングテーブルには含めるべきではありません。

最終的に、ポリシーベースルーティングルールを定義することによって、このルーティングテーブルをVLANインタフェースに関連付けする必要があります。

透過モードをインタフェースで直接有効化する

上で説明した通り、透過モードを有効にするためにはswitchルートを追加することを推奨します。別の方法は、直接インタフェースの透過モードを有効にすることです。Webインタフェースでは、チェックボックスを使用して設定することができます。このような方法で有効化されると、デフォルトのswitchルートは、自動的にインタフェースのルーティングテーブルに追加され、すべての対応するnon-switchルートが自動的に削除されます。後述する例題で、この方式を使用しています。

高可用性と透過モード

switchルートは高可用性と共に使用できないため、正しい透過モードはNetDefendOS高可用性クラスタと共に実行できません。

高可用性の構成におけるソリューションとして、switchルートの代わりに、2つのネットワークを分離するためにプロキシARPを使用します。これは「4.2.6 プロキシARP」でより詳しく説明されています。この手法における主な短所は、第一にクライアントが同じIPアドレスを保持したままでNetDefendOSインタフェース間を移動できないということです。第二はより重要であり、プロキシARP用にネットワークルートを手動で設定する必要があるということです。

DHCP を使用した透過モード

多くの透過モードシナリオでは、クライアントの IP アドレスは、定義済みで固定となっており、DHCP による動的な取得を行いません。透過モードの主な利点は、ARP 交換により NetDefendOS がユーザの位置と IP アドレスを検出した後は、ユーザがどこでも接続でき、正しくルーティングを行えることです。

しかし、いくつかの透過モードのシナリオでは、ユーザの IP アドレスは DHCP サーバによって割り当てられるかもしれません。例えば、透過モードで動作するファイアウォールの背後に位置するクライアントにパブリック IPv4 アドレスを与える ISP の DHCP サーバであるかもしれません。この場合、NetDefendOS は、クライアントと DHCP サーバ間に DHCP トラフィックを送信するために DHCP リレイヤとして正しく設定される必要があります。

DHCP サーバの正確な IP アドレスがわからないが、DHCP サーバに接続しているイーサネットインタフェースがわかっている場合もあります。

ファイアウォールを通じた DHCP リクエストのリレーを有効にするためには、プロパティ DHCP Passthrough を、透過モードにかかわるすべてのインタフェースで有効にする必要があります。詳しくは、「3.4.11 レイヤ 2 のパススルー」を参照してください。

重要 透過モードをインタフェースで有効にする必要があります。

また、DHCP パススルーが機能するためには、ルートが自動的に追加されるように透過モードをインタフェースで有効にする必要があります。switch ルートを手動で追加すると、DHCP パススルーは機能できません。

4.9.2 インターネットアクセスを有効にする

透過モードを設定する場合に一般的に誤解されることは、インターネットへのアクセスを正しく設定する方法です。以下は、IP ネットワーク lannet の多くのユーザが、IP アドレス gw-ip を持つ ISP のゲートウェイを通じてインターネットにアクセスする典型的なシナリオです。

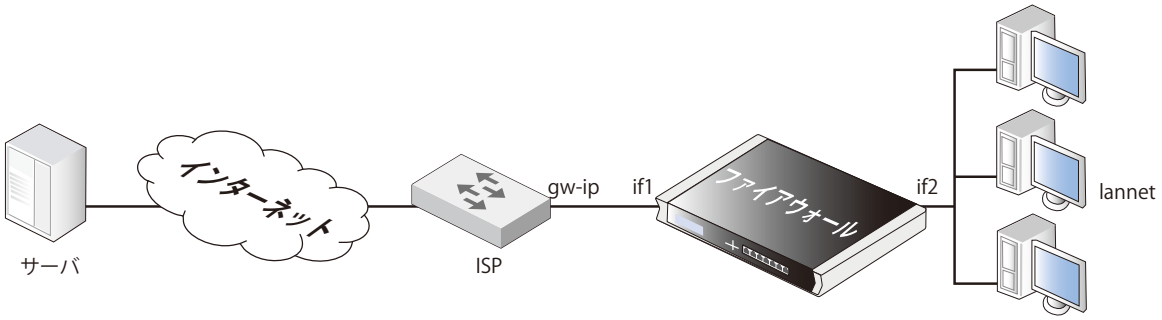


図 4-24 透過モードでないインターネットアクセス

通常、インターネットアクセスを許可するために必要な non-switch ルートは、以下の通りです。

経路タイプ	インタフェース	送信先	ゲートウェイ
Non-switch	if1	all-nets	gw-ip

D-LInk ファイアウォールは、ユーザと ISP 間の透過モードで動作すると仮定します。以下の図では、switch ルートを使用して、ファイアウォールが内部の物理イーサネットネットワーク（pn2）と ISP のゲートウェイ（pn1）へのイーサネットネットワークの間で透過になるように設定する方法を示しています。2 つのイーサネットネットワークは、一般的なアドレス範囲（この例では 192.168.10.0/24）を持つ透過モードにおける一つの論理 IP ネットワークとして扱われます。

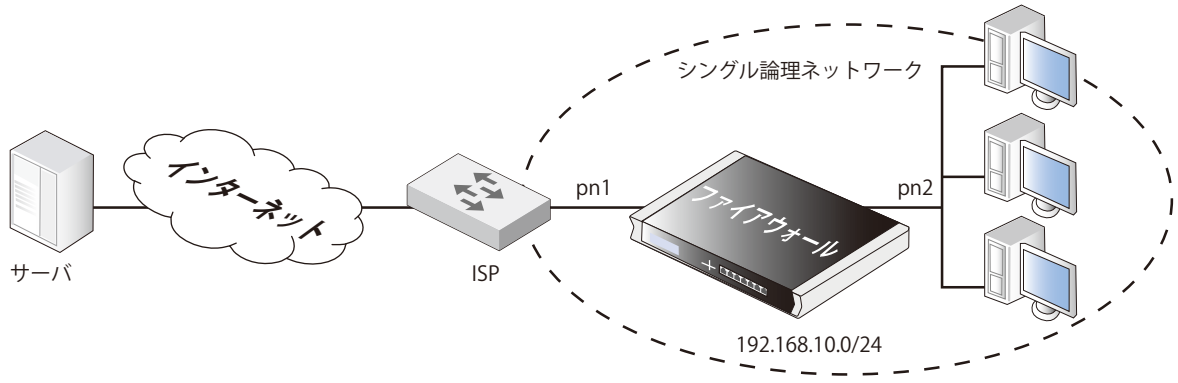


図 4-25 透過モードのインターネットアクセス

この状況では、ルーティングテーブル内のどの「正常な」non-switch「all-nets」ルートも削除され、switch ルート「all-nets」と交換する必要があります。設定中に、これを行わないのは、よくある誤りです。本 switch ルートにより、イーサネットネットワーク pn2 上のローカルユーザからのトラフィックは ISP ゲートウェイを見つけることができます。

また、これらの同じユーザは、ローカルコンピュータ上のインターネットゲートウェイが ISP ゲートウェイアドレスになるように設定します。非透過モードでは、ユーザのゲートウェイ IP はファイアウォールの IP アドレスとなりますが、透過モードでは、ISP のゲートウェイは、ユーザと同じ論理 IP ネットワークにあるため、gw-ip となります。

NetDefendOS におけるインターネットアクセスの必要性

DNS 検索、Web コンテンツフィルタリング、またはアンチウィルスと IDP 更新などの NetDefendOS 機能を実行する場合、D-Link ファイアウォールは、インターネットを検出する必要があります。これを行うためには、ルーティングテーブルに、ISP と ISP ゲートウェイの IP アドレスに接続するインタフェースを指定して、各 IP アドレスに対する個別の「通常の」non-switch ルートを設定する必要があります。

NetDefendOS により到達する必要がある IP アドレスが、85.12.184.39 と 194.142.215.15 であると、上記の例の完全なルーティングテーブルは以下の通りとなります。

経路タイプ	インタフェース	送信先	ゲートウェイ
Switch	if1	all-nets	
Switch	if2	all-nets	
Non-switch	if1	85.12.184.39	gw-ip
Non-switch	if1	194.142.215.15	gw-ip

また、D-Link ファイアウォール経由でインターネットアクセスを許可するために、適切な IP ルールを IP ルールセットに追加する必要があります。

IP アドレスのグループ化

すべてのアドレスを一つのグループ IP オブジェクトにまとめ、一つの定義ルートでそのオブジェクトを使用することが、より迅速に多くの IP アドレスに対応できます。上記の例では、85.12.184.39 と 194.142.215.15 を一つのオブジェクトにグループ化しています。

NAT の使用

以前に説明した通り、D-Link ファイアウォールがレベル 2 スイッチのように動作するため、NAT は透過モードで NetDefendOS に対して有効にされるべきではありません。アドレス変換は、より高い IP OSI レイヤで行われます。

NAT を使用しない場合はまた、通常、インターネットにアクセスするユーザの IP アドレスがパブリック IPv4 アドレスである必要があります。

NAT が、インターネットから個別アドレスを隠すために上記の例で行われる必要がある場合、192.168.10.0/24 ネットワークとインターネット間のデバイス（別の D-Link ファイアウォールの可能性もあります）で実施する必要があります。この場合、ユーザはイーサネットネットワーク pn2 で内部 IPv4 アドレス（プライベートアドレス）を使用します。

4.9.3 透過モードの利用例

以下の図に示す利用例では、インターネットアクセスルータと内部ネットワークの間に透過モードのファイアウォールを配置します。
ルータは 1 つのパブリック IPv4 アドレスを使用してインターネット接続を共用しています。ファイアウォールの背後にある内部の NAT されるネットワークは、10.0.0.0/24 のアドレス空間にあります。内部ネットワークのクライアントには、HTTP プロトコルによるインターネットアクセスを許可します。実際の設定手順は下の例題にあります。

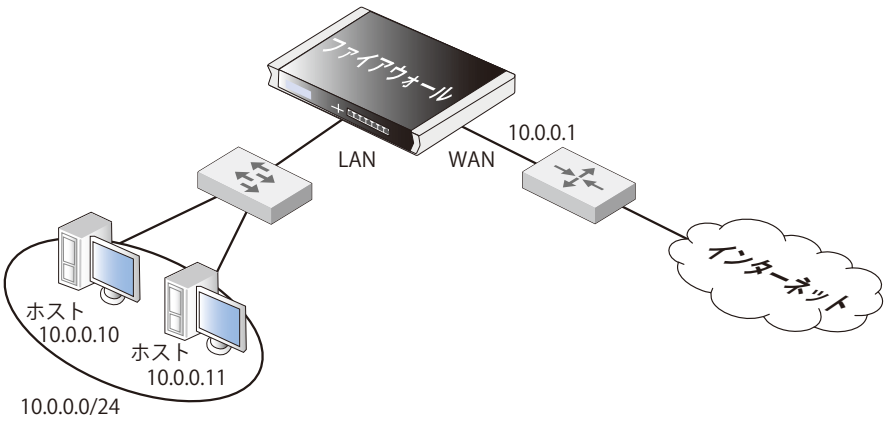


図 4-26　透過モードの利用例

例題 4.21

透過モードの利用例

CLI

wan インタフェースを設定する :

```
DFL-xxxx:/> set Interface Ethernet wan IP=10.0.0.1 Network=10.0.0.0/24 DefaultGateway=10.0.0.1
            AutoSwitchRoute=Yes
```

lan インタフェースを設定する :

```
DFL-xxxx:/> set Interface Ethernet lan IP=10.0.0.2 Network=10.0.0.0/24 AutoSwitchRoute=Yes
```

IP ルールを追加する :

```
DFL-xxxx:/> add IPRule Action=Allow Service=http SourceInterface=lan SourceNetwork=10.0.0.0/24
            DestinationInterface=any DestinationNetwork=all-nets Name=http_allow
```

Web Interface

wan インタフェースを設定する :

1. **Network > Interfaces and VPN > Ethernet** の順にメニューをクリックします。
2. wan インタフェースを選択します。
3. 以下の情報を入力します。
   - IP Address: 10.0.0.1
   - Network: 10.0.0.0/24
   - Default Gateway: 10.0.0.1
4. Enable Transparent Mode を選択します。
5. 「OK」ボタンをクリックします。

lan インタフェースを設定する :

1. **Network > Interfaces and VPN > Ethernet** の順にメニューをクリックします。
2. lan インタフェースを選択します。
3. 以下の情報を入力します。
   - IP Address: 10.0.0.2
   - Network: 10.0.0.0/24
4. Enable Transparent Mode を選択します。
5. 「OK」ボタンをクリックします。

IP ルールを設定する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: http_allow
   - Action: Allow
   - Service: http
   - Source Interface: lan
   - Destination Interface: any
   - Source Network: 10.0.0.0/24
   - Destination Network: all-nets
3. 「OK」ボタンをクリックします。

4.9.4 スパニングツリー BPDU のサポート

NetDefendOS は、D-Link ファイアウォール経由で BPDU（Bridge Protocol Data Units）をリレーします。BPDU フレームは、ネットワークにおけるレイヤ 2 スイッチ間にスパニングツリープロトコル（STP）メッセージを送信します。STP により、スイッチはパケットの交換時にネットワークトポロジを理解して、ループの出現を回避することができます。

下の図例では、管理者によりスイッチが STP プロトコルを実行できるようにする場合に BPDU メッセージが生じる状況を示しています。2 つの D-Link ファイアウォールがネットワークの両側に透過モードで配置されます。ファイアウォールのいずれか一方にあるスイッチが通信を行い、ファイアウォール間ではパケットがループしないようにスイッチ BPDU メッセージをリレーすることを NetDefendOS に要求することが必要となります。

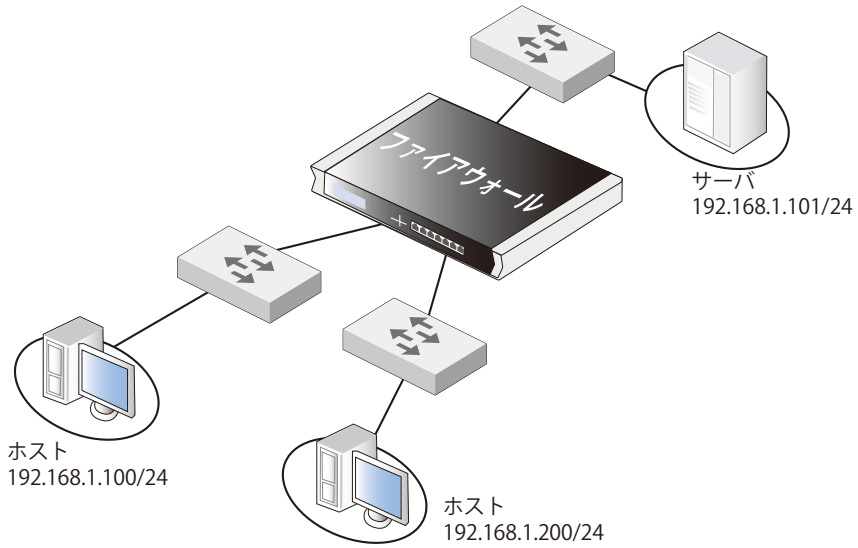


図 4-27　BPDU リレーシナリオの例

BPDU リレーの実行

NetDefendOS BPDU リレーの実行だけが、STP メッセージを送信します。以下の STP メッセージがあります。

- 通常のスパニングツリープロトコル（STP）
- Rapid Spanning Tree Protocol（RSTP）
- Multiple Spanning Tree Protocol（MSTP）
- シスコ社の PVST+ プロトコル（Per VLAN Spanning Tree Plus）

NetDefendOS は、BDPU メッセージの内容をチェックし、コンテンツタイプがサポートされていることを確認します。コンテンツがサポートされていない場合は、廃棄されます。

BPDU リレーの有効化 / 無効化

BPDU リレーは初期値では無効です。アドバンスド設定の「Relay Spanning-tree BPDUs」を通じて制御することができます。さらに、この設定を通じて BPDU メッセージのログへの出力も制御できます。有効にすると、すべての到来する STP、RSTP、および MSTP BPDU メッセージは、入力インタフェースを除き、同じルーティングテーブルにあるすべての透過インタフェースにリレーされます。

4.9.5 MPLS パススルー

Multi-protocol Label Switching（MPLS）は、パケットの最後の宛先に関する情報を提供するために、IP パケットにラベルを付加することを許可する標準規格です。初めに MPLS ラベルを付加されたルータは、イングレスルータとして知られています。

MPLS をサポートするネットワークノードは、パケットを送信するためにこの付加情報を使用できます。経路検索を実行する必要はないため、その結果処理速度は向上します。また、全体的に速いトラフィックの移動に加えて、MPLS は Quality of Service (QoS) の管理をより簡単にします。

MPLS は Internet Protocol、Asynchronous Transport Mode (ATM)、およびフレームリレーネットワークで正常に動作するため、「マルチプロトコル」であると見なされます。OSI ネットワークモデルと関連を考慮する場合、MPLS は、パケットがレイヤ 3 レベルではなくレイヤ 2 レベルで送信されるのを許可します。そのため、2.5 レベルで動作すると言われています。

NetDefendOS MPLS サポート

NetDefendOS は MPLS パススルーをサポートしています。これは、MPLS のラベルが付加されたパケットが、ファイアウォールを横断できる透過モードのシナリオに適しています。NetDefendOS はこれらの MPLS パケットの保全性をオプションで有効にすることができます。また、管理者は、実行するべき特定のアクションを指定するために高度な設定の Relay MPLS を変更することができます。この設定で可能な値は以下の通りです。

項目	説明
Ignore	パケットを検証し、検証済みの MPLS ラベルが付加されたすべてのパケットの通過を許可します。検証に失敗するパケットはログに出力されます。
Log	パケットを検証し、検証済みのすべての MPLS パケットの通過を許可すると共にログにも出力します。検証に失敗するパケットもログに出力されます。
Drop	検証やログ出力なしで MPLS パケットを破棄します。
Drop/Log	検証なしですべての MPLS パケットを破棄し、これらの破棄をログに出力します。

4.9.6 透過モードのアドバンスド設定

項目	説明
CAM To L3 Cache Dest Learning	有効にすると、宛先アドレス情報と CAM テーブルで見つかった情報を組み合わせて、ホストの宛先を学習します。 初期値 : Enabled（有効）
Decrement TTL	有効にすると、パケットが透過モードのファイアウォールを通過するたびに TTL は減少します。 初期値 : Disabled（無効）
Dynamic CAM Size	本設定は、手動で CAM テーブルのサイズを設定する場合に使用します。通常、「Dynamic」が適しています。 初期値 : dynamic
CAM Size	「Dynamic CAM Size」が無効の場合の各 CAM テーブルにおけるエントリの最大数です。初期値 : 8192
Dynamic L3C Size	L3 Cache Size 値ダイナミックに割り当てます。初期値 : Enabled（有効）
L3 Cache Size	手動で Layer 3 Cache のサイズを設定するために使用されます。通常、「Dynamic L3C Size」を有効にすることが適しています。初期値 : Dynamic
Relay Spanning-tree BPDUs	「Ignore」に設定すると、すべての到来する STP、RSTP、および MSTP BPDU は入力インタフェースを除き、同じルーティングテーブルの透過インタフェースすべてにリレーされます。 • Ignore - パケットを通過させますが、ログへの出力は行いません。 • Log - パケットを通過させ、イベントをログに出力します。 • Drop - パケットを破棄します。（初期値） • DropLog - パケットを破棄し、イベントをログに出力します。
Relay MPLS	「Ignore」に設定すると、すべての入力 MPLS パケットは、透過モードでリレーされます。 • Ignore - パケットを通過させますが、ログへの出力は行いません。 • Log - パケットを通過させ、イベントをログに出力します。 • Drop - パケットを破棄します。（初期値） • DropLog - パケットを破棄し、イベントをログに出力します。

第 5 章 DHCP サービス

この章では、NetDefendOS 内の DHCP サービスについて記述します。

- 「5.1 概要」
- 「5.2 IPv4 DHCP クライアント」
- 「5.3 IPv4 DHCP サーバ」
- 「5.4 IPv4 DHCP リレー」
- 「5.5 IP プール」
- 「5.6 DHCPv6」

5.1 概要

DHCP（Dynamic Host Configuration Protocol）は、ネットワーク管理者がネットワーク上のコンピュータに IP 番号を自動的に割り当てることを許可するプロトコルです。IPv4 と IPv6 アドレスの両方で本機能を実行できます。

IP アドレスの割り当て

DHCP サーバは DHCP クライアントに IP アドレスを割り当てるタスクを実行します。これらのアドレスは、DHCP が管理する事前定義された IP アドレスプールから割り当てられます。DHCP サーバは DHCP クライアントからのリクエストを受け取ると、IP アドレス、MAC アドレス、ドメイン名、IP アドレスのリース期間などの設定パラメータをユニキャストメッセージでクライアントに返します。

DHCP リース

スタティックな割り当てはクライアントが自身のアドレスを保持するのに対し、ダイナミックな割り当ては事前に定義した一定の期間 DHCP サーバからそれぞれのクライアントに対してリースされます。リース期間、クライアントは割り当てられたアドレスを使い続けることができ、他のクライアントとのアドレス衝突がないことが保証されます。

リース期限

リース期間が終了する前に、クライアントはサーバからリースの更新を受け、その IP アドレスを使い続けることができます。クライアントは割り当てられた IP アドレスを使う必要がなくなったと判断すると、いつでも IP アドレスを解放してリースを終了することができます。

リース期間は管理者が DHCP サーバに設定することができます。

5.2 IPv4 DHCP クライアント

D-LInk ファイアウォールでは、イーサネットインタフェースや VLAN インタフェースは IPv4 DHCP クライアントとして動作することが可能であり、そのインタフェースの IPv4 アドレスやネットワークは外部 DHCP サーバから割り当てられます。NetDefendOS コンフィグレーションのインタフェースオブジェクトの Enable DHCP Client プロパティを変更することで、本機能を有効または無効にすることができます。
初期設定は以下の通りです。

- **Ethernet interfaces** - イーサネットインタフェースのための初期設定はハードウェアプラットフォームに依存します。NetDefendOS 製品シリーズについては、関連するハードウェアガイドを参照してください。
- **VLAN interfaces** - DHCP は VLAN インタフェースに対して初期値では常に無効です。

重要 IPv4 DHCP クライアントは HA クラスタではサポートされません。

IPv4 DHCP クライアントは NetDefendOS HA クラスタのインタフェースではサポートされません。クライアントがクラスタで有効であると、コンフィグレーションのコミットを行う時に Shared HA IP アドレスが設定されないというエラーが発生します。

DHCP がインタフェースで有効になると、変更された NetDefendOS コンフィグレーションが直ちに配布されて、以下の処理が発生します。

- DHCP リース要求は DHCP が有効であるインタフェースで送信されます。
- リスニング DHCP サーバはインタフェースにリースを発行します。
- NetDefendOS は、リースに基づく値になるようにインタフェースの IPv4 アドレスとネットワークを変更します。
- インタフェースに関連している NetDefendOS アドレス帳オブジェクトは、それらの元の値を失って、IPv4 アドレス用に 0.0.0.0 と IPv4 ネットワーク用に 0.0.0.0/0 を取得します。インタフェースコンフィグレーションオブジェクトのプロパティを調べる時に DHCP により割り当てられた値を参照しますが、アドレス帳オブジェクトにはそれらの値を表示しません。

また、NetDefendOS が再起動すると、同様のリース要求処理が発生します。DHCP がインタフェースで無効にされると、管理者は、手動で IPv4 アドレスとネットワークを割り当てる必要があります。

注意 IP アドレスアイコンは Web インタフェース上で変わります。

IP アドレスがインタフェースに割り当てられると、IPv4 アドレスとネットワークのアイコンは、Web インタフェースのインタフェースプロパティの表示上で左隅に「*」（アスタリスク）を持つように変わります。

以下の例はオプションがイーサネットインタフェースで有効になる方法を示しています。手順は VLAN インタフェース用とほぼ同じです。

例題 5.1

イーサネットインタフェースを DHCP クライアントとして有効にする

この例は、DHCP クライアントとしてイーサネットインタフェース If1 を有効にする方法を示しています。

CLI

```
DFL-xxxx:/> set Interface Ethernet If1 DHCPEnabled=Yes
```

Web Interface

1. **Network > Ethernet > If1** の順にメニューをクリックします。
2. Enable DHCP Client を有効にします。
3. 「OK」ボタンをクリックします。

5.3 IPv4 DHCP サーバ

NetDefendOS DHCP サーバオブジェクトは、指定のアドレスプールから取得した IP アドレスの割り当てと管理を行います。NetDefendOS DHCP サーバは、1 つの範囲の IP アドレスを配布するだけでなく、NetDefendOS IP アドレスオブジェクトが指定できる IP アドレス範囲であればどれでも使用することができます。

DHCPServer オブジェクトは IPv4 アドレスに、DHCPv6Server オブジェクトは IPv6 オブジェクトに使用されます。基本的なインプリメンテーションは非常に異なりますが、2 つはとてもよく似た方法で設定されます。また、IPv6 サーバは IPv4 に存在しないいくつかのオプションを提供します。現在、IPv6 DHCP を使用した DHCP リレーと IP プールを使用することはできません。

複数の DHCP サーバ

管理者は、NetDefendOS 内に複数の論理 DHCP サーバを設定することができます。各 DHCP サーバに対する DHCP クライアント要求のフィルタリングは、以下の DHCP サーバプロパティの組み合わせに基づきます。

- インタフェース
  NetDefendOS の各インタフェースには、1 台までの論理 DHCP サーバを紐づけることができます。つまり、NetDefendOS は、インタフェースごとに DHCP クライアントに異なるアドレス範囲の使用を提供することができます。

- リレーフィルタ
  また、Relay Filter プロパティの値は、使用する DHCP Server オブジェクトを決定するのに使用されます。「all-nets」が初期値の場合、すべてのアドレスは受容され、DHCP サーバ選択を行う際に考慮されるのはインタフェースのみです。このパラメータの他のオプションについては、後で説明します。

サーバリストの検索

複数の DHCP サーバが登録された場合、最後に定義されたものがリストの先頭になります。NetDefendOS が要求を処理する DHCP サーバを検索する時、リストの先頭から検索して、インタフェースとリレイヤ IP によるフィルタリング値の組み合わせに最初に適合したサーバを選択します。リストに適合するサーバがない場合は、その要求は無視されます。

リスト内の DHCP サーバの順番は、ユーザインタフェースの 1 つを通じて変更することができます。

リレーフィルタプロパティの設定

上で説明されるように、クライアントに使用される DHCP Server オブジェクトは、Interface Filter と Relay Filter プロパティの両方のマッチに基づいて選択されます。DHCP Server サーバでは、必ず Relay Filter 値を指定してください。
値は以下のようになります。

項目	説明
0.0.0.0/0	初期値は 0.0.0.0/0（all-nets）です。DHCP 要求がローカルネットワーク上のクライアントから送信されるか、または DHCP リレイヤ経由で受信したかなどに関係なく、すべての DHCP 要求がフィルタリング値に適合します。
0.0.0.0	「0.0.0.0」の値は、ローカルクライアントから到来する DHCP リクエストに一致します。DHCP リレイヤによってリレーされた DHCP 要求は無視します。
指定の IP アドレス	DHCP 要求が経由する DHCP リレイヤの IP アドレスです。ローカルネットワークのクライアントや他の DHCP リレイヤからの要求は無視します。

IPv4 DHCP オプション

以下のオプションが DHCP サーバに設定できます。

General

オプション	説明
Name	サーバ名を指定します。インタフェースの参照として使用されますが、また、ログメッセージにおける参照としても使用されます。
Interface Filter	NetDefendOS が DHCP リクエストをリッスンするソースインタフェース。これは、単一のインタフェースまたはインタフェースのグループとして指定することができます。
Relay Filter	リレーアドレスのためのフィルタ。設定可能な値とその意味は、このセクションより前に記載されています。
IP Address Pool	DHCP サーバが DHCP リースを付与するために IP アドレス範囲として使用する IP アドレス、グループまたはネットワークです。
Netmask	DHCP クライアントに送信されるネットマスク。

Options

オプション	説明
Default GW	デフォルトゲートウェイとしての使用のためにクライアントに送信される IP を指定します。（クライアントが接続するルータ）
Domain	ユーザが位置しているドメイン。ユーザが有効な URL の代わりにブラウザに簡単な文字列を入力するとき、URL を形成するためにブラウザがドメインプロパティの値を追加することができます。例えば、Domain の値が "example.com" であれば、ユーザが "wiki." という言葉をタイプすると、ブラウザは "wiki.example.com" という URL を試みることができます。
Lease Time	DHCP リースが提供される時間（秒）。この期間が経過すると、DHCP クライアントはリースを更新する必要があります。
Primary/Secondary DNS	プライマリおよびセカンダリの DNS サーバの IP。
Primary/Secondary NBNS/WINS	IP アドレスを NetBIOS 名に割り当てるために NetBIOS Name Server（NBNS）を使用したマイクロソフト環境で使用される Windows Internet Name Service（WINS）サーバの IP。
Next Server	ブートプロセスにおけるネクストサーバの IP アドレスを指定します。通常、これは TFTP サーバです。
Leases Require Authentication	RADIUS 認証クライアントのみにリースを行います。例：認証システムに MAC アドレスで登録されたクライアントのみ等

Advanced Settings（DHCP サーバの高度な設定）

すべての DHCP サーバに適用される 2 個の高度な設定があります。

項目	説明
Auto Save Policy	リースデータベースをディスクに保存するためのポリシー。 オプションは以下の通りです。 • Disabled - データベースを保存しません。 • ReconfShut - 再構成またはシャットダウン時にデータベースを保存します。 • ReconfShutTimer - 再構成またはシャットダウン時、そして定期的にデータベースを保存します。定期保存の時間は次のパラメータ「Lease Store Interval」によって指定されます。
Lease Store Interval	リースデータベースをディスクに自動保存する間隔（秒）。初期値は 86400（秒）です。

例題 5.2

IPv4 DHCP サーバを設定する

この例題は、DHCPRange1 という IPv4 アドレスプールから IP アドレスを割り当てて管理する、DHCPServer1 という DHCP サーバのセットアップの方法を示します。ここでは、ご使用の DHCP サーバの IP 範囲を既に作成しているものと想定します。

CLI

```
DFL-xxxx:/> add DHCPServer DHCPServer1 Interface=lan IPAddressPool=InterfaceAddresses/DHCPRange1
            Netmask=255.255.255.0
```

Web Interface

1. **Network > Network Services > DHCP Servers > Add > DHCP Server** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : DHCP サーバ名を指定します。（例 : DHCPServer1）
- Interface Filter : lan
- IP Address Pool : DHCPRange
- Netmask : 255.255.255.0

IP の MAC アドレスマッピングの表示

DHCP リース割り当て後に IP アドレスの MAC アドレスへのマッピングを表示するためには、「dhcpserver」コマンドを使用します。以下のように出力されます。

```
DFL-xxxx:/> dhcpserver -show -mappings
DHCP server mappings:
Client IP       MAC/Identifier        Mode
--------------- ---------------- -------------
10.4.13.240 <00-1e-0b-a0-c6-5f>   ACTIVE(STATIC)
10.4.13.241 <00-0c-29-04-f8-3c>   ACTIVE(STATIC)
10.4.13.242 <00-1e-0b-aa-ae-11>   ACTIVE(STATIC)
10.4.13.243 <00-1c-c4-36-6c-c4>   INACTIVE(STATIC)
10.4.13.244 <00-00-00-00-02-14>   INACTIVE(STATIC)
10.4.13.254 <00-00-00-00-02-54>   INACTIVE(STATIC)
10.4.13.1   <00-12-79-3b-dd-45>   ACTIVE
10.4.13.2   <00-12-79-c4-06-e7>   ACTIVE
10.4.13.3   [00-a0-f8-23-45-a3]   ACTIVE
10.4.13.4   [00-0e-7f-4b-e2-29]   ACTIVE
```

[] で囲まれている MAC アドレスは、MAC アドレスを使用する代わりに、クライアントがサーバに提供したクライアント識別子によって、DHCP サーバがクライアントをトラッキングしたことを示します。<> で囲まれている MAC アドレスは、アドレスを使用してトラッキングが行われたことを示しています。

すべての DHCP 情報を表示するには、オプションなしで「dhcpserver」コマンドを使用します。それぞれ個別に設定している DHCP サーバは独自の番号が付与されているルールとして参照されます。この番号は、CLI 出力時に、どのリースがどのサーバに所属するかを特定するのに使用されます。定義した DHCP サーバを参照するためには、以下のコマンドを使用します。

```
DFL-xxxx:/> dhcpserver -show -rules
```

参照 リースデータベースは不揮発性メモリに保存されます。

DHCP リースのデータベースは定期的に不揮発性メモリに保存されるため、多くのリースは NetDefendOS の再起動後にも記憶された状態となります。DHCP の「Advanced Settings」の設定により、データベースが保存される間隔を制御するように管理者によって調整されます。

DHCP サーバブラックリスト

リースで提供された IP アドレスがクライアントに拒否される場合があります。これは、ARP リクエストを発行することで、既に使用中である IP アドレスをクライアントが検出するためです。クライアントにより IP アドレスが拒否された場合、NetDefendOS DHCP サーバは、自身のブラックリストにその IP アドレスを追加します。

コマンドで DHCP サーバブラックリストをクリアするには、以下のコマンドを使用します。

```
DFL-xxxx:/> dhcpserver -release=blacklist
```

追加サーバ設定

NetDefendOS DHCP サーバには、設定可能な別の 2 つのオブジェクトセットがあります。

- スタティックなホスト。
- カスタムオプション。

以下の図はこれらのオブジェクト間の関係を示しています。

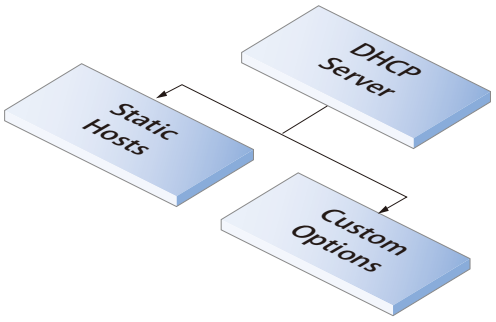


図 5-1 DHCP サーバオブジェクト

以下のセクションではこれらの 2 つの DHCP サーバオプションについて説明します。

5.3.1 Static IPv4 DHCP Host（スタティック IPv4 DHCP ホスト）

管理者が、クライアントとその割り当て IP アドレスの対応関係の対応関係を固定させたい場合、NetDefendOS は特定の MAC アドレスに特定の IP の割り当てを行うことができます。つまり、スタティックなホストの新規作成です。

スタティックホストエントリのパラメータ

1 つの DHCP サーバに上記のような割り当てを多く作成することができます。各オブジェクトには以下の項目があります。

項目	説明
Host	クライアントに割り当てられる IP アドレスです。
MAC Address	クライアントの MAC アドレスです。「MAC Address」または「Client Identifier」項目のいずれかが使用されます。
Client Identifier	「MAC Address」がクライアントを識別するのに使用されない場合、クライアントは DHCP リクエスト内に識別子を送信することができます。この識別子の値を、このパラメータとして指定できます。オプションによって、識別子が ASCII または 16 進数値として送信されるかどうか指定することもできます。

例題 5.3

スタティック IPv4 DHCP ホストの割り当て

この例題では、IPv4 アドレス 192.168.1.1 を MAC アドレス 00-90-12-13-14-15 に割り当てる方法を示しています。ここでは、DHCP サーバ、DHCPServer1 が既に定義されているものとします。

CLI

1. まず、カテゴリを DHCPServer1 というコンテキストに変更します。

```
DFL-xxxx:/> cc DHCPServer DHCPServer1
```

2. スタティック DHCP アサインメントを追加します。

```
DFL-xxxx:/DHCPServer1> add DHCPServerPoolStaticHost Host=192.168.1.1 MACAddress=00-90-12-13-14-15
```

3. すべてのスタティック割り当てはインデックス番号を付けられてリストアップされます。

```
DFL-xxxx:/DHCPServer1> show

   #  Host         MAC address        Comments
   -  -----------  -----------------  --------
+  1  192.168.1.1  00-90-12-13-14-15  <empty>
```

4. 個々のスタティックな割り当てはインデックス番号を用いて表示することができます。

```
DFL-xxxx:/DHCPServer1> show DHCPServerPoolStaticHost 1

Property     Value
-----------  -----------------
     Index:  1
      Host:  192.168.1.1
MACAddress:  00-90-12-13-14-15
  Comments:  <empty>
```

5. 以下のコマンドにより、割り当てを IP アドレス 192.168.1.12 に変更できます。

```
DFL-xxxx:/DHCPServer1> set DHCPServerPoolStaticHost 1 Host=192.168.1.12 MACAddress=00-90-12-13-14-15
```

Web Interface

1. **Network > DHCP Services > DHCP Servers > DHCPServer1** の順にメニューをクリックします。

2. Static Hosts を選択します。

3. **Add > Static Host Entry** を選択します。

4. 以下の情報を入力します。
- Host: 19.168.1.1
- MAC: 00-90-12-13-14-15

5. 「OK」ボタンをクリックします。

5.3.2 Custom IPv4 Options（カスタム IPv4 オプション）

DHCP サーバ定義にカスタムオプションを追加すると、管理者は送出された DHCP リース中の DHCP クライアントに情報の一部を送信することができます。

例えば、特定の追加情報を取得できる TFTP サーバの IP アドレスを必要とするスイッチです。

Custom Option

以下の項目がカスタムオプションに使用できます。

項目	説明
Code	クライアントに送信される情報の種類を説明するコードです。多くの使用可能なコードリストがあります。
Type	送信されるデータのタイプについて説明しています。例えば、タイプが「STRING」であれば、データは文字列です。
Parameter	リース中に送信される実際の情報です。これは、1 つの値または「,」（カンマ）で区切ったリストとすることができます。 データの意味は「Code」または「Type」によって決定されます。例えば、「Code」が 66（TFTP サーバ名）であれば、「Type」は String であるかもしれません。また、「Data」は、tftp.example.com のようなサイト名である可能性があります。

単一の DHCP サーバに関連付けされる多くのカスタムオプションがあり、これらは「RFC 2132 - DHCP Options and BOOTP Vendor Extensions」で説明されています。

「Code」は RFC 2132 に示された値に従って入力します。NetDefendOS では、「Code」に紐づくデータは「Type」「Parameter」として指定されています。

5.4 IPv4 DHCP リレー

注意 DHCP リレーは、現在 IPv4 DHCP でのみ利用できる機能です。

DHCP 問題

DHCP では、クライアントはブロードキャストメッセージを使用して DHCP サーバの場所を検出するリクエストを行います。しかし、通常ブロードキャストはローカルネットワーク内だけに到達します。これは、DHCP サーバとクライアントは、常に同じ物理ネットワーク内にいる必要があるということです。これでは、巨大なインターネット環境においては、すべてのネットワークごとに異なるサーバをおくことになります。この問題を解決するために「DHCP リレイヤ」を使います。

DHCP リレイヤソリューション

DHCP リレイヤは、リモート DHCP サーバとクライアントの間の中継点として、ローカルネットワークにある DHCP サーバの代わりになります。DHCP リレイヤは、クライアントからの要求を受け取り、DHCP サーバに転送します。サーバはレスポンスをリレイヤに返し、リレイヤはレスポンスをクライアントに転送します。DHCP リレイヤは、BOOTP パケットをリレーすることも可能であり、しばしば BOOTP リレーエージェントとも呼ばれます。

DHCP リレーオブジェクト

DHCP リレーは、DHCP リレーオブジェクトを作成することにより、NetDefendOS で設定されます。
このオブジェクトには以下のプロパティがあります。

項目	説明
Name	オブジェクトのコンフィグレーション名。
Action	以下のいずれかの設定となります。 1. Ignore - DHCP リクエストは無視されます。これは初期値となります。 2. Relay- DHCP（および BOOTP）パケットは定義済みの DHCP サーバへリレーされ、応答もリレーされて返されます。 3. BOOTPFoward - BOOTP（Bootstrap プロトコル）パケットのみリレーされます。
Source Interface	リクエストのためにリレイヤがリッスンするインタフェース。複数のインタフェースが含まれる Interface Group オブジェクトに設定することも可能です。リレーを行うにはこのオプションを指定する必要があります。
DHCP Server to relay to	クライアント要求がリレーされる DHCP サーバの IPv4 アドレス。リレーを行うにはこのオプションを指定する必要があります。
Additional DHCP Servers	オプションとして、複数の DHCP サーバにリレーするように設定することが可能です。最初の 1 台に加えて、追加の 2 台の DHCP サーバの IP アドレスを指定することができます。 リレーが実行されると、NetDefenOS によってクライアントからの同じ要求が同時にすべての定義済みサーバにリレーされます。すべての応答がクライアントにリレー経由で返され、クライアントによって応答への処理が決定されます。
Allowed IP offers from server	リレーされるリースに含まれる IP アドレスの許可範囲（オプション）。これはネットワーク（例：203.0.113.0/24）やアドレス範囲（例：203.0.113.0-203.0.113.100）として指定することができます。初期値では、すべての IPv4 アドレスが許可されています。

DHCP Relayer オブジェクトにおける他の追加のプロパティは次のセクションで説明します。

リレーされた DHCP トラフィックの送信元 IP

オプションとして、サーバへリレーされた DHCP トラフィックの送信元 IPv4 アドレスとして次のいずれかを使用できます。

- クライアント要求をリッスンするインタフェースの IPv4 アドレス。これは初期値であり、DHCP サーバがリクエストの送信元ネットワークを識別できるようにするものです。DHCP サーバが、リクエストの送信元 IP に基づいて IP アドレスを割り当てるように設定されている場合、この設定が重要になるかもしれません。
- リレーされるリクエストをサーバに送信するインタフェースの IPv4 アドレス。リレイヤに対するリッスン用のインタフェース IP が関連していない、または VLAN 使用時に利用不可な場合に使用されます。

Web インタフェース上の DHCP Relayer オブジェクトの Options タブで設定することができます。

Core ルーティングは適用されない

NetDefenOS のインタフェース IP は、通常 core にルーティングされますが、リレーされた DHCP リクエストに対しては、この core ルーティングは適用されません。「core」の代わりに、インタフェースは送信元インタフェースとなります。

リレーされる DHCP リースにダイナミックルートを追加する

「Add dynamic routes for this relayed DHCP lease」プロパティ（Web インタフェースの Add Route タブ）は初期値で無効化されています。したがって、DHCP サーバによって割り当てられた IP アドレスのためにルートは追加されません。正しいインタフェース上でルーティングを行うスタティックルートが既にセットアップされている場合、DHCP サーバによってアドレス範囲がクライアントに配布されます。

しかしながら、複数のネットワークに配置されたクライアントが 1 台のリレイヤを介して DHCP リクエストを送信する場合、1 つのスタティックルートを設定することがルーティングのソリューションとして適切ではない場合もあります。このような場合、アドレスが割り当てられた各クライアントに対して自動的にルートを追加する設定を有効にする方が簡単です。多くのクライアントが存在する場合、たくさんのルートが追加され、NetDefenOS システムの多大なオーバーヘッドが発生してしまう可能性があることに注意してください。

ダイナミックルートのパラメータを設定する

「Add dynamic routes for this relayed DHCP lease」プロパティが有効化されている場合、追加されるルートに対して以下の設定を行うことも可能です。

- Routing Table - ルートが追加されるルーティングテーブル（初期値は main）を指定します。
- Local IP - 指定したアドレスに送信された ARP クエリに対し、NetDefendOS が応答します。詳細は「4.2 スタティックルーティング」を参照してください。
- Gateway IP - リレーされるクライアントがルーティングデバイスの後方に配置されている場合に使用されます。

インタフェース 1 つあたりのリレークライアントの最大数を設定する

オプションの「Max relays per interface」設定では、1 つのインタフェース上で DHCP リクエストの送信が許可される最大クライアント数を指定することができます。

プロキシ ARP を有効にする

いくつかのシナリオでは、上で説明したプロパティを使用して各 DHCP リースにルートを追加することが必要です。以下に示すレイアウトを考えてみます。ここでは、1 つの DHCP サーバが NetDefendOS のリレー経由で個別のインタフェース If1 と If2 にある 2 つのクライアントに同じネットワーク範囲の IP を付与しています。

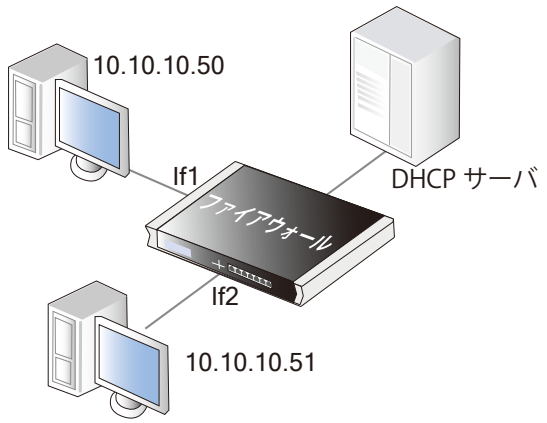


図 5-2 プロキシ ARP を使用した DHCP リレー

この場合、各リースに自動的にルートを追加する必要があります。さらに、2 つのクライアントは、同じネットワーク範囲から IP アドレスを取得しており、同じネットワークに存在するものと見なすことができます。しかし、相互に通信を行うためには、各クライアントが DHCP サーバによって付与された IP アドレスを見つけることができるように、DHCP Relay リレーオブジェクトの Proxy ARP Interfaces プロパティをインタフェース If1 と If2 に設定する必要があります。

PXE サポートと NULL Offer

Preboot Execution Environment (PXE) では DHCP を使用して、ネットワーク経由でサーバからのクライアントの起動を有効にします。PXE では、IP アドレス 0.0.0.0（アドレスオファーなし）を提供する DHCP サーバの応答「NULL Offer」を使用します。

初期値では、NetDefenOS は NULL Offer をリレーしません。リレーを有効にするには、以下の設定を行う必要があります。

- DHCP Relay オブジェクトを作成し、Action を Relay に設定します。これにより多くのオプションを設定することができます。
- Allow NULL offers オプションを有効にします。

例題 5.4

DHCP リレーを設定する

この例題では、VLAN インタフェース上のクライアントが DHCP サーバから IP アドレスを取得することができます。ファイアウォールには VLAN インタフェース「vlan1」「vlan2」が定義済みであり、それらのインタフェース上のクライアントが DHCP リクエストを生成し、DHCP サーバに送信されるものとします。DHCP サーバの IP アドレスはアドレスオブジェクト「ip-dhcp」として NetDefenOS のアドレス帳に定義済みとします。また、NetDefenOS は、DHCP リレープロセスによってクライアントに割り当てられた IP アドレスに対して、自動的にルートを追加します。

CLI

「ipgrp-dhcp」という名前の新しいインタフェースグループに、VLAN インタフェース「vlan1「vlan2」を追加します。

```
DFL-xxxx:/> add Interface InterfaceGroup ipgrp-dhcp Members=vlan1,vlan2
```

「vlan-to-dhcpserver」という名前で DHCP リレーを追加します。

```
DFL-xxxx:/> add DHCPRelay vlan-to-dhcpserver Action=Relay TargetDHCPServer=ip-dhcp SourceInterface=ipgrp-dhcp
            AddRoute=Yes
```

Web Interface

「ipgrp-dhcp」という名前の新しいインタフェースグループに、VLAN インタフェース「vlan1「vlan2」を追加します。

1. **Network > Interfaces and VPN > Interface Groups > Add > Interface Group** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : ipgrp-dhcp

Interfaces

- 「Available」リストから「vlan1」と「vlan2」を選択し、「Selected」リストに移動します。

「vlan-to-dhcpserver」という名前で DHCP リレーを追加します。

1. **Network > Network Services > DHCP Relays > Add > DHCP Relay** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ General タブ

General

- Name : vlan-to-dhcpserver
- Action : Relay
- Source Interface : ipgrp-dhcp
- DHCP Server to relay to : ip-dhcp
- Allowed IP offers from server : all-nets

◇ Add Route タブ

General

- Add dynamic routes for this relayed DHCP lease. : チェックして有効にします。

DHCP リレーアドバンス設定

DHCP リレーには以下のアドバンス設定が可能です。

項目	説明
Max Transactions	同時に可能なトランザクションの最大数。 初期値 : 32
Transaction Timeout	DHCP のトランザクションに許可される時間。 初期値 : 10（秒）
Max PPM	NetDefendOS を経由してクライアントが 1 分間に DHCP サーバに DHCP パケットを送信できる最大数。 初期値 : 500 パケット
Max Hops	クライアントと DHCP サーバ間で取得できる DHCP リクエストのホップ数。 初期値 : 5

項目	説明
Max lease Time	NetDefendOS によって許可される最大リース時間。DHCP サーバのリース時間がこれより長い場合、本設定値まで下げられます。初期値 : 10000（秒）
Max Concurrent Relays	同時に、アクティブにできるリレー数。 初期値 : 256
Auto Save Policy	リレーリストをディスクに保存するために使用されるポリシー（Disabled、ReconfShut、または ReconfShutTimer）を指定します。 初期値 : ReconfShut
Auto Save Interval	「DHCPServer_SaveRelayPolicy」が ReconfShutTimer に設定された場合、リレーリストがディスクに保存されるべき間隔を指定します。 初期値 : 86400

5.5 IP プール

注意 IP プールは IPv4 DHCP のみで使用可能です。

概要

IP プールは、他のサブシステムを DHCP IP アドレスのキャッシュにアクセスさせるように機能します。これらのアドレスは、一連の DHCP クライアント（1IP あたり 1 つ）を内部で管理することで、1 箇所にプールされます。1 つのプールが使用する DHCP サーバには、NetDefendOS 内で定義される DHCP サーバや外部サーバが考えられます。複数の IP プールは、異なる識別名で設定します。

2 つの方法のいずれかで外部 DHCP サーバを指定できます。

- 特定インタフェース上の単一の DHCP サーバとして指定できます。
- 固有の IP アドレスのリストによって 1 つ以上の DHCP サーバを指定できます。

コンフィグモードを使用した IP プール

IP プールの一般的な利用例は、IPsec トンネル経由で接続しているリモートクライアントに IP アドレスを割り当てる機能を持つ IKE コンフィグモードと共に使用することです。これに関する詳しい情報は、「10.3.11 コンフィグモード」を参照してください。

General（IP プールの基本オプション）

IP プールで可能な基本オプションは以下の通りです。

項目	説明
DHCP Server Behind Interface	IP プールは必ず指定されたインタフェース上に置かれた DHCP サーバを使用します。
Specify DHCP Server Address	DHCP サーバの IP を推奨の昇順リストで指定して使用します。behind interface オプションを指定しない場合はこちらが使用されます。IP ループバックアドレス 127,0.0.1 は、DHCP サーバが NetDefendOS 自身であることを示しています。
Server Filter	使用するサーバを指定するオプションです。指定しない場合、インタフェース上のすべての DHCP サーバが使用されます。提供されるアドレスやアドレス範囲（複数の場合）のリストは推奨サーバを示すのに使われます。
Client IP Filter	提供された IP のどれが使用可能かを指定するオプションです。多くの場合、これは、すべてのアドレスがアクセス可能な初期値の「all-net」に設定されます。そうでない場合、一連のアクセス可能な IP 範囲を指定することができます。このフィルタは、到達不可の IP アドレスを返答する DHCP サーバがあるかもしれない状況に備えて使用されます。

Advanced（IP プールの高度なオプション）

IP プール設定での高度なオプションは以下の通りです。

項目	説明
Routing Table	ポリシールーティングテーブルは、DHCP サーバ設定の送信先インタフェースを解決する時のルックアップ用に使用されます。
Receive Interface	疑似的な仮想 DHCP サーバの受信インタフェース。この設定は、IP プールが内部の DHCP サーバから IP アドレスを取得している場合に受信インタフェースを疑似するのに使用されます。DHCP サーバのフィルタリング基準が受信インタフェースを含むため、本設定が必要となります。 サーバとプールの両方が NetDefendOS 内部であるので、内部の DHCP サーバはインタフェースの IP プールサブシステムからリクエストを受信することはできません。この設定により、プールからのそのようなリクエストは特定のインタフェースから来るように見えるため、関連する DHCP サーバが応答できるようになります。
MAC Range	一連の MAC アドレスは、フェイクの DHCP クライアントを作成するのに使われます。また、DHCP サーバが MAC アドレスを使ってクライアントをマッピングする時に使用されます。MAC 範囲は、DHCP サーバが各クライアントに同じ IP を継続的に振り分ける場合に必要になります。
Prefetch Leases	プリフェッチしておくリースの IP アドレス数を設定します。プリフェッチリースでは、システムが IP を要求する時（プリフェッチ IP が存在しているため）待ち時間がなくなり、性能が向上します。
Maximum Free	不使用 IP の数に制限はありません。最大値はプリフェッチパラメータ値以上である必要があります。不使用クライアントの数がこの値を超えると、プールは IP を DHCP サーバに戻します。
Maximum Clients	プールできるクライアント（IP）の最大値を指定するオプションです。

項目	説明
Sender IP Address	DHCP サーバとの通信時に使用する送信元 IP。

プリフェッチリース用のメモリアロケーション

前項で述べたように、プリフェッチリースオプションでは、NetDefendOS が管理するリースのキャッシュサイズを設定します。このキャッシュは、迅速なリース配分を可能にし、システムの総合的な性能を向上させます。しかし、システム起動時に全体のプリフェッチリース数がリクエストされ、この数が大きすぎる場合には初期性能を下げることになるので注意が必要です。

プリフェッチキャッシュ内のリースが割り当てられる度に DHCP サーバへのリクエストが行われるため、キャッシュは常に一杯になります。従って、管理者はプリフェッチキャッシュの初期サイズが最適になるよう見極める必要があります。

IP プールステータスの表示

CLI コマンド「ippool」は、IP プールの現在のステータスを参照するために使用されます。

コマンドの最も簡単な形式は以下の通りです。

```
DFL-xxxx:/> ippool -show
```

これはステータスに伴うすべての定義済み IP プールを表示します。ステータス情報は 4 つに分かれています。

項目	説明
Zombies	割り当てられていますが、アクティブでない数。
In progress	割り当て処理中のアドレス数。
Free maintained in pool	割り当てに利用可能なアドレス数。
Used by subsystems	割り当てられ、かつアクティブなアドレス数。

「ippool」コマンドにおける別のオプションにより、管理者はプールサイズの変更と IP アドレスの解放を行うことができます。コマンドオプションの一覧については、「CLI Reference Guide」を参照してください。

例題 5.5

IP プールの作成

この例題では、10 個のプリフェッチリースを持つ IP アドレス 28.10.14.1 の DHCP サーバを使用する IP プールを作成します。この IP アドレスは、IP オブジェクト ippool_dhcp としてアドレス帳に登録済みであるものとします。

CLI

```
DFL-xxxx:/> add IPPool ip_pool_1 DHCPServerType=ServerIP ServerIP=ippool_dhcp PrefetchLeases=10
```

Web Interface

1. **Objects > IP Pools > Add > IP Pool** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ **General**

- Name : ip_pool1
- Specify DHCP Server Address : チェックし、「ippool_dhcp」を「Selected」リストに追加します。

◇ **Advanced**

- Prefetch Leases : 10

5.6 DHCPv6

NetDefendOS は、IPv6 のために IPv4 DHCP に相当する DHCPv6 をサポートします。これは以下の 2 つのセクションで説明されます。

- 「5.6.1 DHCPv6 クライアント」
- 「5.6.2 DHCPv6 サーバ」

5.6.1 DHCPv6 クライアント

概要

各インタフェースに対し、DHCPv6 クライアントになるように設定することができます。つまり、NetDefendOS が再起動する時はいつでも、または、DHCPv6 が有効なコンフィグレーションが保存されてアクティブ化される時には、インタフェースは接続する DHCPv6 サーバから自動的に IPv6 のリースを取得しようとします。以下のインタフェースタイプだけが DHCPv6 クライアント機能をサポートします。

- イーサネットインタフェース
- VLAN インタフェース
- リンクアグリゲーションインタフェース

本セクションでは、上記のいずれかのタイプを意味する汎用的な用語として「インタフェース」を使用します。

重要 DHCPv6 クライアントは HA クラスタではサポートされません。

DHCPv6 クライアントは NetDefendOS HA クラスタのインタフェースではサポートされません。インタフェースで有効にすると、コンフィグレーションをコミットするときにエラーメッセージが出ます。

サーバリースで受信されたアドレス

DHCPv6 サーバから受信したリースは、以下を含みます。

- インタフェースの IPv6 アドレス
- 最大 3 つの IPv6 DNS サーバのアドレス。NetDefendOS は最初の 2 つしか読みません。3 番目は破棄されます。

また、後のセクションで説明される通り、インタフェースプロパティ Router Discovery が有効であると、自動的に IPv6 ネットワークアドレスと IPv6 ゲートウェイアドレスを取得できます。

作成されるアドレス帳オブジェクト

以下は、DHCP クライアントが、例えば if1 インタフェースで有効な場合に作成される IPv6 アドレス帳オブジェクトのリストです。

オブジェクト	説明
if1_ip6	インタフェースアドレス。
if1_dns6_1	DHCP リース内の最初の IPv6 DNS アドレス。
if1_dns6_2	DHCP リース内の 2 番目の IPv6 DNS アドレス。
if1_net6	インタフェースネットワーク（Router Discovery を有効にする必要があります）。
if1_gw6	ゲートウェイ（Router Discovery を有効にする必要があります）。

DHCP クライアントメカニズムはこれらのオブジェクトを作成するだけではなく、インタフェースの関連プロパティにそれらを割り当てます。Router Discovery オプションの使用については、本セクションの後半で説明します。

DHCPv6 を有効にする

IPv4 を使用した DHCP と同じく、特定のインタフェースに Enable DHCPv6 プロパティを使用して、DHCPv6 を有効にします。初期値では本プロパティは無効です。

さらに、他の多くのプロパティをオプションでインタフェースに指定できます。

プロパティ	説明
Preferred IP	DHCPv6 サーバに送信されるインタフェースの IP 提案です。
Preferred Lifetime と Valid Lifetime	DHCPv6 サーバに送信される有効期限の提案です。これらのオプションの最小値は 7600 であり、このオプションの値は常に Preferred Lifetime より大きくなければいけません。これのオプションの詳細は「5.6.2 DHCPv6 サーバ」で説明します。
Lease Filter	インタフェースに割り当てられる IPv6 アドレスの許可される範囲です。提案されたリースがこのアドレスを含まないと、拒否されます。
Server Filter	NetDefendOS がリースを受け付けるサーバの IPv6 アドレス範囲です。

Router Discovery オプション

イーサネットコンフィグレーションオブジェクトには、Router Discovery プロパティがあり、有効または無効にされます。

初期値ではこのオプションは無効化されており、DHCPv6 クライアント機能によってインタフェースの IPv6 アドレスと DNS サーバの IPv6 アドレスのみが設定されます。管理者は手動でネットワークアドレスとゲートウェイアドレスを設定しなければなりません。

Router Discovery オプションが有効である時に、IPv6 ネットワークと IPv6 ゲートウェイアドレスを含むクライアントアドレスの完全なセットが、DHCPv6 プロセスによって提供されます。これは IPv4 が機能する標準の方法と同様です。

参照 ISP に正しい IPv6 接続方法を確認します。

IPv6 を使用して ISP に接続する際、NetDefendOS をどのように設定するべきかは ISP に問い合わせてください。IPv6 ネットワークの他に、ISP ゲートウェイの IPv6 アドレスを取得するために、ISP は Router Discovery が有効な DHCP クライアントの使用が必要かもしれません。

また、DHCP クライアント機能を無効化し、インタフェースの IPv6 アドレスを自動設定する場合に Router Discovery を使用することができます。この使用方法については、「3.2 IPv6 のサポート」を参照してください。

DNS サーバを割り当てる

DHCPv6 サーバが認可したリースは、DNSv6 サーバの最大 3 つの IPv6 アドレスを含むことができます。しかし、NetDefendOS は Primary および Secondary サーバとして知られるこれらの 1 番目と 2 番目だけを使用します。リースに存在する 3 番目のサーバは無視されます。

DHCP サーバから取得した DNSv6 アドレスは、インタフェースコンフィグレーションオブジェクト DHCPv6DNS1 と DHCPv6DNS2 に保存されます。

DNS アドレスオブジェクトの作成

リースの最初の DNSv6 サーバアドレスのために、NetDefendOS は、名前 <interface>_dns6_<num> を持つ新しい IPv6 アドレス帳オブジェクトを作成します。<interface> はリースを受信するインタフェースで、<num> はリースの DNSv6 サーバの順番です。

例えば、DHCPv6 リースを受信するインタフェースが、wan インタフェースであれば、最初のリースのために作成されたアドレス帳オブジェクトは、wan_dns6_1 と名付けられます。リースが 2 番目の DNSv6 サーバアドレスを含んでいると、これは wan_dns6_2 というように呼ばれます。

DNSv6 サーバアドレスを NetDefendOS にスタティックに設定することができます。スタティックに設定した場合、これらの手動で設定されたアドレスが、リースの際に受信されるアドレスより優先されます。しかし、NetDefendOS は、リースの際に受信した各 DHCPv6 サーバアドレス用に自動的にアドレス帳オブジェクトを <interface>_dns6_<num> の形式で作成します。スタティックに定義された DNS アドレスのこの優先度については、「3.10 DNS 設定」に記載されています。

リース満了時の動作

DHCP リースが終了し、更新されなくても、DHCPv6 メカニズムが作成したアドレス帳オブジェクトはアドレス帳に残ります。しかし、インタフェースに関連しているアドレス帳オブジェクトの値は以下の通り影響を受けます。

- ネットワークとゲートウェイオブジェクトは最後に DHCPv6 が割り当てた値を保持します。
- 他のすべてのオブジェクトは IPv6 未指定アドレス（::/128）に設定されます。

例題 5.6

DHCPv6 クライアントセットアップ

この例題は、wan インタフェースで DHCPv6 を有効にする方法を示しています。IPv6 がインタフェースで既に有効であるものとします。

CLI

```
DFL-xxxx:/> set Interface Ethernet wan DHCPv6Enabled=Yes
```

Web Interface

1. **Network > Interfaces and VPN > Ethernet** の順にメニューをクリックします。
2. wan インタフェースを選択します。
3. Enable DHCPv6 Client を選択します。
4. 「OK」ボタンをクリックします。

5.6.2 DHCPv6 サーバ

NetDefendOS は 1 つ以上の DHCPv6 サーバをセットアップできます。これらの設定は、IPv4 DHCP サーバを設定するのとほぼ同じです。しかし、DHCPv6 で利用可能ないくつかのオブジェクトプロパティがありますが、標準の IPv4 DHCP とは異なります。これらは以下の通りです。

プロパティ	説明
Handle Rapid Commit Option	初期値では、これは無効です。本オプションはサーバ要請の手続きの時に意味があります。クライアントが solicit メッセージに rapid commit オプションを持ち、rapid commit 設定が有効であると、DHCPv6 サーバは solicit メッセージに応答します。応答メッセージを送信する前に、サーバはアドレスの割り当てを行います。クライアントは、応答メッセージのアドレスに割り当てられたと仮定するため、それらのアドレスに要求メッセージを送信する必要はありません。 このオプションが無効の初期値のままであると、サーバは rapid commit オプションを無視し、 クライアントの solicit メッセージに rapid commit オプションが存在しないものとして動作します。
Send Preference Option	優先度の送信を有効 / 無効に設定します。送信を有効にするのであれば、デフォルト優先度値は 0 ですが、これを 0 ～ 255 に手動で設定できます。 優先度を設定すると、1 つの DHCPv6 サーバを他のものより優先させることができます。サーバ要請の手続きの間、クライアントは、DHCPv6 サーバから受信した通知メッセージを収集します。クライアントは最も高いサーバ優先度値を持つ通知メッセージを送信したサーバに通常コンタクトを行います。 優先度値 255 は、最も高い優先度があります。そして、そのような値を通知メッセージで受信すると、クライアントは直ちに DHCPv6 サーバから送信されたメッセージとのメッセージ交換を開始します。他のサーバが無視されるため、この値は 1 つのサーバだけの環境で使用するべきです。 多くの場合、優先度は、管理者が 1 つのサーバをプライマリサーバにしたい場合により高い優先度、他のバックアップサーバにしたい場合により低い優先度を割り当てる際に使用されます。
Send Unicast Option	初期値では、クライアントとサーバとのネゴシエーションでは、クライアントはすべてのメッセージに宛先としてマルチキャスト IPv6 アドレスを使用します。本オプションは、DHCPv6 サーバが、クライアントに送信されるメッセージにサーバのユニキャストオプションを含めることを有効にします。一度、そのようなオプションをクライアントが受信すると、サーバの IPv6 アドレス（サーバユニキャストオプションで送信される）を使用することで、クライアントはサーバと直接コンタクトをとることができます。 これにより、ネットワーク負荷の軽減とネットワークで利用可能な他の DHCPv6 サーバへの負荷の移動が可能になります。
Clear Universal Local Bit	本オプションを有効にすると、サーバから付与された IPv6 アドレスの unversal/local bit (u/l bit) を常にクリアし、従ってこの値は常に 0 になります。これは一般に使用されるべきでないローカルに作成されたものとしてアドレスにフラグをつけます。この設定は /64 のネットワークに適用されます。 この設定の初期値は無効であるため、ビットは自動的に NetDefendOS によってゼロにセットされません。
Valid lease time/ Preferred lease time	クライアントに送信される IP の有効期限です。Valid lease time オプションの値は常に Preferred lease time より大きくなければいけません。 Preferred lease time の期限が切れると、その IP アドレスは新規または既存の接続に使用されるかもしれませんが、これはできる限り避けるべきです。例えば、あるアプリケーションが処理中のプロセスのために同じ IP を必要とするかもしれません。Valid lease time の有効期限が切れた場合は、IP は無効となり新規または既存の接続に使われることはありません。

アドレスの割り当てのスピードアップ

1 つの DHCPv6 サーバだけが設定される場合、rapid commit を有効にし、その優先度値を 255 に設定することで、IPv6 アドレスの割り当てが著しく速くなります。

優先度値255を使用すると、クライアントがsolicitメッセージを受信すると直ちに、メッセージ交換処理が起動します。Rapid commitにより、クライアントは、DHCPv6 サーバと solicit-reply メッセージの交換を行う間に、リプライメッセージにあるコミットされたアドレスを取得することができます。同時に、これらはアドレスの割り当て速度を著しく向上できます。

使用可能メモリはリース割り当てを制限できる

DHCPv6 リースを付与する場合、NetDefendOS はファイアウォールのローカルメモリにリースの詳細を保存します。このリースのリストに対して事前に割り当てられたメモリはなく、使用するメモリ容量は 0 から全ての使用可能メモリが枯渇するポイントまで拡張可能です。

メモリが利用できなくなると、NetDefendOS は、新しいリースを割り当てるのをやめて、フリーな IP がプール内に残っていないかのように振る舞います。NetDefendOS は一般的なメモリ不足の状態を通知し、これは管理コンソールに表示されます。この状態は、大量のリースが割り当てられていることが前提となります。

DHCPv6 サーバ設定

NetDefendOS で DHCPv6 サーバを設定する手順は以下の通りです。

- DHCPv6 サーバの listening インタフェースで IPv6 が有効となっており、そのインタフェースに IPv6 アドレスが割り当てられていることを確認してください。これを行うには、「3.2 IPv6 のサポート」を参照してください。
- 新しい DHCPv6 Server オブジェクトを作成します。これは特定のインタフェースでリッスンし、指定した IPv6 Address Pool オブジェクトから付与された IPv6 アドレスを取得します。
- 高度な IP 設定 Multicast HopLimit Min は 1 の値に設定しなければなりません（初期値は 1）。

・DHCPv6 サーバとして機能するファイアウォールが、サーバのルータ通知を送信する場合、以下の設定を行う必要があります。

i. DHCPv6 サーバに指定された同じインタフェースに Router Advertisement オブジェクトを追加します。

ii. ネットワークに DHCPv6 サーバがあることを告知するために、Router Advertisement オブジェクトの「Use Global Settings」オプションを無効にし、Managed Flag 設定を有効にします。DHCPv6 サーバが DNS アドレスに関する情報を提供している場合 Other Config Flag 設定を有効にします。

iii. Router Advertisement オブジェクトに Prefix オブジェクトを追加します。これはオプションですが、通常設定されます。指定されたプレフィックスは、DHCPv6 サーバがリッスンするインタフェースに割り当てられたネットワークと同じです。

iv. ネットワークのホストが、ステートレス自動コンフィグレーションのために定義されたプレフィックスの使用を希望しないのであれば、Prefix オブジェクトの Autonomous Flag 設定を無効にします。DHCPv6 サーバがネットワークアドレスに追加されているため、このような設定となるでしょう。

ネットワーク上の他のデバイス（D-Link ファイアウォールまたはサードパーティのデバイスのいずれか）が DHCPv6 サーバにルータ通知を送っている場合、デバイスを上記の設定と同様に設定する必要があります。

例題 5.7

DHCPv6 サーバの設定

この例題では、DHCPv6 サーバ dhcpv6_server1 をイーサネットインタフェース lan にセットアップする方法を示しています。利用可能な IP アドレスのプールが IPv6 アドレスオブジェクト dhcpv6_range1 によって既に定義されているものとします。

また、サーバは rapid commit オプションを使用し、自身に優先度値 100 を割り当てます。IPv6 機能が、グローバルかつ listening インタフェース lan で有効になっているものとします。

ルータ通知が同じファイアウォールにより生成され、使用するプレフィックスは 2001:DB8::/64 となります。

CLI

サーバを作成します。:

```
DFL-xxxx:/> add DHCPv6Server dhcpv6_server1 Interface=lan IPv6AddressPool=dhcpv6_range1 RapidCommit=Yes
            PreferenceConfigured=Yes PreferenceValue=100
```

ホップリミットを 1 に設定します。:

```
DFL-xxxx:/> set Settings IPSettings HopLimitMin=1
```

ルータ通知を作成します。:

```
DFL-xxxx:/> add RouterAdvertisement Name=my_ra Interface=lan UseGlobalRASettings=No RAManagedFlag=Yes
            RAOtherConfigFlag=Yes
```

コンテキストをルータ通知に変更します。:

```
DFL-xxxx:/> cc RouterAdvertisement 1
```

プレフィックスオブジェクトを追加します。:

```
DFL-xxxx:/1(my_ra)> add RA_PrefixInformation Name=my_prefix Prefix=2001:DB8::/64 RAAutonomousFlag=No
```

初期値の CLI コンテキストに戻します。:

```
DFL-xxxx:/1(my_ra)> cc
```

Web Interface

サーバを作成します。:

1. **Network > Network Services > DHCPv6 Servers >Add > DHCPv6Server** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: dhcpv6_server1
   - Interface Filter: lan
   - IP Address Pool: dhcpv6_range1
3. Options タブを選択します。
4. Handle Rapid Commit を有効にします。
5. Send Preference Option を有効にします。
6. Preference Value を 100 に設定します。
7. 「OK」ボタンをクリックします。

ホップリミットを 1 に設定します。:

1. **System > Advanced Settings > IP Settings** の順にメニューをクリックします。
2. IPv6 の下で Multicast HopLimit Min を 1 に設定します。
3. 「OK」ボタンをクリックします。

ルータ通知を作成します。:

1. **Network > Routing > Router Advertisements > Add > Router Advertisement** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_ra
   - Interface: lan
3. Advanced タブを選択します。
4. Use Global Settings を無効にします。
5. Managed Flag を有効にします。
6. Other Config Flag を有効にします。
7. 「OK」ボタンをクリックします。

さらに、ルータ通知定義にプレフィックスオブジェクトを追加します。:

1. **Network > Routing > Router Advertisements > my_ra** の順にメニューをクリックします。
2. **Prefix Information > Add > Prefix Information** の順にメニューをクリックします。
3. 以下の情報を入力します。
   - Name: my_prefix
   - Network Prefix: 2001:DB8::/64
4. Autonomous Flag 設定を無効にします。
5. 「OK」ボタンをクリックして、プレフィックスを保存します。
6. 「OK」ボタンをクリックして、通知を保存します。

スタティックな DHCPv6 ホスト

クライアントに対し IP アドレスを固定で割り当てる場合、NetDefendOS では IPv6 アドレスの指定 MAC アドレスへの割り当てを行うことができます。これは、「5.3.1 Static IPv4 DHCP Host（スタティック IPv4 DHCP ホスト）」に記載されている IPv4 への割り当てと同様です。

例題 5.8

スタティックな DHCPv6 ホストアサインメント

この例題では、IPv6 アドレス 2001:DB8::1 を MAC アドレス 00-90-12-13-14-15 に割り当てる方法を示しています。ここでは、DHCPv6 サーバ dhcpv6_server1 が既に定義されているとします。

CLI

まず、カテゴリを dhcp_ipv6_server1 というコンテキストに変更します。:

```
DFL-xxxx:/> cc DHCPv6Server dhcpv6_server1
```

スタティック DHCP アサインメントを追加します。:

```
DFL-xxxx:/dhcpv6_server1> add DHCPv6ServerPoolStaticHost Host=2001:DB8::1 MACAddress=00-90-12-13-14-15
```

初期値の CLI コンテキストに戻します。:

```
DFL-xxxx:/dhcpv6_server1> cc
DFL-xxxx:/>
```

Web Interface

1. **Network > Network Services > DHCPv6 Servers > dhcpv6_server1** の順にメニューをクリックします。
2. Static Hosts を選択します。
3. **Add > Static Host Entry** を選択します。
4. 以下の情報を入力します。
   - Host: 2001:DB8::1
   - MAC: 00-90-12-13-14-15
5. 「OK」ボタンをクリックして DHCPv6 サーバの設定を保存します。

第 6 章 アプリケーションレイヤのセキュリティ

この章では、NetDefendOS セキュリティ機能について記述します。

- 「6.1 アプリケーションレイヤゲートウェイ」
- 「6.2 Web コンテンツフィルタリング」
- 「6.3 メールフィルタリング」
- 「6.4 アンチウィルススキャン」
- 「6.5 ファイルコントロール」

6.1 アプリケーションレイヤゲートウェイ

6.1.1 概要

IP、TCP、UDP、ICMP といったプロトコルのパケットヘッダの検査のみを実行する、低いレベルのパケットフィルタリングを実装するために、アプリケーションレイヤゲートウェイ（ALG : Application Layer Gateway）を実装し、より高いアプリケーション OSI レベルのフィルタリングをサポートしています。

ALG オブジェクトは Web アクセス、ファイル転送、およびマルチメディア転送などの保護されているネットワークの外側にあるインターネットアプリケーションにアクセスするための仲介者として動作します。特定のサービスプロトコルに対してすべてのトラフィックを綿密に調べる能力を持ち、TCP/IP スタックのトップレベルでチェックを実行するため、ALG はパケットフィルタリングよりも高いセキュリティを提供します。

以下は NetDefendOS がサポートするプロトコルです。

- HTTP
- FTP
- TFTP
- SMTP
- POP3
- IMAP
- PPTP
- SIP
- H.323
- TLS
- DNS

注意 IPv6 ベースのトラフィックをサポートしていない ALG もあります。

IPv6 アドレスを参照する IIP ルールセットのエントリと共に使用する場合、HTTP（および LW-HTTP）ALG のみ IPv6 をサポートします。

ALG の設定方法

ALG は、ターゲットのトラフィックに対して起動される IP ルールセットエントリに紐づけることで使用することができます。以下のいずれかの方法で設定を行います。

- **IP ポリシーを使用する**

  IP ルールを使用するよりも簡単かつ追加の機能も含まれているため、IP ポリシーを使用する方式が推奨されます。一部の ALG 機能は IP ポリシーを使用している場合のみ利用可能です。また、DNS や IMAP などの一部の ALG は IP ポリシーのみで展開することができます。

  この方式の要件は、IP ポリシーで指定されているサービスプロパティのプロトコルプロパティが ALG タイプに設定されていることです（例：FTP）。定義済みサービスを使用するケースもありますが、通常は、この目的のためにカスタムサービスを作成することをお勧めします。

- **IP ルールを使用する**

  この方式では、特定のプロトコル用の ALG オブジェクトをサービスオブジェクトに割り当て、それを IP ルールに割り当てます。通常、この ALG 設定方法は古い NetDefendOS バージョンとの互換性の要件に対してのみ必要となります。

  定義済み ALG オブジェクトを IP ルールに使用することもできますが、カスタム ALG オブジェクトを使用する方が通常は適しています。

このセクションではすべての利用可能な方法を使用した ALG 設定について説明します。

注意 ALG は同期される状態ではありません。

ALG のどのアスペクトも、NetDefendOS 高可用性クラスタで同期する状態ではありません。これは、クラスタがもう一方のピアにフェイルオーバする際に、ALG に処理されるすべてのトラフィックがフリーズすることを意味します。しかし、クラスタが 30 秒程度で本来のピアにフェイルバックすると、フリーズセッションと関連する転送は再び動作を開始します。新しい構成がアップロードされるたびに、フェイルオーバと即時のフォールバックが発生することに注意してください。

最大の接続セッション

ALG に関連づけされたサービスは、それに紐づく Max Sessions と呼ばれる設定可能なパラメータを持っており、デフォルト値は ALG のタイプによって変わります。例えば、HTTP ALG の初期値は 200 です。これは、200 個の接続がすべてのインタフェースを通過する HTTP サービスのための合計として許可されていることを表しています。

注意 HTTP の最大のセッションが低過ぎる場合があります。

D-Link ファイアウォールを経由して接続しているクライアントが多数存在する場合、デフォルト値では低過ぎることがよくあります。そのため、より高い値を使用することをお勧めします。

ALG は NetDefendOS バージョン 11.01 以降から変更されています

NetDefendOS バージョン 11.01 以降、NetDefendOS の新しい設定から定義済み ALG オブジェクトの多くが削除されています。古い NetDefendOS からアップグレードしても定義済み ALG オブジェクトは変更されませんが、必要に応じて、欠けている ALG を手動で再作成することができます。

NetDefendOS バージョン 11.01 以降では、多くの ALG オブジェクトを直接使用するのを回避することが可能です。これは、IP ルールオブジェクトに代わって IP Policy オブジェクトを使用することで行われます。11.01 以降から、IP ポリシーと共に多くの定義済みサービスオブジェクトを直接使用できます。また、ALG オブジェクトで以前利用可能であったプロパティのすべてが IP ポリシーオブジェクトのプロパティになっています。

このトピックは、「3.3 サービス」で詳しく説明します。

6.1.2 HTTP ALG

概要

HTTP（Hyper Text Transfer Protocol）は、WWW（World Wide Web）にアクセスするために使用される主要なプロトコルです。それは接続のない、ステートレスなアプリケーション層プロトコルであり、リクエスト / レスポンス構造に基づいています。Web ブラウザのようなクライアントは、リモートサーバの特定のポート（通常ポート 80）に TCP/IP 接続を確立することでリクエストを送信します。サーバは、自身のメッセージに従いレスポンスの文字列で応答します。メッセージは、例えば Web ブラウザで参照される HTML ファイル、クライアント上で実行される ActiveX コンポーネント、またはエラーメッセージの可能性があります。

HTTP プロトコルは、アクセスされる広く多岐にわたる Web サイトとアクセスが成功した際にダウンロードされるファイルタイプの範囲のために、特定の問題に直面します。

HTTPS における制限

HTTPS ではトラフィックが暗号化されるため、HTTP ALG ではトラフィックに対して以下の 2 つのアクションのみを行います。

- URL フィルタリング
- WEB コンテンツフィルタリング

IP ルールセットのエントリで使用されるサービスで HTTPS が含まれる場合（http-all を使用している場合など）、この点に注意する必要があります。

HTTP と LW-HTTP ALG は IPv6 をサポートしています

HTTP ALG は、IPv6 アドレスとネットワークを参照する IP ルールオブジェクトと共に使用することができます。また、同様に、IPv6 ベースの IP ポリシーオブジェクトはこれらの ALG 機能を利用できます（IP ポリシーを使用すると ALG オブジェクトは非表示となります）。

HTTP フィルタリングの順序

HTTP フィルタリングは、以下の処理順序に従います。これは、SMTP ALG の順序に似ています。

1. ホワイトリスト
2. ブラックリスト
3. Web コンテンツフィルタリング（有効な場合）
4. アンチウィルススキャン（有効な場合）

上述の通り、URL がホワイトリストで見つけられると、ブラックリストにあってもブロックされません。

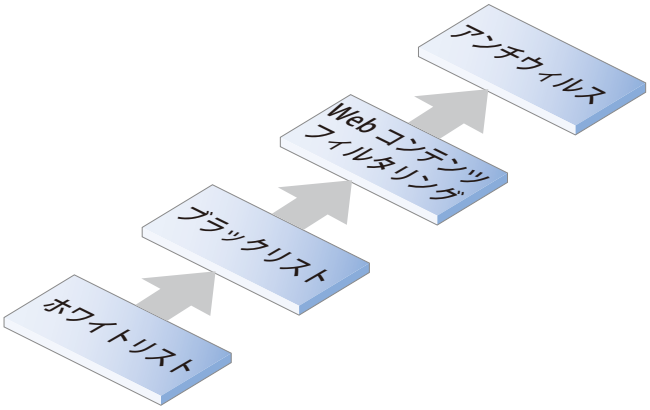


図 6-1　HTTP ALG 処理の順序

HTTP ALG の設定方法

HTTP ALG は、以下のいずれかの方法で設定を行います。

- **IP ポリシーを使用する**
  HTTP ALG オプションの一部が IP ポリシーで設定可能になりますが、多くの項目は Web Profile オブジェクトを IP ポリシーに紐づけることで設定可能です。詳細は「6.1.2.2. IP ポリシーを使用した HTTP ALG のセットアップ」を参照して下さい。

  IP ポリシーで指定されているサービスプロパティのプロトコルプロパティが HTTP タイプに設定されている必要があります。

  HTTP ALG を設定する場合は IP ポリシーを使用することをお勧めします。

- **IP ルールを使用する**
  この方式では、HTTP ALG オブジェクトをサービスオブジェクトに割り当て、それを IP ルールに割り当てます。すべての ALG オプションは HTTP ALG オブジェクトで直接設定することができます。詳細は「6.1.2.3 IP ルールを使用した HTTP ALG のセットアップ」を参照して下さい。

6.1.2.2. IP ポリシーを使用した HTTP ALG のセットアップ

HTTP ALG オプションは、IP ポリシーオブジェクト内で以下の通り設定することができます。

1. ターゲットのトラフィックで起動するフィルタリングプロパティを持つ IP ポリシーオブジェクトを作成します。

2. IP ポリシーのサービスプロパティに指定されているプロトコルプロパティは、ターゲットのトラフィックに応じて以下のいずれかに設定されている必要があります。
   i. HTTP
   ii. HTTPS
   iii. HTTP and HTTPS

HTTPS については、サービスに HTTPS 用のポート番号 443 が含まれている必要があります。

3. IP ポリシーで直接設定可能な HTTP ALG 設定の値を設定します。これらの項目については別途説明します。

4. Web プロファイルオブジェクトを作成し、IP ポリシーに紐づけます。このプロファイルにより、Web コンテンツフィルタリングや URL フィルタリングといった多くの ALG 機能の設定が可能になります。

5. 関連する他のオブジェクトを IP ポリシーに紐づけます。例えばファイルコントロールプロファイルを作成し、IP ポリシーに割り当てて、HTTP 経由でダウンロードされたファイルの制限を実行することができます。

IP ポリシーで直接設定可能な HTTP ALG オプション

以下のオプションは IP ポリシーで直接設定することが可能です。

- **Enable HTTP Inspection**
  ALG により HTTP トラフィックが有効な HTTP であるか検証されます。この検証には、URL に不正な UTF8 エンコーディングが含まれるかどうかの確認も含まれます。初期値では無効です。

- **Allow Unknown Protocols**
  非 HTTP 準拠トラフィックが許可されます。初期値では無効です。

Web プロファイルオブジェクト

IP ポリシーを使用する場合、HTTP ALG 機能の多くは Web プロファイルオブジェクトで設定することが可能であり、設定後、IP ポリシーに割り当てることが可能です。Web プロファイルには以下の設定可能なプロパティがあります。

- **Name**
  コンフィグレーションオブジェクトの論理名。

- **Allow Protocol Upgrade**
  HTTP 接続が他のプロトコルにアップグレードされることを許可します。例えば、HTTPS へのアップグレードは初期値で許可されます。

- **Fail Mode**
  NetDefendOS 処理のエラーが発生した場合のアクションを指定します。例えば、WCF データベースが到達不可といった場合です。初期値は Allow で何もブロックされません。

- **HTML Banner**
  アクセスが拒否された場合に HTTP クライアントに表示される HTML バナーファイルを選択します。

- **Web Contents Filtering**
  Web コンテンツフィルタリングを有効化します。初期値では無効です。Web コンテンツフィルタリングの詳細は「6.2 Web コンテンツフィルタリング」を参照してください。

URL フィルタリング

特定の URL をホワイトリスト（すべての検査をスキップ）またはブラックリスト（接続破棄）に追加することができます。Web プロファイルオブジェクトに 1 つ以上の URL オブジェクトを追加することで設定します。URL はワイルドカードを使用して指定することが可能であり、その詳細はこのセクションの最後で説明しています。

URL Filter オブジェクトには 2 つの主要なプロパティとして、URL と Action があり、Action では以下の値を指定することができます。

- **Blacklist**

URL への接続は破棄されます。

- **Whitelist**
  URL は常にアクセス可能であり、追加の ALG 検査は実行されません。

  ホワイトリストに追加するということはブラックリストには追加できないということであり、Web コンテンツフィルタリングで破棄されないことに注意してください（有効化されている場合、ログは出力されます）。アンチウイルススキャンは、設定が有効化されている場合であっても、ホワイトリストに含まれる URL からの HTTP トラフィックに対しては適用されません。

- **Redirect**
  URL は指定された 2 番目の URL へ自動的にリダイレクトされます。

  URL リダイレクションはブラックリストと同じ優先度です。つまり、ホワイトリストの方が優先度が高く、同じ URL に対するリダイレクションは無視されます。管理者の設定ミスにより同じ URL がブラックリストとリダイレクション両方の対象となっている場合、アクション実行時にどちらかのアクションがランダムで実行されます。

  URL リダイレクションのループについてはこのセクションで後述します。こうした問題が発生しないように、新規の URL をホワイトリストに追加することを推奨します。

ホワイトリストとブラックリスト処理の優先順位

ホワイトリストは常にブラックリストよりも優先されます。設定ミスにより同じ URL がブラックリストとホワイトリストに追加された場合、ホワイトリストが常に先に処理されるため、ブラックリストのアクションは無視されます。

複数 URL の処理

ワイルドカードを使用して URL を指定した場合、URL に一致するフィルタが複数存在する可能性があります。NetDefendOS ではより限定的となる一致を選択するわけではないことに注意してください。最初の一致に対してアクションが実行され、それ以降のフィルタ検索は行われません。

ホワイトリストとブラックリストでワイルドカードを使用する

ホワイトリストとブラックリストに作成されるエントリは、一つのエントリが多くの想定される URL と同等になるようにワイルドカードを使用することができます。ワイルドカードの文字「*」はどんなシーケンスの文字も表すことができます。

例えば、エントリ「*.example.com」は URL で「example.com」が終わりにある URL のすべてのページをブロックします。

ある特定のページを明示的に許可する場合には、my_page.example.com の形式のホワイトリストを使用して行い、この場合、ブラックリストは、ホワイトリストが優先されるため、本ページを防御できません。

Wildcard Examples ワイルドカードの例

以下は、ワイルドカードを含むブラックリスト URL のよい例と悪い例です。

.example.com/	よい例。ホストに配信された example.com ドメイン内のすべてのホストと、そのサイトによって配信される全ての Web ページを防御します。これは、HTTPS と共に使用できる唯一の正しい形式です。
www.example.com/*	よい例。www.example.com Web サイトとすべての Web ページを防御します。
***/*.gif**	よい例。ファイル名の拡張子として .gif を持つすべてのファイルを防御します。
www.example.com	悪い例。Web サイトへのはじめのリクエストだけを防御します。例えば www.example.com/index.html へのサーフィンは、防御されません。
example.com/	悪い例。example.com で終了するすべてのサイトを防御するため、www.myexample.com も防御されてしまいます。

HTTPS ではドメインだけをターゲットにできます。

HTTPS の暗号化の性質上、ドメインレベルでのホワイトリストまたはブラックリストのみが可能です。例えば、形式 *.example.com/* のみ HTTPS でブラックリストまたはホワイトリストに使用できます。形式 *.example.com を使用するのは不十分です。

*.example.com/ サーバを HTTPS トラフィックに指定すると、これは正常に動作せず、一致する URL を取得できません。

ブラックリスト / ホワイトリストは Web コンテンツフィルタリングより優先される

ブラックリストおよびホワイトリストは Web コンテンツフィルタリングよりも先に実行されます。この仕様により、WCF 処理から例外を設定することができます。特定のオンラインストアから商品を購入するシナリオにおいて、WCF の設定により「Shopping」カテゴリをブロックしてショッピングサイトへのアクセスを制限することができます。一方で、オンラインストアの URL をホワイトリストに追加すると、ダイナミックコンテンツフィルタリングよりも優先されるため、その URL は常に許可されます。

同様に、スタティックコンテンツフィルタによる URL のブラックリスト化を行うと、その URL はダイナミックコンテンツフィルタリングによって処理されません。

IP ポリシーを使用した URL フィルタリング

IP Policy オブジェクトを使用した URL フィルタリングを有効にする場合、異なる手順を実施します。

- Web Profile オブジェクトを作成します。
- Web Profile の子供として 1 つ以上の URL Filter オブジェクトを追加して、ホワイトリスト、またはブラックリストにのせる URL を定義します。URL を指定する場合、ワイルドカードが使用できます。

  Web Profile オブジェクトのみで利用可能な 3 つ目の URL フィルタリングオプションとして、リダイレクト URL を指定します。指定した場合、トリガーとなった URL が指定したリダイレクト URL へ遷移します。また、この場合新しい URL をホワイトリストに追加する必要があるかもしれません。詳細は後述します。
- HTTP および / または HTTPS のために新しい Service オブジェクトを作成します。定義済みのオブジェクトを使用することもできます。この Service オブジェクトでは、Protocol プロパティを HTTP に設定する必要があります。HTTPS では、サービスは HTTPS のポート番号 443 を含む必要があります。
- 関連トラフィックをフィルタする IP ポリシーを持つ Service オブジェクトを使用します。
- IP ポリシーの Web Profile プロパティを前に作成したプロファイルに設定します。

URL リダイレクションとリダイレクションループの回避

URL リダイレクションを使用する際に注意すべき重要な点は、新規の URL をホワイトリストに追加してループの発生を回避する必要があるということです。これは、URL 置換後に新しい URL が再度 URL フィルタでチェックされるためです。以下の例では本問題について説明します。

URL フィルタオブジェクトで対象の URL をワイルドカード記号「*」と指定すると、すべての URL がフィルタを起動することを意味します。このフィルタに対してリダイレクトオプションを選択し、リダイレクト URL を www.example.com とします。置換が実行されると、新しい URLwww.example.com が再度フィルタに対して検索され、同様に起動してループが発生します。www.example.com が明示的に最初にホワイトリストに含まれていると、フィルタは実行されずループを回避することができます。

反対に、URL フィルタオブジェクトが www.anotherexample.com に対して起動し、www.example.com にリダイレクトされた場合を想定します。この場合、www.example.com が別の URL フィルタオブジェクトを起動していないのであれば、この URL をホワイトリストに含める必要はありません。

注意 HTTPS リダイレクションは IP ポリシーで動作しない

URL リダイレクションは IP ポリシーオブジェクトを経由する HTTPS トラフィックに適用できません。これをアクティブ化しようとするとエラーが表示されます。

例題 6.1

IP ポリシーを使用した URL リダイレクションの設定

この例題では、IP ポリシーを使用したスタティックコンテンツフィルタリングにより、URL リダイレクションを実行するように設定します。事前に定義済みの my_web_profile を使用して、URL「www.anotherexample.com」を URL「www.example.com」にリダイレクトします。

CLI

新規の WebProfile オブジェクトを作成する：

```
DFL-xxxx:/> add Policy WebProfile my_web_profile
```

CLI コンテキストを作成したプロファイルに変更する：

```
DFL-xxxx:/> cc Policy WebProfile my_web_profile
```

プロファイルの配下にフィルタを追加する：

```
DFL-xxxx:/my_web_profile> add URLFilterPolicy_URL URL=www.anotherexample.com Action=Redirect RedirectTo=http://
            www.example.com
```

デフォルトのコンテキストに戻す：

```
DFL-xxxx:/my_web_profile> cc
DFL-xxxx:/>
```

プロファイルを関連する IP ポリシーに紐づける：

```
DFL-xxxx:/> set IPPolicy my_ip_policy WebControl=Yes Web_Policy=my_web_profile
```

Web Interface

WebProfile オブジェクトを作成する：

1. **Policies > Web > Add > Web Profile** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - name: my_web_profile
3. 「OK」ボタンをクリックします。

URL フィルタを追加する：

1. プロファイル一覧から「my_web_profile」を選択します。
2. 「URL Filter」を選択します。
3. **Add > URL** を選択します。
4. 以下の設定を行います。
   - Action: Redirect
   - URL: www.anotherexample.com
   - Redirect To: www.example.com
5. 「OK」ボタンをクリックします。

プロファイルを関連する IP ポリシーに紐づける：

1. Policies > Main IP Rules の順にメニューをクリックします。
2. my_ip_policy を選択します。
3. Web Control を選択します。
4. Enable Web Control を有効化します。
5. Web Profile を my_web_profile に設定します。
6. 「OK」ボタンをクリックします。

6.1.2.3. IP ルールを使用した HTTP ALG 設定

このセクションでは、IP ルールと HTTP ALG オブジェクトを使用した HTTP 設定を説明します。HTTP ALG 設定に IP ポリシーを使用する場合はこのセクションの内容は適用されません。

IP ルールを使用した HTTP ALG

HTTP ALG オブジェクトは、サービスオブジェクトに紐づけ、それを IP ルールセットの IP ルールに紐づけることで使用することができます。多くの定義済み HTTP サービスを ALG で使用できます。例えばこの目的のために http サービスを使用することもできます。関連するサービスが IP ルールに紐づいている場合、ALG はその IP ルールの対象トラフィックに適用されます。

Light Weight HTTP ALG 代案

本セクションでは標準の HTTP ALG について説明します。多くの状況で、より少ないハードウェア資源でより高いトラフィック処理能力を提供できることから、代案の Light Weight HTTP ALG（LW-HTTP ALG）がより適切な選択となる可能性があります。IP ポリシーを使用する場合は、必要に応じて LW-HTTP ALG が自動的に使用されます。ただし、スタティックコンテンツの除去と HTTPS 処理は LW-HTTP ALG では利用できません。

2 つの ALG の違いに関する詳しい情報については、「6.1.2.4 Light Weight HTTP ALG」を参照してください。

HTTP ALG 機能

HTTP ALG では以下のオプションを提供します。

- **アクティブコンテンツ処理（Active Content Handling）**
  以下のいずれかのオプションのブロックができます。

  i. フラッシュを含む Web ページから ActiveX オブジェクトを削除できます。
  ii. Web ページから Java アプレットを削除できます。
  iii. Web ページから Javascript と Visual Basic Scripts を削除できます。
  iv. Web サイトのクッキーをブロックできます。

IP ポリシーに紐づく HTTP ALG を設定する場合、アクティブコンテンツ処理は利用できません。

注意 オブジェクトを削除した結果を検討する

どのようなオブジェクトも Web コンテンツからオブジェクトタイプを削除する前に、慎重に検討が行われる必要があります。

多くの Web サイトは Java スクリプトと他のクライアント側のコードタイプを使用し、多くの場合コードには不正はありません。一般的には、例えばドロップダウンメニューの実装に使用されるスクリプトや、Web 上で要素を表示・非表示にする場合に使用されています。

そのような正当なコードを削除することは、最善のケースでは Web サイトの内容をゆがめ、最悪のケースではブラウザを動作不能にします。そのため、アクティブコンテンツ処理は、その重大性がよく理解されている場合以外使用されるべきではありません。

- **URL 検証**
  いくつかの攻撃では無効なエンコードを含む不正な形式の URL を形成しています。本オプションが有効であることは、ALG が不正な形式の URL がないかどうかチェックすることを意味します。

- **ファイル保全性**
  HTTP でダウンロードされたすべてのファイルにも以下のチェックが行われます。

  i. **File Size** - ただ一つのダウンロードに対してもファイルサイズの制限を指定できます。本のオプションは HTTP および SMTP ALG ダウンロードにだけ有効です。
  ii. **File Type Policy** - 特定のファイルタイプを許可またはブロックすることができます。
  iii. **Allow/Block 選択タイプ**
  このオプションは上で説明した MIME 検証オプションに関係なく操作しますが、「付録 C アンチウィルス MIME ファイルタイプ」にある定義済みのファイルタイプに基づいています。有効な場合、機能は「Block Selected」または「Allow Selected」モードのいずれかで動作します。これらの 2 つのモードは以下の通り機能します。

モード	説明
Block	リストにマークされたファイルタイプは、ダウンロードで破棄されます。ファイル名を変更することでブロックが回避されることを防ぐために、NetDefendOS は、MIME チェックと同じ方法でファイルの内容を見て、それが要求したものであることを確認します。 例えば「.exe」ファイルがブロックされ、ファイルタイプ「.jpg」のファイル (ブロックされていない) に「.exe」データが含まれていることを見つけると、そのデータはブロックされます。「Blocking」が選択され、リストに何もマークされていない場合、ブロックは行われません。
Allow	マークされたファイルタイプだけが、ダウンロードを許可されてその他は破棄されます。ブロックの時と同様に、ファイルの内容が検証されます。例えば「.jpg」ファイルが許可され、ファイルタイプ「.jpg」のファイルに「.exe」データが含まれていることを見つけると、そのダウンロードはブロックされます。このモードで何もマークされていない場合、どのファイルもダウンロードされません。 初期状態で含まれない追加のファイルタイプは「Allow/Block」リストに追加できますが、ファイル拡張子がファイルの中身に対して正しいとして信頼されることを意味する MIME タイプのチェックにはなりません。

  iv. **MIME タイプの検証**
  本オプションにより、ファイルダウンロードのファイルタイプ（ファイル名の拡張子）がファイルのコンテンツに適合するかをチェックできます。

  NetDefendOS がチェックするすべてのファイルタイプが、「付録 C アンチウィルス MIME ファイルタイプ」に記載されています。有効な場合、MIME 検証に失敗するどんなダウンロードも、言い換えると、ファイルタイプがそのコンテンツに適合しないすべてのファイルダウンロードは、セキュリティ上の脅威であるかもしれないと見なし、NetDefendOS は破棄します。

- **Web コンテンツフィルタリング**
  特定のタイプの Web コンテンツのポリシーに従って、指定 URL へのアクセスを許可または拒否します。ニュースサイトへのアクセスは許可されるかもしれませんが、ゲームサイトへのアクセスはブロックされる可能性もあります。本機能は「6.2 Web コンテンツフィルタリング」に詳しく記述されています。

- **Anti-Virus Scanning**
  HTTP ファイルダウンロードの内容をウィルスチェックすることができます。疑わしいファイルを破棄、またはログ取得のみ行うことができます。「6.4 アンチウィルススキャン」で詳しく記述されています。

- **URL フィルタリング**
  管理者は特定の URL のブラックリストとホワイトリストを定義することができます。親の HTTP ALG オブジェクトの子供として、1 つ以上の HTTP ALG URL オブジェクトを追加することで行います。IP ポリシーを使用して実行する場合、1 つ以上の URL フィルタオブジェクトが子供として次に IP ポリシーに割り当てられる Web プロファイルオブジェクトに加えられます。

項目	説明
URL ブラックリスト	特定の URL をブラックリストに載せることができ、それらの URL にはアクセスできなくなります。これらの URL の指定にワイルドカードが使用できます。
URL ホワイトリスト	ブラックリストの反対であり、これは、特定の URL だけが常に許可されます。さらに、ワイルドカードをこれらの URL に使用できます。URL をホワイトリストに載せると、それをブラックリストに載せることができません。 また、Web コンテンツフィルタリングによっても指定した URL は破棄されないことに注意することが重要です。アンチウィルススキャンは、有効になっても、ホワイトリストに掲載された URL からの HTTP トラフィックには適用されません。

  URL 指定でワイルドカードを使用する方法については「6.1.2.2. IP ポリシーを使用した HTTP ALG のセットアップ」で説明しています。

例題 6.2

ActiveX と Java アプレットを除去する

この例題では、ActiveX と Java アプレットを除去するために HTTP アプリケーションレイヤゲートウェイを設定する方法を説明します。ここでは、content_filtering ALG オブジェクトを使用します。また、前述の例題のひとつが実行されているものとします。

CLI

```
DFL-xxxx:/> set ALG ALG_HTTP content_filtering RemoveActiveX=Yes RemoveApplets=Yes
```

Web Interface

1. **Objects** > **ALG** の順にメニューをクリックし、コンテンツフィルタリングを実施する HTTP ALG オブジェクト（ここでは、「content_filtering」）をクリックします。

2. 「Strip ActiveX objects (including Flash)」と「Strip Java applets」をチェックし、「OK」ボタンをクリックします。

IP ルールを使用した URL フィルタリングの設定

IP ルールを使用して URL フィルタリングの設定を行うには、以下の手順を実施します。

- HTTP ALG オブジェクトを作成します。HTTPS トラフィックに対しては、Allowed Protocol プロパティに HTTPS を設定します。
- ALG の子オブジェクトとして 1 つ以上の HTTP ALG URL オブジェクトを追加して、ホワイトリスト、またはブラックリストにのせる URL を定義します。

  リダイレクションは IP ルール使用時は実行できません。IP ポリシーオブジェクトに対応付けられた Web プロファイルオブジェクトが必要です。本セクションで別途説明します。

- Service オブジェクトでこの ALG を使用します。サービスオブジェクトは、HTTP 及び（または）HTTPS トラフィックを許可する既存のオブジェクトまたは作成したオブジェクトとなります。HTTPS の場合、サービスにはポート番号 443 が含まれている必要があります。
- IP ルールオブジェクトにそのサービスオブジェクトを使用します。IP ルールには、対象トラフィックで起動するための適切なフィルタが設定されている必要があります。

例題 6.3

IP ルールを使用した URL フィルタリング

この例題では、特定の URL をブラックリストまたはホワイトリストに記載するスタティックなコンテンツフィルタリングの使用を示しています。

また、ワイルドカードを使用して特定ファイルタイプのダウンロードを制限します。
ワイルドカードを使用したブラックリストにより、HTTP クライアントが Web サイトから exe ファイルをダウンロードできないように設定します。例外として、Web サイト www.example.com からの exe ファイルのダウンロードはホワイトリストによって許可されます。

CLI

はじめに HTTP トラフィックをフィルタするために HTTP ALG を追加します。:

```
DFL-xxxx:/> add ALG ALG_HTTP my_content_filter
```

ALG になるように CLI コンテキストを変更します。:

```
DFL-xxxx:/> cc ALG ALG_HTTP my_content_filter
```

次に、URL をブラックリストに載せるために、HTTP ALG URL を子供として追加します。:

```
DFL-xxxx:/my_content_filter> add ALG_HTTP_URL URL=*/*.exe Action=Blacklist
```

ホワイトリストを追加することでブラックリストからの例外を作成します。:

```
DFL-xxxx:/my_content_filter> add ALG_HTTP_URL URL=www.example.com/*.exe Action=Whitelist
```

追加のフィルタ設定がなければ、初期値の CLI コンテキストに戻します。:

```
DFL-xxxx:/my_content_filter> cc
DFL-xxxx:/>
```

Web Interface

はじめに HTTP トラフィックをフィルタするために HTTP ALG を追加する :

1. **Objects > ALG > Add > HTTP ALG** の順にメニューをクリックします。
2. 適切な ALG 名を入力します。例 : my_content_filter
3. 「OK」ボタンをクリックします。

次に HTTP ALG URL を作成し、ブラックリストを設定します。:

1. **Objects > ALG** の順にメニューをクリックします。
2. テーブルで、上記で作成した HTTP ALG をクリックして、プロパティを参照します。
3. URL Filter タブをクリックします。
4. **Add > HTTP ALG URL** の順にクリックします。
5. Action として Blacklist を選択します。
6. URL のテキストボックスに */*.exe を入力し、「OK」ボタンをクリックします。
7. 「OK」ボタンをクリックします。

最後にホワイトリストを作成することでブラックリストからの例外を作成します。:

1. **Objects > ALG** の順にメニューをクリックします。
2. テーブルで、最近作成した HTTP ALG をクリックして、プロパティを参照します。
3. URL Filter タブをクリックします。
4. **Add > HTTP ALG URL** の順にクリックします。Action として Whitelist を選択します。
5. URL テキストボックスに「www.dlink-jp.com/*.exe」を入力し、「OK」ボタンをクリックします。
6. 「OK」ボタンをクリックします。

フィルタの内容が要件を満たすまで、特定のブラックリストとホワイトリストの追加を続けます。

6.1.2.4 Light Weight HTTP ALG

IP ルールを使用して HTTP ALG を設定する際に、標準の HTTP ALG の代わりに Light Weight HTTP ALG(LW-HTTP ALG) を使用することができます。IP ポリシーを使用する場合、LW-HTTP ALG は必要に応じて自動的に展開されるため、本セクションはスキップしてかまいません。ALG 設定で IP ルールが使用されている場合に本セクションが関連します。

LW-HTTP ALG の利点

以下の通り、LW-HTTP ALG は標準の HTTP ALG より高い利点があります。

- 標準の HTTP ALG より高いスループット性能を提供します。
- 標準の HTTP ALG よりメモリの消費ははるかに少なくて済みます。これにより、NetDefendOS は大量の同時接続をサポートすることができます。
- 以下で示す標準の HTTP ALG が実行できない特定の機能を実行できます。
- IPv6 ベースのトラフィックで使用できます。

LW-HTTP ALG だけが実行できる機能

以下の機能は、LW-HTTP だけで利用可能であり、標準の HTTP ALG には存在していません。

項目	説明
HTTP Pipeline Support	対応する応答を待たずに、クライアントは 1 つの TCP 接続で複数の HTTP 要求を送信できます。これは、特に高い遅延時間を持つネットワーク接続におけるページのロード時間に顕著な改善をもたらします。標準の HTTP ALG はパイプライン接続サポートしていません。
User Agent Filter Support	特定のブラウザ、および / またはブラウザバージョンを許可し、他のすべてのブラウザをブロックできます。
Protocol Upgrade Support	LW-HTTP ALG ではプロトコルの変更が可能です。例えば、Web Sockets プロトコル。

LW-HTTP ALG が実行できない機能

以下の機能は LW-HTTP では提供できません。標準の HTTP ALG のみ提供します。
LW-HTTP ALG は HTTPS トラフィックをサポートしていません。

- ファイアウォールを通過するとき、LW-HTTP は、HTTP データのストリームを変更できません。このため、以下のスタティックなフィルタリングを実行できません。

  i. Active X オブジェクトのストリッピング
  ii. Javascript のストリッピング
  iii. Java アプレットのストリッピング
  iv. クッキーのブロック

- アンチウイルススキャンは LW-HTTP ALG を IP ポリシーと共に使用している場合のみサポートされます。アンチウイルススキャン用に IP ルールオブジェクトと一緒に使用することはできません。

- ファイルコントロールは LW-HTTP ALG を IP ポリシーと共に使用している場合のみサポートされます。IP ルールオブジェクトと一緒に使用することはできません。

ユーザエージェントフィルタリング

HTTP プロトコルの User-Agent フィールドでは HTTP 対話にかかわるクライアントソフトを特定します。多くの HTTP 通信で使用されるクライアントソフトは、Web ブラウザです。例えば、Firefox™ ブラウザによって生成された User-Agent フィールドは、以下のようなものがあります。

```
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
```

ネットワーク管理者は、セキュリティリスクを引き起こすため、または他のものが望ましいとの理由で、特定の Web ブラウザやブラウザバージョンを拒否または許可したい場合があります。

LW-HTTP ALG は、トラフィックがファイアウォールを通過する際に User-Agent フィールドを調べて、特定の文字列にマッチするエージェントへのアクセスを許可、または拒否するだけです。これは、親の LW-HTTP ALG オブジェクトに子供として 1 つ以上の User-Agent フィルタオブジェクトを付加することで設定されます。各フィルタオブジェクトは文字列を明示し、文字列が接続の User-Agent フィールドにマッチすると、フィルタが実行されます。実行時の動作は、親 LW-HTTP ALG オブジェクトの User-Agent Filter Mode プロパティで決定され、これは以下の 2 つの値のうちの 1 つを持つことができます。

- **Deny Selected** - フィルタが指定したエージェントのみ拒否されます。他のすべてのエージェントが許可されます。（初期値）

- **Allow Selected** - フィルタが指定したエージェントのみ許可されます。他のすべてのエージェントが拒否されます。

Firefox における上記のエージェントの例から参照できる通り、全体のエージェント文字列が長い場合があります。従って、フィルタにエージェント文字列を指定する場合には、ワイルドカードを使用するのがよいと言えます。以下のワイルドカードを使用できます。

- アスタリスク「*」文字は任意の文字列を表します。

- 疑問符「?」文字は任意の 1 文字を表します。

例えば、Firefox ブラウザだけを許可している場合、以下の文字列でフィルタを指定できます。

```
*Firefox/*
```

User-Agent がブロックされると、NetDefendOS は、フィルタリングが発生したことを警告するためにクライアントのブラウザに定義済みの Web ページを送信します。このページは現在のところ管理者が編集することはできません。

注意 フィルタを何も指定しないと、すべてのエージェントが許可されます。
User Agent Filter オブジェクトを 1 つも LW-HTTP ALG オブジェクトに追加しないと、すべての User-Agent が許可されます。

例題 6.4

Light Weight HTTP ALG を使用する

この例では、保護されたネットワークからパブリックインターネットまで HTTP を使用して Web サーフィンしているクライアントのために Light Weight HTTP(LW-HTTP)ALG をセットアップする方法を示しています。Firefox と Chrome ブラウザのみ許可するように設定します。（他のブラウザはすべて拒否されます。）

さらに、プロトコルの更新を許可します。内部ネットワークからインターネットまでのトラフィックを許可する 1 つの NAT IP ルールが既に設定されているものとします。このルールを int_to_ext_http_ と呼びます。

CLI

まず、LW-HTTP ALG オブジェクトを作成します。:

```
DFL-xxxx:/> add ALG ALG_LWHTTP my_lw_http_alg AllowProtocolUpgrade=Yes UserAgentMode=AllowSelected
```

新しい ALG になるように CLI コンテキストを変更します。:

```
DFL-xxxx:/> cc ALG ALG_LWHTTP my_lw_http_alg
```

Firefox を許可する User-Agent フィルタを追加します。:

```
DFL-xxxx:/my_lw_http_alg> add ALG_HTTP_UA UserAgent=*Firefox/*
```

Chrome を許可する User-Agent フィルタを追加します。:

```
DFL-xxxx:/my_lw_http_alg> add ALG_HTTP_UA UserAgent=*Chrome/*
```

初期値の CLI コンテキストに戻します。:

```
DFL-xxxx:/my_lw_http_alg> cc
DFL-xxxx:/>
```

今度は、サービスオブジェクトを作成し、この新しい ALG に関連付けます。:

```
DFL-xxxx:/> add Service ServiceTCPUDP my_http_service Type=TCP DestinationPorts=80,443 ALG=my_lw_http_alg
```

最後に、新しいサービスを使用するために NAT IP ルールを編集します。

```
DFL-xxxx:/> set IPRule int_to_ext_http Service=my_http_service
```

Web Interface

まず、LW-HTTP ALG オブジェクトを作成します。:

1. **Objects > ALG > Add > LW-HTTP ALG** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_lw_http_alg
   - Allow Protocol Upgrade: 有効
   - User-Agent Filter Mode: Allow Selected
3. 「OK」ボタンをクリックします。

今作成した LW-HTTP ALG を編集します。:

1. my_lw_http_alg を選択します。
2. User-Agent Filter を選択します。
3. **Add > User-Agent** を選択します。
4. 以下を入力して Firefox を許可します。
   - User-Agent: *Firefox/*
   - 「OK」ボタンをクリックします。
5. **Add > User-Agent** を選択します。
6. 以下を入力して Chrome を許可します。
   - User-Agent: *Chrome/*
   - 「OK」ボタンをクリックします。
7. 「OK」ボタンをクリックします。

今度は、サービスオブジェクトを作成し、この新しい ALG に関連付けます。:

1. **Objects > Services > Add > TCP/UDP service** の順にメニューをクリックします。

2. 以下を入力します。
   - Name: my_http_service
   - Type: TCP
   - Destination Port: 80
   - ALG: my_lw_http_alg

最後に、新しいサービスを使用するために NAT IP ルールを編集します。:

1. **Policies > Firewalling > Main IP Rules** の順にメニューをクリックします。

2. IP ルール int_to_ext_http を選択します。

3. Service リストから my_http_service を選択します。

4. 「OK」ボタンをクリックします。

6.1.3 FTP ALG

概要

FTP（File Transfer Protocol）はクライアントとサーバ間でファイル交換するための TCP/IP ベースのプロトコルです。クライアントは FTP サーバに接続することで接続を開始します。通常クライアントは事前に定義したログイン名とパスワードを指定することで認証される必要があります。アクセスの許可後、サーバはファイルをダウンロードまたはアップロード可能なファイル / ディレクトリのリストをクライアントに供給します。（可能なファイルはアクセス権によって異なります。）FTP ALG は D-Link ファイアウォールを経由して FTP 接続を管理するために使用されます。

FTP 接続

FTP は制御コマンドに 1 チャンネル、実ファイルの転送に 1 チャンネルの 2 つの通信チャンネルを使用します。FTP セッションがオープンされると、FTP クライアントは FTP サーバのポート 21（初期値）への TCP 接続（制御チャンネル）を確立します。この後に発生する内容は FTP が使用されるモードによって異なります。

FTP 接続モード

FTP は「Active」と「Passive」の 2 つのモードで操作します。クライアントとサーバ間のデータチャンネルがオープンな場合、これらのモードはサーバの役割を決定します。

- Active
  FTP クライアントは FTP サーバが接続を行う IP アドレスとポートを指示したコマンドを FTP サーバに送信します。FTP サーバは受信したアドレス情報を使用して FTP クライアントに対してデータチャンネルを確立します。
- Passive
  データチャンネルはコマンドチャンネルと同じように FTP サーバに対して FTP クライアントによってオープンされます。逆を推奨する場合もありますが、本モードが多くの場合 FTP クライアントの初期モードに推奨されています。

FTP セキュリティ問題の検討

FTP 操作における「Active」と「Passive」の両モードはファイアウォールに問題を提起します。内部ネットワーク上の FTP クライアントがインターネット上の FTP サーバにファイアウォール経由で接続するシナリオをよく考えてみます。IP ルールはその時 FTP クライアントから FTP サーバ上のポート 21 にネットワークトラフィックを許可するように設定されます。

Active モードが使用される場合、NetDefendOS は FTP サーバが FTP クライアントに新しい接続を確立することを認識しません。そのため、データチャンネルに到達する通信はドロップされます。データチャンネルに使用されるポート番号がダイナミックであるため、これを解決する唯一の方法は FTP サーバの全ポートから FTP クライアントの全ポートへのトラフィックを許可することです。明らかにこれはよい解決方法ではありません。

Passive モードが使用される場合、ファイアウォールは FTP サーバからの接続を許可する必要がありません。一方 NetDefendOS は FTP クライアントがデータチャンネルのために使用しようとするポートが何かをまだ知りません。これはファイアウォールが FTP クライアントの全ポートから FTP サーバの全ポートへのトラフィックを許可することを意味します。これはアクティブモードと同じく安全でないというわけではありませんが、セキュリティにとっての脅威となる可能性を提供しています。また、すべての FTP クライアントが Passive モードを使用できるというわけではありません。

NetDefendOS ALG ソリューション

NetDefendOS FTP ALG はコマンドチャンネルの TCP ストリームを完全に再組み立てし、その内容を検査することによってこの問題を解決します。これを行うことによって、NetDefendOS はデータチャンネルのためにオープンするポート番号を知ることができます。さらに、特定の制御コマンドをフィルタし、基本バッファのオーバランを防御する機能を提供します。

ハイブリッドモード

NetDefendOS FTP ALG の最も重要な機能はアクティブモードとパッシブモード間を自動で高速に切り替える固有の機能で、FTP 接続モードを組み合わせることができます。パッシブモードはファイアウォールの 1 つの側面で使用され、アクティブモードは別の側面で使用されます。このタイプの FTP ALG 使用法はハイブリッドモードと呼ばれることもあります。

ハイブリッドモードの利点を以下の通り要約することができます。

- FTP クライアントは、クライアントに推奨されるモードであるパッシブモードを使用するように設定できます。
- FTP サーバは、サーバのためにより安全であるアクティブモードを使用するように設定できます。
- FTP セッションが確立されると、ファイアウォールは自動的および透過的に FTP クライアントからパッシブデータチャンネルを、またサーバからアクティブデータチャンネルを受信し、正しくそれらを結合します。

この実装により、FTP クライアントと FTP サーバの両方が最も安全なモードで動作できます。もちろん、この切り替えは他の方法、すなわちアクティブモードを使用した FTP クライアントやパッシブモードを使用した FTP サーバとともに動作します。

以下の図では典型的なハイブリッドモードのシナリオを示しています。

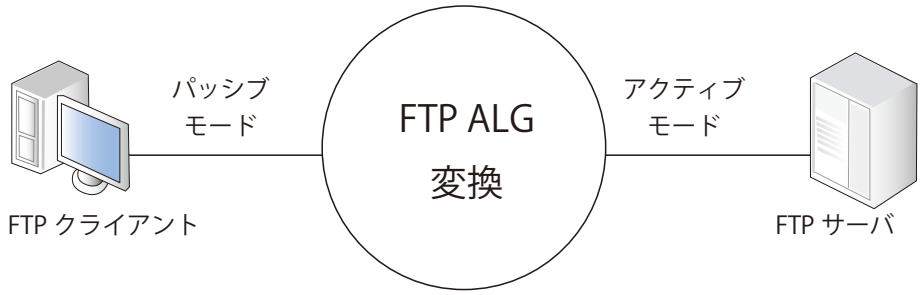


図 6-2　FTP ALG ハイブリッドモード

参照 ハイブリッドの切り替えは自動です。

ハイブリッドモードは有効にする必要はありません。モード間の切り替えは FTP ALG 内部で自動的に行われます。

Data Channel Restriction（接続制限オプション）

FTP ALG には、以下の 2 つのオプションがあり、FTP クライアントと FTP サーバが使用するモードタイプを制限します。

- **Allow client to use active mode (unsafe for client)**

  有効にすると、FTP クライアントはパッシブおよびアクティブ変換モードの両方を使用することができます。無効にすると、クライアントはパッシブモードの使用を制限されます。FTP サーバがアクティブなモードを必要とすると、NetDefendOS FTP ALG は自動的にアクティブモードに切り替えます。

  クライアントデータポートの範囲はこのオプションで指定されます。クライアントがアクティブモードを使用している場合、サーバはこれらのいずれにも接続できます。初期値は 1024-65535 です。

- **Allow server to use passive mode (unsafe for client)**

  有効にすると、FTP サーバはパッシブおよびアクティブ変換モードの両方を使用することができます。このオプションを無効にすると、サーバはパッシブモードのデータチャンネルを受信しません。クライアントがパッシブモードを使用している場合、NetDefendOS は自動的に切り換えを行います。

  サーバデータポートの範囲はこのオプションで指定されます。クライアントがパッシブモードを使用している場合、サーバはこれらのいずれにも接続できます。初期値は 1024-65535 です。

これらのオプションは、ハイブリッドモードが接続を終了するかどうかを検証することができます。例えば、クライアントがパッシブモードで接続しているが、サーバに許可されていないと、ハイブリッドモードは自動的に使用され、FTP ALG は 2 つのモード間の切り替えを実行します。

NetDefendOS バージョン 11.01 以前の定義済み FTP ALG とサービス

NetDefendOS の以前のバージョンでは、クライアント / サーバモード制限の異なる組み合わせによって 4 つの定義済み FTP ALG と Service オブジェクトを提供していました。これらの ALG と Service オブジェクトの名称は以下の通りです。

項目	説明
ftp-inbound	クライアントはどんなモードも使用できますが、サーバはパッシブモードを使用できません。
ftp-outbound	クライアントはアクティブモードを使用できませんが、サーバはどんなモードも使用できます。
ftp-passthrough	クライアントとサーバの両方ともどんなモードも使用できます。
ftp-internal	クライアントはアクティブモードを使用できません。また、サーバはパッシブモードを使用できません。

NetDefendOS バージョン 11.01 以降、新しい NetDefendOS インストールからこれらの各サービスが削除されています。しかし、11.01 以降にアップグレードする構成には残っています。新しいインストールでは手動で再度設定できますが、お勧めのオプションは定義済みの IP Policy オブジェクトを持つ ftp サービスを利用することです。その場合、以前に ALG で利用可能であったすべてのオプションが、直接ポリシーで利用可能です。

FTP ALG Command Restriction（FTP ALG コマンドの制限）

FTP プロトコルはサーバとクライアント間に送信される 1 セットの標準コマンドから構成されています。NetDefendOS FTP ALG は認識しないコマンドを見つけると、そのコマンドをブロックします。このブロックは、明示的に解除される必要があります。ブロックの解除のためのオプションは以下の通りです。

- **Allow unknown commands**
  未知の FTP コマンドを許可します。これらは ALG が標準セットの一部と見なさないコマンドです。

- **Allow SITE EXEC**
  クライアントが FTP サーバに送信する SITE EXEC コマンドを許可します。

- **Allow RESUME even in case of content scanning**
  コンテンツのスキャンが接続を終了しても、RESUME コマンドを許可します。

いくつかのコマンドは決して許可されません。

暗号化を指示するようないくつかのコマンドは許可されません。暗号化は、ALG が FTP コマンドのチャンネルを検証できず、ダイナミックなデータチャンネルをオープンできなかったことを意味します。
以下は ALG で許可されないコマンド一覧です。

- CLNT
- MLST
- MLSD
- FILT
- EPRT
- EPSV
- AUTH
- ADAT
- PBSZ
- PROT
- CCC
- MIC
- CONF
- ENC

Control Channel Restriction（制御チャンネルの制限）

FTP ALG により、FTP 制御チャンネルに対して制限を設定することで、FTP 接続のセキュリティを向上させることも可能です。オプションは以下の通りです。

- **Maximum line length in control channel**
  非常に大きい制御チャンネルコマンドの作成は、バッファオーバフローを引き起こしてサーバを攻撃する方法として使用されます。本設定による制限はこの脅威と戦います。初期値は 256（秒）です。

  サーバに非常に長いファイル名またはディレクトリ名が使用されると、この制限を長くする必要があるかもしれません。制限が短いほど、セキュリティは向上します。

- **Maximum number of commands per second**
  FTP サーバに対して自動化された攻撃を防ぐために、コマンドの回数を制限することは効果があります。制限の初期値は 20 コマンド / 秒です。

- **Allow 8-bit strings in control channel**
  8 ビット文字を制御チャンネルで許可するかどうか決定します。8 ビット文字を許可すると、国際文字を含むファイル名のサポートが有効になります。例えば、アクセント記号やウムラウト記号です。

FTP 転送のファイルタイプの検査

IP ポリシーでファイルタイプの検査を設定するには、ファイルコントロールプロファイルを定義し、FTP 転送を許可する IP ポリシーに紐づける必要があります。詳細は、「6.5 ファイルコントロール」を参照してください。

FTP 転送のアンチウィルススキャン

NetDefendOS アンチウィルスサブシステムを有効にすると、すべての FTP ダウンロードに対して不正なコードを検索します。疑わしいファイルを破棄、またはログに出力のみ行うことができます。

詳しくは「6.4 アンチウィルススキャン」に詳しく記述されています。

Passive モードで FTP サーバをセットアップする

FTP サーバの設定に関して、FTP ALG が Passive モードで使用される場合に注意が必要です。
通常、FTP サーバは D-Link ファイアウォールの後方で保護され、インターネット経由の外部クライアントからの通信が NetDefendOS によって SAT Allow ポリシーで許可されます。FTP の Passive モードが有効化され、このモードでクライアントが接続する場合、FTP サーバからクライアントに対して IP アドレスとポートが返され、それに基づいてデータ転送通信がセットアップされます。

この IP アドレスは、基本的には管理者が FTP サーバソフトウェアに対して手動で設定し、通常はインターネットに接続するファイアウォールのインタフェース外部 IP アドレスを指定します。FTP ALG を使用する場合は、FTP サーバを設定する際に FTP サーバのローカルの内部 IP アドレスを指定する必要があります。

ZoneDefense と FTP ALG

ZoneDefense は、特定のタイプの外部ネットワークスイッチに管理コマンドを送信することで、NetDefendOS がホストとネットワークをブロックできる機能です。FTP ALG と一緒に使用される場合、ZoneDefense は、ウィルスなど有害ソフトの拡散からネットワークを保護するために設定されます。

これは以下の 2 つのシナリオに関連しています。
- A - ブロックする必要がある感染したクライアント。
- B - ブロックする必要がある感染したサーバ。

A. 感染したクライアントのブロック
管理者は、ネットワークのローカルホストを含むようにネットワーク範囲を設定します。ローカルなクライアントが、ウィルス感染ファイルを FTP サーバにアップロードしようとすると、NetDefendOS は、クライアントがローカルネットワークに所属することに気付いて、ブロックする指示をローカルなスイッチにアップロードします。ホストは、ローカルネットワークへのアクセスをブロックされて、もはや危害を加えることができなくなります。

注意 ZoneDefense は感染したサーバをブロックしません。
クライアントがインターネット上のリモート FTP サーバから感染ファイルをダウンロードする場合、そのサーバは、設定されているネットワークの範囲外にあるため、ZoneDefense によってブロックされません。しかし、ウィルスはファイアウォールによってブロックされます。

B. 感染サーバのブロック
会社の方針によっては、管理者はローカルホストとサーバを感染から防御するために感染した FTP サーバをオフラインすることを希望するかもしれません。このシナリオでは、管理者は、サーバのアドレスをブロックするネットワーク範囲に設定します。クライアントが感染ファイルをダウンロードする場合、サーバはネットワークから隔離されます。

FTP ALG を使用した ZoneDefense 設定手順は以下の通りです。

- Web インタフェースの ZoneDefense セクションの ZoneDefense で使用される ZoneDefense スイッチを設定します。
- 有効なアンチウィルススキャンを使用するために FTP ALG を設定します。
- ウィルスが検出される場合に ZoneDefense によって影響を受ける ALG のアンチウィルス設定で ZoneDefense ネットワークを選択します。

本機能に関する詳細は、「7.9 ZoneDefense」を参照してください。

FTP ALG の設定方法

FTP ALG は、以下のいずれかの方法で設定を行います。

- **IP ポリシーを使用する**
  IP ポリシーオブジェクトを使用する方法が、推奨される設定方法です。最も簡単であり、IP ルールで利用できない追加のオプションを提供しています。FTP ALG オプションは、IP ポリシーのプロパティを設定することで直接設定することができます。IP ポリシーで FTP オプションを設定するには、ポリシーの Service プロパティに指定したサービスの Protocol プロパティが FTP に設定されている必要があります。

- **IP ルールを使用する**
  IP ルールオブジェクトを使用する場合、FTP ALG オブジェクトをサービスオブジェクトに割り当て、それを IP ルールに割り当てます。
  この方式は古い NetDefendOS バージョンとの互換性を保つ場合に役に立ちますが、IP ポリシーと比較して利点はありません。

IP ポリシーを使用した FTP ALG のセットアップ

IP ポリシーを使用して FTP ALG を設定するには、以下の手順を実行します。

1. FTP 用の新しいサービスオブジェクトを作成し、プロトコルプロパティに FTP を指定します。もしくは、プロトコルプロパティが FTP に設定されているのであれば、定義済み FTP サービスオブジェクト「ftp」を使用することも可能です。

2. ターゲットのトラフィックに対して起動される新しい IP ポリシーを作成し、そのサービスプロパティを手順 1 で作成したサービスに設定します。これにより、IP ポリシーですべての FTP ALG オプションがる利用可能となります。これらのプロパティを適切に設定します。

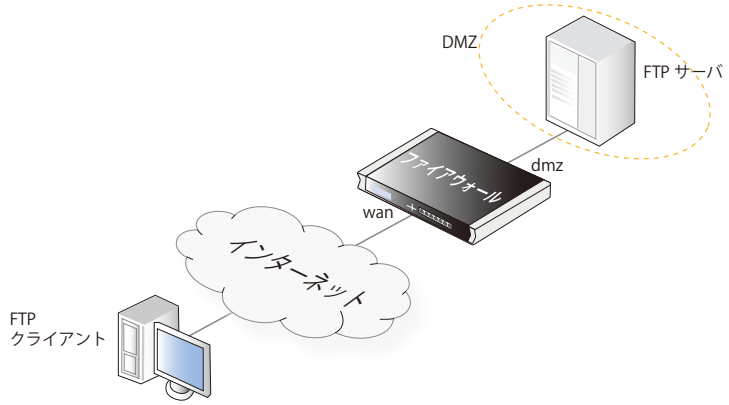
3. 必要に応じてその他の機能を IP ポリシーで設定します。例えば、ファイル制御を行うファイルコントロールポリシーオブジェクトや、ファイルに対してアンチウイルススキャンを行うアンチウイルスプロファイルを設定します。

次の 2 つの例題では FTP クライアント / サーバ保護のための IP ポリシーを使用した FTP ALG の設定手順です。

例題 6.5

IP ポリシーを使用した FTP ALG 設定による FTP サーバの保護

以下の図で示すように、FTP サーバは、DMZ 上の D-Link ファイアウォールに接続し、プライベートな IPv4 を持っています。この例では、FTP ALG オブジェクトを使用してサーバを保護する方法を示しています。



以下のように FTP ALG 制限を設定します。

- 「Allow client to use active mode」を有効にすると、クライアントがアクティブおよびパッシブ両方を使用できるような FTP ALG オプションを使用します。
- 「Allow server to use passive mode」を無効にします。これは、パッシブモードのデータを受信しないため、サーバにとってより安全と言えます。クライアントがパッシブモードを使用して接続すると、FTP ALG はすべての変換を行います。

FTP サーバのプライベート IPv4 アドレスがアドレス帳に定義済みで、名前は ftp-internal であるものとします。

CLI

A. サービスを定義する :

```
DFL-xxxx:/> add Service ServiceTCPUDP ftp-inbound-service DestinationPorts=21 Type=TCP Protocol=FTP
```

B. ポート 21 上のパブリック IP への接続を許可し、内部 FTP サーバに転送する SAT ポリシーを定義します。:

```
DFL-xxxx:/> add IPPolicy Name=sat-ftp-inbound SourceInterface=any SourceNetwork=all-nets
            DestinationInterface=core DestinationNetwork=wan_ip Service=ftp-inbound-service Action=Allow
            SourceAddressTranslation=None DestAddressTranslation=SAT DestAddressAction=SingleIP DestNewIP=ftp-
            internal FTPControl=Yes FTPAllowServerPassive=Yes FTPAllowClientActive=Yes
```

C. 内部インタフェースからのトラフィックはパブリック IPv4 アドレスを経由して NAT する必要があります。:

```
DFL-xxxx:/> add IPPolicy Name=nat-ftp SourceInterface=dmz SourceNetwork=dmznet DestinationInterface=core
            DestinationNetwork=wan_ip Service=ftp-inbound-service Action=Allow SourceAddressTranslation=NAT
            NATSourceAddressAction=OutgoingInterfaceIP FTPControl=Yes FTPAllowServerPassive=Yes
            FTPAllowClientActive=Yes
```

Web Interface

A. サービスを定義する :

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

- Name : ftp-inbound-service
- Type : TCP
- Destination : 21
- Protocol: FTP

B. ポート 21 上のパブリック IP への接続を許可し、内部 FTP サーバに転送する SAT ポリシーを定義します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ **General タブ**

General

- Name : sat-ftp-inbound
- Action : Allow

Address Filter
- Interface - Source : any
- Interface - Destination : core
- Network - Source : all-nets
- Network - Destination : wan1_ip
- Service : ftp-inbound-service

Source Translation
- Address Translation: None

Destination Translation
- Address Translation: SAT
- Address Action: Single IP
- New IP Address : ftp-internal

◇ **FTP タブ**
- Use custom FTP settings: ON
- Allow active mode for client: Enabled
- Allow passive mode for server: Enabled

C. 内部インタフェースからのトラフィックを 1 つのパブリック IPv4 アドレスを経由して NAT する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ **General タブ**

General
- Name : nat-ftp
- Action : Allow

Souce Interface
- Interface - Source : dmz
- Interface - Destination : core
- Network - Source : dmznet
- Network - Destination : wan_ip
- Service : ftp-inbound-service

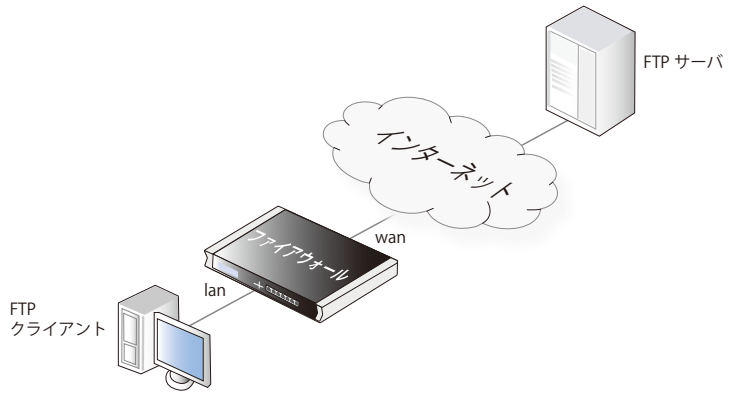
Source Transelation
- Address Translation: NAT
- Address Action: Outgoing Interface IP

◇ **FTP タブ**
- Use custom FTP settings: ON
- Allow active mode for client: Enabled
- Allow passive mode for server: Enabled

例題 6.6

IP ポリシーを使用した FTP ALG による FTP クライアントの保護

以下の図で示すように、FTP サーバは、DMZ 上のファイアウォールに接続し、プライベートな IPv4 を持っています。この例では、FTP ALG オブジェクトを使用しクライアントを保護する方法を示しています。



以下のように FTP ALG 制限を設定します。

- 「Allow active mode for client」を無効にすると、クライアントはパッシブモードだけを使用するような FTP ALG オプションを使用します。クライアントにとって、この方法がはるかに安全です。
- 「Allow passive mode for server」を有効にすると、内側のクライアントはインターネットを経由してアクティブおよびパッシブモードをサポートする FTP サーバに接続することができます。

CLI

A. FTP サービスを定義する :

```
DFL-xxxx:/> add Service ServiceTCPUDP ftp-outbound-service DestinationPorts=21 Type=TCP Protocol=FTP
```

B. IP ポリシーを作成する :

IP ルールは、FTP トラフィックが通過できるように作成される必要があります。また、それらはプライベートまたはパブリック IP アドレスが使用されるかどうかによって異なります。

i. パブリック IP を使用する :

パブリック IP を使用する場合、これらのルールの前に同じ種類のポート / トラフィックを許可する、または許可しないというエントリがないことを確認します。

```
DFL-xxxx:/> add IPPolicy Name=allow-ftp-outbound SourceInterface=lan SourceNetwork=lannet
            DestinationInterface=wan DestinationNetwork=all-nets Service=ftp-outbound-service Action=Allow
            SourceAddressTranslation=None FTPControl=Yes FTPAllowServerPassive=Yes FTPAllowClientActive=No
```

ii. プライベート IP を使用する :

ファイアウォールが 1 つの外部パブリック IP を使用したプライベート IP を使用している場合、以下の NAT IP ルールを上記ルールの代わりに追加する必要があります。

```
DFL-xxxx:/> add IPPolicy Name=nat-ftp-outbound SourceInterface=lan SourceNetwork=lannet
            DestinationInterface=wan DestinationNetwork=all-nets Service=ftp-outbound-service Action=Allow
            SourceAddressTranslation=NAT NATSourceAddressAction=OutgoingInterfaceIP FTPControl=Yes
            FTPAllowServerPassive=Yes FTPAllowClientActive=No
```

Web Interface

A. FTP サービスを定義する :

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

   - Name : ftp-outbound-service
   - Type : TCP
   - Destination : 21
   - Protocol: FTP

B. IP ポリシーを作成する :
IP ルールは、FTP トラフィックが通過できるように作成される必要があります。また、それらはプライベートまたはパブリック IP アドレスが使用されるかどうかによって異なります。

i. パブリック IP を使用する :
パブリック IP を使用する場合、これらのルールの前に同じ種類のポート / トラフィックを許可する、または許可しないというエントリがないことを確認します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。
◇ General タブ
General
- Name : sat-ftp-outbound
- Action : Allow

Address Filter
- Interface - Source : lan
- Interface - Destination : wan
- Network - Source : lannnet
- Network - Destination : all-nets
- Service : ftp-outbound-service

Source Transelation
- Address Translation: None

◇ FTP タブ
- Use custom FTP settings: ON
- Allow active mode for client: Disabled
- Allow passive mode for server: Enabled

ii. プライベート IP を使用する :
ファイアウォールが 1 つの外部パブリック IP を使用したプライベート IP を使用している場合、以下の NAT IP ポリシーを上記ポリシーの代わりに追加する必要があります。
1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ General タブ
General
- Name : nat-ftp-outbound
- Action : Allow

Address Filter
- Interface - Source : lan
- Interface - Destination : wan
- Network - Source : lannnet
- Network - Destination : all-nets
- Service : ftp-outbound-service

Source Transelation
- Address Translation: NAT
- Address Action: Outgoing Interface IP

◇ FTP タブ
- Use custom FTP settings: ON
- Allow active mode for client: Disabled
- Allow passive mode for server: Enabled

IP ルールを使用した FTP ALG の設定

FTP ALG の設定で IP ポリシーを使用する代わりに IP ルールを使用することもできます。以下の手順が必要となります。
1. 必要なオプションを設定した FTP ALG オブジェクトを作成します。

2. FTP 用の新しいカスタムサービスオブジェクトを作成し、その ALG プロパティに、手順 1 で作成したオブジェクトを設定します。

3. 1 つ前の手順で設定したサービスを使用する IP ルールを作成します。SAT アドレス変換には複数のルールが必要です。

次の 2 つの例題は、FTP クライアント / サーバ保護のための IP ルールを使用した FTP ALG の設定手順です。IP ポリシーを使用した 1 つ前の例題と同等の内容です。

例題 6.7

IP ルールを使用した FTP ALG 設定による FTP サーバの保護

この例題は、「IP ポリシーを使用した FTP ALG 設定による FTP サーバの保護」と同等の内容ですが、IP ポリシーの代わりに IP ルールを使用しています。

CLI

A. ALG を定義する :

```
DFL-xxxx:/> add ALG ALG_FTP ftp-inbound AllowClientActive=Yes AllowServerPassive=Yes
```

B. サービスを定義する :

```
DFL-xxxx:/> add Service ServiceTCPUDP ftp-inbound-service DestinationPorts=21 Type=TCP ALG=ftp-inbound
```

C. ポート 21 上のパブリック IP への接続を許可し、内部 FTP サーバに転送する SAT ルールを定義します。:

```
DFL-xxxx:/> add IPRule Action=SAT Service=ftp-inbound-service SourceInterface=any SourceNetwork=all-nets
            DestinationInterface=core DestinationNetwork=wan_ip SATTranslate=DestinationIP
            SATTranslateToIP=ftp-internal Name=SAT-ftp-inbound
```

D. 内部インタフェースからのトラフィックはパブリック IPv4 アドレスを経由して NAT する必要があります。:

```
DFL-xxxx:/> add IPRule Action=NAT SourceInterface=dmz SourceNetwork=dmznet DestinationInterface=core
            DestinationNetwork=wan_ip Service=ftp-inbound-service NATAction=UseInterfaceAddress Name=NAT-ftp
```

E. 内向き接続を許可する（SAT には関連した Allow ルールが必要です。）:

```
DFL-xxxx:/> add IPRule Action=Allow SourceInterface=any SourceNetwork=all-nets DestinationInterface=core
            DestinationNetwork=wan_ip Service=ftp-inbound-service Name=Allow-ftp
```

Web Interface

A. ALG を定義する :

（ALG ftp-inbound が NetDefendOS によって定義済みですが、この例では、最初から作成する方法を示しています。）

1. **Objects > ALG > Add > FTP ALG** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : ftp-inbound-ex
- Allow client to use active mode : チェックします。
- Allow server to use passive mode : チェックを外します。

B. サービスを定義する :

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : ftp-inbound-ex
- Type : TCP
- Destination : 21（FTP サーバがあるポート）

Application Layer Gateway

- ALG : 上で作成した「ftp-inbound-ex」を選択します。

C. ポート 21 上のパブリック IP への接続を許可し、内部 FTP サーバに転送する SAT ルールを定義します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ **General タブ**

General

- Name : SAT-ftp-inbound-ex
- Action : SAT
- Service : ftp-inbound-ex

Address Filter

- Interface - Source : any
- Interface - Destination : core
- Network - Source : all-nets
- Network - Destination : wan1_ip

Static Address Translation

- SAT translate : Destination IP を選択します。
- New IP Address : ftp-internal
- New Port : 21

D. 内部インタフェースからのトラフィックを 1 つのパブリック IPv4 アドレスを経由して NAT する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ General タブ

General

- Name : NAT-ftp
- Action : NAT
- Service : ftp-inbound-ex

Address Filter

- Interface - Source : dmz
- Interface - Destination : core
- Network - Source : dmznet
- Network - Destination : wan1_ip

Network Address Translation

- NAT action: Use interface address を選択します。

E. incoming 接続を許可する（SAT には 2 つ目の Allow ルールが必要です。）:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : Allow-ftp
- Action : Allow
- Service : ftp-inbound-ex

Address Filter

- Interface - Source : any
- Interface - Destination : core
- Network - Source : all-nets
- Network - Destination : wan1_ip

例題 6.8

IP ルールを使用した FTP ALG による FTP クライアントの保護

この例題は、「IP ポリシーを使用した FTP ALG による FTP クライアントの保護」と同等の内容ですが、IP ポリシーの代わりに IP ルールを使用しています。

CLI

A. ALG を定義する :

```
DFL-xxxx:/> add ALG ALG_FTP ftp-outbound AllowClientActive=Yes AllowServerPassive=Yes
```

B. FTP サービスを定義する :

```
DFL-xxxx:/> add Service ServiceTCPUDP ftp-outbound-service DestinationPorts=21 Type=TCP ALG=ftp-outbound
```

C. IP ルールを作成する :

IP ルールは、FTP トラフィックが通過できるように作成される必要があります。また、それらはプライベートまたはパブリック IP アドレスが使用されるかどうかによって異なります。

i. *パブリック IP を使用する :*

パブリック IP を使用する場合、これらのルールの前に同じ種類のポート / トラフィックを許可する、または許可しないというルールがないことを確認します。

```
DFL-xxxx:/> add IPRule Action=Allow SourceInterface=lan SourceNetwork=lannet DestinationInterface=wan
            DestinationNetwork=all-nets Service=ftp-outbound-service Name=Allow-ftp-outbound
```

ii. *プライベート IP を使用する :*

ファイアウォールが 1 つの外部パブリック IP を使用したプライベート IP を使用している場合、以下の NAT ルールを上記ルールの代わりに追加する必要があります。

```
DFL-xxxx:/> add IPRule Action=NAT SourceInterface=lan SourceNetwork=lannet DestinationInterface=wan
            DestinationNetwork=all-nets Service=ftp-outbound-service NATAction=UseInterfaceAddress
            Name=NAT-ftp-outbound
```

Web Interface

A. FTP ALG を作成する :

（ALG ftp-outbound が NetDefendOS によって定義済みですが、この例では、最初から作成する方法を示しています。）

1. **Objects > ALG > Add > FTP ALG** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : ftp-outbound

Data Channel Restrictions

- Allow client to use active mode : チェックを外します。
- Allow server to use passive mode : チェックします。

B. FTP サービスを定義する :

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : ftp-outbound-service
- Type : TCP
- Destination : 21（FTP サーバにあるポート）
- ALG : ftp-outbound（作成済みの ALG）

C. IP ルールの作成

IP ルールは、FTP トラフィックが通過できるように作成されます。また、それらは プライベートまたはパブリック IPv4 アドレスが使用されるかどうかによって異なります。

i. *パブリック IP を使用する*

パブリック IP を使用する場合、これらのルールの前に定義したのと同じ種類のポート / トラフィックを許可する、または許可しないというルールがないことを確認します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : Allow-ftp-outbound
- Action : Allow

- Service : ftp-outbound-service

Address Filter

- Interface - Source : lan
- Interface - Destination : wan
- Network - Source : lannet
- Network - Destination : all-nets

ii. *ルール（プライベート IP を使用する）*

ファイアウォールが 1 つの外部パブリック IP を持つプライベート IP を使用している場合、以下の NAT ルールを IP ルールの代わりに追加する必要があります。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ **General タブ**

General

- Name : NAT-ftp-outbound-ex
- Action : NAT
- Service : ftp-outbound-ex

Address Filter

- Interface - Source : lan
- Interface - Destination : wan
- Network - Source : lannet
- Network - Destination : all-nets

Network Address Translation

- NAT action: Use interface address を選択します。

6.1.4 TFTP ALG

概要

TFTP（TrivialFileTransferProtocol）は、限定的な機能を持つ FTP のより簡易なバージョンです。その目的は、クライアントがホストシステムからファイルをアップロードまたはファイルをダウンロードすることを可能にすることです。

TFTP データ伝送は、UDP プロトコルに基づき、UDP にあるトランスポートおよびセッション制御プロトコルを提供します。
TFTP は、ネットワーク装置でソフトウェアを更新し、設定をバックアップするために企業環境で広く使用されます。TFTP は本来セキュアでないプロトコルであるとして認識されており、使用は通常内部のネットワークに制限されます。NetDefendOS ALG は、TFTP に対してセキュリティの追加レイヤを提供することで、その使用を制限することができます。

TFTP ALG の設定方法

TFTP ALG は、以下のいずれかの方法で設定を行います。

- **IP ポリシーを使用する**
  IP ポリシーオブジェクトを使用する方法が、推奨される設定方法です。最も簡単であり、IP ルールで利用できない追加のオプションを提供しています。TFTP ALG オプションは、IP ポリシーのプロパティを設定することで直接設定することができます。IP ポリシーで TFTP オプションを設定するには、ポリシーの Service プロパティに指定したサービスの Protocol プロパティが TFTP に設定されている必要があります。

- **IP ルールを使用する**
  IP ルールオブジェクトを使用する場合、TFTP ALG オブジェクトをサービスオブジェクトに割り当て、それを IP ルールに割り当てます。
  この方式は古い NetDefendOS バージョンとの互換性を保つ場合に役に立ちますが、IP ポリシーと比較して利点はありません。本セクションでは特に説明を行いません。

IP ポリシーを使用した TFTP ALG のセットアップ

このセクションでは、IP ポリシーを使用した TFTP ALG を設定について説明します。本設定は以下の手順を実行します。

1. 定義済みの tftp サービスをコピーして新しいサービスオブジェクトを作成し、プロトコルプロパティを TFTP に指定します。もしくは、定義済みのサービス「tftp」のプロトコルプロパティに TFTP を指定して使用します。

2. ターゲットのトラフィックに対して起動される新しい IP ポリシーを作成し、そのサービスプロパティを手順 1 で作成したサービスに設定します。これにより、IP ポリシーですべての TFTP オプションが利用可能となります。これらのプロパティを適切に設定します。

3. IP ポリシーの関連プロパティを編集して TFTP ALG の動作を調整します。利用可能なオプションについては下記で説明します。

Command restrictions

項目	説明
Allow both read (Get) and write (Put)	読み取り（GET コマンド）および書き込み（PUT コマンド）を許可します。
Allow only read	読み取り（GET コマンド）を許可します。
Allow only write	書き込み（PUT コマンド）を許可します。

Options restrictions

項目	説明
Remove options	オプションをリクエストから削除するかどうかを指定します。初期値は、「False」で削除しないことを意味します。
Allow unknown options	無効な場合、ブロックサイズ、タイムアウト時間、およびファイル転送サイズ以外のリクエスト内のオプションをブロックします。初期値では無効です。
Max blocksize	許可される最大ブロックサイズを指定します。許容範囲は 0-65464（バイト）です。初期値は 65464（バイト）です。

Other restrictions

上で説明した「Remove options」が「False」（オプションは削除されない）に設定されている場合、以下のリクエストオプション設定が適用されます。

項目	説明
Block directory traversal	このオプションは、連続したピリオド（".."）を含むファイル名の使用によりディレクトリトラバーサルを禁止することができます。
Max file transfer size	ファイル転送の最大サイズを制限することができます。初期値は、999,999（KBytes）で許可される絶対最大値です。

繰り返し送信されるリクエスト

NetDefendOS TFTP ALG は、一定期間に同じ送信元アドレス / ポートから繰り返し送信される TFTP リクエストをブロックします。これは、TFTP クライアントによっては適切なタイムアウト期間を持たずに同じ送信元ポートからリクエストを発行する場合があるためです。

例題 6.9

IP ポリシーを使用した TFTP ALG 設定

この例題では、インターネットから DMZ 上の Web サーバへの Read-Only TFTP 接続が許可されます。D-Link ファイアウォールは、IP アドレスとしてアドレスオブジェクト wan_ip を持つ wan インタフェースを経由してインターネットに接続します。Web サーバにはプライベート IPv4 アドレス 198.168.0.1 が割り振られているため、wan インタフェースに到達する接続は SAT 変換の対象となります。

事前定義済みの NetDefendOS サービス tftp が使用されますが、このプロトコルプロパティを最初に適切に設定する必要があります。

CLI

tftp サービスのプロトコルプロパティを設定する :

```
DFL-xxxx:/> set Service ServiceTCPUDP tftp Protocol=TFTP
```

TFTP 用の SAT IP ポリシーを作成する :

```
DFL-xxxx:/> add IPPolicy Name=SAT_TFTP_To_DMZ SourceInterface=wan SourceNetwork=all-nets
            DestinationInterface=core DestinationNetwork=wan_ip Service=tftp Action=Allow
            SourceAddressTranslation=None DestAddressTranslation=SAT DestAddressAction=SingleIP Dest-
            NewIP=192.168.0.1 TFTPControl=Yes TFTPAllowedCommands=ReadOnly
```

Web Interface

tftp サービスのプロトコルプロパティを設定する :

1. **Objects > Services** の順にメニューをクリックします。
2. tftp を選択します。
3. Protocol に TFTP を指定します。
4. 「OK」ボタンをクリックします。

TFTP 用の SAT IP ポリシーを作成する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ **General タブ**

General

- Name : SAT_TFTP_To_DMZ
- Action : Allow

Address Filter

- Source Interface: wan
- Source Network: all-nets
- Destination Interface: core
- Destination Network: wan_ip
- Service : tftp

Source Transelation

- Address Translation: None

Destination Transelation

- Address Translation: SAT
- Address Action: Single IP
- New IP Address : 10.0.0.5

◇ **TFTP タブ**

- Use custom TFTP settings: ON
- Allow read: Enabled

6.1.5 SMTP ALG

概要

Simple Mail Transfer Protocol（SMTP）は、インターネット経由で E-mail を送信するために使用されるテキストベースのプロトコルです。通常、ローカルメールサーバは、DMZ に置かれるため、リモート SMTP サーバが送信したメールは、ローカルサーバに到達するように D-Link ファイアウォールを横断します。

ファイアウォールの背後にあるローカルクライアントは、E メールクライアントソフトを使用してサーバからメールを受信し、パブリックインターネット上の他のメールサーバに送信するためにメールをサーバに送信します。様々なプロトコルがクライアントとメールサーバ間の通信に使用される可能性があります。マイクロソフト ActiveSync™ は一般的に利用されています。また、受信は POP3 または IMAP プロトコルで行われますが、サーバへのメールの送信は SMTP が使用されます。これらの疎通は以下のように図示されます。

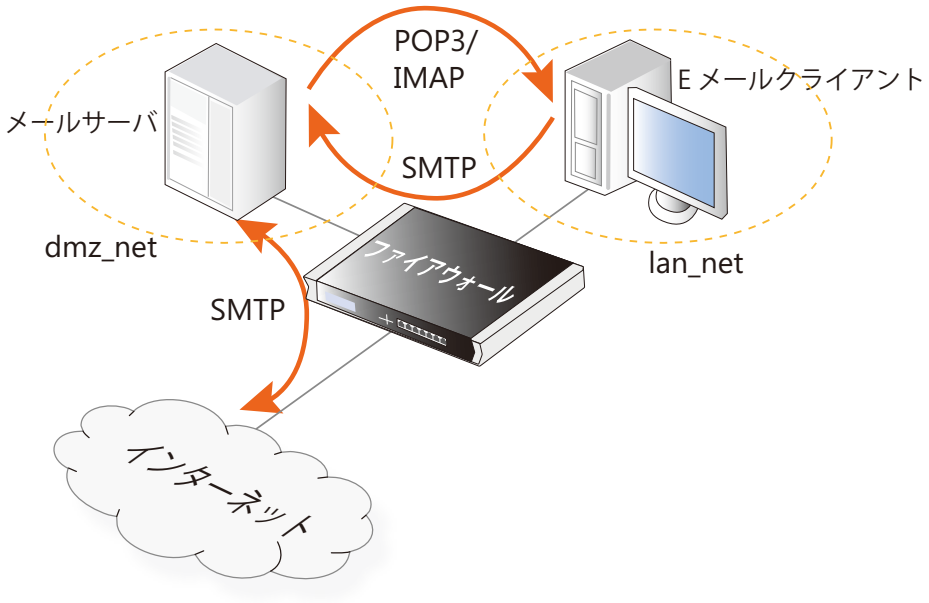


図 6-3　SMTP ALG の利用方法

SMTP ALG は、クライアントとサーバ間と同様にメールサーバ間の SMTP トラフィックを処理するのに使用されます。典型的なメール送信の順序は以下の通りです。

1. ローカルユーザはメールサーバにメールを送信します。この送信は、SMTP、Microsoft Activesync™、または他のプロトコルを使用して行われます。
2. ローカルなメールサーバは宛先ドメイン名に関する DNS ルックアップを実行し、メールを転送するリモートメールサーバの IP アドレスを決定します。
3. SMTP を使用してメールをリモートサーバに転送します。
4. リモートユーザは、POP3、IMAP、Activesync または他のプロトコルを使用してリモートメールサーバからのメールを受信します。

SMTP ALG の最も一般な使用はパブリックインターネットからメールサーバに送出されるメールトラフィックを調べることであり、これは後ほど例題で説明します。しかし、マルウェアが、保護されたクライアント、そして / またはメールサーバのいずれかを感染させる可能性があります。その場合、クライアントから送出されるメールトラフィック、および（または）メールサーバがパブリックインターネットにリレーするメールトラフィックをモニタするのに SMTP ALG を使用できます。

SMTP ALG の設定方法

SMTP ALG は、以下のいずれかの方法で設定を行います。

• IP ポリシーを使用する

IP ポリシーオブジェクトを使用する方法が、推奨される設定方法です。最も簡単であり、IP ルールで利用できない追加のオプションを提供しています。IP ポリシーで SMTP オプションを設定するには、ポリシーの Service プロパティに指定したサービスの Protocol プロパティが SMTP に設定されている必要があります。

• IP ルールを使用する

IP ルールオブジェクトを使用する場合、SMTP ALG オブジェクトをサービスオブジェクトに割り当て、それを IP ルールに割り当てます。

この方式は古い NetDefendOS バージョンとの互換性を保つ場合に役に立ちますが、IP ポリシーと比較して利点はありません。

IP ポリシーを使用した SMTP ALG のセットアップ

IP ポリシーを使用して SMTP ALG をセットアップするには、以下の手順を実行します。

1. 以下のプロパティを持つ SMTP の新しいカスタム Service オブジェクトを作成します。

プロパティ	説明
Type	TCP
Destination:	25
Syn Flood Protection	トラフィックがインターネットから来る場合、Syn Flood Protection を有効にします。これを無効にすると、NetDefendOS のリソースはあまり使用しませんが、DoS（denial-of-service）攻撃が起こりにくい場合にのみ無効にしてください。

あるいは、定義済みサービス smtp のプロトコルプロパティを SMTP に指定し、使用することも可能です。
定義済みサービス smtmp-in は、SYN Flood Protection オプションが有効化されていることを除いて smtp と同等です。

2. ターゲットトラフィックに対して起動される新しい IP ポリシーオブジェクトを作成し、そのサービスプロパティで上記のカスタムサービスを指定します。これにより、IP ポリシーですべての SMTP ALG オプションが利用可能になります。

IP ポリシーの送信元 / 送信先フィルタは以下のいずれかに指定します。

i. SMTP を使用してクライアントからサーバにメールを送信するためには、送信元がクライアントで宛先がメールサーバとなります。
ii. インターネットからサーバにメールを送信するためには、宛先がメールサーバで、送信元がインターネットとなります。メールサーバに自身のパブリック IP アドレスがない場合、パブリック IP アドレスをサーバのプライベートアドレスに変換するために SAT アドレス変換が必要です。
iii. メールサーバによりクライアントからのメールをインターネットに送信するためには、サーバが送信元でインターネットが宛先となります。

3. 新しい E メールコントロールプロファイルを作成、設定し、IP ポリシーに割り当てます。

4. オプションで、新しく作成したファイルコントロールプロファイルおよび（または）アンチウイルスプロファイルを割り当てて、それらの機能を SMTP トラフィックに適用することも可能です。IP ポリシーでアプリケーションコントロールを設定することもできます。

SMTP ALG オプション

IP ポリシーを使用する場合、E メールコントロールプロファイルオブジェクトをポリシーに紐づけることで SMTP ALG を有効化することができます。SMTP の E メールコントロールプロファイルでは以下のオプションが設定可能です。

SMTP ALG の主要なオプション：

項目	説明
Max Email Rate	同じホストから送信される 1 分辺りの最大メッセージ数を指定します。
Max Email Size	E-mail メッセージの許容できる最大容量を指定します。本機能は 1 つの E-mail の送信バイトの合計（E-mail がコード化された後のヘッダサイズ、ボディサイズおよび添付ファイルのサイズ）をカウントします。例えば、100K バイトの添付ファイルを持つメールは、100K バイトより大きくなることに注意してください。 自動的に添付ファイルに行われるコード化は、実際には転送ファイルサイズを増加させるため、転送されたサイズは 120K バイト以上である可能性もあります。そのため、この制限を設定する場合、管理者は想定される E メールサイズに適切なマージンを追加する必要があります。
Allow STARTTLS	SMTP ネゴシエーションにおける STARTTLS コマンドを許可します。初期値は無効です。
Email address blacklisting	送信者または受信者の E-mail アドレスのブラックリストを指定し、このアドレスから（へ）のメールをブロックします。ブラックリストは、ホワイトリストの後に適用されるため、アドレスがホワイトリストエントリにした場合、ブラックリストにチェックされなくなります。
Email address whitelisting	E-mail アドレスのホワイトリストを指定します。このアドレスからのメールまたはこのアドレスへのメールは、たとえそのアドレスがブラックリストにあっても、またはメールに SPAM としてフラグがついていても、ALG の通過を許可されます。
Verify MIME-type	定義したファイルタイプに一致しているかを確認するために添付ファイルの内容がチェックされます。「付録 C アンチウィルス MIME ファイルタイプ」でチェックされるファイルタイプのリストを確認することができます。また、同じオプションが、HTTP ALG でも有効です。動作方法については、「6.1.2 HTTP ALG」を参照してください。
Block/Allow filetype	定義済みリストのファイルタイプは、オプションでメールの添付ファイルとしてブロックまたは許可することが可能であり、新しいファイルタイプをリストに追加することもできます。また、同じオプションが、HTTP ALG でも有効です。動作方法については、「6.1.2 HTTP ALG」を参照してください。
Anti-Virus Scanning	NetDefendOS アンチウィルスシステムは、E-mail の添付ファイルに対して不正なコードを検索します。疑わしいファイルを破棄、またはログへの出力のみ行うことができます。詳しくは「6.1 アプリケーションレイヤゲートウェイ」および「6.4 アンチウィルススキャン」参照してください。
Anti-Spam	NetDefendOS アンチスパムは、スパムメールに対してフィルタリング機能を提供します。詳しくは「6.3 メールフィルタリング」参照してください。
Application Control	アプリケーションコントロールは SMTP トラフィックに適用することができます。詳細は「3.7 アプリケーションコントロール」を参照してください。IP ルールではこのオプションは利用できません

SMTP ALG 処理の順序

SMTP フィルタリングは、以下の処理順序に従います。また、SPAM フィルタリングを除き、HTTPALG が従う順序と同様です。:

1. ホワイトリスト
2. ブラックリスト
3. SPAM フィルタリング（有効な場合）
4. アンチウィルススキャン（有効な場合）

上述の通り、アドレスがホワイトリストで見つけられると、ブラックリストにあってもブロックされません。SPAM フィルタリングが有効な場合、ホワイトリストに掲載されているアドレスに適用されますが、SPAM としてフラグがついている E-mail はタグ付けまたは廃棄も行われず、ログへの出力のみ行われます。アンチウィルススキャンが有効である場合、E-mail アドレスがホワイトリストに掲載されたとしても、常に適用されます。

メールの送信者または受信者のアドレスが、はじめのフィルタリング段階の 1 つによってブロックされるベースになることにご注意ください。

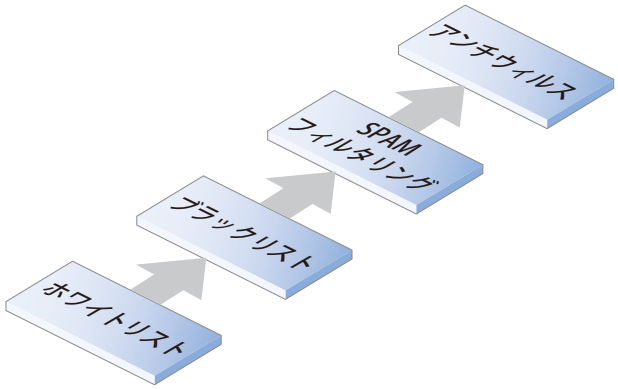


図 6-4　SMTP ALG 処理の順序

ホワイトリストとブラックリストでワイルドカードを使用する

ホワイトリストとブラックリストに作成されたエントリは、一つのエントリが多くの潜在的な E-mail アドレスを含むようにワイルドカードを使用することができます。ワイルドカードの文字「*」はどんなシーケンスの文字も表すことができます。

例えば、アドレスエントリ *@some_example.com は、some_example.com ドメインに関連した、全ての想定し得る E-mail アドレスを指定するために使用できます。

my_department へのメール送信を明示的に許可するためには、ホワイトリストエントリ my_department@example.com を追加します。これはワイルドカードを持つブラックリストエントリより優先度が高くなります。

Enhanced SMTP と拡張機能

Enhanced SMTP（ESMTP）は、RFC 1869 に定義されており、標準の SMTP プロトコルに多くの拡張機能を許可しています。

SMTP クライアントが ESMTP を使用して SMTP サーバとのセッションをオープンする場合、クライアントは初めに EHLO コマンドを送信します。サーバが ESMTP をサポートしていると、サポートする拡張機能のリストを使用して応答します。これらの拡張は、各種の独立した RFC によって定義されます。例えば、RFC 2920 は SMTP パイプラインの拡張を定義しています。他の一般的な拡張は、RFC 3030 で定義される Chunking です。

NetDefendOS SMTP ALG はパイプラインと Chunking を含むすべての ESMTP の拡張機能をサポートしているわけではありません。そのため、ALG はファイアウォール配下の SMTP サーバがクライアントに返すサポート拡張機能リストから未サポートの拡張を削除します。拡張機能を削除する場合、ログメッセージがテキストで生成されます。

```
unsupported_extension
capability_removed
```

ログメッセージのパラメータ「capa=」は、ALG がどの拡張をサーバレスポンスから削除したかを示すものです。例えば、このパラメータは以下のようにログメッセージに表示されます。

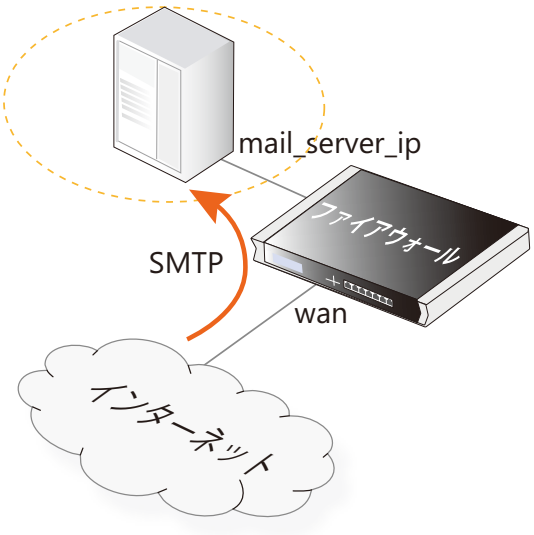
```
capa=PIPELINING
```

パイプラインの拡張が SMTP サーバから削除されたことを示すために、EHLO クライアントコマンドにリプライします。

ESMTP の拡張が ALG によって削除され、関連するログメッセージが生成されるかもしれませんが、これは、どの E-mail も破棄されることを意味するわけではありません。ALG によって削除された未サポートの拡張機能を利用せずに、いつものように E-mail 転送が行われます。

例題 6.10

IP ポリシーを使用した SMTP ALG のセットアップ



上記に図示したこの例題では、SMTP ALG は、パブリックインターネットから DMZ ネットワーク上のメールサーバに送信されるメールトラフィックをモニタするのに使用されます。メールサーバがアドレス帳オブジェクト mail_server_ip で定義されるプライベート IPv4 アドレスを持っているため、SAT IP ルールがファイアウォールのパブリック IP アドレスをこのプライベートアドレスに変換する必要があるものとします。

ファイアウォールの wan インタフェースがパブリップインターネットに接続し、インタフェースのパブリック IP アドレスをアドレス帳オブジェクト wan_ip で定義するものとします。

SMTP ALG は以下の操作を実行します。

- 添付された .exe または .msi ファイルをすべてブロックします。
- ファイルの拡張子がファイルの MIME タイプと異なる添付ファイルをブロックします。
- 残りの添付ファイルをウィルススキャンし、ウィルスが検出されるとそれらの通過を許可しません。
- zen.spamhaus.org（重み付け 5）と dnsbl.dronebl.org（重み付け 3）で DNSBL ルックアップを行うことであらゆるメールに SPAM としてタグ付けをします。
- ドメイン example.com から到来するあらゆるメールを破棄します。

CLI

A. 内向き SMTP トラフィック用に新しい Service オブジェクトを作成します。:

```
DFL-xxxx:/> add Service ServiceTCPUDP smtp_inbound_service Type=TCP DestinationPorts=25 SYNRelay=Yes
            Protocol=SMTP
```

B. EmailControlProfile オブジェクトを作成します。:

```
DFL-xxxx:/> add Policy EmailControlProfile my_ec_profile AntiSpam=Yes DNSBL=Yes DNSBL1=Yes DNSBL1Name=b.barra-
            cudacentral.org DNSBL1Score=5 DNSBL2=Yes DNSBL2Name=dnsbl1.droneb1.org DNSBL2Score=3
```

ブラックリストの E メール送信元をプロファイルの子オブジェクトとして追加します。:

```
DFL-xxxx:/> cc Policy EmailControlProfile my_ec_profile
DFL-xxxx:/my_ec_profile> add EmailFilter SrcEmail=*@example.com SrcType=Email Action=Blacklist
DFL-xxxx:/> cc
DFL-xxxx:/>
```

C. AntiVirusPolicy オブジェクトを作成します。:

```
DFL-xxxx:/> add Policy AntiVirusPolicy my_av_policy
```

D. FileControlPolicy オブジェクトを作成します。:

```
DFL-xxxx:/> add Policy FileControlPolicy my_fc_policy FileListType=Block File=exe,msi VerifyContentMimeType=Yes
```

E. インターネットからの E メールトラフィックに対して IP ポリシーを作成します。:

```
DFL-xxxx:/> add IPPolicy Name=smtp_inbound_sat SourceInterface=wan SourceNetwork=all-nets
            DestinationInterface=core DestinationNetwork=wan_ip Service=smtp_inbound_service Action=Allow
            SourceAddressTranslation=None DestAddressTranslation=SAT DestAddressAction=SingleIP DestNewIP=mail_
            server_ip EmailControl=Yes EC_Policy=my_ec_profile AntiVirus=Yes AV_Mode=UsePolicy AV_Policy=my_
            av_policy FileControl=Yes FC_Mode=UsePolicy FC_Policy=my_fc_policy
```

Web Interface

A. 内向き SMTP トラフィック用に新しい Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: smtp_inbound_service
- Type: TCP
- Destination: 110
- Protocol: SMTP

3. 「OK」ボタンをクリックします。

B. EmailControlProfile オブジェクトを作成します。:

1. **Policies > Firewalling > Email Control > Add > Email Control Profile** の順にメニューをクリックします 。

2. 以下の情報を入力します。
- Name: my_ec_profile

◇ **General**
- ANTI-SPAM: ON
- DNS Blacklists: Enable
- Blacklist1: 5, b.barracudacentral.org
- Blacklist2: 3, dnsb1.droneb1.org

3. Whitelist/Blacklist タブで **Add > Email Filter** の順にクリックします。

4. 以下の設定を行い、「OK」をクリックします。
- Action: Blacklist
- Source Type: Email Address
- Source Email Address: *@example.com

5. 「OK」をクリックします。

C. Anti-Virus Profile オブジェクトを作成します。

1. **Policies > Firewalling > Anti-Virus > Add > Anti-Virus Profile** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: my_av_profile

3. 「OK」をクリックします。

D. File Control Profile オブジェクトを作成します。

1. **Policies > Firewalling > File Control > Add > File Control Profile** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: my_fc_profile
- File Type Action: Block
- File Types: exe.msi
- Validate File Extension: Enabled

3. 「OK」をクリックします。

E. インターネットからメールサーバへの E メールトラフィックに対して IP ポリシーを作成します。:

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします 。

2. 以下の情報を入力します。
- Name: smtp_inbound_sat
- Action: Allow

◇ **Filter**
- Source Interface: wan
- Source Network: all-nets
- Destination Interface: core
- Destination Network: wan_ip
- Service: smtp_inbound_service

◇ **Source Translation**
- Address Translation: None

◇ **Destination Translation**
- Address Translation: SAT
- Address Action: Single IP
- New IP Address: mail_server_ip

3. Email Control タブで以下の情報を入力します。
- Enable Email Control: ON
- Email Control Profile: my_ec_profile

4. Anti-Virus タブで以下の情報を入力します。
- Enable Anti-Virus: ON
- Anti-Virus Profile: my_av_profile

5. File Control タブで以下の情報を入力します。
- Enable File Control: ON
- File Control Profile: my_fc_profile

6. 「OK」をクリックします。

IP ルールを使用した SMTP ALG のセットアップ

SMTP ALG を使用してセキュリティをセットアップするには、以下の手順を実行します。

1. 新規の SMTP ALG オブジェクトを作成します。必要に応じて、ファイルのブロックやウイルススキャンなどのオプションを有効化します。

2. 以下のプロパティを使用して SMTP 用に新規のカスタムサービスを作成します。

i. Type: TCP
ii. Destination: 25
iii. インターネットからトラフィックが送信される場合は Syn Flood Protection を有効化します。
iv. ALG: 手順 1 のサービスから割り当てます。

3. 手順 2 で作成したサービスを使用して IP ルールを作成します。SAT アドレス変換を行うには複数のルールが必要です。

例題 6.11

IP ルールを使用した SMTP ALG のセットアップ

この例題は、「IP ポリシーを使用した SMTP ALG のセットアップ」と同等の内容ですが、IP ポリシーの代わりに IP ルールを使用しています。

CLI

A. SMTP ALG オブジェクトを作成します。:

```
DFL-xxxx:/> add ALG ALG_SMTP smtp_inbound_alg VerifySenderEmail=Yes FileListType=Block File=exe,msi
            VerifyContentMimetype=Yes Antivirus=Protect DNSBL=Yes DNSBlackLists={b.barracudacentral.org;5},
            {dnsbl.dronebl.org;3}
```

この ALG では、example.com ドメインから送信されるすべてのメールをブラックリストに入れます。

```
DFL-xxxx:/> cc ALG ALG_SMTP smtp_inbound_alg
DFL-xxxx:/smtp_inbound_alg> add ALG_SMTP_Email Action=Blacklist Type=Sender Email=*@example.com
DFL-xxxx:/smtp_inbound_alg> cc
DFL-xxxx:/>
```

B. 内向き SMTP トラフィック用に新しい Service オブジェクトを作成します。:

```
DFL-xxxx:/> add Service ServiceTCPUDP smtp_inbound_service Type=TCP DestinationPorts=25 SYNRelay=Yes
            ALG=smtp_inbound_alg
```

C. インターネットからのメールトラフィック用の IP ルールを作成します。:

i. サーバアドレスを変換する SAT IP ルールを作成します。

```
DFL-xxxx:/> add IPRule Action=SAT Service=smtp_inbound_service SourceInterface=wan SourceNetwork=all_nets
            DestinationInterface=core DestinationNetwork=wan_ip SATTranslate=DestinationIP
            SATTranslateToIP=mail_server_ip Name=smtp_inbound_sat
```

ii. 変換されたトラフィックを許可するために照合する ALLOW IP ルールを作成します。

```
DFL-xxxx:/> add IPRule Action=Allow Service=smtp_inbound_service SourceInterface=wan SourceNetwork=all_nets
            DestinationInterface=core DestinationNetwork=wan_ip Name=smtp_inbound_allow
```

Web Interface

A. SMTP ALG オブジェクトを作成します。:

1. **Objects > ALG > Add > SMTP ALG** の順にメニューをクリックします。

2. General を入力します。
   - Name: SMTP_inbound_alg

3. File Integrity タブを選択します。
   - ブロックするファイルタイプとして exe と msi を選択します。
   - オプション「Block files with a file extension that does not match the MIME type of the file」を有効にします。

4. Anti-Virus タブを選択します。
   - Mode: Protect

5. Anti-Spam タブを選択します。
   -「DNSBL Anti-Spam Filter」を有効にします。
   - DNS Blacklists の下に、値 5 の b.barracudacentral.org と値 3 の dnsbl.dronebl.org を追加します。

6. Whitelist/Blacklist で **Add > Email Sender/Recipient** を選択し、以下の設定を行って「OK」をクリックします。
   - Sender/Recipient to classify: Sender
   - Classify the email address: Blacklist
   - Email: *@example.com

7.「OK」ボタンをクリックします。

B. 内向き SMTP 用に新しい Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: smtp_inbound_service
- Type: TCP
- Destination: 110
- 「SYN Flood Protection」を有効にします。
- ALG: smtp_inbound_alg

3. 「OK」ボタンをクリックします。

C. インターネットからメールサーバへのメールトラフィック用の IP ルールを作成します。:

i. サーバアドレスを変換する SAT IP ルールを作成します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします 。

2. 以下の情報を入力します。
- Name: smtp_inbound_sat
- Action: SAT
- Service: smtp_inbound_service
- Source Interface: wan
- Source Network: all-nets
- Destination Interface: core
- Destination Network: wan_ip
- SAT Translate: Destination IP
- New IP Address: mail_server_ip

3. 「OK」ボタンをクリックします。

ii. 変換されたトラフィックを許可するために照合する ALLOW IP ルールを作成します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: smtp_inbound_allow
- Action: Allow
- Service: smtp_inbound_service
- Source Interface: wan
- Source Network: all-nets
- Destination Interface: core
- Destination Network: wan_ip

3. 「OK」ボタンをクリックします。

6.1.5.1 SMTP ALG を使用した ZoneDefense

ZoneDefense は、特定のタイプの外部ネットワークスイッチに管理コマンドを送信することで、NetDefendOS がホストとネットワークをブロックできる機能です。SMTP は、メールを他のメールサーバにリレーするメールサーバと同様に、メールの送信を希望するメールクライアントに使用されます。SMTP ALG と共に ZoneDefense を使用する時、対象となる唯一のシナリオは、送信するメールでウィルスを広げようとするローカルなクライアントをブロックすることです。

incoming SMTP サーバにリレーされた E-mail をブロックするために ZoneDefense を使用すると、ブロックされた E-mail サーバから到来するすべての E-mail が拒否されるためお勧めしません。例えば、リモートユーザが周知の無料メール会社を使用して感染メールを送信する場合、ZoneDefense の使用により送信側サーバをブロックすると、どのローカルな受信者も将来同じ会社から来る E-mail も含めすべてブロックされます。従って、主にローカルなメールクライアントを防御するために SMTP ALG と共に ZoneDefense を使用するべきです。ブロックを行うためには、管理者は、すべてのローカルな SMTP クライアントを含むように ZoneDefense ネットワークの範囲を設定します。

SMTP サーバ自身がこの範囲から除外されている必要があります。

注意 除外は手動で設定できます。

特定のホストとサーバをブロックから除外するためには、ZoneDefense 除外リストにそれらを追加することで手動で設定することができます。

クライアントがウィルスに感染しているメールを送信しようとすると、ウィルスはブロックされ、ZoneDefense はホストを残りのネットワークから隔離します。

設定手順

- Web インタフェースの ZoneDefense セクションに行き ZoneDefense で使用される ZoneDefense スイッチを設定します。
- 有効なアンチウィルススキャンを使用するために SMTP ALG を設定します。
- ウィルスが検出される場合に ZoneDefense によって影響を受ける ALG のアンチウィルス設定で ZoneDefense ネットワークを選択します。

本機能に関する詳細は、「7.9 ZoneDefense」を参照してください。

6.1.6 POP3 ALG

POP3 はメールクライアントが使用するメール転送プロトコルで、メールサーバからメールをダウンロードするために受信者側で動作しています。IMAP プロトコルとの主な違いは、メールを検証する前に、すべてのメールと添付ファイルをクライアントにダウンロードすることです。メールは続いてクライアントコンピュータで保存され、メールサーバから削除される可能性があります。

以下の図は、NetDefendOS POP3 ALG の典型的な使用法の例です。DMZ ネットワーク dmz_net に置かれたメールサーバは、SMTP プロトコルを使用してパブリックインターネットからメールを受信します。ネットワーク lan_net 上で保護されたクライアントは、POP3 プロトコルを使用して、このサーバからメールをダウンロードします。クライアントは POP3 を使用して転送を開始し、メールのダウンロード要求をメールサーバに送信します。

メールがファイアウォールを通過するとき、NetDefendOS POP3 ALG はデータを調べて、ALG 構成オブジェクトに指定されている動作に従って、それらをブロックまたは許可します。

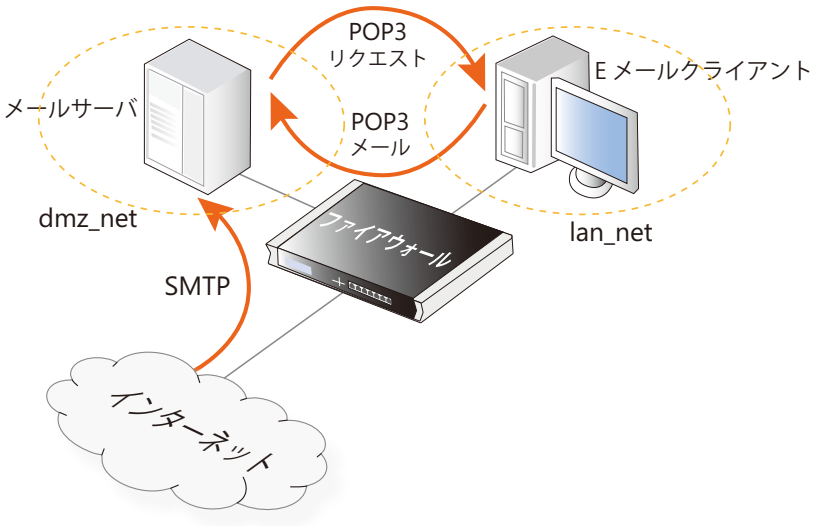


図 6-5 POP3 ALG 利用法

このシナリオでは、DMZ のメールサーバに到着する SMTP トラフィックはファイアウォールを通過し、NetDefendOS SMTP ALG を使用することでこのトラフィックを検証することができます。詳しくは、「6.1.5 SMTP ALG」を参照してください。

POP3 ALG の設定方法

POP3 ALG は、以下のいずれかの方法で設定を行います。

- **IP ポリシーを使用する**
  IP ポリシーオブジェクトを使用する方法が、推奨される設定方法です。最も簡単であり、IP ルールで利用できない追加のオプションを提供しています。POP3 ALG オプションは、IP ポリシーのプロパティを設定することで直接設定することができます。IP ポリシーで POP3 オプションを設定するには、ポリシーの Service プロパティに指定したサービスの Protocol プロパティが POP3 に設定されている必要があります。

- **IP ルールを使用する**
  IP ルールオブジェクトを使用する場合、POP3 ALG オブジェクトをサービスオブジェクトに割り当て、それを IP ルールに割り当てます。
  この方式は古い NetDefendOS バージョンとの互換性を保つ場合に役に立ちますが、IP ポリシーと比較して利点はありません。

IP ポリシーを使用した POP3 ALG のセットアップ

IP ポリシーを使用した POP3 ALG をセットアップするには、以下の手順を実行します。

1. 定義済みの pop3 サービスをコピーして新規のカスタムサービスを作成し、そのプロトコルプロパティを POP3 に指定します。もしくは、定義済みの pop3 サービスのプロトコルプロパティを POP3 に設定して使用します。
2. ターゲットトラフィックに対して起動される新規の IP ポリシーを作成し、そのサービスプロパティとして上記で設定したサービスを指定します。これにより、IP ポリシーですべての POP3 ALG オプションが利用可能になります。
3. 新規の Email コントロールプロファイルを作成し、IP ポリシーに割り当てます。
4. オプションで、新規に作成したファイルコントロールプロファイルおよび（または）アンチウイルスプロファイルを割り当てて、それらの機能を POP3 トラフィックに対して適用することも可能です。IP ポリシーではアプリケーションコントロールを設定することもできます。

POP3 ALG のプロパティ

POP3 ALG オブジェクトの主なプロパティは以下の通りです。

項目	説明
SPAM Filtering	SPAM に対して E メールをフィルタすることができます。詳細は「6.3.1 IP ポリシーベースのメールフィルタリング」を参照してください。 メールサーバに到達する前のメールトラフィックに対して既にスキャンが実行されている場合、POP3 ALG によるアンチスパムを冗長化することができます。このスキャンは NetDefendOS SMTP ALG によって実行されます。
Hide User	このオプションを使用すると、POP3 サーバはユーザが存在するかどうかを表示しません。これにより、有効なユーザ名を見つけるまでに異なるユーザ名を試すことを防ぐことができます。IP ポリシーでは Email コントロールプロファイルタブで設定可能であり、デフォルトでは無効となっています。
Allow Unknown Commands	ALG で認識できない非標準 POP3 を許可するかどうかを指定します。IP ポリシーでは、Email コントロールプロファイルタブで設定可能であり、デフォルトでは無効となっています。
Block USER/PASS Commands	読み取り可能なプレーンテキストでユーザ名 / パスワードの組み合わせを送信するクライアント / サーバ間の通信をブロックします（サーバによってはこれ以外の方式をサポートしていないかもしれません）。IP ポリシーでは、Email コントロールプロファイルタブで設定することが可能であり、デフォルトでは無効となっています。
Allow STARTTLS	POP3 ネゴシエーションにおける STARTTLS コマンドを許可します。初期値は無効です。

その他のオプション

POP3 トラフィックで起動される IP ポリシーでは、以下のオプションを設定することも可能です。

項目	説明
File Control	ファイルコントロールプロファイルは IP ポリシーに割り当ててファイル転送のチェックを行うことができます。IP ルールでは、使用される ALG オブジェクトでこのオプションを設定することができます。
Anti-Virus scanning	アンチウイルスプロファイルは IP ポリシーに割り当てて、転送ファイルに対してウイルスのスキャンを行うことができます。IP ルールでは、POP3 ALG オブジェクトでこのオプションを設定することができます。
Application Control	アプリケーションコントロールを POP3 トラフィックに適用することが可能です。詳細は「3.7 アプリケーションコントロール」を参照してください。このオプションは IP ルールでは使用できません。

例題 6.12

IP ポリシーを使用した POP3 ALG のセットアップ

この例題は本セクションの始めに図示したネットワークトポロジを仮定しています。POP3 トラフィックは、ネットワーク dmz_net 上のメールサーバとネットワーク lan_net 上の保護されたクライアント間で許可されます。メールサーバがアドレス帳オブジェクト mail_server_ip によって定義されるプライベート IPv4 アドレスを持っているものとします。
POP3 ALG は以下の操作を実行します。

- メールサーバがメールアドレスの存在有無を明らかにすることを防ぎます。
- ALG がスキャンに失敗したメールすべてを拒否します。
- 添付されている exe または msi ファイルをすべてブロックします。
- ファイルの拡張子がファイルの MIME タイプと異なる添付ファイルをブロックします。
- 許可されたすべての添付ファイルをウィルススキャンします。

CLI

A. POP3 用の新しいサービスオブジェクトを作成します。:

```
DFL-xxxx:/> add Service ServiceTCPUDP pop3_client_service Type=TCP DestinationPorts=110 Protocol=POP3
```

B. EmailControlProfile オブジェクトを作成します。:

```
DFL-xxxx:/> add Policy EmailControlProfile my_ec_profile POP3_HideUser=Yes
```

C. AntiVirusPolicy オブジェクトを作成します。:

```
DFL-xxxx:/> add Policy AntiVirusPolicy my_av_policy
```

D. FileControlPolicy オブジェクトを作成します。:

```
DFL-xxxx:/> add Policy FileControlPolicy my_fc_policy FileListType=Block File=exe,msi VerifyContentMimeType=Yes
```

E. メールサーバからの E メールトラフィックに対して IP ポリシーを作成します。:

```
DFL-xxxx:/> add IPPolicy Name=pop3_policy SourceInterface=lan SourceNetwork=lan_net DestinationInterface=dmz
            DestinationNetwork=mail_server_ip Service=pop3_client_service Action=Allow
            SourceAddressTranslation=None EmailControl=Yes EC_Policy=my_ec_profile AntiVirus=Yes AV_
            Mode=UsePolicy AV_Policy=my_av_policy FileControl=Yes FC_Mode=UsePolicy FC_Policy=my_fc_policy
```

Web Interface

A. POP3 用の新しいサービスオブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: pop3_client_service
   - Type: TCP
   - Destination: 110
   - Protocol: POP3

3. 「OK」ボタンをクリックします。

B. EmailControlProfile オブジェクトを作成します。:

1. **Policies > Firewalling > Email Control > Add > Email Control Profile** の順にメニューをクリックします 。

2. 以下の情報を入力します。
   - Name: my_ec_profile

3. POP3 Settings タブで以下の設定を行います。
   - Hide User: Enabled

4. 「OK」ボタンをクリックします。

C. Anti-Virus Profile オブジェクトを作成します。

1. **Policies > Firewalling > Anti-Virus > Add > Anti-Virus Profile** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: my_av_profile

3. 「OK」をクリックします。

D. File Control Profile オブジェクトを作成します。

1. **Policies > Firewalling > File Control > Add > File Control Profile** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: my_fc_profile
- File Type Action: Block
- File Types: exe.msi
- Validate File Extension: Enabled

3. 「OK」をクリックします。

E. メールサーバからの E メールトラフィックに対して IP ポリシーを作成します。:

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします 。

2. 以下の情報を入力します。
- Name: pop3_policy
- Action: Allow

◇ **Filter**
- Source Interface: lan
- Source Network: lan_net
- Destination Interface: dmz
- Destination Network: mail_server_ip
- Service: pop3_client_service

◇ **Source Translation**
- Address Translation: None

3. Email Control タブで以下の情報を入力します。
- Enable Email Control: ON
- Email Control Profile: my_ec_profile

4. Anti-Virus タブで以下の情報を入力します。
- Enable Anti-Virus: ON
- Anti-Virus Profile: my_av_profile

5. 5. File Control タブで以下の情報を入力します。
- Enable File Control: ON
- File Control Profile: my_fc_profile

6. 「OK」をクリックします。

IP ルールを使用した POP3 ALG の設定

IP ルールで POP3 ALG を設定するには以下の手順を実行します。

1. 新規の POP3 ALG オブジェクトを作成し、必要に応じてファイルブロックやウイルススキャンなどのオプションを有効化します。NetDefendOS では定義済みの POP3 ALG は用意されていません。

2. POP3 用に新規のカスタムサービスオブジェクトを作成し、以下の通り設定します。
   i. Type: TCP
   ii. Destination: 110

   これで、定義済み pop3 サービスのコピーが作成されました。この定義済みサービスを使用することも可能です。

3. 新規の POP3 ALG オブジェクトを新規のサービスオブジェクトに紐づけます。

4. IP ルールオブジェクトを作成し、送信先ネットワークにメールサーバ、送信元ネットワークに Email クライアントを指定します。接続を開始するのはクライアントとなります。

5. IP ルールにサービスオブジェクトを割り当てます。

例題 6.13

IP ルールを使用した POP3 ALG のセットアップ

この例題は「IP ポリシーを使用した POP3 ALG のセットアップ」と同等ですが、IP ポリシーではなく IP ルールを使用しています。

CLI

A. POP3 ALG オブジェクトを作成します。:

```
DFL-xxxx:/> add ALG ALG_POP3 pop3_client_alg HideUser=Yes FileListType=Block File=exe,msi
            VerifyContentMimetype=Yes Antivirus=Protect
```

B. POP3 に新しい Service オブジェクトを作成します。:

```
DFL-xxxx:/> add Service ServiceTCPUDP pop3_client_service Type=TCP DestinationPorts=110 ALG=pop3_client_alg
```

C. メールサーバからのメールトラフィック用の IP ルールを作成します。:

```
DFL-xxxx:/> add IPRule Action=Allow Service=pop3_client_service SourceInterface=lan SourceNetwork=lan_net
            DestinationInterface=dmz DestinationNetwork=mail_server_ip Name=pop3_mail
```

Web Interface

A. POP3 ALG オブジェクトを作成します。:

1. **Objects > ALG > Add > POP3 ALG** の順にメニューをクリックします。

2. General タブで以下の設定を行います。
   - Name: pop3_client_alg
   - オプション「Prevent a user from revealing a user does not exist」を有効にします。

3. File Integrity タブで以下の設定を行います。
   - ブロックするファイルタイプとして exe と msi を選択します。
   - オプション「Block files with a file extension that does not match the MIME type of the file」を有効にします。

4. Anti-Virus タブで以下の設定を行います。
   - Mode: Protect

5. 「OK」ボタンをクリックします。

B. POP3 に新しい Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: pop3_client_service
   - Type: TCP
   - Destination: 110
   - ALG: pop3_client_alg

3. 「OK」ボタンをクリックします。

C. メールサーバからのメールトラフィック用の IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: pop3_mail
   - Action: Allow
   - Service: pop3_client_service
   - Source Interface: lan
   - Source Network: lan_net
   - Destination Interface: dmz
   - Destination Network: mail_server_ip

3. 「OK」ボタンをクリックします。

クライアントが POP3 接続を開始するため、クライアントが IP ルールの送信元となることに注意してください。

6.1.7 IMAP ALG

IMAP は、受信者側の E メールクライアントがメールサーバからメールをダウンロードする際に使用される、メール転送プロトコルです。POP3 プロトコルとの主要な違いとして、IMAP ではメールヘッダと一緒にメール全体と添付がクライアントにダウンロードされません。そのかわりに、メールヘッダのみがダウンロードされます。ユーザは本文を読むかどうか選択し、その後メール全体と添付ファイルがダウンロードされます。ダウンロードされない場合、そのままサーバ上で削除されます。

IMAP ALG の設定

IMAP ALG の設定は IP ポリシーを使用した設定のみが可能です。以下の手順で実施します。

1. 定義済みの imap サービスをコピーして新しいサービスオブジェクトを作成し、プロトコルプロパティを imap に指定します。もしくは、定義済みのサービス「imap」のプロトコルプロパティに IMAP を指定して使用します。

2. ターゲットのトラフィックに対して起動される新しい IP ポリシーを作成し、そのサービスプロパティを手順 1 で作成したサービスに設定します。これにより、IP ポリシーですべての TFTP オプションが利用可能となります。

3. 新規の Email コントロールプロファイルを作成、設定して IP ポリシーに割り当てます。

4. オプションで新規に作成したファイルコントロールプロファイルおよび（または）アンチウイルスプロファイルを割り当て、それらの機能を IMAP トラフィックに適用することもできます。IP ポリシーではアプリケーションコントロールを設定することも可能です。

IMAP ALG オプション

3 ALG オブジェクトの主なプロパティは以下の通りです。

項目	説明
SPAM Filtering	SPAM に対して E メールをフィルタすることができます。詳細は「6.3.1 IP ポリシーベースのメールフィルタリング」を参照してください。このセクションでは IMAP プロトコルにおける NetDefendOS SPAM フィルタリングの違いについても説明しています。メールサーバに到達する前のメールトラフィックに対して既にスキャンが実行されている場合、IMAP ALG によるアンチスパムを冗長化することができます。このスキャンは NetDefendOS SMTP ALG によって実行されます。
Hide User	このサーバに誤った認証情報が送信された場合、このオプションによってサーバのエラーメッセージがクライアントに返されます。サーバによっては、どの認証情報が不正であるかというメッセージを送信するため、セキュリティ攻撃の検出にも役に立ちます。NetDefendOS ではクライアントに対して一般的なエラーメッセージを返します。初期値では無効です。
Block Plain Text Authentication	有効の場合、プレーンテキストで送信された認証情報を使用した認証はブロックされます。
Allow STARTTLS	IMAP ネゴシエーションにおける STARTTLS コマンドを許可します。初期値は無効です。

その他のオプション

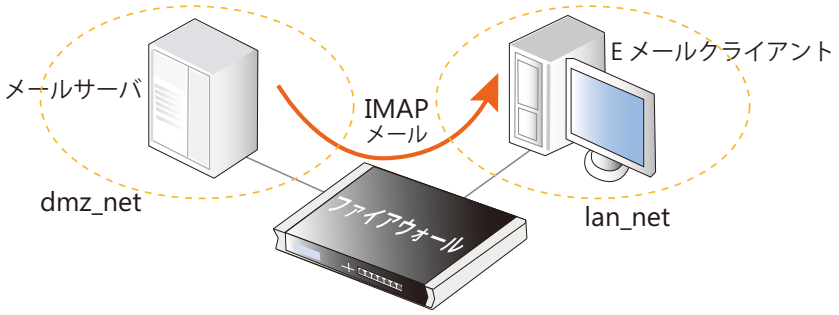
IMAP トラフィックで起動される IP ポリシーでは、以下のオプションを設定することも可能です。

項目	説明
File Control	ファイルコントロールプロファイルは IP ポリシーに割り当ててファイル転送のチェックを行うことができます。
Anti-Virus scanning	アンチウイルスプロファイルは IP ポリシーに割り当てて、転送ファイルに対してウイルスのスキャンを行うことができます。
Application Control	アプリケーションコントロールを IMAP トラフィックに適用することが可能です。詳細は「3.7 アプリケーションコントロール」を参照してください。

例題 6.14

IMAP ALG のセットアップ

この例題では、IMAP プロトコルを使用して dmz_net にあるメールサーバからのメールを lan_net 上の内部クライアントが取得することを許可する IP Policy オブジェクトを設定する方法を示しています。
このシナリオについては、以下で図と共に説明します。



追加の要件は以下の通りです。

- アンチスパム機能を有効にします。
- スパムとして破棄またはマークされように example.com からの全メールをホワイトリストにおきます。
- ドメイン検証とリンク保護の両方にサブスコア 5 を割り当てます。
- スパムに追加される件名のテキストを「*** Probably SPAM ***」に変更します。
- b.barracudacentral.org にある 1 つの DNSBL サーバを使用します。

CLI

A. メールをフィルタするために EmailControlProfile オブジェクトを作成します。:

```
DFL-xxxx:/> add Policy EmailControlProfile my_email_profile AntiSpam=Yes SubjectTag="*** Probably SPAM ***"
            DomainVerificationScore=5 LinkProtectionScore=5 DNSBL=Yes DNSBL1=Yes DNSBL1Name=zen.spamhaus.org
```

B. ホワイトリスト用のプロファイルに EmailFilter オブジェクトを追加します。:
CLI コンテキストをプロファイルになるように変更します。:

```
DFL-xxxx:/> cc EmailControlProfile my_email_profile
```

EmailFilter オブジェクトを子供としてを追加します。:

```
DFL-xxxx:/my_email_profile> add EmailFilter Action=Whitelist SrcType=Email SrcEmail=*@example.com
```

初期値の CLI コンテキストに戻します。:

```
DFL-xxxx:/main> cc
DFL-xxxx:/>
```

C. IMAP にカスタムサービスを作成します。:

```
DFL-xxxx:/> add Service ServiceTCPUDP my_imap_service Type=TCP DestinationPorts=143 Protocol=IMAP
```

D. IMAP トラフィックを許可する IPPolicy を追加し、これにプロファイルを関連付けます。:

```
DFL-xxxx:/> add IPPolicy Name=lan_to_dmz SourceInterface=lan SourceNetwork=lan_net DestinationInterface=dmz
            DestinationNetwork=dmz_net Service=my_imap_service Action=Allow SourceAddressTranslation=None
            EmailControl=Yes EC_Policy=my_email_profile
```

Web Interface

A. メールをフィルタするために EmailProfile オブジェクトを作成します。:

1. **Policies > Firewalling > Email Control > Add > Email Control Profile** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: my_email_profile
- Anti-Spam: Enable
- Domain Verfication Score: 5
- Malicious Link Protection Score: 5
- DNS Blacklists: Enable
- Blacklist 1: b.barracudacentral.org
- Tag Subject Text: *** Probably SPAM ***

3. 「OK」ボタンをクリックします。

B. ホワイトリスト用のプロファイルに EmailFilter オブジェクトを追加します。:

1. **Policies > Firewalling > Email Control** の順にメニューをクリックします。

2. my_email_profile を選択します。

3. Whitelist/Blacklist を選択します。

4. **Add > Email Filter** を選択します。

5. 以下の情報を入力します。
- Action: Whitelist
- Source Type: Email Address
- Source Email Address: *@example.com
- OK を選択します。

6. 「OK」ボタンをクリックします。

C. IMAP にカスタムサービスを作成します。:

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Type: TCP
- Destination: 143
- Protocol: IMAP

3. 「OK」ボタンをクリックします。

D. IMAP トラフィックを許可する IP Policy を追加し、これにプロファイルを関連付けます。:

1. **Policies > Firewalling > Main IP Rules >Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: lan_to_dmz
- Action: Allow
- Source Interface: lan
- Source Network: lan_net
- Destination Interface: dmz
- Destination Network: dmz_net
- Service: my_imap_service

3. Email control タブを選択し、以下の設定を行います。
- Enable Email Control: enable
- Email Control Profile: my_email_profile

4. 「OK」ボタンをクリックします。

6.1.8 PPTP ALG

PPTP トンネルが NAT と共に使用される場合、特定の問題に対処するために PPTP ALG が提供されます。

D-Link ファイアウォールの背後にある保護された内部ネットワークに、2 つのクライアント A と B があるとします。ファイアウォールは外部のインターネットに接続しており、NAT ルールは、クライアントからのトラフィックがインターネットにフローすることを許可するように定義されています。そのため、両方のクライアントには、インターネットを経由して同じ IP アドレスからサーバに接続するように見えます。

クライアント A が現在、インターネット経由で外部ホスト C に PPTP トンネルを確立します。トンネルのエンドポイントは、クライアントと外部サーバです。NAT IP ルールのため、トンネル接続は、ファイアウォールの外部 IP アドレスから来るように見えます。

この最初の接続は成功しますが、2 番目のクライアント B が同じエンドポイント IP アドレスで同じサーバ C に接続しようとすると、A の最初の接続は失われます。これは、両方のクライアントが同じ外部 IP アドレスから同じエンドポイントに PPTP トンネルを確立しようとしているためです。

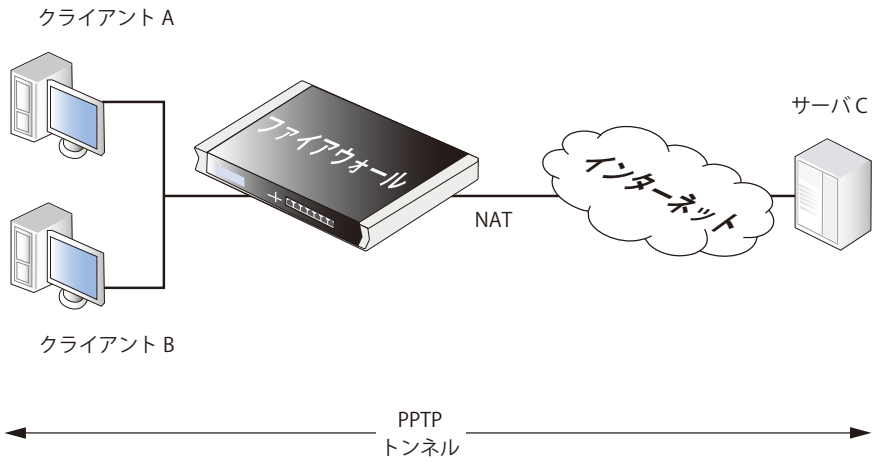


図 6-6　PPTP ALG の使用

PPTP ALG がこの問題を解決します。ALG を使用することによって、すべてのクライアントからのトラフィックを、ファイアウォールとサーバ間の単一の PPTP トンネルを通じて多重化して送信することができます。

PPTP ALG の設定方法

PPTP ALG は、以下のいずれかの方法で設定を行います。

- **IP ポリシーを使用する**
  IP ポリシーオブジェクトを使用する方法が、推奨される設定方法です。最も簡単であり、IP ルールで利用できない追加のオプションを提供しています。PPTP ALG オプションは、IP ポリシーのプロパティを設定することで直接設定することができます。IP ポリシーで PPTP オプションを設定するには、ポリシーの Service プロパティに指定したサービスの Protocol プロパティが PPTP に設定されている必要があります。

- **IP ルールを使用する**
  IP ルールオブジェクトを使用する場合、PPTP ALG オブジェクトをサービスオブジェクトに割り当て、それを IP ルールに割り当てます。
  この方式は古い NetDefendOS バージョンとの互換性を保つ場合に役に立ちますが、IP ポリシーと比較して利点はありません。

IP ポリシーを使用した PPTP ALG セットアップ

このセクションでは、IP ポリシーオブジェクトを使用した PPTP ALG の設定方法について説明しています。以下の手順で実施します。

1. 以下のプロパティを持つ新規の TCP/UDP カスタムサービスオブジェクトを作成します。
   - Type（プロトコル）を TCP として選択します。
   - ソースポート範囲の初期値は 0-65535 です。
   - 宛先ポートに 1723 を設定します。
   - Protocol に PPTP を指定します。

2. ターゲットトラフィックに対して起動される新規の IP ポリシーオブジェクトを作成し、そのサービスプロパティを上記で作成したサービスに指定します。これにより、IP ポリシーで PPTP ALG オプションが利用可能になります。

3. IP ポリシーの関連するプロパティを変更して、PPTP ALG の動作を調整します。利用可能なオプションは下記で説明します。

PPTP ALG 設定

PPTP 用のサービスを IP ポリシーに設定した後、以下の設定が利用可能です。

項目	説明
Enable PPTP settings	ON に設定すると、PPTPALG がアクティブ化されます。
Echo timeout	PPTP トンネルにおける Echo メッセージのタイムアウト。
Idle timeout	PPTP トンネルのユーザトラフィックメッセージのタイムアウト。

多くの場合、名前のみを定義する必要があります。その他の設定は初期値のままにしておくことが可能です。

例題 6.15

IP ポリシーを使用した PPTP ALG のセットアップ

この例題では、内部ネットワークの lan から wan インタフェース経由でインターネットへ送信されるすべての PPTP トラフィックに対してアドレス変換を実行する NAT IP ポリシーを追加します。すべての通信に対し、wan インタフェースの IP アドレスは NAT アドレスとして使用されます。

PPTP ALG がトラフィックに対して適用され、デフォルトの PPTP ALG 設定が使用されます。lannet 上のクライアントは PPTP トンネルのローカルエンドポイントとなります。設定をまとめると以下の表になります。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
Allow/NAT	lan	lannet	wan	all-nets	pptp_ctl

CLI

```
DFL-xxxx:/> add IPPolicy Name=nat_pptp SourceInterface=lan SourceNetwork=lannet DestinationInterface=wan
            DestinationNetwork=all-nets Service=pptp-ctl Action=Allow SourceAddressTranslation=NAT NATSourceAd
            dressAction=OutgoingInterfaceIP PPTPControl=Yes
```

Web Interface

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします 。

2. 以下の情報を入力します。
   - Name: nat_pptp
   - Action: Allow

◇ **Filter**
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: wan
   - Destination Network: all-nets
   - Service: pptp_ctl

◇ **Source Translation**
   - Address Translation: NAT
   - Address Action: Outgoing Interface IP

3. PPTP タブで以下の情報を入力します。
   - Enable PPTP settings: ON

4. 「OK」をクリックします。

IP ルールを使用した PPTP ALG の設定

PPTP ALG を設定する場合 IP ポリシーを使用する方法が推奨される手順ですが、代替の方法として、より複雑な方法ではありますが IP ルールオブジェクトを使用する方法があります。設定手順は以下の通りです。

1. 適切な名前を付けて新規の PPTP ALG オブジェクトを定義します。定義済みの PPTP ALG は用意されていません。

2. ALG オブジェクトを適切なサービスオブジェクトに割り当てます。事前定義済みの pptp-ctl サービスを使用するか、または pptp-ctl のコピーであるカスタムサービスを作成することもできます。

3. 必要に応じて ALG プロパティを変更します。

4. クライアントから PPTP トンネルのリモートエンドポイントへ送信されるトラフィックを許可する NAT IP ルールに、このサービスを割り当てます。IP ルールは、送信先ネットワークが「all-nets」であるインターネットへのトラフィックを NAT する設定であるケースも考えられます。

6.1.9 SIP ALG

概要

Session Initiation Protocol（SIP）は、IP ネットワークにおいてピア間のセッションを確立するために使用される ASCII（UTF-8）テキストベースの信号プロトコルです。それは、HTTP と SMTP に類似したリクエスト - レスポンスプロトコルです。SIP がセットアップされるセッションは Voice-Over-IP（VoIP）通話から成っているか包括的なマルチメディアカンファレンスであるかもしれません。VOIP と共に SIP を使用することは、電話が他のサービスに統合できる別の IP アプリケーションになることが可能であることを意味します。

SIP のセッション設定

SIP は、セッションの内容の詳細についてはわからないため、セッションの開始、終了、変更に対してだけ責任を負います。SIP によって設定されたセッションは、UDP ベースの RTP/RTCP プロトコルを使用してインターネットでオーディオやビデオなどのストリーミングに使用されますが、TCP プロトコルに基づくトラフィックに関連する可能性もあります。また、RTP/RTCP ベースのセッションも同じセッションで TCP または TLS ベースのトラフィックに関連するかもしれません。

SIP RFC

SIP は、IETF の RFC 3261 によって定義され、VoIP 通信の重要な標準とされています。これは、H.323 と比較されますが、SIP の設計目標は H.323 よりスケーラブルにすることでした。VoIP については、「6.1.10 H.323」を参照してください。

注意 サードパーティの機器とのコンプライアンス

NetDefendOS は RFC 3261 に記述されている SIP インプリメンテーションに基づいています。しかし、プロキシと同様にローカルおよびリモートクライアントも RFC 3261 に準じて設定されていないと、正しい SIP メッセージの処理およびメディアの確立を保証することはできません。

残念ながら、サードパーティの SIP 装置によっては RFC 3261 外の技術を使用している可能性があり、これを無効にするように装置の設定を実施できないかもしれません。このため、そのような装置では NetDefendOS SIP ALG を使用した操作は成功しない可能性があります。

例えば、サービスプロバイダが、限られた構成で SIP ALG を使用しないで動作させるアナログからのデジタル変換を事前に設定しているかもしれません。

STUN のような NAT トラバーサル技術は、RFC 3261 規格外にあり、無効にする必要があります。

NetDefendOS は 3 つのシナリオをサポートする

より詳細な SIP の説明を続ける前に、NetDefendOS が以下の異なる 3 つのシナリオで SIP 使用をサポートすることを理解することが重要です。

- ローカルクライアントを保護する
  このシナリオでは、プロキシはパブリックインターネットのいずれかに位置しています。

- プロキシとローカルなクライアントを保護する
  プロキシは、クライアントと同じローカルネットワークに位置しています。しかし、このケースは以下の 2 つのシナリオに分けられます。
  i. クライアントとプロキシは内部の信頼できるネットワークにあります。
  ii. クライアントとプロキシは DMZ ネットワークにあります。

SIP 設定における制限

SIP ALG を介して送信される SIP トラフィックには、以下の NetDefendOS コンフィグレーションに関する制限があります。

- SIP ALG トラフィックは、main ルーティングテーブル以外のテーブルを使用して設定できません。つまり、NetDefendOS の仮想ルーティング機能の設定や、ポリシーベースルーティング（PBR）ルールの SIP ALG との使用ができません。

- ルートフェイルオーバー機能は使用できません。

- トラフィックシェーピングは SIP ALG に対して適用できません。

SIP コンポーネント

以下のコンポーネントは SIP 通信のための論理的な構造用ブロックです。

項目	説明
User Agents	クライアント to クライアント通信に関係したエンドポイントまたはクライアントです。これらは、通常、IP 電話の会話に使用されるワークステーションまたはデバイスです。クライアントという用語は、ユーザエージェントについて説明するために本セクション内で使用されます。
Proxy Servers	クライアントのリクエストを受信する場合、クライアントとサーバの両方として動作しながら SIP プロトコル内ではルータとして動作します。これらは、サービスに対するアクセスを認証し権限を与えるだけでなく、クライアントの現在の位置にリクエストを送信します。また、プロバイダをコールするルーティングポリシーを実行します。 プロキシは、ァイアウォールの外部の保護されていない面に通常配置されていますが、他の場所に配置することもできます。NetDefendOS は、これらのシナリオのすべてをサポートしています。
Registrars	SIP REGISTER リクエストを処理するサーバは Registrar（レジストラ）という特別な名前が付与されています。レジストラサーバには、他方のクライアントが到達するホストの場所を見つけるタスクがあります。 そして、レジストラとプロキシサーバは論理エンティティであり、同じ物理サーバに存在することも可能です。

SIP メディアに関連したプロトコル

SIP セッションは以下のような多くのサブプロトコルを利用します。

項目	説明
SDP	記述プロトコル（RFC 4566）はメディアセッションの初期化に使用されます。
RTP	Real-time Transport Protocol（RFC 3550）は、UDP プロトコルを使用して IP 経由でオーディオやビデオストリーミングを送信するための基本的なパケットフォーマットとして使用されます。
RTCP	Real-time Control Protocol（RFC 3550）は、帯域外制御フローマネジメントを提供するために RTP と共に使用されます。

SIP ALG の設定方法

以下のいずれかの方法により、SIP ALG の設定を行うことができます。

- **IP ポリシーオブジェクトと共に VoIP プロファイルを使用する**
  SIP ALG は IP ポリシーオブジェクトを使用して設定可能であり、この設定方法が推奨されます。VoIP プロファイルオブジェクトを作成し、SIP オプションを指定して設定します。その後、ターゲットのトラフィックに対して起動される IP ポリシーオブジェクトに VoIP プロファイルオブジェクトを割り当てます。

  SIP トラフィックに設定されるサービスオブジェクトは、IP ポリシーオブジェクトにも使用されている必要があります。また、このサービスオブジェクトのプロトコルプロパティは SIP に設定されている必要があります。

  NetDefendOS 11.03 以降のデフォルトコンフィグレーションの定義済みの SIP サービスオブジェクトでは、プロトコルプロパティが既に SIP に設定されています。ただし、古い NetDefendOS からアップグレードされたシステムではこのように設定されていません。

- **IP ルールオブジェクトと共に VoIP プロファイルを使用する**
  一方で、SIP ALG オブジェクトを SIP プロトコルが設定されたサービスプロパティに割り当てることも可能です。その後、SIP トラフィックに対して起動される IP ルールオブジェクトにサービスオブジェクトを割り当てます。

  NetDefendOS 11.03 以降では、デフォルトコンフィグレーションに定義済みの SIP ALG が存在しません。したがって、SIP 用の IP ルールを作成する場合は新規の SIP ALG を作成する必要があります。古い NetDefendOS から 11.03 以降にアップグレードされたシステムでは、定義済みの SIP ALG オブジェクトは保持されます。

IP ポリシーオブジェクトを使用した SIP セットアップ

IP ポリシーを使用して設定する場合、以下の手順が必要です。

- SIP 通信のために一つのサービスオブジェクトを定義します。サービスを IP ポリシーオブジェクトと共に使用する場合、Protocol プロパティを SIP に設定する必要があります。
- VoIP Profile オブジェクトを定義します。SIP ALG を使用する際に入力する設定を、このオブジェクトに入力します。
- 定義した Service オブジェクトを使用する SIP 通信のために、適切な IP ルールまたは IP ポリシーを定義します。
- 以前に作成した VoIP Profile オブジェクトを IP ポリシーオブジェクトに関連付けます。

定義済みの SIP サービスが使用可能

P ルールオブジェクトまたは IP ポリシーオブジェクトを使用する場合のどちらも、定義済みの Service オブジェクト sip-udp を使用できます。しかしながら、新しい Service オブジェクトを作成することをお勧めします。本セクションの例題ではそのような手順となっています。

IP ポリシーで使用される SIP サービスオブジェクトについて、サービスプロパティに SIP が指定されている必要があります。古い NetDefendOS バージョンからアップグレードされたシステムでは、定義済みの sip-udp オブジェクトにはそのような設定はされていないことに注意してください。

SIP ALG オプション

IP ALG オブジェクトで設定可能なオプションは以下の通りです。IP ポリシーでは、VoIP オブジェクトで設定可能です。

項目	説明
Max Sessions per ID	1 つのクライアントが関係する同時に可能なセッション数は、本値によって制限されます。初期値は 5 です。
Max Registration Time	SIP レジストラでの登録のための最大時間。初期値は 3600（秒）です。
SIP Signal Timeout	SIP セッションに許可される最大時間。初期値は 43200（秒）です。
Data Channel Timeout	SIP セッションにおいてトラフィックなしで待機を許可される最大時間。この値を超えると、タイムアウトとなります。初期値は 120（秒）です。
Allow TCP data channels	SIP セッションの間、TCP データチャンネルを使用できます。初期値は有効です。
Maximum number of TCP channels per call	Allow TCP data channels が有効であると、SIP セッションに許可される最大の TCP チャンネル数を指定するために本オプションを利用できます。
Allow clients to exchange media directly when possible	本オプションを有効にすると、RTP/RTCP 通信などのデータは、ファイアウォールにかかわらずに 2 つのクライアント間で直接交換されます。2 つのクライアントが同じインタフェースの配下にあり、同じネットワークに所属する場合にだけ可能です。初期値は有効です。

SIP プロキシ Record-Route オプション

NetDefendOS を使用した SIP シナリオの設定方法を理解するために、はじめに SIP プロキシ Record-Route オプションを理解することが重要です。SIP プロキシは、Record-Route オプションを有効または無効にすることができます。有効になっている場合、プロキシはステートフルプロキシとして知られています。Record-Route が有効な場合、プロキシは、2 つのクライアント間で交換する全 SIP 信号のために中継となることを伝えます。

SIP セッションが設定されると、発信元のクライアントは外向きの SIP プロキシサーバに INVITE メッセージを送信します。SIP プロキシは、着呼側リモートクライアントのコンタクト情報に対して責任を持つリモートプロキシサーバにこのメッセージをリレーします。そして、リモートプロキシは着呼側クライアントに INVITE メッセージをリレーします。一度、2 つのクライアントが互いの IP アドレスを学習すると、それらは相互に直接通信できるようになり、SIP メッセージはプロキシを迂回することができます。プロキシが初期の SIP メッセージの交換処理にだけ使用されるため、規模の拡大を容易にします。

セッションからプロキシを削除することの端緒として、ファイアウォールを通じてすべての SIP がメッセージを許可するためには、NetDefendOS IP ルール（または IP ポリシー）の設定が必要となります。そして、メッセージの送信元のネットワークがわからない場合、IP ルールセットにより非常に多くの潜在的に危険な接続を許可しなければならないという点です。ローカルなプロキシが Record-Route オプションを有効にしていると、この問題は起こりません。このモードでは、すべての SIP メッセージはプロキシから送信されてくるだけです。

Record-Route オプションが有効な場合と無効な場合に必要とされる各ルール / ポリシーの違いは、以下で示すシナリオ 1「ローカルクライアントを保護する - インターネットに位置するプロキシ」にあげられた 2 つの異なる IP ルール / ポリシーで見ることができます。

メディアデータ用 IP ルールセット

SIP のデータフローには、2 つの異なるタイプの交換があります。

- メディアデータの交換の前に 2 つのクライアント間の通信を設定する SIP セッション。
- メディアデータ自体の交換、例えば、VoIP 電話を構成するコード化された音声データ。

以下で説明される SIP 設定では、IP ルールセットのエントリは、上記メディアの交換のうち、前者を処理するために定義される必要があるだけです。IP ルールセットエントリも他のオブジェクトも、上記の後者を処理するために定義される必要はありません。SIP ALG は、ファイアウォールを通じてメディアデータのトラフィックのフローを許可するために必要とされる（時々 SIP ピンホールと記述されます。）接続を自動的に、かつ目につかないように注意して作成することが必要です。

注意 SIP トラフィックを非許可とする先行の IP ルールセットエントリが存在しないことを確認してください。

SIP を使用したシナリオ

NetDefendOS は、さまざまな SIP の利用のシナリオをサポートしています。以下の 3 つのシナリオが、想定されるタイプの使用法をほぼ網羅しています。例題の設定は、IP ルールオブジェクトを使用して説明されていますが、それらの代わりとして、簡単に IP ポリシーオブジェクトとすることもできます。

- シナリオ 1
  ローカルなクライアントを保護する - インターネットに位置するプロキシ
  SIP セッションは、D-LInk ファイアウォールの保護されている面のクライアントと保護されていない外部にあるクライアント間のセッションです。SIP プロキシはファイアウォールの外部で保護のない面に位置しています。内部の保護された側のクライアントが、パブリックの保護されていない側のプロキシへ登録することにより、通常、パブリックインターネット上で通信が行われます。

- シナリオ 2
  プロキシとローカルなクライアントを保護する - クライアントと同じネットワークにあるプロキシ
  SIP セッションは、D-Link ファイアウォールの保護されている面のクライアントと保護されていない外部にあるクライアント間のセッションです。SIP プロキシは、ファイアウォールのローカルで保護されている面に位置し、外部で保護されていない面にあるクライアントと、同じローカルネットワークに位置するクライアントの両方からの登録を処理します。通信は、通常パブリックインターネットまたはローカルネットワークのクライアント間を通じて行われます。

- シナリオ 3
  プロキシとローカルなクライアントを保護する - DMZ インタフェース上のプロキシ
  SIP セッションは、D-Link ファイアウォールの保護されている面のクライアントと外部で保護されていない面にあるクライアント間のセッションです。SIP プロキシは、DMZ インタフェースに位置していて、リモートクライアントネットワークやプロキシネットワークと同様にローカルなクライアントネットワークと物理的に切り離されています。

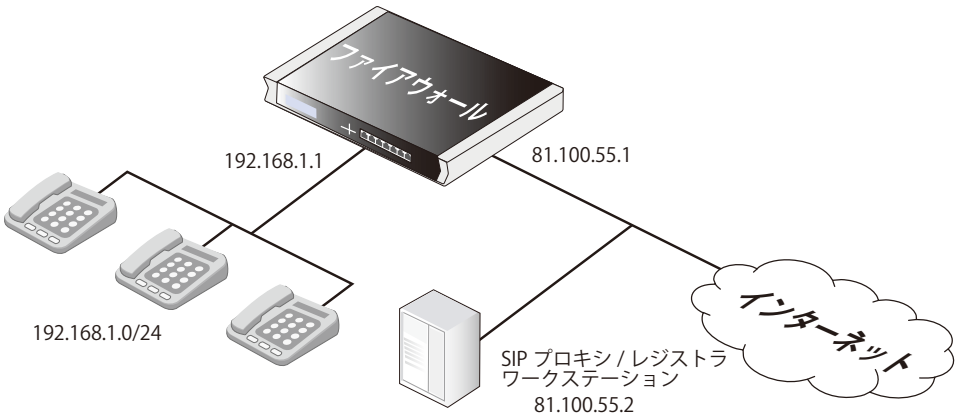
上記のすべてのシナリオは、同じネットワークにあるセッションに 2 つのクライアントが存在するという状況を示しています。

これらのシナリオをこれから詳細に検証していきます。

シナリオ 1

ローカルなクライアントを保護する - インターネットに位置するプロキシ

NAT を使用してネットワークのトポロジが隠されている、プライベートな内部ネットワークに VoIP ユーザがいるオフィスというシナリオを想定します。このシナリオについては、以下で図と共に説明します。



上記の図の SIP プロキシは、インターネットを横切る形でリモートに位置できます。プロキシは、クライアントが SIP プロキシを経由して送信されるオフィスへの、およびオフィスからの SIP トラフィックのすべてを保証するために、「Record-Route」機能を有効に設定する必要があります。これは、SIP プロキシからの SIP 信号のみ、ローカルネットワークへの入力を許可することによって攻撃面を最小化するため推奨されます。

2 つの方法でこのシナリオを実行することができます。
- NAT を使用してネットワークトポロジを隠します。
- 従って、NAT を使用しないと、ネットワークトポロジは危険にさらされてしまいます。

注意 NAT トラバーサルを設定するべきではありません。

NAT トラバーサルを使用するために、SIP のユーザエージェントと SIP プロキシを設定しないでください。例えば NAT（STUN）技術による UDP の Simple Traversal を使用しないでください。NetDefendOS SIP ALG は、SIP シナリオにおけるすべての NAT のトラバーサル問題を解決します。

本シナリオのための設定手順は以下の通りです。

1. 上記オプションを使用して、SIP ALG オブジェクトを定義します。

2. サービスオブジェクトを定義し、これに SIP ALG オブジェクトを関連付けます。サービスは、以下である必要があります。
- 宛先ポートは 5060 に設定します。（SIP 信号ポートの初期値）
- タイプは TCP/UDP に設定します。

3. 2 つの IP ルールセットエントリを定義します。
- 内部ネットワークのクライアントから外部に位置する SIP プロキシサーバへの外向きトラフィックへの NAT エントリ。SIP ALG は NAT ルールに必要とされるすべてのアドレス変換を行います。この変換は IP レベルおよびアプリケーションレベルの両方に生じます。クライアントまたはプロキシのいずれも、ローカルユーザが NAT 変換されることを知る必要はありません。

- SIP プロキシからファイアウォールの IP までの内向き SIP トラフィックに対する「Allow」エントリ。本ルールは宛先インタフェースとして core（つまり NetDefendOS 自身）を使用します。これは、上記 NAT ルール用です。着呼を受ける場合、NetDefendOS は自動的にローカルなレシーバの場所を見つけて、アドレス変換を実行し、さらにレシーバに SIP メッセージを送信します。これは ALG の内部状態に基づいて実行されます。

ALG は、正しい内部ユーザに到来する SIP リクエストを自動的にリダイレクトするため、到来する SIP を変換する SAT ルールは必要ではありません。NAT 変換を行うファイアウォールの背後にいる SIP クライアントが外部の SIP プロキシを登録すると、NetDefendOS は、SIP プロキシにコンタクト情報として自身の IP アドレスを送信します。NetDefendOS は、クライアントのローカルなコンタクト情報の問い合わせ先を登録し、これを利用して受信リクエストをユーザへリダイレクトします。ALG は必要とされるアドレス変換を行います。

4. クライアントが正しく設定されたことを確認します。SIP プロキシサーバはセッションにおける一方のクライアントの現在位置を見つける際に重要な役割を果たします。プロキシの IP アドレスは直接 ALG では指定されません。その代わりに、位置情報は、クライアントが使用するクライアントソフトウェアに直接に入力するか、クライアントには DHCP 経由などで自動的にプロキシの IP アドレスを取得する方法があります。

Record-Route オプションが有効である IP ルールセットのエントリは、以下の通りです。NAT を使用する場合に適用する変更は括弧（ ）内に示しています。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク
Allow（または Allow/NAT）	lan	lannet	wan	ip_proxy
Allow	wan	ip_proxy	lan（または core）	lannet（または wan_ip）

Record-Route オプションを有効にしない場合の IP ルールセットのエントリは以下の通りです。
NAT を使用する場合に適用する変更は括弧（ ）内に示しています。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク
Allow（または Allow/NAT）	lan	lannet	wan	< すべての有効な IP>
Allow	wan	< すべての有効な IP>	lan（または core）	lannet（または wan_ip）

外向きのトラフィックのための送信先ネットワーク、および内向きトラフィックのための送信元ネットワークは、利用可能なすべての IP アドレスを持つ必要があるため、Record-Route を使用する利点は明らかです。

注意 テーブルは Service オブジェクトを省略します。

本セクションでは、上記のような IP ルールセットのエントリを示すテーブルは、各エントリに関連するサービスオブジェクトを省略します。また、カスタムのサービスオブジェクトはすべての SIP シナリオに使用されます。

例題 6.16

IP ポリシーを使用したローカルクライアント / インターネットプロキシを持つ SIP

この例題では、上で説明したシナリオ 1 を実行する正確な手順を示しています。ローカルネットワークトポロジは、NAT を使用することで隠されます。プロキシサーバは D-Link ファイアウォールの外部で保護のない面に位置しています。クライアントは、インタフェース if1 に接続するネットワーク if1_net にあるものとします。SIP プロキシがインタフェース ext の IP アドレス proxy_ip にあるものとします。

Web Interface

A. 必要な IP オブジェクトを定義します。:

- if1_net: 192.168.1.0/24
  （内部のネットワーク）
- proxy_ip: 81.100.55.2
  （SIP プロキシ）
- ip_wan: 81.100.55.1
  （ファイアウォールのパブリック IPv4 アドレス）

B. VoIP Profile オブジェクトを定義します。:

1. **Policies > Firewalling > VoIP > Add > VoIP Profile** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_sip_profile
   - Enable SIP: ON
   - Enable H.323: OFF
3. 「OK」をクリックします。

C. SIP 用のカスタム Service オブジェクトを定義します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。
2. サービスの名前 (ここでは my_sip_service) を指定します。
3. Type として UDP を選択します。
4. Destination プロパティには、ポート番号 5060 を入力します。
5. プロトコルプロパティを SIP に設定します。
6. 「OK」ボタンをクリックします。

D. 外向きの SIP トラフィックに IP ポリシーを定義します。:

1. **Rules > IP Rule Set > main > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: sip_nat
   - Action: Allow
   - Source Interface: if1
   - Source Network: if1_net
   - Destination Interface: ext
   - Destination Network: proxy_ip
   - Service: my_sip_service
   - Address Translation (Source Translation): NAT
   - Address Action: Outgoing interface IP
   - Comment: Allow outgoing SIP calls
3. VoIP タブを選択し、VoIP を有効にして、my_sip_profile を選択します。
4. 「OK」ボタンをクリックします。

E. 内向きの SIP トラフィックに IP ポリシーを定義します。:

1. **Rules > IP Rule Set > main > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: sip_allow
   - Action: Allow
   - Source Interface: ext
   - Source Network: proxy_ip
   - Destination Interface: core
   - Destination Network: ip_wan
   - Service: my_sip_service
   - Comment: Allow incoming SIP traffic

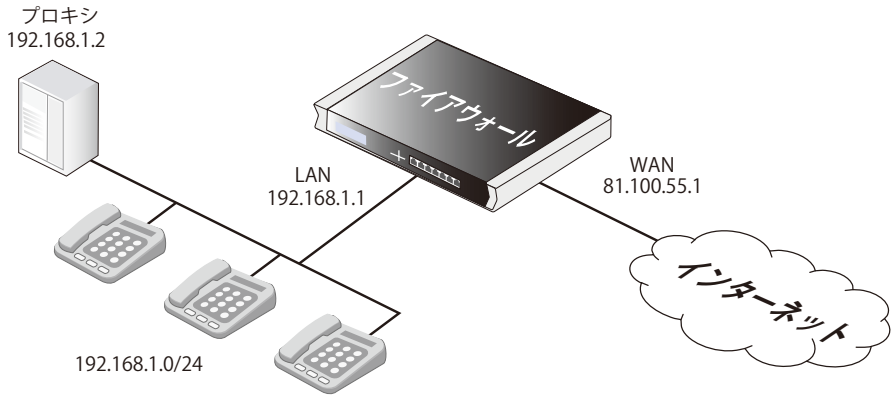
3. VoIP タブを選択し、VoIP を有効にして、my_sip_profile を選択します。

4. 「OK」ボタンをクリックします。

シナリオ 2

プロキシとローカルなクライアントを保護する - クライアントと同じネットワークにあるプロキシ

このシナリオでは、SIP プロキシと同様にローカルなクライアントを保護することを目的としています。プロキシは、クライアントと同じローカルネットワークに位置し、SIP 信号の送受信および 2 つのインタフェースにメディアデータのフローを行います。このシナリオについては、以下で図と共に説明します。



2 つの方法でこのシナリオを実行することができます。:
- NAT を使用してネットワークトポロジを隠します。
- 従って、NAT を使用しないと、ネットワークトポロジは危険にさらされてしまします。

ソリューション A - NAT を使用する

ここでは、プロキシとローカルクライアントが D-Link ファイアウォールの IP アドレスの背後に隠されます。設定手順は以下の通りです。

1. 上記オプションを使用して、SIP ALG オブジェクトを定義します。

2. サービスオブジェクトを定義し、これに SIP ALG オブジェクトを関連付けます。サービスは、以下である必要があります。
   - 宛先ポートは 5060 に設定します。(SIP 信号ポートの初期値)
   - タイプは TCP/UDP に設定します。

3. IP ルールセットに 3 つの IP ルールセットのエントリを定義します。

- 内部ネットワークのローカルプロキシやクライアントからの、インターネットなどのリモートクライアントへの外向きトラフィックに対する NAT ルール。SIP ALG は NAT ルールに必要とされるすべてのアドレス変換を行います。この変換は IP レベルおよびアプリケーションレベルの両方に生じます。クライアントまたはプロキシのいずれも、ローカルユーザが NAT 変換されることを知る必要はありません。

  Record-Route が SIP プロキシで有効であると、NAT ルールの送信元ネットワークにはローカルなクライアントではなく、SIP プロキシしか含むことができません。

- NAT 変換されるローカルプロキシのプライベート IPv4 アドレスに対する内向き SIP トラフィックをリダイレクトするための SAT ルール。SIP プロキシのプライベート IPv4 アドレスにインバウンドトラフィックを送信するため、このルールは、宛先インタフェース（つまり、NetDefendOS 自身）として core を持っています。

- 前の手順で定義した SAT ルール確定と同じタイプのトラフィックに適合する「Allow」ルール。

ルール	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク
OutboundFrom ProxyUsers	Allow/NAT	lan	lannet (ip_proxy)	wan	all-nets
InboundTo ProxyAndClients	Allow/SAT Dest IP: ip_proxy	wan	all-nets	core	wan_ip

Record-Route が有効になると、プロキシユーザからの外向きトラフィックの送信元ネットワークは、上記の通り「ip_proxy」を使用することによって、さらに制限されます。

着呼を受ける場合、SIP ALG は SAT ルールに従い、プロキシサーバに SIP リクエストを送信します。プロキシは順番にクライアントである最終送信先にリクエストを転送していきます。

Record-Route ルートがプロキシサーバで無効であると、SIP セッションの状態によっては、SIP ALG は、SIP プロキシを迂回して内向き SIP メッセージを直接クライアントに転送するかもしれません。これは、それ以上の設定はせずに自動的に起こります。

ソリューション B - NAT を使用しない

NAT を使用しない場合、外向き NAT エントリは Allow エントリに交換されます。内向きの SAT と AllowIP ルールセットのエントリは Allow エントリに交換されます。

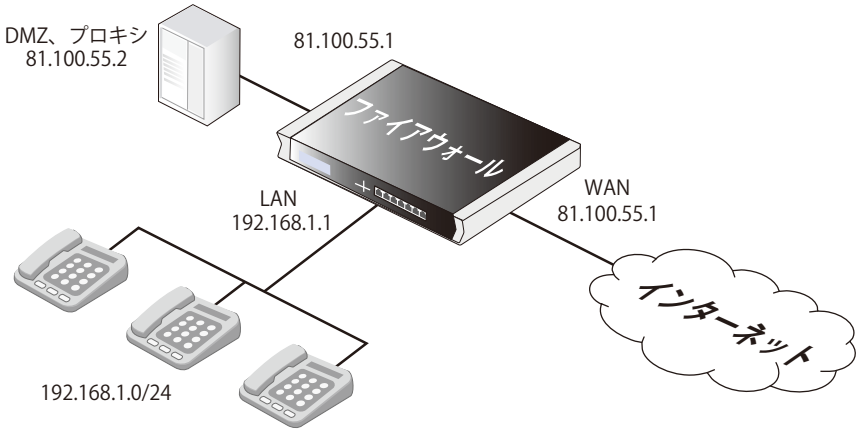
ルール	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク
OutboundFrom Proxy&Clients	Allow	lan	lannet (ip_proxy)	wan	all-nets
InboundTo Proxy&Clients	Allow	wan	all-nets	lan	lannet (ip_proxy)

Record-Route が有効になると、ネットワークは上記の通り「ip_proxy」を使用することによって、さらに制限されます。

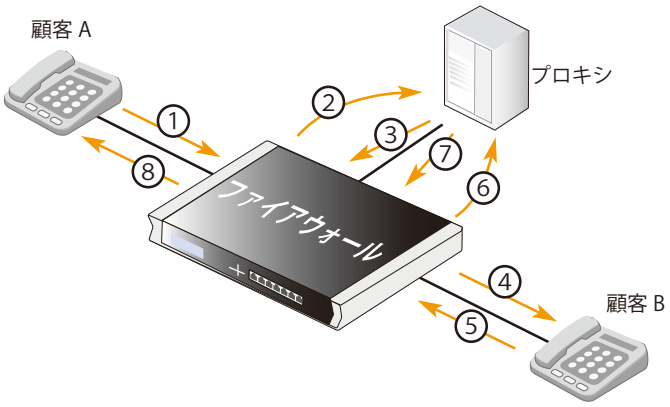
シナリオ 3

プロキシとローカルなクライアントを保護する - DMZ インタフェース上のプロキシ

このシナリオは前と同じですが、主な違いは、ローカルの SIP プロキシサーバの場所です。サーバはローカルなクライアントに対して別々のインタフェースとネットワークに置かれます。リモートのエンドポイントとローカルで保護されたクライアント間では初期の SIP トラフィックを決して直接交換しないため、この設定は付加的なセキュリティのレイヤを追加します。



SIP メッセージが 3 つのインタフェース（呼のイニシエータからの受信インタフェース、プロキシに向かう DMZ インタフェース、および呼のターミネータに向かう宛先インタフェース）をまたいで流れるので、このシナリオでは複雑性が増します。このシナリオでは呼が設定される場合に起こる初期のメッセージ交換について、以下の図に示しています。



図示された交換は以下の通りです。

順番	説明
1 と 2	DMZ の外向きのローカルプロキシサーバに初期の INVITE を送信します。
3 と 4	プロキシサーバはインターネット上の宛先に向かって SIP メッセージを送信します。
5 と 6	リモートクライアントまたはプロキシサーバがローカルのプロキシサーバに応答します。
7 と 8	ローカルのプロキシはローカルなクライアントに応答します。

本シナリオは、NAT（以下のソリューション B）のない設定と同様に DMZ（以下のソリューション A）におけるトポロジを隠す設定で実装することができます。

ソリューション A - NAT を使用する

この設定に関して注意する事項は以下の通りです。

- SIP プロキシの IP アドレスはグローバルにルーティング可能な IP アドレスとします。D-Link ファイアウォールは DMZ でのプロキシの隠蔽をサポートしていません。

- DMZ インタフェースの IP アドレスはグローバルにルーティング可能な IP アドレスとします。このアドレスは外部インタフェースで使用したものと同じにします。

設定手順は以下の通りです。

1. 上記オプションを使用して、SIP ALG オブジェクトを定義します。

2. サービスオブジェクトを定義し、これに SIP ALG オブジェクトに関連付けます。サービスは、以下である必要があります。

- 宛先ポートは 5060 に設定します。（SIP 信号ポートの初期値）
- タイプは TCP/UDP に設定します。
- プロトコルは SIP に設定します。

3. IP ルールセットに 4 つの IP ルールセットエントリを定義します。

- 内部ネットワークのクライアントから DMZ に位置するプロキシへの外向きトラフィックへの NAT エントリ。SIP ALG は NAT ルールに必要とされるすべてのアドレス変換を行います。この変換は IP レベルおよびアプリケーションレベルの両方に生じます。

注意 DMZ 上のプロキシに登録するクライアントは、コンタクトアドレスとして DMZ インタフェースの IP アドレスを持っています。

- DMZ インタフェースの背後のプロキシからインターネット上のリモートクライアントまでの外向きトラフィックに対する Allow エントリ。

- DMZ の背後にある SIP プロキシからファイアウォールの IP アドレスまでの内向き SIP トラフィックに対する AllowIP ルールセットエントリ。本ルールは宛先インタフェースとして core（つまり NetDefendOS 自身）を使用します。

  これは、上記 NAT エントリ用です。着呼を受ける場合、NetDefendOS は自動的にローカルなレシーバの場所を見つけて、アドレス変換を実行し、さらにレシーバに SIP メッセージを送信します。SIP ALG の内部状態に基づいてこれを行います。

- DMZ インタフェースの背後のプロキシまでの内向きトラフィック（インターネットなど）に対する AllowIP ルールセットエントリ。

4. また、Record-Route がプロキシで有効であると、プロキシを迂回した SIP メッセージの直接交換が、クライアント間で許可されます。従って、Record-Route が無効である場合、以下の追加のルール / ポリシーが必要となります。

- 内部ネットワークのクライアントからインターネットなどの外部クライアントおよびプロキシへの外向きトラフィックの NAT エントリ。SIP ALG は NAT ルールに必要とされるすべてのアドレス変換を行います。この変換は IP レベルおよびアプリケーションレベルの両方に生じます。

- インターネットなどから DMZ インタフェースの IP アドレスまでの内向き SIP トラフィックに対する「Allow」ルールセットエントリ。これは、ローカルなクライアントが、DMZ に位置するプロキシに登録する場合に DMZ インタフェースの IP アドレスを使用して NAT 変換されるためです。

本 IP ルールセットエントリは宛先インタフェースとして core（つまり NetDefendOS 自身）を持っています。着呼を受ける場合、NetDefendOS は自動的にローカルなレシーバの登録情報を使用し、アドレス変換を実行して、さらにレシーバに SIP メッセージを送信します。これは ALG の内部状態に基づいて実行されます。

Record-Route を有効とする必要がある IP ルールセットエントリは、以下の通りです。

	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク
OutboundToProxy	Allow/NAT	lan	lannet	dmz	ip_proxy
OutboundFromProxy	Allow	dmz	ip_proxy	wan	all-nets
InboundFromProxy	Allow	dmz	ip_proxy	core	dmz_ip
InboundToProxy	Allow	wan	all-nets	dmz	p_proxy

Record-Route が無効であると、以下の IP ルールセットエントリを上記に追加する必要があります。

	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク
OutboundBypassProxy	Allow/NAT	lan	lannet	wan	all-nets
InboundBypassProxy	Allow	wan	all-nets	core	ipdmz

ソリューション B - NAT を使用しない。
設定手順は以下の通りです。

1. 上記オプションを使用して、SIP ALG オブジェクトを定義します。

2. SIP ALG オブジェクトに関連するサービスオブジェクトを定義します。サービスは、以下である必要があります。

- 宛先ポートは 5060 に設定します。（SIP 信号ポートの初期値）
- タイプは TCP/UDP に設定します。
- IP ポリシーオブジェクトを使用するとき、Protocol プロパティを SIP に設定する必要があります。

3. IP ルールセットエントリに 4 つのルールを定義します。
- 内部ネットワークのクライアントから DMZ インタフェースに位置するプロキシへの外向きトラフィックへの Allow IP ルールセットのエントリ。

- DMZ インタフェースの背後のプロキシからインターネット上のリモートクライアントまでの外向きトラフィックに対する AllowIP ルールセットのエントリ。

- SIP プロキシから DMZ インタフェース背後の SIP プロキシまでの内向き SIP トラフィックへの Allow ルール / ポリシー。

- インターネット上のクライアントとプロキシから DMZ インタフェース背後のプロキシまでの内向きトラフィックに対する Allow ルール / ポリシー。

4. また、Record-Route がプロキシで有効であると、プロキシを迂回した SIP メッセージの直接交換が、クライアントの間で許可されます。従って、Record-Route が無効である場合、以下の 2 つの追加ルールが必要となります。

- ローカルネットワークのクライアントからインターネット上の外部クライアントおよびプロキシへの外向きトラフィックに対する AllowIP ルールセットのエントリ。

- インターネットからローカルネットワークのクライアントプロキシまでの内向き SIP トラフィックに対する AllowIP ルールセットのエントリ。

Record-Route が有効な IP ルールセットのエントリは、以下の通りです。

	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク
OutboundToProxy	Allow	lan	lannet	dmz	ip_proxy
OutboundFromProxy	Allow	dmz	ip_proxy	lan	lannet
InboundFromProxy	Allow	dmz	ip_proxy	core	dmz_ip
InboundToProxy	Allow	wan	all-nets	dmz	ip_proxy

Record-Route が無効であると、以下の IP ルールセットのエントリを上記に追加する必要があります。

	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク
OutboundBypassProxy	Allow	lan	lannet	wan	all-nets
InboundBypassProxy	Allow	wan	all-nets	lan	lannet

IP ルールを使用した SIP ALG の設定

このセクションでは、先に示した例題と同様の SIP ALG 設定内容を説明しますが、IP ポリシーではなく IP ルールを使用して説明します。IP ルールを使用した SIP セッションの設定手順は以下の通りです。

- SIP ALG オブジェクトを作成します。NetDefendOS バージョン 11.03.00 よる古いシステムでは、定義済み SIP ALG オブジェクトが使用されている可能性がありますが、カスタムサービスを作成することをお勧めします。
- SIP 通信用のサービスオブジェクトを作成し、ALG に割り当てます。
- SIP 通信用に、定義したサービスオブジェクトを使用する IP ルールまたは IP ポリシーオブジェクトを作成します。

例題 6.17

IP ルールを使用したローカルクライアント / インターネットプロキシを持つ SIP

この例題は、「IP ポリシーを使用したローカルクライアント / インターネットプロキシを持つ SIP」と同等の内容ですが、IP ポリシーではなく IP ルールを使用しています。

Web Interface

A. 以下の IP オブジェクトを定義します。:

- if1_net: 192.168.1.0/24
  （内部のネットワーク）
- proxy_ip: 81.100.55.2
  （SIP プロキシ）
- ip_wan: 81.100.55.1
  （ファイアウォールのパブリック IPv4 アドレス）

B. SIP ALG オブジェクトを定義します。

1. **Objects > ALG > Add > SIP ALG** の順にメニューをクリックします。
2. ALG の名前（ここでは my_sip_alg）を指定します。
3. 「OK」ボタンをクリックします。

C. SIP 用のカスタム Service オブジェクトを定義します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。
2. サービスの名前（ここでは my_sip_service）を指定します。
3. Type として UDP を選択します。
4. ALG として my_sip_alg を選択します。
5. Destination プロパティには、ポート番号 5060 を入力します。
6. 「OK」ボタンをクリックします。

D. 外向きの SIP トラフィックに IP ルールを定義します。:

1. **Rules > IP Rule Set > main > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: sip_nat
   - Action: NAT
   - Source Interface: if1
   - Source Network: if1_net
   - Destination Interface: ext
   - Destination Network: proxy_ip
   - Service: my_sip_service
   - Comment: Allow outgoing SIP calls.

3. 「OK」ボタンをクリックします。

E. 内向きの SIP トラフィックに IP ルールを定義します。:

1. **Rules > IP Rule Set > main > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: sip_allow
   - Action: Allow
   - Source Interface: ext
   - Source Network: proxy_ip
   - Destination Interface: core
   - Destination Network: ip_wan
   - Service: my_sip_service
   - Comment: Allow incoming SIP traffic

3. 「OK」ボタンをクリックします。

6.1.10 H.323

概要

H.323 は、ITU（International Telecommunication Union）によって承認された規格で、IP ネットワーク上のビデオカンファレンスの互換性を可能にします。これは、インターネットなどのパケットベースのネットワーク上でリアルタイムオーディオ、ビデオおよびデータ通信に使用されます。H.323 は、IP 電話や VoIP を含むマルチメディア通信を提供するコンポーネント、プロトコルおよび手順を規定しています。

H.323 コンポーネント

H.323 規格は以下の 4 つの主要なコンポーネントで構成されています。

項目	説明
ターミナル	例えば、電話、カンファレンス用のユニット、またはソフトウェアフォン（例 : NetMeeting）などのオーディオおよびオプションでビデオ、またはデータ通信に使用されるデバイスです。
ゲートウェイ	H.323 ゲートウェイは 2 つの異なるネットワークを接続し、それらの間でトラフィックを変換します。H.323 ゲートウェイは H.323 ネットワークと公衆交換電話網（PSTN）などの H.323 ではないネットワーク間に接続性を提供します。また、異なるネットワーク間でプロトコルの変換とメディアの変換を行います。ゲートウェイは 2 つの H.323 ターミナル間の通信には必要ありません。
ゲートキーパー	ゲートキーパーはターミナルとゲートウェイのアドレッシング、許可、および認証に使用される H.323 システム内のコンポーネントです。これは帯域管理、アカウンティング、請求書の送付、料金の請求などを行うこともできます。ゲートキーパーはエンドポイント間で直接通話することを許可し、または follow-me/find-me（追跡転送機能）などの機能を実行し、話し中などに転送するためにコールシグナリングの経路を決めることが可能です。ゲートキーパーはパブリック IP だけを使用している NAT 配下で 1 個以上の H.323 ターミナルがある場合に必要となります。
MCU（Multipoint Control Units: 多地点接続装置）	MCU は 3 個以上の H.323 ターミナルのカンファレンスをサポートします。カンファレンスコールに参加するすべての H.323 ターミナルは MCU との接続を確立する必要があります。MCU は通話、リソース、ビデオおよび通話に使用されるオーディオコードを管理します。

H.323 プロトコル

H.323 で使用されるプロトコルを以下に簡単に説明します。

項目	説明
H.225 RAS シグナリングとコール制御（設定）シグナリング	H.225 プロトコルはコールシグナリングに使用されます。これは、H.323 エンドポイント間の接続を確立するために使用されます。このコールシグナルチャンネルが 2 つの H.323 エンドポイント間または H.323 とゲートキーパー間でオープンされます。H.323 エンドポイント間の通信のためには、TCP 1720 が使用されます。ゲートキーパーに接続する場合、UDP ポート 1719（H.225 RAS メッセージ）が使用されます。
H.245 メディア制御と転送	H.323 エンドポイント間に確立されたマルチメディアセッションの制御を提供します。最も重要なタスクは論理チャンネルのオープンとクローズをネゴシエーションすることです。論理チャンネルは、例えば音声通信に使用されるオーディオチャンネルです。ビデオと T.120 チャンネルもネゴシエーション中は論理チャンネルと呼ばれます。
T.120	通信とアプリケーションのプロトコル群です。H.323 製品のタイプによっては、T.120 プロトコルはホワイトボードのようなアプリケーション共有、ファイル転送およびカンファレンス機能に使用されます。

H.323 ALG 機能

H.323 ALG は D-Link ファイアウォールによって安全を確保されたプライベートネットワークに接続中に H.323 電話やアプリケーションなどの H.323 デバイスにデバイス間で電話をかけたり、受けたりすることを許可する柔軟なアプリケーションレイヤゲートウェイです。

IP アドレスやポートは H.323 メッセージのペイロードに送信されるため、H.323 の仕様は NAT を処理するためには設計されませんでした。H.323 ALG は、H.323 メッセージが正しい到達先へルーティングされ、ファイアウォールの経由が許可されるように、H.323 メッセージを編集し、変換します。

NetDefendOS が処理する H.323 ALG には以下の機能があります。

- NetDefendOS は H.323 のバージョン 5 仕様をサポートしています。この仕様は H.225.0 v5 と H.245 v10 に基づいています。
- 音声とビデオコールに加え、NetDefendOS は T.120 プロトコルによりアプリケーション共有をサポートしています。音声とビデオが UDP により転送される間、T.120 はデータを転送するために TCP を使用します。
- ゲートキーパーをサポートするため、ファイアウォールをコールが通過するように正しく設定されるように、NetDefendOS は H.323 エンドポイントとゲートキーパー間の RAS トラフィックをモニタします。
- NAT と SAT ルール / ポリシーがサポートされており、クライアントとゲートキーパーがファイアウォールの配下のネットワークでプライベート IPv4 アドレスを使用することができます。

NetDefendOS H.323 設定

NetDefendOS では、以下の 2 つの方法のうちのいずれかで H.323 の設定を行うことができます。

- IP ポリシーオブジェクトを持つ VoIP Profile オブジェクトを使用します。

  IP ポリシーオブジェクトを使用することで H.323 を設定することができます。これは、H.323 ALG の代わりに VoIP Profile オブジェクトを作成し、H.323 オプションを指定することで行われます。VoIP Profile オブジェクトをトラフィックを制御する IP ポリシーオブジェクトに関連付けます。また、H.323 トラフィックに設定された Service オブジェクトを、IP ポリシーオブジェクトと共に使用する必要があります。

  この Service オブジェクトでは、Protocol プロパティを H.323 に設定する必要があります。

  NetDefendOS 11.03 以降の初期設定では定義済み H.323 サービスオブジェクトで既に H.323 に設定された Protocol プロパティを持っています。これは、NetDefendOS11.03 以降にアップグレードされた環境では当てはまりません。

- IP ルールオブジェクトを持つ H.323 ALG オブジェクトを使用します。

  H.323 ALG オブジェクトは H.323 プロトコルに設定される Service オブジェクトに関連付けられます。サービスオブジェクトは H.323 トラフィックフローを制御する IP ルールオブジェクトと共に使用されます。

  NetDefendOS バージョン 11.03 以降、定義済みの H.323 ALG は初期設定では存在していません。そのため、H.323 を持つ IP Rule オブジェクトを使用する際には、常に新しい H.323 ALG オブジェクトを作成する必要があります。11.03 以降にアップグレードされる前の NetDefendOS バージョンでは、定義済みの H.323 ALG オブジェクトは保持されます。

H.323 設定

IP ポリシーを使用する場合、以下の H.323 ALG プロパティを関連する VoIP プロファイルで設定し、ALG の動作を制御することが可能です。

項目	説明
Allow TCP Data Channels	TCP ベースのデータチャンネルがネゴシエートされます。データチャンネルが例えば T.120 プロトコルによって使用されます。
Max TCP Data Channels	TCP データチャンネルの最大数を指定できます。
Max Gatekeeper Registration Lifetime	ゲートキーパー登録期間は、指定された時間枠内でクライアントの再登録を行うために NetDefendOS によって制御されます。短い時間を設定すると、クライアントからゲートキーパーへの頻繁な登録を生じさせ、ネットワークが利用不可になり、クライアントがまだ登録中である認識でいる場合に、問題が発生しづらくなります。
Translate Addresses	アドレス変換の初期値は Automatic です。Specific に設定されると、特定のネットワークと IP アドレスを設定できます。有効にしないと、論理チャンネルアドレスでアドレス変換は行われず、管理者は特定のシナリオで使用される IP アドレスとルートについて確認する必要があります。
Network と IP Address	Translate Address オプションが Specific に設定されると、本オプションを利用できます。NAT されるトラフィックに対して、Network は変換できるものを指定します。IP アドレスは、NAT する IPv4 アドレスを指定します。Translate Addresses が Automatic である場合、外部 IP アドレスは経路検索を通じて自動的に検出されます。
Channel Setup mode	Optimistic（初期値）または Normal を指定します。Optimistic 設定は、片方向のみが確立した場合に H.323 論理チャンネルがオープンします。Normal 設定は、両方向の通信が確立された場合に論理チャンネルがオープンします。

H.323 Service オブジェクト設定

次に提示されているのは、H.323 設定のいくつかの例です。各設定で、Service オブジェクトが使用されています。H.323 に作成される Service オブジェクトのプロパティは以下の通りである必要があります。

- **H.323 Service** - Type: TCP、Destination port: 1720
- **H.323 Gatekeeper Service** - Type: UDP、Destination port: 1719

h323 および h323-gatekeeper という定義済み Service オブジェクトが NetDefendOS にあり、例題で使用されるカスタム Service オブジェクトの代わりにこれらを使用できます。しかし、IP ポリシーとこれらのオブジェクトを使用する時、Service の Protocol プロパティが H.323 に設定されていることをチェックする必要があります。NetDefendOS11.03 以降の初期設定では、自動的にそのように設定されていますが、11.03 より前のバージョンから 11.03 にアップグレードした場合には当てはまりません。

IP ポリシーを使用した ALG セットアップの例

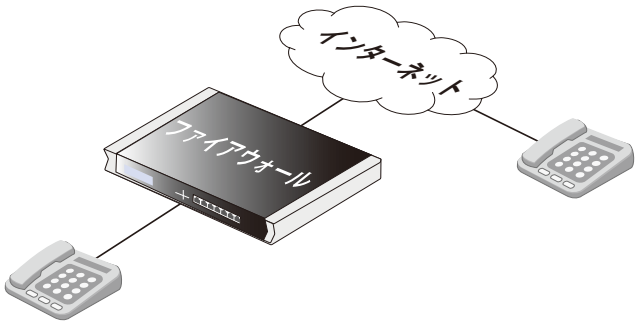
以下の例は、さまざまなシナリオで、IP ルールセットの IP ポリシーオブジェクトを使用して ALG をセットアップする方法を示しています。

例題 6.18

IP ポリシーオブジェクトを使用して内部 H.323 電話を保護する

この例題では、内部の H.323 電話は、lannet に位置していて、パブリック IP アドレスを持っています。この電話がインターネット上の別の H.323 電話に電話をかけ、インターネット上の H.323 電話が逆にこの電話に電話をかけることを許可するためには、IP ルールオブジェクトを設定する必要があります。

注意 : この例題では IP ルールの前に同じ種類のポート / トラフィックを許可する、または拒否するルール / ポリシーがないことを確認します。



Web Interface

新しい VoIP Profile オブジェクトを作成します。:

1. **Policies > Firewalling > VoIP > Add > VoIP Profile** の順にメニューをクリックします。

2. プロファイルの名前 (ここでは my_h323) を指定します。

3. 「OK」ボタンをクリックします。

H.323 にカスタム Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_h323_policy_service
   - Type: TCP
   - Destination port: 1720
   - Protocol: H.323

3. 「OK」ボタンをクリックします。

外向きの H.323 トラフィックに IP ポリシーを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: H323AllowOut
   - Action: Allow
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: any
   - Destination Network: all-nets
   - Service: my_h323_policy_service
   - Comment: Allow outgoing H.323 calls.

3. VoIP タブを選択し、VoIP を有効にして、my_h323_profile を選択します。

4. 「OK」ボタンをクリックします。

内向きの H.323 トラフィックに IP ポリシーを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: H323AllowIn
   - Action: Allow
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: lan
   - Destination Network: lannet
   - Service: my_h323_policy_service
   - Comment: Allow incoming H.323 calls.

3. VoIP タブを選択し、VoIP を有効にして、my_h323_profile を選択します。

4. 「OK」ボタンをクリックします。

例題 6.19

IP ポリシーを使用したプライベートアドレスを持つ H.323

この例題には、内部の H.323 電話がプライベート IPv4 アドレスを持つネットワークにあります。この電話がインターネット上の別の H.323 電話に電話をかけ、インターネット上の H.323 電話が逆にこの電話に電話をかけるためには、以下の IP ルールセットエントリを追加する必要があります。

注意 : 設定する IP ルールセットエントリの前に、同じ種類のトラフィックを許可 / 拒否するエントリがないことを確認します。

電話にプライベート IP を使用している場合、内向きのトラフィックには以下の例のとおり SAT が行われる必要があります。オブジェクト ip-phone は H.323 電話の内部 IP である必要があります。

Web Interface

VoIP プロファイルオブジェクトを作成する :

1. **Policies > Firewalling > VoIP > Add > VoIP Profile** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_h323_profile
   - SIP: Disable

3. 「OK」ボタンをクリックします。

H.323 のカスタムサービスを作成する :

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_h323_service
   - Type: TCP
   - Destination: 1720
   - Protocol: H.323

3. 「OK」ボタンをクリックします。

外向きの IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: h323_nat_out
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: any
   - Destination Network: all-nets
   - Service: my_h323_service
   - Comment: Allow outgoing H.323 calls.

4. Source Translation で以下の情報を入力します。
   - Address Translation: NAT
   - Address Action: Outgoing Interface IP

5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

6. 「OK」ボタンをクリックします。

内向き H.323 トラフィックに対する SAT IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: h323_sat_in
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip (ファイアウォールの外部 IP)
   - Service: my_h323_service
   - Comment: Allow incoming calls to H.323 phones via ip-phone.

4. Source Translation で以下の情報を入力します。
   - Address Translation: None

5. Destination Translation で以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Single IP
   - New IP Address: ip-phone

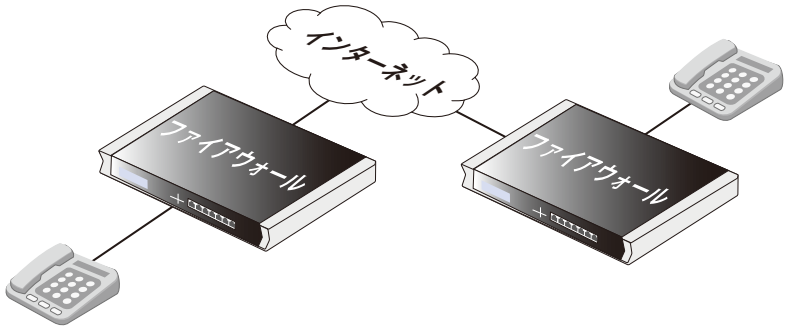
6. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

7. 「OK」ボタンをクリックします。

例題 6.20

IP ポリシーを使用した異なるファイアウォール内にある 2 つの電話

このシナリオは 2 つの H.323 電話で構成されます。 2 つの H.323 電話は、それぞれパブリック IPv4 アドレスを持つネットワーク上の D-LInk ファイアウォール内に接続しています。インターネット経由でこれらに電話をかけるためには、以下のエントリを両方のファイアウォールの IP ルールセットに追加します。これらのエントリの前に同じ種類のポート / トラフィックを許可する、または許可しないというエントリがないことを確認します。



Web Interface

VoIP プロファイルオブジェクトを作成する :

1. **Policies > Firewalling > VoIP > Add > VoIP Profile** の順にメニューをクリックします。

2. 以下の情報を入力します。

   - Name: my_h323_profile
   - SIP: Disable

3. 「OK」ボタンをクリックします。

H.323 にカスタム Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_h323_service
   - Type: TCP
   - Destination: 1720
   - Protocol: H.323

3. 「OK」ボタンをクリックします。

外向きトラフィックに適用する IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: h323_allow_out
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: any
   - Destination Network: all-nets
   - Service: my_h323_service
   - Comment: Allow outgoing H.323 calls.

4. Source Translation で以下の設定を行います。
   - Address Translation: None

5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

6. 「OK」ボタンをクリックします。

内向きトラフィックに対する IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: h323_allow_in
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: lan
   - Destination Network: lannet
   - Service: my_h323_service
   - Comment: Allow incoming calls.

4. Source Translation で以下の情報を入力します。
   - Address Translation: None

5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

6. 「OK」ボタンをクリックします。

例題 6.21

IP ポリシーの設定によりプライベート IPv4 アドレスを使用する

このシナリオは 2 つの H.323 電話で構成されます。 2 つの H.323 電話はそれぞれプライベート IPv4 アドレスを持つネットワーク上の D-Link ファイアウォール内に接続されています。インターネット経由でこれらに電話をかけるためには、以下のエントリを両方のファイアウォールの IP ルールセットに追加する必要があります。また、これらのエントリの前に同じ種類のポート / トラフィックを許可する、または許可しないというエントリがないことを確認します。

電話にプライベート IP を使用しているため、内向きのトラフィックには以下の例の通り SAT が行われる必要があります。以下のオブジェクトの ip-phone は各ファイアウォール内の H.323 電話の内部 IP である必要があります。

Web Interface

VoIP プロファイルオブジェクトを作成する :

1. **Policies > Firewalling > VoIP > Add > VoIP Profile** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_h323_profile
   - SIP: Disable

3. 「OK」ボタンをクリックします。

H.323 にカスタム Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_h323_service
   - Type: TCP
   - Destination: 1720
   - Protocol: H.323

3. 「OK」ボタンをクリックします。

外向きトラフィックに適用する NAT IP ポリシーを作成する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: h323_nat_out
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: any
   - Destination Network: all-nets
   - Service: my_h323_service
   - Comment: Allow outgoing H.323 calls.

4. Source Translation で以下の設定を行います。
   - Address Translation: NAT
   - Address Action: Outgoing Interface IP

5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

6. 「OK」ボタンをクリックします。

内向きトラフィックに対する SAT IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: h323_sat_in
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip (ファイアウォールの外部 IP)
   - Service: my_h323_service
   - Comment: Allow incoming calls to H.323 phone at ip-phone.

4. Source Translation で以下の情報を入力します。
   - Address Translation: None

5. Destination Translation で以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Single IP
   - New IP Address: ip-phone

6. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

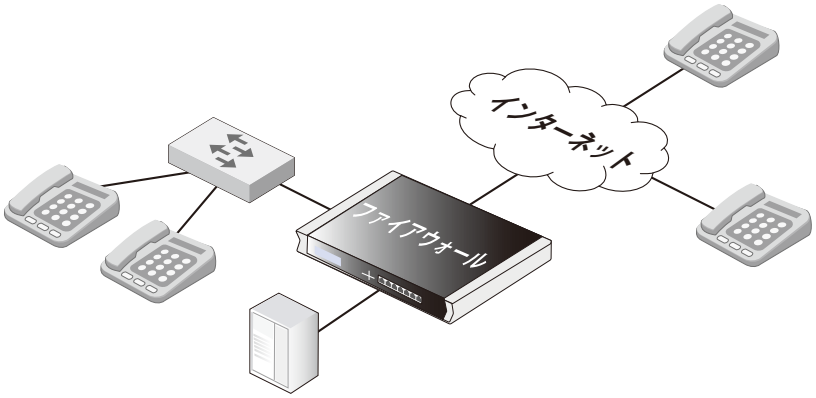
7. 「OK」ボタンをクリックします。

ファイアウォールの内側の電話にかけるために、ファイアウォール上の外部 IP アドレスに電話をかけます。複数の H.323 電話がファイアウォール内にある場合、 1 つの SAT IP ルールセットエントリを各電話に対して設定する必要があります。これは、複数の外部アドレスが使用される必要があることを意味します。しかし、1 つの外部アドレスだけを必要とする H.323 ゲートキーパーを使用することをお勧めします。

例題 6.22

IP ポリシーを使用したゲートキーパーを持つ H.323

このシナリオでは、H.323 ゲートキーパーがファイアウォールの DMZ 内に置かれています。H.323 電話が内部ネットワークに接続しているプライベートネットワークと DMZ 上のゲートキーパー間のトラフィックを許可するようにファイアウォールに IP ポリシーを設定します。DMZ 上のゲートキーパーはプライベートアドレスで設定されます。



Web Interface

VoIP プロファイルオブジェクトを作成する :

1. **Policies > Firewalling > VoIP > Add > VoIP Profile** の順にメニューをクリックします。

2. 以下の情報を入力します。

   - Name: my_h323_profile
   - SIP: Disable

3. 「OK」ボタンをクリックします。

H.323 ゲートキーパーにカスタム Service オブジェクトを作成します。

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_h323_gatekeeper_service
   - Type: UCP
   - Destination: 1719
   - Protocol: H.323

3. 「OK」ボタンをクリックします。

内向きのゲートキーパートラフィックに適用する SAT IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: h323_sat_gk_in
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip (ファイアウォールの外部 IP)
   - Service: my_h323_gatekeeper_service
   - Comment: SAT rule for incoming communication with the gatekeeper located at ip-gatekeeper.

4. Source Translation で以下の設定を行います。
   - Address Translation: None

5. Destination Translation で以下の設定を行います。
   - AAddress Translation: SAT
   - Address Action: Single IP
   - New IP Address: ip-gatekeeper

6. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

7. 「OK」ボタンをクリックします。

インターネットからゲートキーパーに送信されるトラフィックを許可する IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: h323_gk_in
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: dmz
   - Destination Network: ip-gatekeeper (ゲートキーパーの IP アドレス)
   - Service: my_h323_gatekeeper_service
   - Comment: Allow incoming communication with the gatekeeper.

4. Source Translation で以下の情報を入力します。
   - Address Translation: None

5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

6. 「OK」ボタンをクリックします。

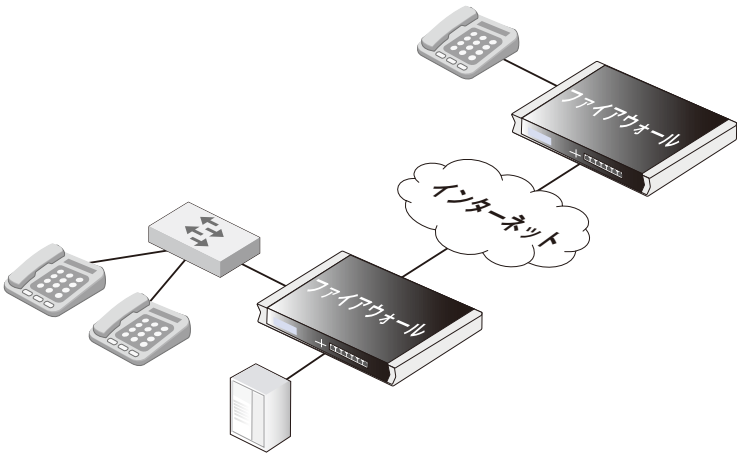
参照 発呼は特定の IP ポリシーを必要としません。

outgoing コールに特定の IP ポリシーを指定する必要はありません。NetDefendOS は、ゲートキーパーに登録されている外部の電話に内部の電話が電話できることを確認するために外部電話とゲートキーパー間の通信をモニタします。

例題 6.23

ゲートキーパーを持つ H.323 と 2 つの D-Link ファイアウォール

このシナリオは、1 つ前の例題に非常に似ていますが、ファイアウォールが「外部」電話を防御するという違いがあります。DMZ に接続しているゲートキーパーを持つファイアウォールは、1 つ前の例題にあるように正確に設定される必要があります。その他のファイアウォールは以下のように設定します。以下の IP ルールセットエントリを追加し、これらのエントリの前に同じ種類のポート / トラフィックを許可する、または許可しないというエントリがないことを確認します。



Web Interface

VoIP プロファイルオブジェクトを作成する :

1. **Policies > Firewalling > VoIP > Add > VoIP Profile** の順にメニューをクリックします。

2. 以下の情報を入力します。

   - Name: my_h323_profile
   - SIP: Disable

3. 「OK」ボタンをクリックします。

H.323 ゲートキーパーにカスタム Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_h323_gatekeeper_service
   - Type: UCP
   - Destination: 1719
   - Protocol: H.323

3. 「OK」ボタンをクリックします。

lannet からインターネットへ送信される外向きのゲートキーパートラフィックに対し、NAT IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: h323_nat_out
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: any
   - Destination Network: all-nets
   - Service: my_h323_gatekeeper_service
   - Comment: Allow outgoing communication from the gatekeeper.

4. Source Translation で以下の設定を行います。
   - Address Translation: NAT
   - Address Action: Outgoing Interface IP

5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

6. 「OK」ボタンをクリックします。

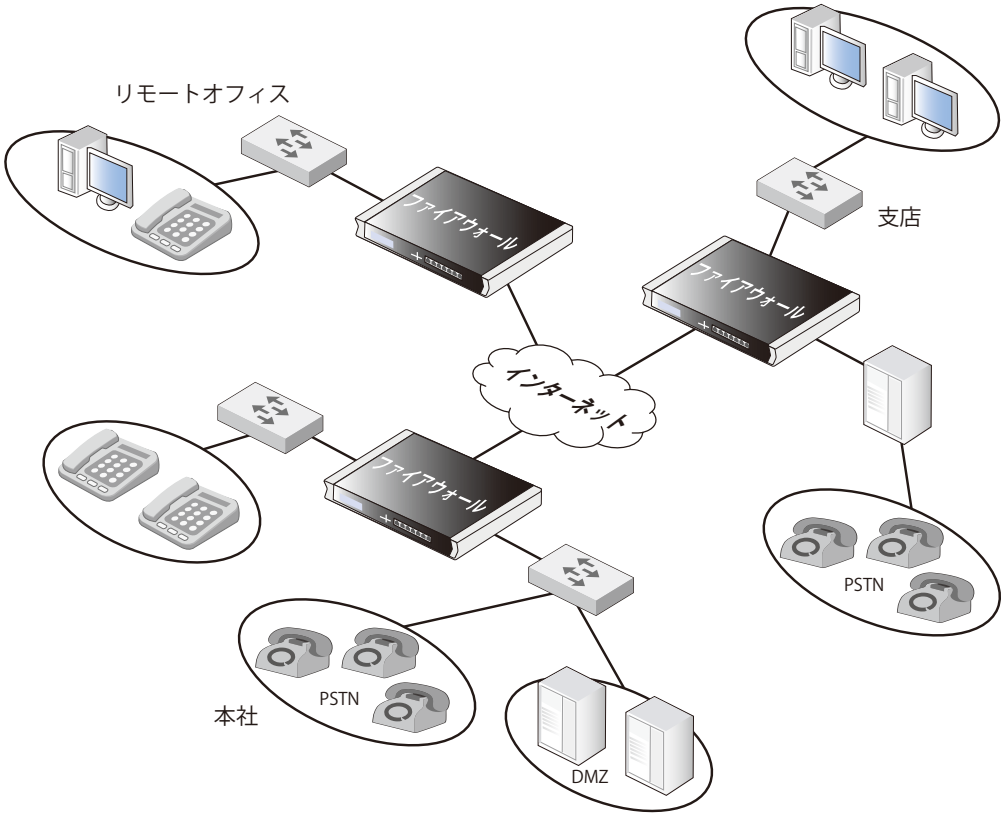
発呼は特定の IP ポリシーを必要としません。

outgoing コールに特定の IP ポリシーを指定する必要はありません。NetDefendOS は、ゲートキーパーに登録されている外部の電話に内部の電話が電話できることを確認するために外部電話とゲートキーパー間の通信をモニタします。

例題 6.24

エンタプライズの環境で H.323 を使用する（IP ポリシーを使用）

これは H.323 ALG をエンタプライズの環境に配置する方法を示すさらに複雑なシナリオの例です。本社の DMZ において、H.323 ゲートキーパーは、本社、支社、リモートオフィスのすべての H.323 クライアントを処理できる場所に置かれます。これによりエンタプライズ全体で音声通信とアプリケーション共有の両方でネットワークが使用可能になります。VPN トンネルが正しく設定され、すべてのオフィスがローカルネットワークのプライベート IP 範囲を使用しているものと仮定します。すべての外部コールが通常の電話網に接続しているゲートウェイ（ip-gateway）を使用して既存の電話網を経由して行われます。



本社には、DMZ の D-Link ファイアウォールに H.323 ゲートキーパーが配置されています。このファイアウォールに対し、以下の設定を行います。

Web Interface

VoIP プロファイルオブジェクトを作成する：

1. **Policies > Firewalling > VoIP > Add > VoIP Profile** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_h323_profile
   - SIP: Disable
3. 「OK」ボタンをクリックします。

H.323 ゲートキーパーにカスタム Service オブジェクトを作成します。：

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_h323_gatekeeper_service
   - Type: UCP
   - Destination: 1719
   - Protocol: H.323
3. 「OK」ボタンをクリックします。

lannet からゲートキーパーに送信されるトラフィックに対し、IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: lan_to_gk
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: dmz
   - Destination Network: ip-gatekeeper
   - Service: my_h323_gatekeeper_service
   - Comment: Allow H.323 entities on lannet to connect to the gatekeeper.

4. Source Translation で以下の設定を行います。
   - Address Translation: None

5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

6. 「OK」ボタンをクリックします。

ゲートウェイから lannet 状の内部電話に送信されるトラフィックに適用対し、IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: gw_to_lan
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: dmz
   - Source Network: ip-gateway
   - Destination Interface: lan
   - Destination Network: lannet
   - Service: my_h323_gatekeeper_service
   - Comment: Allow communication from the gateway to H.323 phones on lannet.

4. Source Translation で以下の設定を行います。
   - Address Translation: None

5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

6. 「OK」ボタンをクリックします。

支社ネットワークから DMZ 上のゲートキーパーに送信されるトラフィックを許可する IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: branch_to_gw
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: vpn-branch
   - Source Network: branch-net
   - Destination Interface: dmz
   - Destination Network: ip-gatekeeper, ip-gateway
   - Service: my_h323_gatekeeper_service
   - Comment: Allow communication with the gatekeeper on DMZ from the branch network.

4. Source Translation で以下の設定を行います。
   - Address Translation: None

5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

6. 「OK」ボタンをクリックします。

VPN からゲートキーパーへのトラフィックを許可する IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: vpn_to_gw
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: vpn-remote
   - Source Network: remote-net
   - Destination Interface: dmz
   - Destination Network: ip-gatekeeper
   - Service: my_h323_gatekeeper_service
   - Comment: Allow communication with the gatekeeper on DMZ from the remote network.

4. Source Translation で以下の設定を行います。
   - Address Translation: None

5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

6. 「OK」ボタンをクリックします。

例題 6.25

リモートオフィスの H.323 設定（IP ポリシーを使用）

支社とリモートオフィスの H.323 電話とアプリケーションが、本社にある H.323 ゲートキーパーを使用する場合、リモートオフィスと支社の D-Link ファイアウォールを以下の通り設定する必要があります。ここでは、インタフェース vpn-hq は、本社に位置するネットワーク hq-net への VPN トンネルです。

注意：この IP ポリシーは、支社およびリモートオフィスのファイアウォール両方に設定する必要があります。

Web Interface

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: to_gk
   - Action: Allow
3. Filter で以下の情報を入力します。
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: vpn-hq
   - Destination Network: hq-net
   - Service: my_h323_gatekeeper_service
   - Comment: Allow communication with the gatekeeper connected to the head office DMZ.
4. Source Translation で以下の設定を行います。
   - Address Translation: None
5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile
6. 「OK」ボタンをクリックします。

例題 6.26

H.323 ゲートウェイのゲートキーパーへの登録を許可する（IP ポリシーを使用）

支社の D-Link ファイアウォールには DMZ に接続する H.323 ゲートウェイがあります。H.323 ゲートウェイが、本社にある H.323 ゲートキーパーに登録を許可されるためには、以下のルールを設定する必要があります。

Web Interface

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: gw_to_gk
   - Action: Allow
3. Filter で以下の情報を入力します。
   - Source Interface: dmz
   - Source Network: ip-branchgw
   - Destination Interface: vpn-hq
   - Destination Network: hq-net
   - Service: my_h323_gatekeeper_service
   - Comment: Allow the gateway to communicate with the gatekeeper connected to the head office.
4. Source Translation で以下の設定を行います。
   - Address Translation: None
5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile
6. 「OK」ボタンをクリックします。

参照 発呼は特定の IP ポリシーを必要としません。
outgoing コールに特定の IP ポリシーを指定する必要はありません。NetDefendOS は、ゲートキーパーに登録されている外部の電話に内部の電話が電話できることを確認するために外部電話とゲートキーパー間の通信をモニタします。

IP ルールを使用した ALG セットアップの例

以降の例では、このセクションの例を繰り返しますが、IP ポリシーオブジェクトの代わりに IP ルールオブジェクトを使用します。
H323 ALG セットアップには IP ポリシーの使用が推奨されます。以降の例は情報を補完するために記載されています。

例題 6.27

IP ルールを使用して内部 H.323 電話を保護する

この例題は、「IP ポリシーオブジェクトを使用して内部 H.323 電話を保護する」と同等の内容ですが、IP ポリシーではなく IP ルールを使用します。

Web Interface

新しい H.323 ALG オブジェクトを作成します。:

1. **Objects > ALG > Add > H.323 ALG** の順にメニューをクリックします。
2. ALG の名前（ここでは my_h323_alg）を指定します。
3. 「OK」ボタンをクリックします。

H.323 にカスタム Service オブジェクトを作成します。:

1. Objects > Services > Add > TCP/UDP の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_h323_service
   - Type: TCP
   - ALG: my_h323_alg
   - Destination port: 1720
3. 「OK」ボタンをクリックします。

外向きの H.323 トラフィックに IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: H323AllowOut
   - Action: Allow
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: any
   - Destination Network: all-nets
   - Service: my_h323_service
   - Comment: Allow outgoing H.323 calls.
3. 「OK」ボタンをクリックします。

内向きの H.323 トラフィックに IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: H323AllowIn
   - Action: Allow
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: lan
   - Destination Network: lannet
   - Service: my_h323_service
   - Comment: Allow incoming H.323 calls.
3. 「OK」ボタンをクリックします。

例題 6.28

IP ルールを使用したプライベートアドレスを持つ H.323

この例題は、「IP ポリシーを使用したプライベートアドレスを持つ H.323」と同等の内容ですが、IP ポリシーではなく IP ルールを使用します。

Web Interface

新しい H.323 ALG オブジェクトを作成します。:

1. **Objects > ALG > Add > H.323 ALG** の順にメニューをクリックします。
2. ALG の名前（ここでは my_h323_alg）を指定します。
3. 「OK」ボタンをクリックします。

H.323 にカスタム Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_h323_service
   - Type: TCP
   - ALG: my_h323_alg
   - Destination port: 1720
3. 「OK」ボタンをクリックします。

外向き IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: H323Out
   - Action: NAT
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: any
   - Destination Network: all-nets
   - Service: my_h323_service
   - Comment: Allow outgoing H.323 calls.
3. 「OK」ボタンをクリックします。

内向きの H.323 トラフィックに SAT IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: H323In
   - Action: SAT
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip（ファイアウォールの外部 IP）
   - Service: my_h323_service
   - Comment: Allow incoming calls to H.323 phones via ip-phone.
3. SAT で以下の設定を行います。
   - SAT translate: Destination IP
   - New IP Address: ip-phone (電話の IP アドレス)
4. 「OK」ボタンをクリックします。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: H323In
   - Action: Allow
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip（ファイアウォールの外部 IP）
   - Service: my_h323_service
   - Comment: Allow incoming calls to H.323 phones via ip-phone.

3. 「OK」ボタンをクリックします。

例題 6.29

IP ルールを使用した異なるファイアウォール内にある 2 つの電話

この例題は、「IP ポリシーを使用した異なるファイアウォール内にある 2 つの電話」と同等の内容ですが、IP ポリシーではなく IP ルールを使用します。

Web Interface

H.323 ALG オブジェクトを作成します。

1. **Objects > ALG > Add > H.323 ALG** の順にメニューをクリックします。

2. ALG の名前（ここでは my_h323_alg）を指定します。

3. 「OK」ボタンをクリックします。

H.323 にカスタム Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_h323_service
   - Type: TCP
   - ALG: my_h323_alg
   - Destination port: 1720

3. 「OK」ボタンをクリックします。

外向きトラフィックの IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: H323AllowOut
   - Action: Allow
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: any
   - Destination Network: all-nets
   - Service: my_h323_service
   - Comment: Allow outgoing H.323 calls.

3. 「OK」ボタンをクリックします。

内向きトラフィックの IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: H323AllowIn
   - Action: Allow
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: lan
   - Destination Network: lannet
   - Service: my_h323_service
   - Comment: Allow incoming H.323 calls.

3. 「OK」ボタンをクリックします。

例題 6.30

プライベート IPv4 アドレスを使用する（IP ルールを使用）

この例題は、「プライベート IPv4 アドレスを使用する（IP ルールを使用）」と同等の内容ですが、IP ポリシーではなく IP ルールを使用します。

Web Interface

新しい H.323 ALG オブジェクトを作成します。:

1. **Objects > ALG > Add > H.323 ALG** の順にメニューをクリックします。

2. ALG の名前（ここでは my_h323_alg）を指定します。

3. 「OK」ボタンをクリックします。

H.323 にカスタム Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_h323_service
   - Type: TCP
   - ALG: my_h323_alg
   - Destination port: 1720

3. 「OK」ボタンをクリックします。

外向きトラフィックの NAT IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: H323Out
   - Action: NAT
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: any
   - Destination Network: all-nets
   - Service: my_h323_service
   - Comment: Allow outgoing H.323 calls.

3. 「OK」ボタンをクリックします。

内向きトラフィックの SAT IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: H323In
   - Action: SAT
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip（ファイアウォールの外部 IP）
   - Service: my_h323_service
   - Comment: Allow incoming calls to H.323 phone at ip-phone.

3. SAT で以下の設定を行います。
   - SAT translate: Destination IP
   - New IP Address: ip-phone (電話の IP アドレス)

4. 「OK」ボタンをクリックします。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: H323In
   - Action: Allow
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: (ファイアウォールの外部 IP)
   - Service: my_h323_service
   - Comment: Allow incoming calls to H.323 phone at ip-phone.

3. 「OK」ボタンをクリックします。

例題 6.31

ゲートキーパーを持つ H.323（IP ルールを使用）

この例題は、「IP ポリシーを使用したゲートキーパーを持つ H.323」と同等の内容ですが、IP ポリシーではなく IP ルールを使用します。

Web Interface

新しい H.323 ALG オブジェクトを作成します。:

1. **Objects > ALG > Add > H.323 ALG** の順にメニューをクリックします。

2. ALG の名前（ここでは my_h323_alg）を指定します。

3. 「OK」ボタンをクリックします。

H.323 ゲートキーパーにカスタム Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_h323_gatekeeper_service
   - Type: UDP
   - ALG: my_h323_alg
   - Destination port: 1719

3. 「OK」ボタンをクリックします。

内向きのゲートキーパートラフィックに SAT IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: H323In
   - Action: SAT
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip（ファイアウォールの外部 IP）
   - Service: my_h323_gatekeeper_service
   - Comment: SAT rule for incoming communication with the gatekeeper located at ip_gatekeeper

3. SAT で以下の設定を行います。
   - SAT translate: Destination IP
   - New IP Address: ip-gatekeeper（ ゲートキーパーの IP アドレス）

4. 「OK」ボタンをクリックします。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: H323In
   - Action: Allow
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip（ファイアウォールの外部 IP）
   - Service: my_h323_gatekeeper_service
   - Comment: Allow incoming communication with the gatekeeper.

3. 「OK」ボタンをクリックします。

lannet からゲートキーパーへのトラフィックを許可する IP ルールを作成します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: H323In
   - Action: Allow
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: dmz
   - Destination Network: ip-gatekeeper（ゲートキーパーの IP アドレス）
   - Service: my_h323_gatekeeper_service
   - Comment: Allow incoming communication with the gatekeeper.

3. 「OK」ボタンをクリックします。

例題 6.32

ゲートキーパーを持つ H.323 と 2 つの D-Link ファイアウォール（IP ルールを使用）

この例題は、「ゲートキーパーを持つ H.323 と 2 つの D-Link ファイアウォール」と同等の内容ですが、IP ポリシーではなく IP ルールを使用します。

Web Interface

新しい H.323 ALG オブジェクトを作成します。:

1. **Objects > ALG > Add > H.323 ALG** の順にメニューをクリックします。
2. ALG の名前（ここでは my_h323_alg）を指定します。
3. 「OK」ボタンをクリックします。

H.323 gatekeeper にカスタム Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_h323_gatekeeper_service
   - Type: UDP
   - ALG: my_h323_alg
   - Destination port: 1719
3. 「OK」ボタンをクリックします。

lannet から外向きのゲートキーパートラフィックがインターネットに NAT されることを許可する IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: H323Out
   - Action: NAT
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: any
   - Destination Network: all-nets
   - Service: my_h323_gatekeeper_service
   - Comment: Allow outgoing communication from the gatekeeper.
3. 「OK」ボタンをクリックします。

例題 6.33

エンタプライズの環境で H.323 を使用する（IP ルールを使用）

この例題は、「エンタプライズの環境で H.323 を使用する（IP ポリシーを使用）」と同等の内容ですが、IP ポリシーではなく IP ルールを使用します。

Web Interface

新しい H.323 ALG オブジェクトを作成します。:

1. **Objects > ALG > Add > H.323 ALG** の順にメニューをクリックします。
2. ALG の名前（ここでは my_h323_alg）を指定します。
3. 「OK」ボタンをクリックします。

H.323 gatekeeper にカスタム Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_h323_gatekeeper_service
   - Type: UDP
   - ALG: my_h323_alg
   - Destination port: 1719
3. 「OK」ボタンをクリックします。

lannet からゲートキーパーまでのトラフィックに IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: LanToGK
   - Action: Allow
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: dmz
   - Destination Network: ip-gatekeeper
   - Service: my_h323_gatekeeper_service
   - Comment: Allow H.323 entities on lannet to connect to the gatekeeper.
3. 「OK」ボタンをクリックします。

ゲートウェイから lannet の上の内部電話へのトラフィックに IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: GWToLan
   - Action: Allow
   - Source Interface: dmz
   - Source Network: ip-gateway
   - Destination Interface: lan
   - Destination Network: lannet
   - Service: my_h323_gatekeeper_service
   - Comment: Allow communication from the gateway to H.323 phones on lannet.
3. 「OK」ボタンをクリックします。

支社ネットワークから DMZ 上のゲートキーパーへのトラフィックに IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: BranchToGW
   - Action: Allow
   - Source Interface: vpn-branch
   - Source Network: branch-net
   - Destination Interface: dmz
   - Destination Network: ip-gatekeeper, ip-gateway
   - Service: my_h323_gatekeeper_service
   - Comment: Allow communication with the gatekeeper on DMZ from the branch network.

3. 「OK」ボタンをクリックします。

VPN からゲートキーパーまでのトラフィックに IP ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: BranchToGW
   - Action: Allow
   - Source Interface: vpn-remote
   - Source Network: remote-net
   - Destination Interface: dmz
   - Destination Network: ip-gatekeeper
   - Service: my_h323_gatekeeper_service
   - Comment: Allow communication with the gatekeeper on DMZ from the remote.

3. 「OK」ボタンをクリックします。

例題 6.34

リモートオフィスの H.323 設定（IP ルールを使用）

この例題は、「リモートオフィスの H.323 設定（IP ポリシーを使用）」と同等の内容ですが、IP ポリシーではなく IP ルールを使用します。

Web Interface

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: ToGK
   - Action: Allow
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: vpn-hq
   - Destination Network: hq-net
   - Service: my_h323_gatekeeper_service
   - Comment: Allow communication with the gatekeeper connected to the head office DMZ.

3. 「OK」ボタンをクリックします。

例題 6.35

H.323 ゲートウェイのゲートキーパーへの登録を許可する（IP ルールを使用）

この例題は、「H.323 ゲートウェイのゲートキーパーへの登録を許可する（IP ポリシーを使用）」と同等の内容ですが、IP ポリシーではなく IP ルールを使用します。

Web Interface

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: GWToGK
   - Action: Allow
   - Source Interface: dmz
   - Source Network: ip-branchgw
   - Destination Interface: vpn-hq
   - Destination Network: hq-net
   - Service: my_h323_gatekeeper_service
   - Comment: Allow the gateway to communicate with the gatekeeper connected to the head office.

3. 「OK」ボタンをクリックします。

6.1.11 TLS ALG

概要

Transport Layer Security（TLS）は、エンドポイント認証の提供ならびに暗号を使用して 2 つのエンドポイント間のパブリックインターネットに安全な通信を提供するプロトコルです。通常、TLS のクライアント / サーバのシナリオでは、暗号化通信の開始前にサーバの識別子だけが認証されます。

カスタマがオンラインバンキングのファシリティにアクセスする場合など Web ブラウザが TLS を使用するサーバに接続すると、TLS に頻繁に遭遇します。これは、HTTPS 接続と呼ばれることもあり、しばしばブラウザのナビゲーションバーに現れる南京錠アイコンによって示されます。

TLS は、サーバに対するクライアントからの安全なアクセスのために便利で簡単なソリューション提供し、IPsec を使用するなど他のタイプの VPN ソリューションのような多くの複雑な面を回避します。多くの Web ブラウザは TLS をサポートしており、ユーザは追加のソフトウェアを必要としないで容易に安全なサーバアクセスを行うことができます。

NetDefendOS は SSL ではなく TLS をサポートしています

TLS は、Secure Sockets Layer（SSL）を継承するものですが、その違いはわずかです。そのため、多くの場合、TLS と SSL は同等と見なされます。しかし、NetDefendOS は TLS のみをサポートしており、NetDefendOS ドキュメント内の SSL への言及は TLS を指しているものとします。TLS ALG は、SSL のエンドポイントとして機能しているため、SSL の終端を提供していると言えます。

NetDefendOS がサポートする暗号スイートと TLS バージョン

NetDefendOS は SSL VPN 用に多くの暗号アルゴリズムをサポートしています。初期値ではその中の一部が有効であり、それぞれを有効または無効にできます。サポートしているすべてのアルゴリズムは「13.9 SSL/TLS 設定」にあります。NetDefendOS は TLS バージョン 1.1 を除き、TLS バージョン 1.0 と 1.2 をサポートしていることに注意してください。バージョン 1.2 を無効にして、1.0 だけを使用する方法については「13.9 SSL/TLS 設定」を参照してください。

また、NetDefendOS TLS ALG と SSL VPN の両方が、RFC 5746 によって定義される通り、再ネゴシエーションをサポートします。

TLS は証明書に基づいています。

TLS セキュリティはデジタル証明書の使用に基づいています。この証明書はサーバ側に存在し、サーバの身元を確立して暗号化のベースとするために、TLS セッションの開始時にクライアントへ送信されます。CA が署名した証明書を使用することが可能であり、この場合、クライアントの Web ブラウザによって自動的に証明書の有効性が認定されます。

サーバの CA 署名入り証明書の代わりに自己署名の証明書を使用することもできます。自己署名の証明書を使用する場合、クライアントの Web ブラウザが、証明書の信頼性が認定されないとユーザに警告します。操作を継続するには、ユーザはブラウザで明示的に証明書を許可する必要があります。

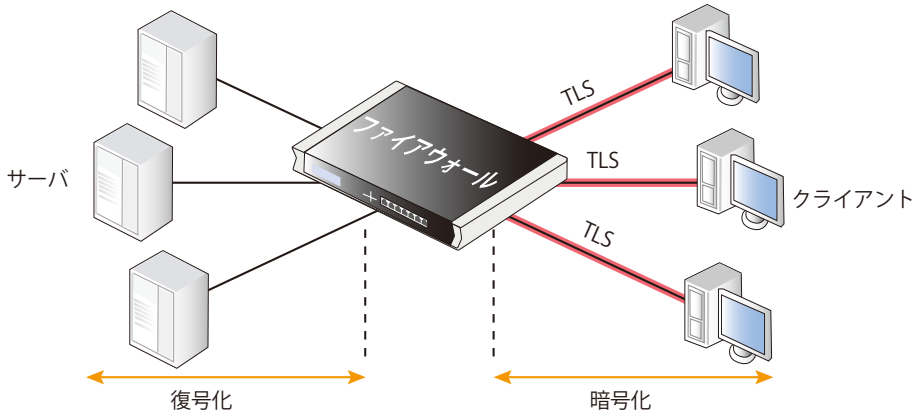


図 6-7　TLS 終端

TLS 終端に NetDefendOS を使用する利点

TLS はクライアントが接続するサーバで直接実装することができますが、サーバが D-Link ファイアウォールの背後で防御されている場合、NetDefendOS は、TLS エンドポイントの役目を果たすことができます。NetDefendOS は、クライアントへ（から）のデータの TLS 認証、暗号化、および復号化、およびサーバへ（から）の復号化データの転送を行います。この手法の利点は以下の通りです。

- 個々のサーバに設定する代わりに D-Link ファイアウォールに TLS のサポートを集約できます。
- 個々のサーバの代わりにファイアウォールで集中的に証明書を管理することができます。ユニークな証明書（または、1 通のワイルドカード証明書）が各サーバに存在する必要はありません。
- TLS によって必要とされる暗号化 / 復号化処理のオーバヘッドはファイアウォールにオフロードすることができます。これは、SSL アクセラレーション呼ばれることもあります。しかし、実現可能な処理の利点はさまざまであり、サーバとファイアウォールの比較処理能力に依存します。
- 復号化された TLS トラフィックは、トラフィックシェーピングや IDP スキャンを使用したサーバの脅威の検索など他の NetDefendOS 機能を受けることがあります。
- 複数サーバにトラフィックを広げる手段を提供するために、NetDefendOS サーバのロードバランシングに TLS を組み合わせることができます。

サーバが提供する URL

TLS 終端に NetDefendOS を使用する場合、D-Link ファイアウォールの背後にあるサーバによって提供された Web ページの URL は変更されないことに注意してください。

つまり、クライアントが https:// プロトコルを使用して D-Link ファイアウォールの背後の Web サーバに接続している場合、NetDefendOS は、http:// プロトコルを持つ絶対的な URL を含んで返送された（恐らく同じサイトの他のページを参照するような）Web ページの URL を https:// には変換しません。この問題のソリューションは、サーバが絶対的な URL の代わりに相対的な URL を使用することです。

NetDefendOS TLS がサポートする暗号スイート

NetDefendOS は TLS 用に多くの暗号アルゴリズムをサポートします。これらを、「13.9 SSL/TLS 設定」で記述される詳細設定を使用して、グローバルに有効または無効にできます。

初期値では、最も高い安全が考慮されている 4 つのアルゴリズムだけが有効です。より弱いアルゴリズムを有効にすることは推奨されません。これは、本来下位互換のために存在するものです。

TLS の制限事項

TLS ALG を使用する場合の制限は以下の通りです。

- クライアント認証はサポートされていません。（NetDefendOS がクライアントのアイデンティティを認証します）
- リネゴシエーションはサポートしていません。
- サーバの鍵交換メッセージの送信は未サポートです。これは、エクスポート暗号を使用するには、証明書の鍵が十分弱くなければならないことを意味します。
- NetDefendOS が使用する証明書チェーンには、最大 2 通の証明書を含むことができます。

TLS ALG の設定方法

TLS ALG は、以下のいずれかの方法で設定を行います。

- **IP ポリシーを使用する**
  IP ポリシーオブジェクトを使用する方法が、推奨される設定方法です。TLS ALG オプションは、IP ポリシーのプロパティを設定することで直接設定することができます。IP ポリシーで TLS オプションを設定するには、ポリシーの Service プロパティに指定したサービスの Protocol プロパティが TLS に設定されている必要があります。

- **IP ルールを使用する**
  IP ルールオブジェクトを使用する場合、TLS ALG オブジェクトをサービスオブジェクトに割り当て、それを IP ルールに割り当てます。

  この方式は古い NetDefendOS バージョンとの互換性を保つ場合に役に立ちますが、IP ポリシーと比較して利点はありません。

IP ポリシーを使用して TLS ALG を設定する

IP ポリシーを使用して TLS を有効にするための手順は以下の通りです。

1. TLS で使用するホストとルート証明書を NetDefendOS にアップロードします。
2. TCP プロトコルに基づいて新しいカスタムサービスオブジェクトを作成し、プロトコルプロパティに TLS を設定します。
3. ターゲットとするトラフィックに IP ポリシーを作成し、カスタムサービスオブジェクトをそれに関連付けます。
4. IP ポリシーに対して TLS を有効化し、ポリシーでホストとルート証明書の設定を行います。ホスト証明書は 1 つのみですが、ルート証明書は複数存在する可能性があります。

自己署名証明書を使用する

TLS ALG で使用する証明書が自己署名証明書の場合、ルート証明書とホスト証明書は両方とも同じ証明書に設定しなければなりません。

例題 6.36

IP ポリシーを使用した TLS ALG のセットアップ

この例題では、インターネット上の TLS クライアントから内部 Web サーバへの接続を許可する IP ポリシーオブジェクトを設定します。インターネットには、IPv4 アドレス wan_ip が割り当てられた wan インタフェースから接続します。Web サーバは DMZ に配置され、プライベート IPv4 アドレス 10.0.0.5 が設定されているものとします。この IP ポリシーでは SAT アドレス変換を行います。

証明書ファイル my_root_cert および my_host_cert がファイアウォールにアップロード済みであると想定します。

CLI

A. TLS 用のカスタムサービスを作成する :

```
DFL-xxxx:/> add Service ServiceTCPUDP my_tls_service Type=TCP DestinationPorts=443 Protocol=TLS
```

B. SAT IP ポリシーを作成する :

```
DFL-xxxx:/> add IPPolicy Name=SAT_TLS_To_DMZ SourceInterface=wan SourceNetwork=all-nets
            DestinationInterface=core DestinationNetwork=wan_ip Service=my_tls_service Action=Allow
            SourceAddressTranslation=None DestAddressTranslation=SAT DestAddressAction=SingleIP Dest-
            NewIP=10.0.0.5 TLSControl=Yes TLSHostCert=my_host_cert TLSRootCert=my_root_cert
```

Web Interface

A. TLS 用のカスタムサービスを作成する :

1. **Objects > Services > Add > TCP/UDP** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_tls_service
   - Type: TCP
   - Destination: 443
   - Protocol: TLS

3. 「OK」ボタンをクリックします。

B. SAT IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: SAT_TLS_To_DMZ
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: wan
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip
   - Service: my_tls_service

4. Source Translation で以下の情報を入力します。
   - Address Translation: None

5. Destination Translation で以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Single IP
   - New IP Address: 10.0.0.5

6. TLS タブを選択し、以下の設定を行います。
   - Enable TLS settings: ON
   - Host certificate: my_host_cert
   - Root certificates: my_root_cert

7. 「OK」ボタンをクリックします。

IP ルールを使用した TLS ALG の設定

TLS ALG の設定手順として、IP ポリシーと比較して間接的な方法となりますが、IP ルールを使用することも可能です。以下の手順で設定します。

1. TLS で使用するホスト証明書、ルート証明書を NetDefendOS にアップロードします。
2. 新規の TLS ALG オブジェクトを定義しして、適切なホスト / ルート証明書に紐づけます。
3. TCP プロトコルに基づく新規のカスタムサービスオブジェクトを作成します。
4. 作成したサービスオブジェクトに TLS ALG オブジェクトを割り当てます。
5. ターゲットのトラフィックに対して NAT または Allow IP ルールを作成し、カスタムサービスを割り当てます。
6. オプションで、非暗号化トラフィックに対して送信先ポートを変更する SAT ルールを作成することも可能です。または、ロードバランシングを行う SLB_SAT ルールを使用することもできます（カスタムサービスオブジェクトにより送信元ポートを変更することも可能）。

6.1.12 DNS ALG

概要

DNS クエリは、悪意ある第三者による攻撃の手段となり得ます。DNS ALG 機能を使用すると、以下のシナリオで示されるような、ファイアウォール経由の DNS クエリのフローをモニタすることができます。

- インターネットからファイアウォール後方の保護されたクライアントに送信される DNS クエリ
- 通常インターネットからファイアウォール後方の DMZ に配置された DNS サーバに送信される DNS クエリ

DNS ALG の設定

DNS ALG の設定は IP ポリシーを使用してのみ可能です。以下の手順で設定します。

- **DNS プロファイルオブジェクトを定義する**
  このオブジェクトでは、ターゲットの DNS 通信に対する DNS ALG の動作を定義します。DNS プロファイルオブジェクトのプロパティは本セクション内で説明します。

- **ターゲットの DNS トラフィック用の IP ポリシーにプロファイルを関連付ける**
  DNS ALG を使用するには、IP ポリシーで以下の 2 つのプロパティを正しく設定する必要があります。

  i. Service
  DNS トラフィックを対象とするサービスオブジェクトを指定します。すべての DNS トラフィック用に、dns-all という名前の定義済みサービスオブジェクトが用意されています。または、UDP と TCP の DNS トラフィックを対象として定義済みオブジェクト dns-udp あるいは dns-tcp を使用します。カスタムサービスを使用することも可能です。複数の IP ポリシーで同じサービスオブジェクトを使用することができます。

  ii. DNS Profile
  定義した DNS プロファイルを指定します。複数の IP ポリシーで同じ DNS プロファイルを使用することができます。1 つのプロファイルオブジェクトで処理できる通信の数には制限がありません。

DNS ALG は IP ルールオブジェクトと一緒に使用することはできません。

DNS プロファイルのプロパティ

DNS プロファイルオブジェクトには以下のプロパティがあります。

項目	説明
Name	プロファイルの適切な名前。
Log resolved DNS entries	本オプションが有効（初期値）の場合、解決される各 DNS クエリについてログメッセージが生成されます。
Populate the system's DNS-cache with IP addresses	本オプションが有効（初期値）の場合、プロファイル経由で送信される各 DNS クエリによって、解決されたアドレスが DNS キャッシュに追加されます。FQDN アドレスオブジェクトに対してワイルドカードを使用する場合、DNS プロファイルを Allow IP ポリシーに関連付けてこのプロパティを有効化する必要があります。詳細は「3.1.7 FQDN アドレスオブジェクト」を参照してください。
Max UDP query length	UDP DNS クエリで許可される最大ペイロードサイズ（Bytes）初期値は 4096 です。指定サイズを超過したサイズのクエリは破棄され、ログメッセージが生成されます。
Max UDP response length	UDP DNS 応答で許可される最大ペイロードサイズ（Bytes）初期値は 4096 です。指定サイズを超過したサイズの応答は破棄され、ログメッセージが生成されます。DNSSEC を使用すると応答サイズが大きくなるため、初期値より大きな値を設定するべきです。
Max TCP query length	TCP DNS クエリで許可される最大ペイロードサイズ（Bytes）初期値は 4096 です。指定サイズを超過したサイズのクエリは破棄され、ログメッセージが生成されます。
Max TCP response length	TCP DNS 応答で許可される最大ペイロードサイズ（Bytes）初期値は 4096 です。指定サイズを超過したサイズの応答は破棄され、ログメッセージが生成されます。DNSSEC を使用すると応答サイズが大きくなるため、初期値より大きな値を設定するべきです。
Recursion Desired flag	DNS recursion は、DNS サーバが他のサーバに問い合わせを行い、元のクエリを完全に解決することを意味します。DNS リクエストには Recursion Desired (RD) フラグを持ち、通常はクライアントブラウザなどにより設定されます。 Recursion Desired フラグを Allow に設定すると、RD フラグ持つリクエストが許可されます。ただし DNS Recursion は、偽装された IP アドレスからの偽の DNS クエリを送信することで、DNS サーバに対する amplification 攻撃を開始する手段としても使用されます。したがって、RD フラグがセットされた DNS クエリをすべて破棄したい場合、Recursion Desired flag の値は Drop に指定することも可能です。
Max question entries	クエリに含まれる最大問い合わせ数。初期値は 1 です。1 つの DNS で複数の FQDN 解決の問い合わせが行われる場合も考えられますが、この動作はクライアントの設定に依存します。
Scramble query IDs	本オプションが有効（初期値）の場合、DNS クエリのトランザクション ID がランダムとなります。ランダムではない ID の場合に DNS クエリの偽装によってキャッシュポイズニングから保護するために役に立ちます。
Allow all classes	初期値は無効です。
Allowed classes	Allow all classes が無効（初期値）の場合、許可されるクラスを設定します。クラス名でのみ指定可能です。初期値は IN（Internet クラス）です。
Allow all types	初期値で有効です。
Allowed types	Allow all types が無効（初期値）の場合、許可されるタイプを設定します。タイプ名でのみ指定可能です。初期値は IN（Internet クラス）です。初期値ではタイプは指定されていません。

ステートトラッキングは常に有効です

DNS ALG ではステートトラッキングが常に有効になっており、これを制御する設定はありません。ステートトラッキングとは、DNS クエリと DNS 応答が互いに一致することを意味します。一致するクエリのない応答は自動的に破棄されます。

DNS 攻撃の形式と DNS ALG 保護のメカニズム

DNS ALG は以下の形式の DNS 攻撃から保護します。

- **DNS Cache Poisoning（DNS キャッシュポイズニング）**

  DNS Cache Poisoning（DNS キャッシュポイズニング）は、DNS 応答を偽装することが可能である場合に行われます。したがって、主に UDP の DNS トラフィックに適用されます。正当な DNS クエリに対し、攻撃者は偽の応答を生成して送信します。元の DNS クエリを送信した DNS クライアントが偽の応答を受容すると、攻撃者が不正なエントリをクライアントの DNS キャッシュへ挿入することが可能になります。DNS ALG を使用すると、この攻撃に対して複数の方法で保護することが可能です。例えば、DNS プロファイルオブジェクトの Scramble query ID プロパティ（攻撃者が適切な応答を生成することが難しくなる）を使用したり、クエリ / 応答ステートを追跡（予期せぬ応答を破棄、常に有効）します。

  また、DNS プロファイルオブジェクトの Recursion Desired flag プロパティは、再帰をリクエストするクエリが DNS クライアントから送信されることを回避するために使用されます。

- **DNS リフレクション / 増幅攻撃**

  このシナリオでは、トラフィックを反射 / 増幅するために DNS サーバが使用されます。攻撃はそれぞれ異なる方法で行われますが、通常、攻撃ターゲットの送信元アドレスを偽装するため、UDP に依存します。攻撃者は 1 台以上の DNS サーバに対して大量の DNS クエリを生成し、それらのサーバは偽装アドレスに応答します。一般的に、攻撃者が DNS クエリを偽装する際、トラフィックの反射だけではなく増幅を行います（例えば 1 つのクエリに多くの問合せを含めます）。

  DNS ALG では、以下の DNS プロファイルオブジェクトのプロパティを使用してこの問題から保護します。
  - Max UDP query length
  - Max UDP response length
  - Max TCP query length
  - Max TCP response length
  - Allowed classes
  - Allowed types
  - Max question entries

- **・DNS トンネリング**

  このシナリオでは、攻撃者は DNS トラフィックを利用してファイアウォールを経由するデータをトンネリングします。DNS ALG を使用することで、正しい形式の DNS トラフィックのみを許可して一般的なトンネリングから保護します。関連する RFC のプロトコル記述に対し、NetDefendOS により DNS トラフィックを検証します。適合していないデータトラフィックは破棄されます。

  より洗練されたトンネリング攻撃では、有効なドメイン名を使用してデータがエンコードされ、DNS クエリ / 応答に保存します。これを検出することは難しくなっています。DNS ALG ではこうした攻撃に対して保護の度合いを設定するために下記の DNS プロファイルオブジェクトのプロパティが使用可能です。

  - Max UDP query length
  - Max UDP response length
  - Max TCP query length
  - Max TCP response length
  - Allowed classes
  - Allowed types

dnscontrol CLI コマンド

CLI コマンド dnscontrol を使用して、DNS プロファイルオブジェクトによるすべての DNS ALG アクティビティの情報を表示することができます。-stats を使用すると、最後のシステム再起動後、各プロファイルを通過したすべての DNS クエリについて、概要を表示します。

```
DFL-xxxx:/> dnscontrol -stats

DNS Control statistics
-------------------------------------
Forwarded DNS Queries : 2411
Forwarded DNS Responses : 2393
Malformed Client Messages : 6
Malformed Server Messages : 12
Dropped Client Messages : 6
Dropped Server Messages : 12
Current DNS Session : 0
Total DNS Sessions : 2401
```

-list オプションを使用すると、すべての設定済み DNS プロファイルオブジェクトを通過したすべての現在アクティブな DNS クエリについて、概要を表示します。

```
DFL-xxxx:/> dnscontrol -list

DNS Control Sessions
ID    Creation time        Outstanding Transactions
----- -------------------- ------------------------
2002  2018-05-14  08:15:14 0
2003  2018-05-14  08:15:14 1
2004  2018-05-14  08:15:14 1
```

上記のコマンド出力結果のテーブルについて、以下の点に注意する必要があります。

- いずれかの DNS プロファイルを通過した各 DNS クエリには、昇順で固有の ID 番号が割り当てられています。
- Creation time は、DNS クエリがプロファイルによって DNS サーバへ転送された時刻を表しています。
- Outstanding Transactions 列の値が 1 以上の場合、DNS サーバへのクエリからの応答で未解決のものがあることを示しています。
- すべての未解決の応答が受信されると、Outstanding の値は 0 になりますが、NetDefendOS がリストからクエリを削除するまでに遅延が発生している可能性もあります。上記の例では、ID 2002 が該当します。

未解決クエリについて詳細な情報を表示するには、-list オプションと一緒に -verbose を使用します。以下のような結果となります。

```
DFL-xxxx:/> dnscontrol -list -verbose

DNS Control Sessions
ID    Creation time        Outstanding Transactions
----- -------------------- ------------------------
2011 2018-06-14 09:18:14   1

UDP
192.26.2.2:36318->192.26.1.2:53 [FW] 192.26.2.2:36318->192.26.1.2:53
```

上記の例では、1 つの DNS クエリが未解決ですが、追加の情報として、使用プロトコル（ここでは UDP）や、DNS 送信の間に実行されるアドレス変換（適用される場合）が表示されます。上記のクエリでは、クエリの送信元クライアントアドレスが 192.26.2.2:36318、送信先のサーバアドレスが 192.26.1.2:53 であり、アドレス変換が実行されていません。通信 g な NAT または SAT 変換の対象である場合、-verbose オプションで確認することができます。

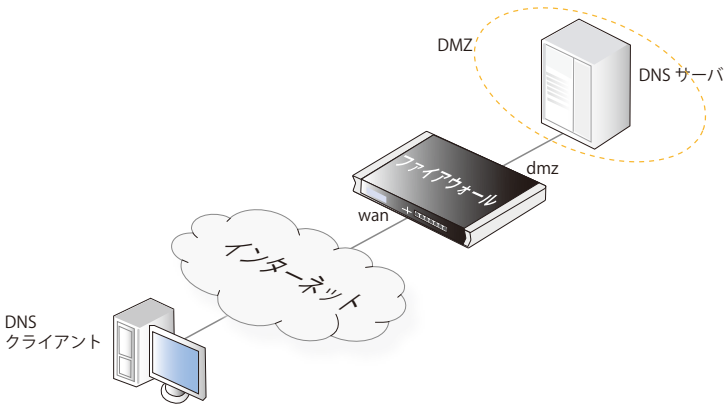
dnscontrol のすべてのオプションについては別紙の「CLI Reference Guide」を参照してください。

dnscontrol で提供される統計は、Web インタフェースで確認することはできません。

例題 6.37

保護された DNS サーバに対する DNS ALG のセットアップ

この例題では、インターネットから DMZ 上の保護された DNS サーバに送信される UDP DNS クエリをフィルタするための DNS ALG を設定します。以下の図の通りです。



CLI

DNSProfile を初期値で作成する :

```
DFL-xxxx:/> add Policy DNSProfile my_server_dns_alg
```

プロファイルを指定して SAT IP ポリシーを作成する :

```
DFL-xxxx:/> add IPPolicy Name=SAT_DNS_To_DMZ SourceInterface=wan SourceNetwork=all-nets
            DestinationInterface=core DestinationNetwork=wan_ip Service=dns-udp Action=Allow
            SourceAddressTranslation=None DestAddressTranslation=SAT DestAddressAction=SingleIP Dest-
            NewIP=10.0.0.5 DNS=Yes DNS_Policy=my_server_dns_alg
```

Web Interface

DNSProfile を初期値で作成する :

1. **Policies > Profiles > DNS > Add > DNS Profile** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_server_dns_alg
3. 「OK」ボタンをクリックします。

プロファイルを指定して SAT IP ポリシーを作成する :

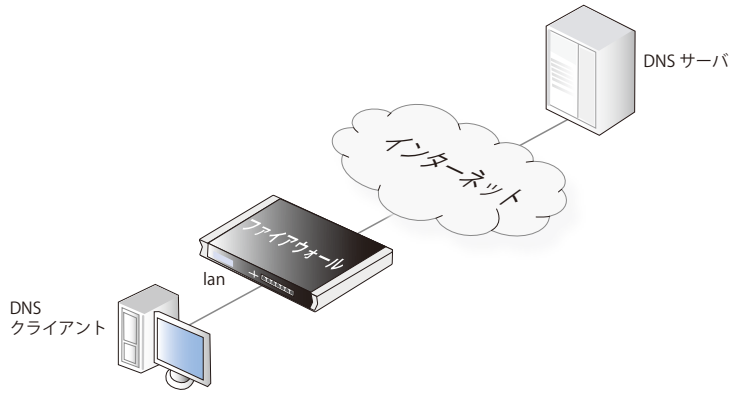
1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: SAT_DNS_To_DMZ
   - Action: Allow
3. Filter で以下の情報を入力します。
   - Source Interface: wan
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip
   - Service: dns-udp
4. Source Translation で以下の情報を入力します。
   - Address Translation: None
5. Destination Translation で以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Single IP
   - New IP Address: 10.0.0.5
6. DNS タブを選択し、以下の設定を行います。
   - Enable DNS Profile: ON
   - DNS Profile: my_server_dns_alg
7. 「OK」ボタンをクリックします。

例題 6.38

保護された DNS クライアントに対する DNS ALG のセットアップ

この例題では、保護されたネットワーク lannet 上のクライアントから、NAT 変換を実行してインタフェース wan 経由でインターネットへ DNS クエリが送信されます。以下の図の通りです。

ここ例題ではすべての DNS クラスが許可されますが、DNS 再帰は許可されません。



CLI

DNSProfile を初期値で作成する :

```
DFL-xxxx:/> add Policy DNSProfile my_client_dns_alg RecursionDesiredFlag=Drop AllowAllClasses=Yes
```

プロファイルを指定して SAT IP ポリシーを作成する :

```
DFL-xxxx:/> add IPPolicy Name=NAT_DNS_to_Internet SourceInterface=lan SourceNetwork=lannet
            DestinationInterface=wan DestinationNetwork=all-nets Service=dns-udp Action=Allow
            SourceAddressTranslation=NAT NATSourceAddressAction=OutgoingInterfaceIP DNS=Yes DNS_Policy=my_cli-
            ent_dns_alg
```

Web Interface

DNSProfile を初期値で作成する :

1. **Policies > Profiles > DNS > Add > DNS Profile** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_client_dns_alg
   - Recursion Desired flag: Drop
   - Allow all classes: Enable
3. 「OK」ボタンをクリックします。

プロファイルを指定して SAT IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: NAT_DNS_To_Internet
   - Action: Allow
3. Filter で以下の情報を入力します。
   - Source Interface: wan
   - Source Network: lannet
   - Destination Interface: wan
   - Destination Network: all-nets
   - Service: dns-udp
4. Source Translation で以下の情報を入力します。
   - Address Translation: NA
   - Address Action: Outgoing Interface IP
5. DNS タブを選択し、以下の設定を行います。
   - Enable DNS Profile: ON
   - DNS Profile: my_client_dns_alg
6. 「OK」ボタンをクリックします。

6.2 Web コンテンツフィルタリング

6.2.1 概要

HTTP ALG の一部として、Web トラフィックに対する Web コンテンツフィルタリング（WCF) 機能を提供しています。この機能では、Web ページのコンテンツタイプに基づいて許可やブロックを行います。Web コンテンツフィルタリングを使用すると、最小限の労力で非常に高い精度のフィルタリングを行うことができます。WCF は HTTP、HTTPS いずれのトラフィックに対しても適用することができます。

WCF の有効化方法

WCF は以下のいずれかの方法で有効化することができます。

- **IP ポリシーを使用する**
  IP ポリシーオブジェクトを使用した Web コンテンツフィルタリングの設定が最も簡単な方法であり、推奨されます。まず、新規の Web プロファイルオブジェクトで WCF を設定し、そのプロファイルをターゲットトラフィックに対して起動される IP ポリシーに割り当てます。IP ポリシーの Service プロパティに指定したサービスの Protocol プロパティが HTTP に設定されている必要があります。

  IP ポリシーを使用した WCF の設定手順は「6.2.2 IP ポリシーを使用した WCF の設定」で説明します。

- **IP ルールを使用する**
  IP ルールオブジェクトを使用する場合、HTTP ALG で WCF を有効化後、HTTP ALG オブジェクトをサービスオブジェクトに割り当て、それを IP ルールに割り当てます。

  IP ルールを使用した WCF の設定手順は「6.2.3 IP Rule を使用した WCF セットアップの概要」で説明します。

ダイナミックな WCF データベース

この機能は自動化されおり、どの URL を防御するか、または許可するかを手動で指定する必要はありません。その代わり、D-Link はショッピング、ニュース、スポーツ、および大人が好むものなどバラエティに富んだ分野にグループ化された非常に多くの Web サイト URL を含むデータベースを保持しています。これらのデータベースは、新しく分類された URL を使用して時間ごとに更新されます。同時により古く、不正な URL は廃棄されます。

データベースにある URL の範囲はグローバルであり、多くの異なった言語の Web サイトをカバーし、世界中の国に位置するサーバへのアクセスを可能にします。

注意 WCF データベースアクセスは TCP ポート 9998 を使用します。

NetDefendOS が外部の WCF データベースにクエリを送信する場合、宛先ポート 9998 に TCP リクエストとして送信します。

そのため、リクエストが通過する、他のファイアウォールを含むどんなネットワーク機器も、送信先ポート 9998 で TCP トラフィックをブロックしてはいけません。

メッセージが通過する機器が別のファイアウォールであれば、アクション Allow を持つ IP ルールは、ルールに関連するカスタムサービスと共に作成されるべきです。

WCF プロセスフロー

ユーザが Web サイトへのアクセスをリクエストする時、NetDefendOS はダイナミック WCF のデータベースにリクエストされたサイトのカテゴリを取得するためにクエリを送信します。その後 URL へのアクセスは、管理者がそのカテゴリのために設定したフィルタリングポリシーに基づいて許可、または拒否されます。

アクセスが拒否されると、Web ページは、リクエストされたサイトが防御されたという説明をユーザに表示します。できるだけ早く検索処理を行うために、NetDefendOS は最近アクセスした URL をメモリのキャッシュに保存しています。ユーザは、限定された Web サイト範囲をサーフィンするため、キャッシングは高い効果があります。

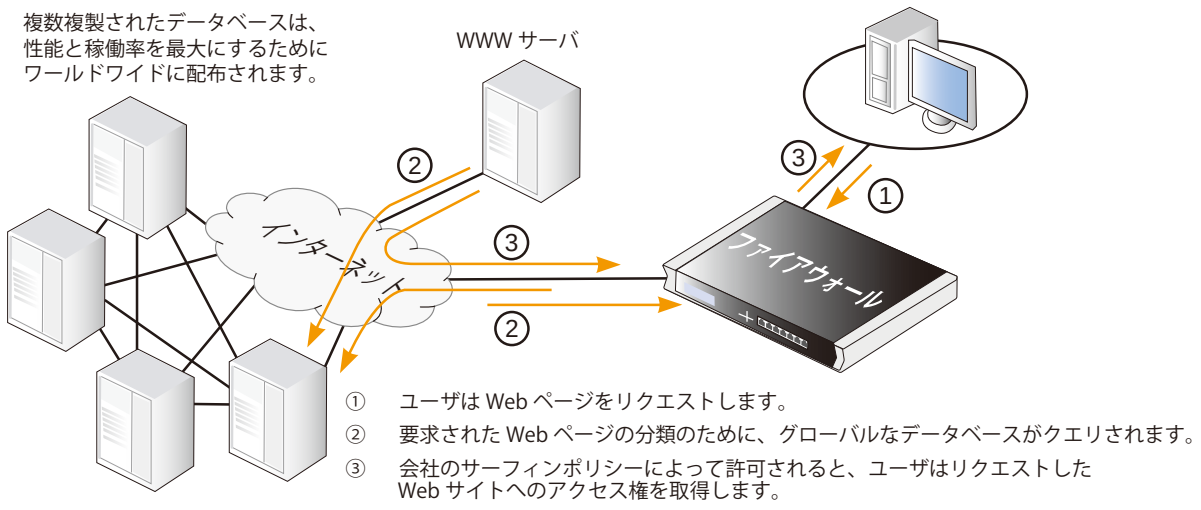


図 6-8　ダイナミックコンテンツフィルタリングフロー

リクエストされたWebページのURLがデータベースに存在しない場合、そのURLのWebページはD-Linkの中央データディスクに自動的にダウンロードされ、ソフトウェア技術の組み合わせを使用して分析されます。一度、分類されると、URL はグローバルデータベースに配信され、NetDefendOS は URL の分類を受信します。そのため、ダイナミック WCF では管理者の作業は最小限に抑えられます。

参照 新しい URL のサブミッションは anonymous で行われます。

D-Link ネットワークに送信された分類されていない URL は、anonymous サブミッションとして処理され、新しいサブミッションのソースの記録は保持されません。

サイトではなくページを分類する

NetDefendOS のダイナミックフィルタリングはサイトではなく、Web ページを分類します。つまり、Web サイトは、サイト全体をブロックせずに個別にブロックされるべき Web ページを含む場合があります。NetDefendOS は、ページレベルにまで具体的にブロックできる機能を提供するため、フィルタリングポリシーにブロックされない Web サイトのページにアクセスできます。

WCF とホワイトリスト

特定の URL がホワイトリストに設定されている場合、それらは WCF サブシステムを迂回します。URL に対して照合は行われず、常に許可されます。URL がホワイトリストにあるエントリと完全に一致する場合、またはワイルドカードを使用するエントリに一致する場合、この処理が適用されます。

WCF はサブスクリプションベースの機能

Web コンテンツフィルタリングはサービスに対するサブスクリプションを取得することで有効になる機能です。このサブスクリプションは、「付録 A セキュリティ更新サービス」にサブスクリプション満了後の WCF の動作の詳細と共に詳しく記載されています。

段階的なブロックを導入する

突然 Web サイトのブロックを導入すると、ユーザを当惑させる場合があります。管理者は一回に一つ、特定のカテゴリへの制限を設定することをお勧めします。これにより、各ユーザは防御のための制限が存在することに徐々に慣れていき、非常に多くを一度に制限された場合に起こりうる大きな反響を回避することができます。また、段階的な導入により、防御の目標が達成されているかどうかについて、よりたやすく評価を行うことができます。

6.2.2 IP ポリシーを使用した WCF の設定

WCF は、HTTP ALG と IP ルールオブジェクトの組み合わせを使用するかわりに、IP ポリシーを使用して有効化することができます。IP ポリシーを使用すると、IP ポリシーで利用可能な他のオプション（トラフィックシェーピングやアンチウイルススキャンなど）と組み合わされて、より直接的に WCF のアクティブ化を行うことができます。

IP ポリシーオブジェクトを使用して WCF を設定するには以下の手順を実行します。

- 対象とするプロトコル用にカスタムサービスを作成します。オブジェクトのプロトコルプロパティを HTTP に指定してください。
- Web プロファイルオブジェクトを作成し、Web コンテンツフィルタリングのタイプに適切な設定を行います。
- IP ポリシーにこれらのサービスと Web プロファイルオブジェクトを割り当てます。

定義済み HTTP サービス

NetDefendOS バージョン 11.03 以降では、デフォルトのコンフィグレーションに、プロトコルプロパティが適切に設定された定義済みのサービスオブジェクトが含まれています。WCF の場合は http-outbound です。11.03 以降にアップグレードされたシステムでは、サービスのプロトコルプロパティを明示的に設定する必要があります。明確に説明するために、このセクションではカスタムサービスオブジェクトを作成して明示的にプロトコルプロパティを設定しています。

Fail Mode アクション

Fail Mode 設定では Web コンテンツフィルタリングが動作しなかった場合のアクションを指定します。NetDefendOS が URL 検索実行のために外部データベースに到達できない場合などが考えられます。

Fail Mode には以下のいずれかを設定します。

- **Allow**
  本プロパティの初期値です。外部 WCF データベースに接続できない場合、（該当 URL が通常は許可されない設定であっても）許可されます。
- **Deny**
  URL 検証のための外部データベースへの接続が不可能となっている場合、WCF が動作しないと、URL は拒否されます。ユーザには「Access denied」のメッセージが表示されます。

例題 6.39

IP ポリシーを使用した WCF を有効にする

この例題では、保護されたネットワークの HTTP クライアントからインターネットへの HTTP トラフィックに対して Web コンテンツフィルタリングを設定する方法を説明します。すべてのショッピングサイトをブロックするように設定します。

IP Policy オブジェクト http_nat_policy が既に存在していて、これがインターネットに対するクライアント接続のために NAT を実行するものとします。

CLI

Service オブジェクトを作成します。:

```
DFL-xxxx:/> add Service ServiceTCPUDP http_wcf_service Type=TCP DestinationPorts=80 Protocol=HTTP
```

Web Profile オブジェクトを作成します。:

```
DFL-xxxx:/> add Policy WebProfile my_wcf_profile WCF=Yes WCFCategories=SHOPPING
```

新しいサービスおよびプロファイルを使用するために IP Policy を編集します。:

```
DFL-xxxx:/> set IPPolicy http_nat_policy Service=http_wcf_service WebControl=Yes Web_Policy=my_wcf_profile
```

Web Interface

トラフィック用の Service オブジェクトを作成します。:

1. **Objects > Services > Add > TCP/UDP service** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: http_wcf_service
   - Type: TCP
   - Destination port: 80
   - Protocol: HTTP
3. 「OK」ボタンをクリックします。

Web Profile オブジェクトを作成します。:

1. **Policies > Firewalling > Web > Add > Web Profile** の順にメニューをクリックします。
2. Name に my_wcf_profile を指定します。
3. Web Content Filtering を有効にします。
4. Restricted Categories リストに Shopping を追加します。
5. 「OK」ボタンをクリックします。

新しいサービスおよびプロファイルを使用するために IP Policy を編集します。:

1. **Policies > Firewalling > Main IP Rules** の順にメニューをクリックします。
2. http_nat_policy を選択します。
3. Service リストから http_wcf_service を選択します。
4. Web Control タブを選択します。
5. Enable Web Control を有効にします。
6. Web Profile リストから my_wcf_profile を選択します。
7. 「OK」ボタンをクリックします。

6.2.3 IP Rule を使用した WCF セットアップの概要

以下の手順は IP ルールと共に使用されます。

- Web コンテンツフィルタリングが有効な HTTP ALG がオブジェクトを定義します。

  あるいは、Light Weight HTTP ALG（LW-HTTP ALG）を使用します。これは、より少ないシステムオーバヘッドで、より高いトラフィックスループットを提供するため好まれます。欠点は、スタティックな Web コンテンツをスキャンおよび削除するアンチウィルスなどの特定の機能がサポートされないという点です。「6.1.2.4 Light Weight HTTP ALG」で、より詳しく LW-HTTP ALG について記述します。

- ALG オブジェクトを Service オブジェクトに関連付けます。定義済オブジェクトが変更されないように、本目的のためのカスタムサービスオブジェクトを作成することをお勧めします。

- トラフィックがフィルタされるサブジェクトを決定するために IP Rule オブジェクトにこの Service オブジェクトを関連付けます。これで、詳細なフィルタリングポリシーが定義されます。

例題 6.40

IP ルールを使用して Web コンテンツフィルタリングを有効にする

この例題では、保護されたネットワークから「all-nets」への HTTP トラフィックに対して Web コンテンツフィルタリングを設定する方法を説明します。すべての検索サイトをブロックするために設定され、HTTP トラフィックを制御する 1 つの NAT IP ルールを使用するものとします。

この例題は IP Rule オブジェクトを使用したフィルタリングを設定することに注意してください。IP ポリシーを使用した設定については 2 番目の例題で説明します。

CLI

はじめに、HTTP アプリケーションレイヤゲートウェイ（ALG）オブジェクトを作成する：

```
DFL-xxxx:/> add ALG ALG_HTTP content_filtering WebContentFilteringMode=Enabled FilteringCategories=SEARCH_SITES
```

次に、新しい HTTP ALG を使用した Service オブジェクトを作成する：

```
DFL-xxxx:/> add Service ServiceTCPUDP http_content_filtering Type=TCP DestinationPorts=80 ALG=content_filtering
```

最後に、新しいサービスを使用するために NAT ルールを編集する：

```
DFL-xxxx:/> set IPRule NATHttp Service=http_content_filtering
```

Web Interface

はじめに、HTTP アプリケーションレイヤゲートウェイ（ALG）オブジェクトを作成する：

1. **Objects > ALG > Add > HTTP ALG** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ General タブ

General

- Name : content_filtering

◇ Web Content Filtering タブ

General

- Mode : Enabled

Categories

- 検索するサイトを「Blocked Categories」リストに追加します。

次に、新しい HTTP ALG を使用したサービスオブジェクトを作成する：

1. **Objects > Services > Add > TCP/UDP service** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : http_content_filtering
- Type : TCP
- Destination Port: 80

Application Layer Gateway

- ALG : content_filtering（先に作成した ALG を選択します。）

最後に、新しいサービスを使用するために NAT IP ルールを編集する :

1. **Policies > Firewall > Main IP Rules** の順にメニューをクリックします。
2. HTTP トラフィックを処理する NAT ルールを選択します。
3. Service リストから http_content_filtering を選択します。
4. 「OK」ボタンをクリックします。

Web コンテンツフィルタリングが lannet から all-nets へのすべての Web トラフィックに有効になります。

以下の手順に従って、機能を確認します。:

1. lannet ネットワーク上のワークステーションで、標準の Web ブラウザを起動します。
2. 例えば検索サイト www.google.com への閲覧を試みます。
3. すべてが正しく設定されている場合、ご使用の Web ブラウザはリクエストされたサイトがブロックされたことについて通知する Web ページを表示します。

例題 6.41

Audit モードを有効にする

ここでは、前の例題と同じシナリオをベースにし、Audit モードを有効にします。

CLI

はじめに、HTTP アプリケーションレイヤゲートウェイ（ALG）を作成する :

```
DFL-xxxx:/> add ALG ALG_HTTP content_filtering WebContentFilteringMode=Audit FilteringCategories=SEARCH_SITES
```

Web Interface

はじめに、HTTP アプリケーションレイヤゲートウェイ（ALG）を作成する :

1. **Objects > ALG > Add > HTTP ALG** の順にメニューをクリックします。
2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ **General タブ**

General

- Name : content_filtering

◇ **Web Content Filtering タブ**

General

- Mode : Audit

Categories

- Search sites を「Blocked」リストに追加します。

新しいサービスを使用するためには、新しい HTTP ALG を使用し、NAT IP ルールを編集してサービスオブジェクトを作成する手順が、前の例で記述されています。

HTTPS を使用した Web コンテンツフィルタリング

HTTP ALG では、HTTP または HTTPS トラフィックのいずれか、あるいは両方に ALG を適用することが可能です。HTTPS トラフィックのフィルタリングを動作させる場合、ALG に関連している Service オブジェクトは、適切なポート番号を許可するものであるべきです。

例えば、HTTP(ポート 80) と HTTPS（ポート 443）トラフィックの両方が許可されている場合、定義済みのサービス http-all が使用できます。定義済みのサービスがトラフィックの要求を満たさないなら、カスタムサービスを定義して、使用する必要があるかもしれません。

HTTPS 接続で WCF を使用する際にそれ以外に注意する点は、特定のサイトへのアクセスを拒否すると、HTTPS 接続が自動的にダウンするということです。これは、ブラウザが、WCF 機能が介在したこととその理由を示すために普通の NetDefendOS が生成したメッセージを表示できないことを意味します。代わりに、ブラウザは接続が失われたことを示すシステム自身のメッセージを表示するだけです。

また、Fail モード設定は HTTP 接続に影響します。暗号化パケットの送信前の最初の HTTPS ハンドシェイクセッションで、ホスト名がクライアントからの ClientHello、またはサーバからの ServerHello で見つけられないと、Fail Mode アクションが Deny の場合、接続はダウンし、アクションが Allow であるとダウンしません。

Audit モード

Audit モードでは、システムがコンテンツフィルタリングポリシーに従ってすべてのネットサーフィンを分類し、ログに出力しますが、制限されている Web サイトは、ユーザにはアクセス可能です。つまり、NetDefendOS のコンテンツフィルタリング機能は分析ツールとして使用することが可能であり、ユーザコミュニティによってどのカテゴリの Web サイトがどのくらいの頻度でアクセスされたかを分析することができます。

特定の期間 Audit モードで動作した後に、異なるユーザグループのネットサーフィンの動作や WCF 機能を有効にすることによって実現できる潜在的影響についてさらに理解することができます。

Allow Override

アクティブコンテンツフィルタリングは正しいタスクを行っているユーザ業務を妨げることがあります。例えば、株のブローカーがオンラインゲームの会社と取り引きすることを検討したとします。日々の業務内で、ユーザは会社の評価を行うためには、投資する Web サイトを閲覧する必要があります。コーポレートポリシーが投資する Web サイトを制限する場合、ユーザは自分の仕事を行うことができなくなります。

このため、NetDefendOS は「Allow Override」と呼ばれる機能をサポートしています。この機能を有効にすると、コンテンツフィルタリングコンポーネントはコーポレートポリシーに従って、ユーザが制限されている Web サイトに入ろうとしているとしてこれを警告、Web サイトへのユーザの訪問はログとして記録されます。これは、restricted site notice（制限サイト通知）とされています。その後ユーザは該当 URL への接続を維持したり、またはログ記録の要求を破棄することも可能です。

この機能を有効にすることで、不適切なサイトを訪問する正当な理由を持っているユーザだけが、正常に接続を行うことができます。他のユーザには、ネットサーフィンする習慣が明らかなリスクであるために、それらのサイトを無効にします。

注意 サイトの制限の無視

ユーザがサイトの制限の通知ページを無視すると、ユーザは再び現れる新しいサイトの制限メッセージなしですべてのページにサーフィンできてしまいます。しかし、ユーザに対してログへの出力は行われています。ユーザが 5 分間操作を行わないと、次に制限されたサイトにアクセスしようとした場合に再度サイトの制限ページを表示します。

防御サイトの再分類

未知の Web サイトを分類する処理が自動化されるため、常にいくつかのサイトは不適切な分類となるリスクがあります。NetDefendOS は、ユーザがサイトの新しい分類を手動で提供できるようなメカニズムを供給します。

このメカニズムは、HTTP ALG レベルごとに有効にされ、これにより管理者は通常のユーザまたは選択ユーザのグループだけにこの機能を有効にするように選択できます。

再分類が有効になり、ユーザが拒否される Web サイトをリクエストすると、防御 Web ページは、プルダウンリストに可能なカテゴリをすべて含めます。ユーザはリクエストした Web サイトが間違って分類されたと思うと、プルダウンリストからより適切なカテゴリを選択し、提案としてそれを提出します。

提案されたカテゴリと同様に、リクエストした Web サイトへの URL は、その後手動の検査のために D-Link 中央ディスクに送信されます。その検査は、提案されたカテゴリ、または適切と思われるカテゴリのいずれかに従って Web サイトで再分類を行います。

例題 6.42

防御したサイトを再分類する

ここでは、間違って分類されていると思った場合に、再分類する方法を説明します。
このメカニズムは各 HTTP ALG のレベルに基づき有効化されます。

CLI

はじめに、HTTP アプリケーションレイヤゲートウェイ（ALG）オブジェクトを作成する：

```
DFL-xxxx:/> add ALG ALG_HTTP content_filtering WebContentFilteringMode=Enabled FilteringCategories=SEARCH_SITES
            AllowFilteringReclassification=Yes
```

次に、以前の例題で実施したようにサービスオブジェクトの設定と NAT の編集を続けます。

Web Interface

はじめに、HTTP アプリケーションレイヤゲートウェイ（ALG）オブジェクトを作成する :

1. **Objects > ALG > Add > HTTP ALG** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

◇ General タブ

General

- Name : content_filtering

◇ Web Content Filtering タブ

General

- Mode : Enabled

Categories

- Search sites を「Blocked Categories」リストに追加します。
- 「Allow Reclassification」にチェックを入れます。

次に、以前の例題で実施したようにサービスオブジェクトの設定と NAT の編集を続けます。
Web コンテンツフィルタリングが lannet から all-nets へのすべての Web トラフィックに有効になり、ブロックされたサイトの再分類が提供されます。
以下の手順に従って、機能を確認します。

1. lannet ネットワーク上のワークステーションで、標準の Web ブラウザを起動します。

2. 例えば検索サイト www.google.com への閲覧を試みます。

3. すべてが正しく設定されている場合、ご使用の Web ブラウザはブロックページを表示し、プルダウンリストには全ての可能なカテゴリが含まれています。

4. ユーザはより適切なカテゴリを選択し、再分類を提供することができます。

注意 request_url メッセージの生成を有効にする

イベントメッセージ生成が「parent」IP ルールで有効であると、request_url イベントメッセージだけが生成されます。

6.2.4 WCF カテゴリ

このセクションでは、ダイナミックコンテンツフィルタリングで使用されるすべてのカテゴリを一覧にし、各カテゴリの目的を記述します。

Academic Fraud（学歴詐称）
学歴詐称に関連するサービスを提供、または提供していると思われるサイトは Academic Fraud カテゴリに分類される可能性があります。第三者による課題やエッセイの執筆、その他、学生や研究者が不正に学歴を入手することを手助けする目的のサービスが含まれます。

Adult Content（アダルトコンテンツ）
主にアダルトコンテンツが含まれる場合、Web サイトは Adult Content カテゴリに分類される可能性があります。

Advertising（広告）
主に広告に関連するコンテンツが含まれる場合、Web サイトは Advertising カテゴリに分類される可能性があります。

Alcohol（アルコール）
コンテンツがドラッグに関連する情報またはサービスを含む場合、Web サイトは Alcohol カテゴリに分類される可能性があります。

Animals:Pets（動物：ペット）
コンテンツが、動物関連の情報や、動物・ペットに関連する画像を含む場合、Web サイトは Animals/Pets カテゴリに分類される可能性があります。

Arts:Culture（芸術：文化）
コンテンツが、芸術関連の情報や、芸術・文化に関連する画像を含む場合、Web サイトは Arts/Culture カテゴリに分類される可能性があります。

Auctions（オークション）
コンテンツがオークション関連の情報や画像を含む場合や、グッズのオークション及び（または）サービスを提供する場合、Web サイトは Auctions カテゴリに分類される可能性があります。

Audio Streaming Services（音楽配信サービス）
音楽配信サービス及び（または）音楽配信を促進するソフトウェア、オンライン音楽配信に関連する情報を提供している場合、Web サイトは Audio Streaming Services カテゴリに分類される可能性があります。ラジオ、テレビ、その他の配信メディアは含まれません。

Backups:Storage（バックアップ：ストレージ）
コンテンツがバックアップ / ストレージに関連する情や画像を含む場合や、（または）オンラインバックアップ / ストレージサービスを提供している場合、Web サイトは Backups/Storage カテゴリに分類される可能性があります。

Botnets（ボットネット）
現在 Botnet に関与し、（または）Botnet マルウェアを含む場合、Web サイトは Botnets カテゴリに分類される可能性があります。Botnets に関連する情報を含むコンピュータセキュリティサイトは IT Security に分類されます。

Business Oriented（ビジネス関連）
コンテンツが主にビジネス関連の情報を含む場合、Web サイトは Business Oriented カテゴリに分類される可能性があります。

Charities（チャリティー）
コンテンツがチャリティーに関連する情報や画像を含む場合、Web サイトは Charities カテゴリに分類される可能性があります。

Child Abuse Material（児童虐待）
コンテンツが児童虐待に関するデータを含む場合、Web サイトは Child Abuse Material カテゴリに分類される可能性があります。このような内容は多くの国の多くの管轄で違法です。

Child Entertainment（子供の娯楽）
コンテンツが子供の娯楽に関連する情報や画像を含む場合、Web サイトは Child Entertainment カテゴリに分類される可能性があります。

Clubs and Societies（クラブと団体）
コンテンツが、クラブまたは団体の情報や関連するサービスを含む場合、Web サイトは Clubs and Societies カテゴリに分類される可能性があります。これはチームまたはカンファレンスの Web サイトを含みます。

Computing/IT（コンピュータ /IT）
コンテンツがコンピュータ関連の情報やサービスを含む場合、Web サイトは Computing/IT カテゴリに分類される可能性があります。

Crime / Terrorism（犯罪 / テロリズム）
コンテンツが犯罪またはテロ活動、文化または世論に関する記述、宣伝または指示を含んでいる場合、Web サイトは Crime / Terrorism カテゴリに分類される可能性があります。

Dating（出会いサイト）
主にに出会い関連のコンテンツが含まれる場合、Dating カテゴリに分類される可能性があります。

Dictionary（辞書）
辞書や辞書サイトに関連する情報や画像を含む辞書サイトまたは類似サービスを提供するサイトの場合、Web サイトは Dictionary カテゴリに分類される可能性があります。

Drugs:Illicit（ドラッグ：不正）
コンテンツが多くの管轄で不正とみなされるドラッグの使用を促進する情報・材料・製品の情報及び（または）画像を含む場合、Web サイトは Drugs:illicit カテゴリに分類される可能性があります。医療の利用または一般的な使用に関わる健康関連の情報は含まれません。

Drugs:Pharmaceuticals（ドラッグ：製薬）
コンテンツが合法のドラッグや製薬に関連する情報や画像を含む場合、Web サイトは Drugs/Pharmaceuticals カテゴリに分類される可能性があります。

Dynamic DNS（ダイナミック DNS）
コンテンツが Dynamic DNS サービスに関連する情報や画像を含む場合、Web サイトは Dynamic DNS カテゴリに分類される可能性があります。

E-Banking（インターネットバンキング）
Web サイトの主要なコンテンツがインターネットバンキングに関連している場合、E-Banking カテゴリに分類される可能性があります。

Educational（教育）
Web サイトの主要なコンテンツが教育に関連している場合、Educational カテゴリに分類される可能性があります。

Educational Games（教育的なゲーム）
教育に関わる閲覧者に向けたソフトウェア、情報、画像またはゲームサイトの場合、Web サイトは Educational Games カテゴリに分類される可能性があります。

Embedded Threats（埋め込みマルウェア）
コンテンツが埋め込みマルウェアを含む場合、Web サイトは Embedded Threats カテゴリに分類される可能性があります。現在何らかの形式のマルウェアに感染している正当なサイトが含まれる可能性があります。

Entertainment（エンターティメント）
Web サイトの主要なコンテンツがエンターテイメントに関連している場合、**Entertainment** カテゴリに分類される可能性があります。

Fashion（ファッション）
コンテンツがファッションに関連する情報や画像を含む場合、Web サイトは Fashion カテゴリに分類される可能性があります。

Gambling（ギャンブル）
Web サイトの主要なコンテンツがギャンブルに関連している場合、Gambling カテゴリに分類される可能性があります。

Game Sites（ゲームサイト）
Web サイトの主要なコンテンツがオンラインゲームに関連する場合、Game Sites カテゴリに分類される可能性があります。

Government（政府）
政府機関（連邦、州、地方、国）によって運営されている場合、Web サイトは Government カテゴリに分類される可能性があります。

Government Blocking List（政府防御リスト）
Web サイトが政府のブロックリストに関連している場合、Government Blocking List カテゴリに分類される可能性があります。

Guns:Weapons（銃：武器）
コンテンツが武器に関連する情報や画像を含む場合、Web サイトは Guns/Weapons カテゴリに分類される可能性があります。

Hacking（ハッキング）
コンテンツが違法なハッキングに関連する情報や画像及び（または）それを手助けするツールを含む場合、Web サイトは Hacking カテゴリに分類される可能性があります。マルウェア保護及び（または）ハッキングやマルウェアに対する防御は IT Security カテゴリに含まれます。

Health Sites（ヘルスサイト）
コンテンツが健康に関連する場合、Web サイトは Health Sites カテゴリに分類される可能性があります。

Hobbies（趣味）
コンテンツが趣味に関連する情報や画像を含む場合、Web サイトは Hobbies カテゴリに分類される可能性があります。

Hosted Services（ホスティングサービス）
ホスティングサービスを提供し、（または）内容にホスティングサービス に関連する情報や画像を含む場合、Web サイトは Hosted Services カテゴリに分類される可能性があります。

Humor（ユーモア）
ジョークサイトなど、コンテンツがユーモアに関連する情報や画像を含む場合、Web サイトは Humor カテゴリに分類される可能性があります。

Instant Messaging（インスタントメッセージ）
コンテンツがリアルタイムオンラインの対話方式のディスカッショングループに焦点を合わせている情報を含む場合、Web サイトは Instant Messaging カテゴリに分類される可能性があります。これは、チャットソフトウェアをダウンロードする URL をはじめ、通知ボード、メッセージボード、オンラインフォーラム、ディスカッショングループも含みます。

Investment（投資サイト）
コンテンツが投資に関する情報を含む場合、Web サイトは Investment カテゴリに分類される可能性があります。

ISPs（ISP）
コンテンツがインターネットサービス提供者（ISP）に関連する情報や画像を含む場合、Web サイトは ISPs カテゴリに分類される可能性があります。

IT Forums:Blogs（IT フォーラム：ブログ）
情報技術に関連する記事・画像と（または）情報を含むインターネットフォーラムやインターネットログ（ブログ）を主催・提供している場合、Web サイトは IT Forums/Blogs カテゴリに分類される可能性があります。

IT Security（IT セキュリティ）
コンテンツが情報技術セキュリティ及び（または）インターネットセキュリティに関連する情報や画像を含む場合、Web サイトは IT Security カテゴリに分類される可能性があります。

Job Search（仕事検索）
Web サイトの主要なコンテンツとして雇用に関連する情報が含まれる場合、Job Search カテゴリに分類される可能性があります。

Keyloggers（キーロガー）
コンテンツがキーロギングソフトウェア及び（または）悪意のある目的でキーロギングアクティビティを促進する情報を含む（可能性がある）場合、Web サイトは Keyloggers カテゴリに分類される可能性があります。

Malicious（不正）
サイト内に悪意あるコードが含まれる場合、Web サイトは Malicious カテゴリに分類される可能性があります。

Media:File Sharing（メディア：ファイル共有）
コンテンツがファイル提供及び（または）他のメディア共有サービスに関連する情報や画像を含む場合、Web サイトは Media Sharing カテゴリに分類される可能性があります。

Military（軍事）
コンテンツが軍事サービス及び（または）軍事用の備品に関連する情報や画像を含む場合、Web サイトは Military カテゴリに分類される可能性があります。

News（ニュース）
Web サイトのコンテンツがニュースに関連する場合、News カテゴリに分類される可能性があります。

Nudity（ヌード）
コンテンツがポルノ以外のヌードに関連する情報やヌードの描写に関連する画像を含む場合、Web サイトは Nudity カテゴリに分類される可能性があります。

Online Meeting & Collaboration（オンライン会議＆コラボレーション）
オンライン会議やコラボレーションサービスを提供、またはオンライン会議やコラボレーションに関連する情報を含む場合、Web サイトは Online Meeting & Collaboration カテゴリに分類される可能性があります。

Pay to Surf（ペイ・ツー・サーフ）
コンテンツがペイ・ツー・サーフアクティビティの促進に関連する情報や画像を含む場合、Web サイトは Pay to Surf カテゴリに分類される可能性があります。

Peer to Peer（ピアツーピア）
コンテンツが Limewire などのピアツーピアを促進する目的のソフトウェアに関連する情報や画像を含む場合、Web サイトは Peer To Peer カテゴリに分類される可能性があります。

Personal（パーソナル）
コンテンツが特定個人に関連する情報や画像を含む場合、Web サイトは Personal カテゴリに分類される可能性があります。SNS（ソーシャルネットワークサイト）は含まれません。

Phishing:Frauds（フィッシング：詐欺）
コンテンツが詐欺目的のフィッシング及び（または）マルウェアコードが含む（可能性がある）場合、Web サイトは Phishing/Frauds カテゴリに分類される可能性があります。

Politics（政治）
Web サイトの主要なコンテンツが政治に関連する場合、Web サイトは Politics カテゴリに分類される可能性があります。

Proxies:Filtering bypass（プロキシ：フィルタリングバイパス）
バイパスプロキシサーバの場合、もしくはユーザ識別情報や閲覧トラフィックの送信元を隠す目的のソフトウェアを提供している場合、Web サイトは Proxies and Filtering-Bypass カテゴリに分類される可能性があります。

Radio（ラジオ）
オンライン配信ラジオへのアクセス及び（または）オンラインラジオ配信を促進するソフトウェアを提供している場合、Web サイトは Radio カテゴリに分類される可能性があります。

Real Estate（不動産）
コンテンツが不動産に関連する情報や画像を含む場合、Web サイトは Real Estate カテゴリに分類される可能性があります。

Religion / Personal Beliefs（宗教 / 個人の信仰）
コンテンツが、宗教的信念のシステムや慣習に関する記述や描写、または教えを含む場合、Web サイトは Religion / Personal Beliefs カテゴリに分類される可能性があります。

Remote Control / Desktop（リモート管理 / デスクトップ）
Web サイトのコンテンツがコンピュータのリモート制御用ソフトウェアに関連する場合、Remote Control/Desktop カテゴリに分類される可能性があります。

Restaurants:Dining Food（レストラン）
コンテンツが外食に関連する情報や画像を含む場合、Web サイトは Restaurants/Dining Food カテゴリに分類される可能性があります。

Search Sites（検索サイト）
インターネット検索エンジンに関連する Web サイトの場合、Search Sites カテゴリに分類される可能性があります。

ShareWare:FreeWare（シェアウェア：フリーウェア）
シェアウェアまたはフリーウェアへのアクセスを提供している場合、Web サイトは ShareWare/FreeWare カテゴリに分類される可能性があります。プロフェッショナルな IT 技術者によって使用される一般的なフリー / シェアソフトウェアを提供するサイトは除外され、Computing/IT に分類されます。

Shopping（ショッピング）
Web サイトのコンテンツがオンラインショッピングに関連する場合、Shopping カテゴリに分類される可能性があります。

Social Networking（ソーシャルネットワーク）
オンラインのソーシャルネットワークサービスを提供している場合、Web サイトは Social Networking カテゴリに分類される可能性があります。

Software Downloading:Sharing（ソフトウェアダウンロード：共有）
様々なソフトウェアの作成者に対しホスティング・ダウンロードサービスを提供している場合、Web サイトは Software Downloading / Sharing カテゴリに分類される可能性があります。

Spam URLs（スパム URL）
コンテンツがスパムに関連する情報や画像を含む場合、Web サイトは Spam URLs カテゴリに分類される可能性があります。

Special Events（催し物）
コンテンツが催し物に関連する情報や画像を含む場合、Web サイトは Special Events カテゴリに分類される可能性があります。

Sports（スポーツ）
コンテンツがスポーツに関係する場合、Web サイトは Sports カテゴリに分類される可能性があります。

Spyware（スパイウェア）
コンテンツがスパイウェアを含む場合、Web サイトは Spyware カテゴリに分類される可能性があります。

Stock Trading（株取引）
オンライン株取引の機能を提供している場合、Web サイトは Stock Trading カテゴリに分類される可能性があります。

Surveillance Monitoring Site Cams（監視モニタサイトカメラ）
ビデオカメラへのアクセスを提供している場合、Web サイトは Surveillance Monitoring Site Cams カテゴリに分類される可能性があります。

Suspicious（怪しいコンテンツ）
怪しいコンテンツやソフトウェアを提供している、または提供していると思われる場合、Web サイトは Suspicious カテゴリに分類される可能性があります。

Swimsuit/Lingerie Models（水着 / ランジェリーモデル）
コンテンツが水着、ランジェリーモデルに関連する場合、Web サイトは Swimsuit/Lingerie Models カテゴリに分類される可能性があります。

Text Messaging（テキストメッセージ）
モバイル端末及び（または）他の端末に対するテキストや SMS メッセージの送信及び（または）受信を目的としている場合、Web サイトは Text Messaging カテゴリに分類される可能性があります。

Tobacco（タバコ）
コンテンツがタバコに関連する情報や画像を含む場合、Web サイトは Tabacco カテゴリに分類される可能性があります。

Travel / Tourism（旅行 / 観光）
コンテンツがリクリエーションのための旅行やトラベル予約の手段を含む旅行に関連する情報を含む場合、Web サイトは Travel / Tourism カテゴリに分類される可能性があります。

TV（テレビ）
テレビ番組のオンライン配信を促進する、オンライン配信の一般的なテレビサービス及び（または）ソフトウェアアプリケーションを提供している場合、Web サイトは TV カテゴリに分類される可能性があります。

Unions:Professional Organizations（組合：プロ組織）
コンテンツが組合及び（または）プロ組織に関連する情報や画像を含む場合、Web サイトは Unions & Professional Organizations カテゴリに分類される可能性があります。

Vehicles（乗り物）
コンテンツが自動車、バイク、その他の電動車両に関連する情報や画像を含む場合、Web サイトは Vehicles カテゴリに分類される可能性があります自動車やモーター雑誌、モーター製造サイトなどの売買も含まれます。

Video（動画）
Web サイトが高い帯域幅の音楽または動画ストリーミングをはじめオンライン音楽や動画のダウンロード、アップロードおよび共有機能を提供する場合、その Web サイトは Video カテゴリに分類される可能性があります。

Violence / Undesirable（暴力 / 犯罪）
Web サイトの主要コンテンツに暴力やその他の望ましくない行為に関連する情報が含まれる場合、Violence/Undesirable カテゴリに分類される可能性があります。

Viral Video（口コミ動画）
コンテンツが頻繁に視聴されたオンライン動画に関連する情報や画像を含む場合、Web サイトは Viral Video カテゴリに分類される可能性があります。

Weather（天気）
コンテンツが天気に関連する情報や画像を含む場合、Web サイトは Weather カテゴリに分類される可能性があります。

Web Mail（Web メールサイト）
コンテンツが Web メールに関連する場合、Web サイトは Web Mail カテゴリに分類される可能性があります。

6.2.5 WCF HTML ページのカスタム

HTTP ALG の Web コンテンツフィルタリング（WCF）機能は、ブロックされるサイトへのアクセスが試みられる状況が発生すると、ユーザに情報を提供する HTML ファイルのセットを使用します。

これらの HTML Web ページは NetDefendOS のファイルとして保存されており、HTTP Banner ファイルとして知られています。管理者は、特定の環境のニーズに合うように、これらのファイルの HTML の外観をカスタマイズすることができます。NetDefendOS の管理インタフェースは、これらのファイルをダウンロード、編集、アップロードする簡単な方法を提供しています。

注意 認証ルールと Web 認証に関連するバナーファイルは別々のサブジェクトであり、「9.3 認証 HTML ページのカスタマイズ」で説明します。

利用可能なバナーファイル

WCF 用に定義済みの HTML ALG バナーファイルは以下の通りです。

- CompressionForbidden
- ContentForbidden
- URLForbidden
- RestrictedSiteNotice
- ReclassifyURL

HTML ページパラメータ

HTML ページには必要とされるいくつかのパラメータがあります。利用可能なパラメータは次の通りです。

- %URL% - 要求された URL
- %IPADDR% - ブラウズを行った IP アドレス
- %REASON% - 接続が拒否された理由
- %RESTRICTED_SITE_NOTICE_BEGIN_SECTION% - 制限サイトセクションを始めます。
- %RESTRICTED_SITE_NOTICE_FORM% - 制限された通知が無視されるのを許可します。
- %RESTRICTED_SITE_NOTICE_END_SECTION% - 制限サイトセクションを終わらせます。
- %RECLASSIFICATION_FORM% - フラグが付けられるサイトの再分類を許可します。

%RESTRICTED_SITE_NOTICE_BEGIN_SECTION% と %RESTRICTED_SITE_NOTICE_END_SECTION% 間にセクションを含めないことで、制限サイト警告を無視する機能を削除することができます。

バナーファイルのカスタマイズ

カスタマイズを実行するためには、まず新規で ALG Banner ファイルオブジェクトを作成する必要があります。この新しいオブジェクトには、自動的に Default ALG Banner ファイルオブジェクト内の全ファイルのコピーが含まれます。次に、これらの新しいファイルを編集し、NetDefendOS にアップロードして戻します。オリジナルのデフォルトオブジェクトを編集することはできません。以下の例では必要な設定手順について説明します。

例題 6.43

コンテンツフィルタリング HTTP バナーファイルの編集

この例題では、URL Forbidden HTML ページの内容を編集する方法を示しています。

Web Interface

バナーファイルの編集

1. **System > Advanced Settings > HTTP Banner files > Add > ALG Banner Files** の順にメニューをクリックします。

2. 名前を入力し、「OK」ボタンをクリックします。

◇ General タブ

General

- Name : my_banner

3. 新しい ALG バナーファイル設定用タブで、以下の情報を入力し、「Save」ボタンをクリックします。

◇ Edit & Preview タブ

Edit

- Page : URLForbidden
- Forbidden URL ページのテキストボックスに表示される HTML ソースを編集します。
- 「Save」ボタンをクリックすると、変更が保存されます。

Preview

- 「Preview」ボタンをクリックすると、レイアウトをチェックすることができます。

4. 「OK」ボタンをクリックし、編集を終了します。

バナーファイルの登録

1. **Objects > ALG** の順にメニューをクリックし、関連する HTML ALG を選択します。
2. HTTP Banners オプションに new_forbidden を設定します。
3. 「OK」ボタンをクリックします。
4. **Configuration > Save and Activate** をクリックし、新しいファイルをアクティブ化します。
5. 「OK」ボタンをクリックします。

新しいファイルが NetDefendOS にアップロードされます。

注意 変更の保存

上記の例では、 1 セッションで 1 個以上の HTML ファイルを編集できますが、「Save」ボタンを押して、別のファイルの編集開始前にすべての編集を保存する必要があります。

SCP を使用したアップロード

SCP を使用して新しい HTTP Banner ファイルをアップロードすることができます。この手順は、以下の通りです。

1. オリジナルのデフォルト HTML のダウンロードを行うために SCP を使用できないので、ソースコードをまず Web インタフェースからコピーして、適切なエディタを使用してローカルなテキストファイルに貼り付けてから編集する必要があります。
2. 編集済みファイルがアップロードされる新しい ALG Banner ファイルオブジェクトが存在する必要があります。オブジェクトが「mytxt」である場合、このオブジェクトは CLI コマンドを使用して以下の通り作成します。

```
DFL-xxxx:/> add HTTPALGBanners mytxt
```

これはすべての Default コンテンツフィルタリングバナーファイルのコピーを含むオブジェクトを作成します。

3. そして、変更されたファイルは、SCP を使用してアップロードされます。それは URLForbidden というプロパティ名でオブジェクトタイプ HTTPALGBanner とオブジェクト mytxt と共にアップロードされます。編集された URLForbidden のローカルファイルが my.html という名前である場合、Open SSH SCP クライアントを使用して、以下のアップロードコマンドを実行します。

```
scp myhtml admin@10.5.62.11:HTTPAuthBanners/mytxt/URLForbidden
```

SCP クライアントについては、「2.1.8 セキュアコピー」を参照してください。

4. CLI を使用して、関連する HTTP ALG が、mytxt バナーファイルを使用するように設定する必要があります。ALG が my_http_alg である場合、コマンドは以下の通りです。

```
set ALG_HTTP my_http_alg HTTPBanners=mytxt
```

5. 通常通り、変更の使用開始のために、CLI コマンド「commit」によるアクティブ化をファイアウォールで行わなければなりません。

6.2.6 WCF 性能ログ

NetDefendOS は Web コンテンツフィルタリングのサブシステムが行っていることを、より確実に参照するためのオプションを提供します。これは WCF 性能ログと呼ばれます。適切なサポート技術者が使用することを意図していますが、本機能があることや有効化する方法を知っておくことは有用です。

有効な場合、この機能は、WCF サブシステムのステータスのスナップショットを取得して、wcf_performance_notice ログイベントメッセージを、Memlog を含め、すべての設定済みログ受信者に出力します。以下は、このログメッセージの例です。

```
2014-10-04 08:47:25 Info ALG 200142 wcf_performance_notice algmod=http cache_
size=88 cache_repl_per_sec=3 trans_per_sec=8 queue_len=7 in_transit=2 rtt=1
queue_delta_per_sec=1 server=10.1.0.10 srv_prec=primary
```

性能ログを有効にしたら、以下の頻度の 1 つからログ生成の発生する頻度を選択します。

- 5 秒ごと
- 10 秒ごと
- 30 秒ごと
- 60 秒ごと
- 300 秒ごと
- 600 秒ごと

各 wcf_performance_notice ログメッセージには以下のフィールドがあります。

項目	説明
cache_size	外部の WCF データベースサーバで検索された最新の URL を含む WCF キャッシュのサイズ。
trans_per_sec	1 秒ごとに送信されるデータベースクエリの数。URL は常に単独で送信されるというわけではありません。データベースに対して処理を待つ URL が 1 つ以上ある場合、NetDefendOS はバッチを送信します。
queue_len	外部の WCF データベースサーバによる処理を待つ URL のキュー長。
in_transit	WCF データベースサーバにリクエストを送信したが、まだ応答を受信していないキューにある URL 数。
rtt	最後の WCF データベースサーバ検索のラウンドトリップ時間。
queue_delta_per_sec	1 秒ごとに増加または減少するリクエスト待ちのキューの量。
server	データベース検索を実行するサーバの IPv4 アドレス。
srv_prec	応答するサーバの優先度。高い優先度を持つサーバが応答しない場合、次に低い優先度が選択されます。

ログメッセージとして最後に送信されたスナップショットは、管理コンソールで NetDefendOS CLI コマンド「httpalg -wcf」を使用することで参照することもできます。以下は、コマンドからの出力の例で、wcf_performance_notice ログイベントメッセージと比較される追加情報があります。

```
DFL-xxxx:/> httpalg -wcf

Dynamic Web Content Filter Statistics
Counter                Value
---------------------- ---------------
Cache Size:            62   URLs
Cache Hit Rate:        0    per second.
Cache Miss Rate:       0    per second.
Request Lookups:       0    per second.
Request Queue Length:  0    URLs.
Requests In Transit:   0    URLs.
RTT per transaction:   40   milliseconds.
Request Queue Delta:   0    URLs per second.
Cache Replacements:    0    URLs per second.
Last Cache Repl. - Hit Rate Idle:    N/A.
Last Cache Repl. - Idle TTL Left:    N/A.
Last Cache Repl. - Session TTL Left: N/A.
Server:                192.168.1.18
Connection Lifetime:   574 seconds.
```

注意 これは techsupport コマンドの出力です。

CLI コマンド「httpalf -wcf」からの出力は「techsupport」コマンドからの出力が含まれています。

WCF の性能ログを有効にする

以下の例題は、WCF 性能ログ機能を有効にする方法を示しています。

例題 6.44

WCF の性能ログを有効にする

この例題では、wcf_performance_notice ログイベントメッセージが 5 秒毎に生成されるように WCF 性能ログ機能を有効にします。このログメッセージは WCF サブシステムのスナップショットを提供します。

CLI

```
DFL-xxxx:/> set Settings MiscSettings WCFPerfLog=5
```

Web Interface

1. **System > Advanced Settings > Misc.Settings** の順にメニューをクリックします。
2. WCF Performance Log を Every 5 Seconds に設定します。
3. 「OK」ボタンをクリックします。

6.3 メールフィルタリング

メールトラフィックはシステム管理者にとって、その量と送られるセキュリティの脅威の両方のために重要な心配事であると言えます。迷惑メールは、非常にやっかいであるだけでなく、パブリックインターネットにおけるセキュリティの問題でもあります。迷惑メールは多くの場合スパムと呼ばれ、スパマとして知られるグループにより大量に送信されます。これは、リソースを浪費し、ウィルスを送り付けるだけでなく、読者にブラウザの脆弱性を悪用する Web ページを開かせようとします。

NetDefendOS は、以下の 2 種類のメールフィルタリングサブシステムを提供します。

- **IMAP、POP3、SMTP 用の IP ポリシーベースメールフィルタリング**

  メールトラフィックを対象とする IP ポリシー上でメールフィルタリングを有効化することが可能であり、この方法が推奨されます。NetDefendOS で利用可能なすべてのフィルタリングツールが利用できます。これには包括的なアンチスパム機能も含まれています。

  このタイプのメールフィルタリングについては、「6.3.1 IP ポリシーベースのメールフィルタリング」で説明されます。

- **SMTP 用の IP ルールベースのメールフィルタリング**

  IP ルールを使用したメールフィルタリングでは、SMTP ALG オブジェクトを介してメールフィルタリングを行います。IP ルールを使用したメールフィルタリングは SMTP トラフィックのみに適用され、通常、古い NetDefendOS バージョンとの互換性を保つ目的でのみ使用されます。

  このタイプのメールフィルタリングについては、「6.3.3 IP ルールを使用した SMTP アンチスパム」で説明されます。

6.3.1 IP ポリシーベースのメールフィルタリング

IP ポリシーを使用して利用可能なメールフィルタリング機能は、フルセットのツールを提供します。IMAP、POP3、および SMTP トラフィックにフィルタリングのこの方式を適用することができます。IMAP と POP3 のフィルタリングの場合、メールのフィルタリングに失敗すると、メールは破棄されるのではなく、失敗したというマークが付くだけです。SMTP の場合、メールの破棄または転送ができます。

IP のポリシーベースのメールは以下の手順でセットアップされます。

- メールをフィルタする方法を定義する Email Control Profile オブジェクトを作成します。アンチスパムフィルタリングが必要であれば、プロファイルで明示的に有効とする必要があります。（初期値は無効）
- オプションとして、Email Control Profile オブジェクトの子として、1 つ以上の Email Filter オブジェクトを追加します。それぞれでメールアドレス（または、ワイルドカードを使用したアドレス）を指定します。これらは、ブラックリスト（フィルタリング前に自動的に拒否する）、またはホワイトリスト（決してフィルタしない）となります。
- 上で作成した Email Control Profile オブジェクトをメールトラフィックで起動する IP Policy オブジェクトに関連付けます。1 つのプロファイルのみ IP ポリシーに関連付けられます。

- この IP ポリシー用の Service プロパティが IMAP、POP3 または SMTP プロトコルのトリガーとなる必要があるため、適切な Service オブジェクトに設定する必要があります。使用される Service オブジェクトは、IMAP、POP3 または SMTP に設定された Protocol プロパティを持ちます。（どれかが適用されます。）

  定義済みの IMAP、POP3、および SMTP サービスは、IMAP、POP3、および SMTP に Protocol プロパティを設定することで使用することができます。しかし、代わりに新しいカスタム Service オブジェクトを作成することをお勧めします。これは、本セクションの終わりにある設定例で行われます。

- IP ポリシーでスキャンされるアンチウイルスをオプションで有効にします。これは、メールに添付されたウィルスをスキャンして、IMAP、POP3 または SMTP プロトコルで機能します。詳しいアンチウィルスのスキャンについては「6.4 アンチウィルススキャン」で説明します。

注意 メールフィルタリングにサービスグループを使用できません。

IMAP、POP3 または SMTP プロトコルのいくつかを組み合わせる IP ポリシーベースのメールフィルタリングにカスタム Service Group オブジェクトを使用することはできません。IMAP、POP3 または SMTP には個別サービスを持つ別 IP ポリシーを設定しなければなりません。

General 設定

以下のオプションは、すべてのトラフィックタイプで利用できます。

項目	説明
Anti-Spam	有効にすると、スパムかどうか決定するためにスパムスコアリングがメールに適用されます。アンチスパム機能については本セクションで後ほど詳しく説明します。 初期値では本オプションは無効です。
Blacklist Subject Tag	このプロファイルのブラックリストで検出された場合にメールの subject フィールドに挿入されるテキストです。

プロトコル固有のオプション

特定の Email 関連プロトコルに対してプロファイルを使用された場合に、以下の追加のオプションが利用できます。

項目	説明
SMTP 設定	この設定は SMTP ALG による処理に関連しています。詳細は「6.1.5 SMTP ALG」を参照してください。
POP3 設定	この設定は POP3 ALG による処理に関連しています。詳細は「6.1.6 POP3 ALG」を参照してください。
MAP 設定	この設定は IMAP ALG による処理に関連しています。詳細は「6.1.7 IMAP ALG」を参照してください。

Whitelist/Blacklist

1 つ以上の Email Filter オブジェクトを Email Control Profile オブジェクトに子供として追加できます。各フィルタは、常に破棄する（ブラックリスト）、または常に許可する（ホワイトリスト）するように 1 つのアドレスまたはワイルドカードを使用して一連のアドレスを指定します。

任意の文字列を指定するのにワイルドカードのアスタリスク「*」を使用できます。例えば、文字列 *.@example.com は example.com ドメインからの任意のメールアドレスを表します。また、疑問符「?」文字は任意の 1 文字を表すために使用されます。

ホワイトリストおよびブラックリストは他のすべてのメールフィルタリングより優先されます。いずれかが有効であるホワイトリストにあるメールに対して、アンチスパムまたはアンチウイルス処理は行われません。

メールがブラックリストにあるドメインから来ても、メールは破棄されません。代わりに、件名の最初にテキスト文字列が挿入されます。初期値ではこの文字列は以下の通りです。

```
***BLACK LISTED***
```

この文字列は変更することができます。

IMAP クライアントによっては E メール本文をダウンロードする前にヘッダをダウンロードして表示する場合があります。この場合、ブラックリストの文字列は件名に適切に表示されない可能性があります。E メールの件名に含まれるスパムフラグにも同様の問題が存在する場合があるため、詳細はアンチスパムのセクションで説明します。

アンチスパムとフィルタスコアリング

IP ポリシーを使用してメールをフィルタするアンチスパム機能は、IP ポリシーと共に使用される Email Control Profile オブジェクトで明示的に有効とされる必要があります。一度有効にすると、スコアは、有効なアンチスパムフィルタのサブスコアを合計することによって算出されます。

スコアは以下の手順で使用されます。

- 総スコアが指定した Tagging Threshold（初期値は 10）以上であると、メールはスパムであるものとしてタグ付けをされます。
- SMTP に対してだけ、総スコアが指定した Reject Threshold（初期値は 20）以上であると、メールは破棄されます。

以下のリストから成る各アンチスパムフィルタを有効または無効にできます。

- **Domain Verification**
  有効であると、NetDefendOS は DNS MX クエリを実行し、メール送信側のドメインに関連しているメールサーバの IP アドレスを要求します。例えば、送信側メールアドレスが some.name@example.com あると、NetDefendOS は example.com のメールサーバ用に設定されている DNS サーバに MX クエリを送信します。

  DNS サーバがドメイン名を認識する場合、NetDefendOS はアクションを行いません。DNS サーバがそのドメインを認識しないと、NetDefendOS はこのフィルタリングオプションのためのサブスコアを全体のアンチスパムスコアに追加します。

  本オプションが正常に動作するために NetDefendOS に少なくとも 1 つの DNS サーバを設定する必要があります。DNS サーバが 1 台も設定されていないと、このテストは実行されません。また、サブスコアも追加されません。DNS サーバの設定については、「3.10 DNS 設定」を参照してください。

  本フィルタリングオプションは、初期値で有効です。

- **Malicious Link Protection**
  本オプションはメール内の望ましくない、または悪意がある HTML リンクを無効にします。初期値では有効であり、本セクションの後で詳しく記載します。トリガとなる 1 つのリンクを見つけると、本オプションのサブスコア（初期値 10）は総スコアに追加されます。

- **DNS Blacklists**
  DNS Blacklists オプションを有効にすることで、最大 10 個の異なる DNS Blacklist(DNBL) サーバを指定できます。それぞれが自身のサブスコアを保持しており（初期値は 1 サーバ辺り 10）、サーバが E メールにスパムとしてフラグを付けると、総スコアに追加されます。

  DNSBL サーバが応答していないと、そのサーバのサブスコアは最終的なスコアの計算に含まれません。DNSBL 機能については「6.3.2. DNSBL データベース」で詳しく説明します。DNLBL アンチスパムフィルタリングの例については「IMAP ALG のセットアップ」を参照してください。

メールのタグ付け

メールスコアが、Tag Threshold プロパティを超過すると、それはスパムであるとしてマークされます。これは以下の 2 つの方法で行われます。

- **Tag Subject**
  初期値で有効で、メールの件名にテキストを追加します。テキストの初期値は「*** SPAM ***」ですが、これを任意の文字列に設定できます。

  オリジナルの「Subject」フィールドが次の場合のタグ付けの例題です。

  ```
  Buy this stock today!
  ```

  タグテキストが「*** Probably SPAM ***」になるように定義されると、変更されたメールの「Subject」フィールドは次のようになります。

  ```
  *** Probably SPAM *** Buy this stock today!
  ```

  上の行は、受信トレイの内容の概要として、メール受信者に表示されます。次に、各ユーザは、そのようなタグ付けをされたメールに対応するためにローカルなクライアントに自身のフィルタを設定するようにして、個別のフォルダに送信します。

- **Tag Header**
  本設定は初期値で有効で、E メールのヘッダデータの最後に X-Spam 情報を挿入します。この情報には、E メールで実行されたアンチスパム処理の説明が含まれています。有効にすると、メールがスパムとみなされるかどうかを示します。この情報を受信者が直ちに見ないかもしれませんが、多くのメールクライアントが、それを見るためのオプションを備えており、多くがクライアントのフィルタリングの重要な基準になるようにオプションを許可しています。

  NetDefendOS によって挿入される X-Spam フィールドは以下の通りです。

  i. **X-Spam-Checker-Version** - メールにタグ付けをしたソフトウェア。
  ii. **X-Spam-Status** - 適用されたスコアリングとフィルタを含むリスト。
  iii. **X-Spam-Flag** - スパムとしてマークされたメールだけに含まれます。常に Yes です。
  iv. **X-Spam-Report** - 適用されたフィルタの処理結果の詳細なリスト。

スパムとしてマークされたメールに挿入された X-SPAM 情報の例は以下の通りです。

```
X-Spam-Checker-Version: D-Link NetDefendOS on Device
X-Spam-Status:
Yes, score=30 required=10 tests=LINK_PROTECTION,DCC,DNS_BLACKLIST_1
X-Spam-Flag: Yes
X-Spam-Report:
* 10 LINK_PROTECTION: Contained undesirable web links
* 10 DCC: Checksum reported >= 16777200 times
* 10 DNS_BLACKLIST_1: Blacklisted source IP address
```

スパムとしてマークされなかったメールに挿入された X-SPAM 情報の例は以下の通りです。

```
X-Spam-Checker-Version: D-Link NetDefendOS on Device
X-Spam-Status: No, score=5 required=10 tests=DNS_BLACKLIST_1
```

Malicious Link Protection

メールが NetDefendOS を通過する時、アンチスパム用の Malicious Link Protection フィルタは、メールトラフィックに望ましくないリンクを無効にできます。それは、アンチスパムフィルタリングの一部であり、アンチスパムが有効である時にだけ、有効にされます。メール内のリンクは、「6.2 Web コンテンツフィルタリング」の Web コンテンツフィルタリングサブシステム使用することで NetDefendOS が評価します。

リンク保護のために以下の点に注意します。

- リンク保護はメールの最初の 10 個分のリンクしか調べません。その後は、subsequent リンクに対してリンク処理が行われません。
- リンクが Web コンテントのフィルタリングのトリガーとなるとき、リンクはメールに表示されたままですが、それをクリックできないように無効にされます。
- 1 つ以上のリンクが指定したリンクのトリガーとなると、保護スコア (以下のプロパティを参照) はメール用に一度だけ全体のアンチスパムスコアに追加されます。

Email Control Profile の以下のプロパティは、リンク保護を制御するのに使用されます。

項目	説明
Link Protection	初期値では、アンチスパムが有効であれば、リンク保護は有効です。このプロパティを無効にすると、常にオフに切り替わります。
Link Protection Score	Web コンテンツフィルタリングのトリガーとなる 1 つのリンクが見つけられると、総アンチスパムスコアに追加されるスコアです。初期値は 10 です。
Link Protection Categories	無効にする 1 つ以上の Web コンテンツフィルタリングカテゴリのリストです。初期値では、MALICIOUS カテゴリだけに設定されます。利用可能な全カテゴリについては「6.2 Web コンテンツフィルタリング」を参照してください。
Non-Managed Action	Web コンテンツフィルタリングのどのカテゴリにも属さないリンクに対するアクションを指定します。Allow（許可：初期値）または Restrict（制限）を指定します。

注意 有効な Web コンテンツフィルタリングのサブスクリプションが必要です。

NetDefendOS において、Web コンテンツフィルタリング機能はリンクの評価に使用されるため、この機能の有効なサブスクリプションがある場合にだけ、悪意あがあるリンクの保護フィルタは機能します。

IMAP クライアントは不正確なヘッダ情報を表示するかもしれない

メールサーバからメールの詳細を取得するのに IMAP を使用するメールクライアントは、メール本文をダウンロードする前に、メールのヘッダをダウンロードして表示できます。これは、ヘッダ情報に基づいて読みたいメールの本体だけをダウンロードできることを意味します。

NetDefendOS はメール本文に基づいてスパムスコアリングのいくつかを実行する可能性があるため、クライアントが表示する最初のヘッダ情報は、まだ正しく件名のスパムテキストを示していないかもしれません。最後にメール本文をダウンロードする時、NetDefendOS はこれを調べて、メールをスパムであると見なすと、ヘッダ情報を更新します。しかし、メールクライアントによっては、表示されたヘッダ情報を更新しない可能性があり、オリジナルタグなしのヘッダ情報を継続して表示します。これは、NetDefendOS が制御できるものではありません。

すべての場合、NetDefendOS が生成したスパムが関連するログメッセージとそれが保持する統計情報は、どのメールをスパムとして分類したかを正しく反映します。

先に説明した通り、ブラックリストと IMAP クライアントについても同様の問題が発生する可能性があります。クライアントによって表示される最初のヘッダ情報では、ブラックリストの文字列が適切に表示されないかもしれません。

6.3.2. DNSBL データベース

DNSBL サーバは、IP ポリシーベースのアンチスパムと SMTP ALG ベースのアンチスパムの両方と共に使用されます。本セクションでは、本機能の動作と、NetDefendOS のアンチスパムと一緒に使用する方法について説明します。この内容は、メールコントロールおよび IP ポリシーと一緒に使用する DNSBL、そして IP ルールと一緒に使用する SMTP ALG にも適用されます。

パブリック DNSBL データベース

信用できる組織の多くは、既知のスパム SMTP サーバの送信元 IP アドレスのデータベースを公開しており、公共のインターネットでこれらを問い合わせることができます。こうしたリストは、DNS ブラックリスト（DNSBL: DNS Black List）データベースと呼ばれており、NetDefendOS がサポートする標準のクエリ方式を用いて、その情報を利用できます。

DNSBL サーバクエリ

NetDefendOS アンチスパムフィルタリング機能が設定されているとき、メールの送信サーバの IP アドレスを複数の DNSBL サーバに送信して、これらがスパマまたはその他から送信されたものであるかどうかを DNSBL サーバに判断させることができます。NetDefendOS は、これを行うために IP パケットのヘッダを調べます。

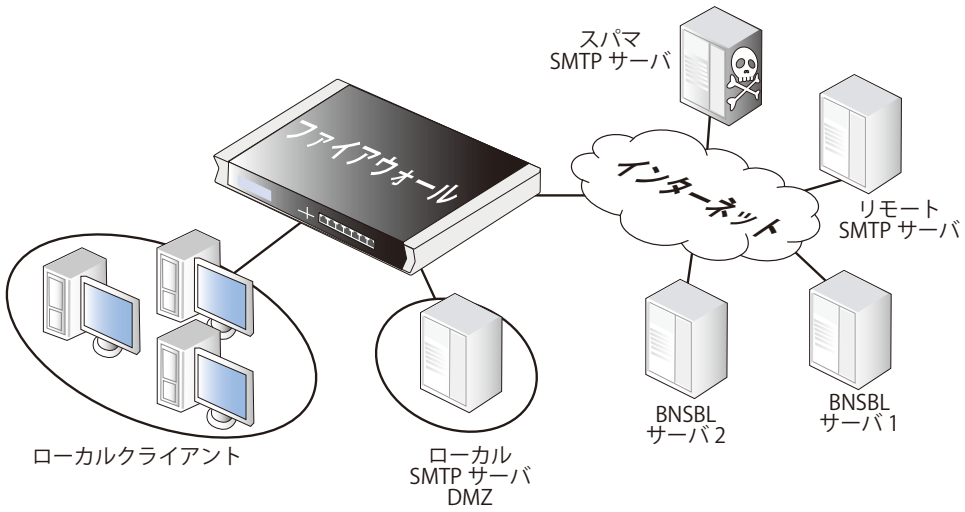


図 6-9　アンチスパムフィルタリング

サーバから送り返される応答は、一覧になっている場合とそうでない場合があります。一覧になっている場合は、DSNBL サーバがそのメールをスパムであると判断したことを示し、通常はこれに加えて、一覧についての説明がテキスト形式で提供されます。

TXT レコードは IP ポリシーベースのアンチスパムによって使用されません。SMTP ALG アンチスパムでは、レコードはメール本体にオプションで挿入される X-SPAM 情報の一部です。

参照 DNSBL サーバ

以下の URL で DNSBL サーバのリストを見つけることができます。
http://en.wikipedia.org/wiki/Comparison_of_DNS_blacklists.

DNSBL コンセンサスの作成

Email コントロールプロファイルオブジェクトには複数の DNSBL サーバを設定することが可能です。このプロファイルはターゲットトラフィックで起動する IP ポリシーに紐づけます。

SNMP ALG では、管理者は、すべてのレスポンスに基づいて加重和が計算できるよう、設定されている各 DNSBL サーバに 0 以上の重み付けを与えます。加重和はすべてのサーバ応答に基づいて計算され、以下の和のしきい値は E メールコントロールプロファイルで設定することができます。

- **タグしきい値**
  合計がこの値以上である場合、メールはスパムの可能性があるとみなされますが、通知テキストが挿入されて受信者へ送信されます。

- **拒否しきい値**
  合計がこの値以下である場合、メールはスパムと判断され、破棄されるか特別なメールボックスへ送信されます。この値は SMTP トラフィックのみに適用されます。

  メールが破棄された場合、送信元の SMTP サーバにエラーメッセージを送り返すオプションがあります（このエラーメッセージはブラックリストで使用されるものと似ています）。

しきい値計算の例

例として、3 台の DNSBL サーバが設定されているものとします。: dnsbl1、dnsbl2、dnsbl3
これらのサーバにそれぞれ 3、2、2 と重みをつけます。その後、「Spam Threshold」を 5 に設定します。

dnsbl1 と dnsbl2 でメールがスパムと判断され、dnsbl3 でスパムではないと判断された場合、和を計算すると 3+2+0=5 になります。5 という和は、しきい値と等しい（しきい値以上）ため、メールはスパムとして扱われます。

この例で「Drop Threshold」が 7 に設定されている場合、加重和 (3+2+2=7) によってメールが破棄されるには、3 台すべての DNSBL サーバが応答する必要があります。

失敗した DNSBL サーバを許可する

DNSBL サーバへのクエリがタイムアウトになった場合、NetDefendOS はクエリが失敗したものとみなし、スコア計算のため、このサーバに与えられている重みが「SPAM」「Drop」しきい値の両方から引かれます。

十分な DNSBL サーバが応答しない場合、この引き算によってしきい値がマイナスになることを意味します。スコア計算では常に 0 以上の値が生成されるので（サーバはマイナスの重みを持ち得ません）、「SPAM」と「Drop」のしきい値が両方マイナスであっても、すべてのメールが許可されます。

設定した DNSBL サーバが要求された時間内に応答しない場合は必ず、ログメッセージが生成されます。不要にメッセージを繰り返さないため、ログメッセージは、1 台のサーバから応答の失敗が連続して起こり始めたときに 1 度だけ生成されます。

ログへの出力

ALG でスパムフィルタリングによって実施されるログへの出力は以下の 3 種類です。

- Logging of dropped or spam tagged emails - これらのログメッセージには、送信元メールアドレスと IP、および重み付けをされた点数とイベントを引き起こした DNSBL サーバが含まれます。
- DNSBLs not responding - DNSBL クエリのタイムアウトがログに出力されます。
- All defined DNSBLs stop responding - この状態が起こるとすべてのメールが許可されるので、重大度の高いイベントです。

6.3.3 IP ルールを使用した SMTP アンチスパム

このセクションでは、IP ルールを使用して設定された SMTP ALG オブジェクトを利用したアンチスパムの設定手順について説明します。

IP ルールを使用したアンチスパム設定手順

SMTP ALG で DNSBL スパムフィルタリングを設定するための手順を、以下の一覧に要約します。

- 使用する DNSBL サーバを指定します。1 つ以上存在できます。複数サーバは、両方を相互のバックアップとしてだけでなく、送信者のステータスの確認のために動作することができます。
- 加重和の算出において、メールがスパムか否かを判断する上での重要度合いを決定付ける重みを、各サーバに指定します。
- メールをスパムと見なすしきい値を指定します。加重和がしきい値に等しいかそれより大きい場合、メールはスパムと見なされます。2 つのしきい値が指定されます。
  - i. Spam Threshold - タグ付きメールをスパムと見なすしきい値。
  - ii. Drop Threshold - メールを破棄するためのしきい値。

  Spam Threshold は Drop Threshold より小さくする必要があります。2 つが等しい場合、Drop Threshol だけを適用します。
- スパムと見なされたメールの「Subject（件名）」フィールドの先頭に付記するテキストタグを指定します。
- オプションで破棄したメールを（単に破棄するのではなく）送信する送信先アドレスを指定することもできます。オプションで、エラーとなった DNSBL サーバから送信されるテキストメッセージをメールヘッダに挿入するよう指定することもできます。

DNSBL コンセンサスの作成

管理者は、電子メールの送信元アドレスについての統一見解を得るため、複数の DNSBL サーバを調べるように NetDefendOS SMTP ALG を設定できます。新しいメールはそれぞれ、設定したサーバに問い合わせられ、元のアドレスに基づいて、メールがスパムである可能性を確認されます。

SNMP ALG では、管理者は、すべてのレスポンスに基づいて加重和が計算できるよう、設定されている各 DNSBL サーバに 0 以上の重み付けを与えます。管理者は、算出された重み付けの和に基づいて、以下のいずれかのアクションを設定できます。

- **廃棄**
  指定した「Drop Threshold」に和が等しいかそれより大きい場合、メールはスパムであると断定され、破棄されるかまたは 1 つの特殊なメールボックスへ送信されます。

  管理者は、メールが廃棄された場合に、送信側の SMTP サーバにエラーメッセージを送り返すというオプションを持っています。このエラーメッセージはブラックリストに使用されるものと似ています。

- **スパムとしてフラグをつける**
  指定した「Spam Threshold」に和が等しいかそれより大きい場合、メールはスパムの可能性があると見なされ、これを知らせるテキストが付与されて受信者に転送されます。

破棄されたスパムに対するの代替アクション

算出された和が「Drop Threshold」に等しいかそれより大きい場合、メールは対象の受信者に転送されません。その代わり、管理者は破棄されたメールについて、以下の 2 つのうちいずれか 1 つを選択できます。

- 破棄されたメールをすべて受信するための、特別なメールアドレスを設定できます。これを行うと、NetDefendOS は、オプションでメールをスパムと判断した DNSBL サーバから送信されるテキストメッセージ（次のセクションで説明します）を転送されるメールヘッダに挿入することができます。
- 受信者のメールアドレスが、破棄されたメールに対する設定を行っていない場合、これらのメールは NetDefendOS によって破棄され、メール送信に失敗した DNSBL サーバから送信されたテキストメッセージとともに、送信者に送り返されます。

スパムメールにタグをつける

算出された和が「Spam Threshold」より大きく「Drop Threshold」より小さい場合、E メールはスパムの可能性があると認識されるため、メールの Subject フィールドが変更され、メッセージにプレフィックスがつけられてから該当の受信者に転送されます。タグメッセージテキストは、管理者が指定しますが、空白のままでも問題ありません（ただしお勧めはできません）。

オリジナルの「Subject」フィールドが次の場合のタグ付けの例題 :

```
Buy this stock today!
```

タグテキストが「***SPAM***」になるように定義されると、変更されたメールの「Subject」フィールドは次のようになります。

```
*** SPAM *** Buy this stock today!
```

そして、この内容について、E-mail の受信者が受信トレイの内容の概要として参照することができます。次に、各ユーザは、そのようなタグ付けをされたメールに対応するためにローカルなクライアントに自身のフィルタを設定するようにして、個別のフォルダに送信します。

X-SPAM 情報の追加

メールがスパムであると判断し、破棄するメールに転送アドレスを設定する場合、管理者はオプションでメールにテキスト記録を追加する必要があります。テキスト記録は、送信者がスパムの送信元であると DNSBL サーバが考えた場合に返送した情報です。この情報は、転送する前に X-SPAM タグ付けの規則を使用してメールヘッダに挿入されます。

追加される X-SPAM の項目は、以下の通りです。

項目	説明
X-Spam-Flag	これは常に Yes です。
X-Spam-Checker-Version	メールにタグ付けをしたソフトウェア。
X-Spam-Status	これは常に DNSBL です。
X-Spam-Report	メールを SPAM としてフラグを付けた DNSB サーバのリスト。
X-Spam-TXT-Records	メールを SPAM として識別した DNSB サーバが送信したテキストのリスト。
X-Spam_Sender-IP	メール送信側が使用した IP アドレス。

これらの項目は、設定したメールサーバのフィルタリングルール内にあり、管理者によって参照することができます。

メールの送信者を確認する

アンチスパムモジュールの一部として、SMTP プロトコルコマンドの「From（差出人）」アドレスと実際の E-mail ヘッダの「From」アドレスの不一致をチェックするオプションがあります。スパミングによってこれらのヘッダの不整合が生じるため、この機能でメールの整合性を詳しくチェックできます。

不一致が検出される場合、以下の 2 つのアクションのいずれかを設定します。

- メールは破棄されます。
- メールが通過することを許可しますが、設定されたスパムタグを使用して、タグ付けをされます。

送信側アドレス検査が有効な場合、「From」アドレス内のドメイン名だけを比較する追加オプションがあります。DNSBL サブシステム全体に対して以下の内容がチェックされます。

- メールの数がチェックされます。
- スパムのタグが付いたメールの数がチェックされます。
- 破棄されたメールの数がチェックされます。

アクセスされる各 DNSBL サーバに対して以下の内容がチェックされます。

- 定義済みの各 DNSBL サーバからの陽性（スパム）とされる応答の数。
- 定義済みの各 DNSBL サーバから送信クエリ数。
- 定義済みの各 DNSBL サーバからの失敗したクエリ（応答なし）数。

「dnsbl」CLI コマンド

「dnsbl」CLI コマンドは、アンチスパムサブシステムの動作を制御および監視する手段を提供します。これは IP ルールを使用して SMTP ALG を設定する場合に使用されます（IP ポリシーの場合は DNSBL の動作を追跡しません）。

オプションなしで「dnsbl」コマンドを単独で使用すると、すべての ALG の全般的状況が表示されます。DNSBL SPAM フィルタリングが有効になっている SMTP ALG の名前が my_smtp_alg である場合、次のように出力されます。

```
DFL-xxxx:/> dnsbl

DNSBL Contexts:
Name                      Status     Spam     Drop   Accept
------------------------ -------- -------- -------- --------
my_smtp_alg                active      156       65    34299
alt_smtp_alg             inactive        0        0        0
```

「-show」オプションは指定 ALG の SPAM フィルタリング処理のサマリを提供します。この場合、ALG オブジェクトは、まだメールの処理をしていませんが、以下のように my_smtp_alg の動作を検証するために使用されます。

```
DFL-xxxx:/> dnsbl my_smtp_alg -show

Drop Threshold        : 20
Spam Threshold        : 10
Use TXT records       : yes
IP Cache disabled
Configured BlackLists : 4
Disabled BlackLists   : 0
Current Sessions      : 0
Statistics:
Total number of mails checked : 0
Number of mails dropped       : 0
Number of mails spam tagged   : 0
Number of mails accepted      : 0
BlackList                Status   Value  Total   Matches   Failed
------------------------ -------- ----- -------- -------- --------
b.barracudacentral.org    active     25        0        0        0
cbl.abuseat.org           active     20        0        0        0
dnsbl.sorbs.net           active      5        0        0        0
asdf.egrhb.net            active      5        0        0        0
```

特定の DNSBL サーバの統計情報を調べるために、以下のコマンドを使用します。

```
DFL-xxxx:/> dnsbl smtp_test b.barracudacentral.org -show

BlackList: b.barracudacentral.org
Status       : active
Weight value : 25
Number of mails checked                  : 56
Number of matches in list                : 3
Number of failed checks (times disabled) : 0
```

my_smtp_alg に対する dnsbl キャッシュをクリアするため、およびすべての統計情報カウンタをリセットするために、以下のコマンドオプションを使用します。

```
DFL-xxxx:/> dnsbl my_smtp_alg -clean
```

パフォーマンスのためにアドレスをキャッシュする

処理を高速化するため、SMTP ALG は、最近検索された送信者の「From」IP アドレスのキャッシュをローカルメモリに保持します。キャッシュが一杯になると、最も古いエントリから上書きされます。アドレスキャッシュには以下の 2 つの SMTP ALG プロパティがあります。

項目	説明
Cache Size	キャッシュが保持できる最大エントリ数です。「0」に設定されると、キャッシュは使用されません。キャッシュサイズを増やすと、アンチスパムに必要とされる NetDefendOS メモリの量は増加します。
Cache Timeout	タイムアウトは、アドレスがキャッシュに保存されてから有効である期間を規定します。この期間が過ぎた後は、キャッシュされた送信者アドレスから新しいクエリが DNSBL サーバに送信される必要があります。 初期値は 600 秒です。

NetDefendOS が再起動する時、または再構成操作が実行される時にアドレスキャッシュが空にされます。

6.4 アンチウィルススキャン

6.4.1 概要

NetDefendOS アンチウィルスモジュールは、ファイアウォール経由でクライアントがファイルをダウンロードする際に侵入する不正なコードを防御します。ウィルスのために、以下の内容をスキャンできます。

- ファイアウォールを経由してサーバ / クライアント間で送信されるファイル。以下のプロトコルを使用して転送されます。
  i. HTTP.
  ii. FTP.
  iii. POP3.
  iv. SMTP.
  v. IMAP（IP ポリシーオブジェクトのみ）

- HTTP 経由で提供される Web ページに含まれるスクリプト。

- HTTP 経由で提供される Web ページに含まれる URL。

ダウンロード時の不正なコードには、単に迷惑行為を行うものから、悪意ある意図によりパスワード、クレジットカード番号および他の秘密の情報を送信させるようなものまで様々な目的があります。「ウィルス」という用語は、ファイルで送られるそのような悪意のあるコードのタイプすべてに対する一般的な記述として使用されます。

クライアントアンチウィルススキャンとの組み合わせ

主としてサーバに対する攻撃に向けられる IDP とは異なり、アンチウィルススキャンはクライアントによるダウンロードに焦点を合わせています。NetDefendOS アンチウィルスは、通常、クライアントコンピュータにインストールされた専門のソフトウェアによってローカルに行われる標準的なアンチウィルススキャンに対応するように設計されています。

IDP はローカルなスキャンに対して完全に置き換わるものとして意図されたものではなく、むしろクライアント保護を高める付加的なシールドという目的があります。最も肝心なのは、ローカルなクライアントのアンチウィルススキャンが何かの理由で機能できない場合に、バックアップとして機能できるということです。

アンチウイルススキャンの有効化方法

アンチウイルススキャンは、以下のいずれかの方法で有効化します。

- **IP ポリシーを使用する**
  スキャンを設定する推奨方法です。アンチウイルスプロファイルオブジェクトを作成し、ターゲットトラフィックに対して起動される IP ポリシーに割り当てます。IP ポリシーの Service プロパティに指定したサービスの Protocol プロパティが対象のプロトコルに設定されている必要があります。

- **IP ルールを使用する**
  IP ルールオブジェクトを使用する場合、まず対象トラフィックに適用する ALG でアンチウイルスを有効化します。その後、サービスオブジェクトにその ALG を割り当て、それをターゲットトラフィックに対して起動される IP ルールに割り当てます。

IP ルールまたは IP ポリシーを使用したアンチウイルススキャンの設定方法は「6.4.3 アンチウイルスキャンのアクティブ化」で説明します。

6.4.2 実行

ストリーミング

データ転送がファイアウォールを経由して継続的に行われるため、NetDefendOS は、アンチウィルスモジュールが有効である場合、ウィルスチェックのためにデータをスキャンします。データが継続して送信されても、メモリに完全に読み込まないため、ファイアウォールの最低限のメモリだけが必要となり、全性能への影響は最低限となります。

パターン照合

検査プロセスは、既知のウイルスパターンのデータベースに対するパターン照合をベースとして高い精度で実行され、ファイアウォール配下のユーザでウイルスがダウンロード中であるかどうかを識別します。一度ファイルの内容にウィルスが認められると、ダウンロードは、完了する前に終了します。

スキャンするデータのタイプ

上記の通り、アンチウィルススキャンは、ALG ベースごとに有効となり、HTTP、FTP、SMTP、および POP3 ALG に関連しているデータダウンロードをスキャンします。詳しくは以下の通りです。

- これらのプロトコルを経由して転送される非圧縮のファイルタイプ。
- 転送されたデータファイルが圧縮されていると、ネストされた圧縮ファイル（最大 10 レベルのネスト）の他、ZIP および GZIP ファイルもスキャンされます。
- HTTP ALG では、Web ページスクリプトと URL がスキャンされます。

HTTP ALG が表示するメッセージ

HTTP ALG を通じて有効にすると、悪質なコードに対して、ファイルと同様に Web ページのスクリプトや URL もスキャンできます。脅威に遭遇すると、接続は破棄され、NetDefendOS はイベントへのログメッセージを生成します。HTTPS トラフィックをスキャンすることはできないので、本機能は HTTPS プロトコルには適用されません。

接続を破棄するだけではなく、影響を受けるユーザの Web ブラウザ HTML に、アクションを取ったことを示すメッセージを挿入しようとします。（これに成功しない場合もあります。）悪意があるファイルとスクリプト用の、挿入されるメッセージの例は以下の通りです。

図 6-10　アンチウィルスの悪意があるファイルメッセージ

悪意がある URL に対して表示されるメッセージは、以下と同様になります。

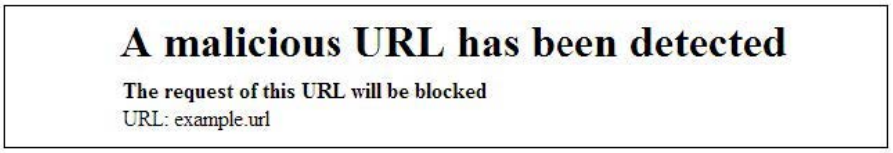


図 6-11　アンチウィルスの悪意がある URL メッセージ

同時のスキャン

１つの D-Link ファイアウォールには、アンチウィルススキャンが同時にいくつ行えるかに関する決まった制限はありません。しかし、使用可能な空きメモリにより、同時に開始できるスキャン数は制限されます。管理者は、AVSE_MAXMEMORY の設定を変更することでアンチウィルススキャンに利用可能な空きメモリのデフォルト量を増加することができます。

この設定では、合計メモリの何パーセントをアンチウィルススキャンに使用するかを指定します。

プロトコルが指定する動作

アンチウィルススキャンはアプリケーションレベルゲートウェイ（ALG）経由で実行されるため、特定のプロトコルを指定する機能が NetDefendOS に実装されています。FTP で、例えばスキャンはオープン状態のデュアルコントロールとデータ転送チャンネルに注意し、ダウンロード中にウィルスを検出すると、コントロール接続を通じ、リクエストを送信してダウンロードを中止します。

IDP との関係

しばしば提起される質問は、IDP スキャンと関連するアンチウィルススキャンの「順番」です。事実上、2 つのスキャンプロセスが異なるプロトコルレベルで同時に起こって動作するため、順番の概念は意味を持ちません。

IDP が有効になると、定義済みの IDP ルールは指定されたすべてのパケットをスキャンし、HTTP などのパケットストリームを生成するより高いプロトコルレベルを注視しません。しかし、アンチウィルスは、より高いレベルのプロトコルを認識しており、ファイル転送にかかわるデータに目を向けます。そのため、アンチウィルススキャンは、ALG に論理的に帰属する機能ですが、IDP は ALG には属しません。

D-Link アンチウィルスサービスへのサブスクリプション

D-Link アンチウイルス機能は、動作するために、更新可能なサブスクリプションの購入を必要とします。これには、サービス期間に最新のウィルスの脅威に関するシグネチャを持つ Kaspersky SafeStream データベースの定期更新も含まれます。

シグネチャデータベース

NetDefendOS アンチウィルススキャンは、「SafeStream™ II」ウィルスシグネチャデータベースを使用して実行されます。「SafeStream」は、ウィルス検知の分野におけるリーディングカンパニーである Kaspersky により開発、維持されています。データベースはトロイの木馬、ワーム、バックドアエクスプロイトなどを含む広く知られているウィルスの脅威に対する保護を提供します。また、データベースは、ほぼゼロの偽陽性を提供するために徹底的にテストされます。

データベース更新

「SafeStream」データベースは、毎日、新種のウィルスシグネチャで更新されます。より古いシグネチャはめったに廃止になることはありませんが、代わりに数個のウィルスをカバーするより汎用的なシグネチャに取り替えられます。そのため、SafeStream データベースのローカルな NetDefendOS のコピーを定期的に更新する必要あります。そして、この更新サービスは、D-Link サブスクリプションの一部として有効にされます。

データベースのアップロードについては、「付録 A セキュリティ更新サービス」にサブスクリプション満了後のアンチウィルスの動作の詳細と共に詳しく記載されています。

正確なシステム時間を設定する

アンチウィルスモジュールにおける自動更新機能が正しく動作する場合、NetDefendOS が正しいシステム時間に設定されていることが重要です。不正確な時間は、自動更新が無効になることを意味します。

CLI コマンドは以下の通りです。

```
DFL-xxxx:/> updatecenter -status
```

上記コマンドは自動更新機能の現在のステータスを示します。これは、Web インタフェースを通じても実行することができます。

高可用性クラスタにおける更新

HA クラスタにおけるファイアウォールのアンチウィルスデータベース更新は、NetDefendOS によって自動的に実行されます。クラスタには、通常アクティブなユニットとアクティブでないユニットがあります。クラスタにおけるアクティブなユニットだけが新しいデータベースの更新がないかどうか定期的にチェックします。新しいデータベースの更新が利用可能な場合、イベントのシーケンスは以下の通りになります。

1. アクティブなユニットは、新しい更新があることを判断して、更新のために必要なファイルをダウンロードします。
2. アクティブなユニットは、データベースを更新するために自動再構成を実行します。
3. この再構成がフェイルオーバを引き起こすため、パッシブユニットはアクティブユニットになります。
4. 更新が完了すると、新たにアクティブになったユニットは、更新用のファイルをダウンロードして、再構成を実行します。
5. この 2 番目の再構成は別のフェイルオーバを引き起こすため、パッシブユニットは再びアクティブに戻ります。

これらの手順により、クラスタ内のファイアウォールの両端が更新されたデータベースを持ち、元々のアクティブ / パッシブの役割を持つ状態となります。HA クラスタ機能に関する詳細は、「第 12 章 High Availability（高可用性）」を参照してください。

6.4.3 アンチウイルススキャンのアクティブ化

アンチウイルススキャン設定は、ALG を使用せずに IP ポリシーを使用して有効化することができます。アクティベーションのより直接的な方法であり、トラックシェーピングやファイルコントロールなど、IP ポリシーで利用可能なその他のオプションと組み合わせて使用することも可能です。

IP ポリシーと一緒に設定する場合、以下のいずれかの方法でアンチウイルスオプションを有効化します。

- アンチウイルススキャンのプロパティを IP ポリシーで直接設定します。
- まずアンチウイルスプロファイルを作成し、スキャンプロパティを定義します。その後、このアンチウイルスプロファイルを複数の IP ポリシーで使用することができます。

アンチウイルスプロファイルのプロパティ

ALG でスキャンされるアンチウィルスを設定する場合、以下のパラメータが設定されます。

- **一般的なオプション**

項目	説明
Mode	これは、以下のうちの 1 つである必要があります。 • Disable - アンチウィルスを無効にします。 • Audit - スキャンはアクティブとなりますが、アクションはログへの出力だけです。 • Protect - アンチウィルスはアクティブになります。疑わしいファイルは破棄され、ログに出力されます。

- **スキャンの除外オプション**

  必要に応じて、特定のファイルタイプをウィルススキャンから明確に除外できます。除外されるファイルタイプが HTTP ダウンロードにおけるイメージファイルなど一般なシナリオで出会うものである場合、全体のスループットは向上します。

  NetDefendOS は、ファイルの本当のファイルタイプを確認するために「付録 C アンチウィルス MIME ファイルタイプ」に示されたすべてのファイルタイプについて MIME コンテンツチェックを実行して、次に除外リストでそのファイルタイプを検索します。内容からファイルのタイプを確認できないと（これは、「付録 C アンチウィルス MIME ファイルタイプ」で指定されていないファイルタイプで起こる可能性があります。）、ファイル名にあるファイルタイプを除外リストでチェックします。

- **Zone Defense の有効化**

  スキャンによって ZoneDefense を起動することができます。

- **Block Range**

  ZoneDefense によるブロック範囲。詳細は「6.4.4 ZoneDefense を使用したアンチウィルス」を参照してください。

- **圧縮比率の最大**

  圧縮ファイルをスキャンする場合、NetDefendOS は、ファイルの内容を調べるために圧縮ファイルの解凍を行わなければなりません。いくつかのデータタイプは、圧縮ファイルがオリジナルの非圧縮ファイルサイズより小さくて非常に高い圧縮率となっています。これは、比較的小さな添付の圧縮ファイルが、NetDefendOS リソース上で過大な負荷をかけるはるかに大きいファイルに解凍される必要があり、著しく遅いスループットとなるかもしれないことを意味します。

  この状況を防ぐために、管理者は圧縮率の制限を指定する必要があります。NetDefendOS で圧縮率に許可される最大値は 500 であり、初期値は 20 です。

項目	説明
Allow	ファイルはウィルススキャンなしで許可されます。
Drop	ファイルを破棄します。

  上記 3 つの場合のすべてにおいてイベントはログに出力されます。

- **暗号化された ZIP ファイルの許可**

  暗号化された ZIP ファイルを許可またはブロックします。

- **アーカイブの深さの最大**

  NetDefendOS は圧縮されたファイル内に含まれる別の圧縮されたファイルにウィルススキャンを実行できます。許可されるネストのレベルは Maximum archive depth で制御されます。これをゼロにセットすると、圧縮ファイルは常にエラー状態になります。1 の値に設定すると、圧縮ファイルはスキャンされますが、他の圧縮ファイルを含むどんな圧縮ファイルもエラー状態になります。2 の値は圧縮ファイル内の圧縮ファイルの 1 つのネストを許可し、両方のレベルがスキャンされます。

  Maximum archive depth 設定は最大値に 10 を持つことができますが、慎重に設定を増やすべきです。denial-of-service 攻撃はネストの高いレベルを持つ圧縮ファイルの送信から構成されるかもしれません。指定した Maximum archive depth によりファイルが拒否されない場合、多量のファイアウォールリソースが、ファイルの階層構造を解凍して、スキャンするために消費されるかもしれません。

- **Fail Mode**
  ウィルススキャンが何らかの理由で失敗すると、その後転送がドロップされるか、イベントのログ出力とともに許可される動作となります。このオプションが「Allow」に設定されると、ウィルスデータベースが利用できない、または現在の購読の有効期限が切れるなどの条件で、ファイルは破棄されません。代わりに、それらは通過を許可され、エラーが発生したことを示すログメッセージが生成されます

IP ルールを使用してアンチウイルスを設定する場合、関連する ALG オブジェクトで上記と同等の設定が利用可能です。

例題 6.45

IP ポリシーでアンチウィルスをアクティブ化する

この例題では、新しい HTTP 接続は、wan インタフェース経由で lan インタフェースの内部ネットワーク lan_net からパブリックインターネットまで許可されます。HTTP ダウンロードはウィルスチェックのために Audit モードだけでスキャンされるため、ファイルは破棄されません。NAT が自動的に変換されるようにアドレス変換はデフォルトの自動設定を使用し、Anti-Virus Profile オブジェクトを使用してウイルススキャンを定義します。

Service オブジェクト http がこの例題で使用されます。コンフィグレーションが前の NetDefendOS バージョンから 11.01 にアップグレードされている場合、プロトコルプロパティが HTTP に設定されると http サービスを利用できますが、定義済みのサービス http-outbound もまだ存在しているのであればこちらを使用することも可能です。

CLI

最初に、Anti-Virus Policy オブジェクトを設定します。:

```
DFL-xxxx:/> add Policy AntiVirusPolicy av_audit_profile AuditMode=Yes
```

次に、IP Policy オブジェクトを定義します。:

```
DFL-xxxx:/> add IPPolicy SourceInterface=lan SourceNetwork=lan_net DestinationInterface=wan DestinationNetwork=all-nets
            Service=http Name=lan_to_wan Action=Allow AntiVirus=Yes AV_Policy=av_audit_profile
```

Web Interface

最初に、Anti-Virus Policy オブジェクトを設定します。:

1. **Policies > Firewalling > Anti-Virus > Add > Anti-Virus Profile** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: av_audit_profile
   - Mode を AUDIT に設定します。
3. 「OK」ボタンをクリックします。

次に、IP Policy オブジェクトを定義します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: lan_to_wan
   - Action: Allow
   - Source Interface: lan
   - Source Network: lan_net
   - Destination Interface: wan
   - Destination Network: all-nets
   - Service: http-outbound
3. Anti-Virus タブを選択します。
4. Anti-Virus を有効にします。
5. Anti-Virus Profile を av_audit_profile に設定します。
6. 「OK」ボタンをクリックします。

IP ルールを使用したアンチウイルスの設定

アンチウイルス機能は IP ルールオブジェクトを使用して設定することも可能です。IP ルールを使用する場合、スキャンするプロトコルを指定した適切なサービスオブジェクトに対し、アンチウイルススキャンを許可する ALG を割り当てます。その後、ALG が適用されるトラフィックの送信元 / 送信先を定義した IP ルールセットの IP ルールに対し、サービスオブジェクトを割り当てます。

例題 6.46

IP ルールでアンチウィルスをアクティブ化する

この例題では、「lannet」から「all-nets」への HTTP トラフィックに対してアンチウィルススキャンを設定する方法を説明します。このトラフィックを NAT するために、IP ルール内には定義済みの NAT ルールがあるものとします。

CLI

はじめに、アンチウィルススキャンが有効な HTTP アプリケーションレイヤゲートウェイ (ALG) オブジェクトを作成する :

```
DFL-xxxx:/> set ALG ALG_HTTP anti_virus Antivirus=Protect
```

次に、新しい HTTP ALG を使用した Service オブジェクトを作成する :

```
DFL-xxxx:/> add Service ServiceTCPUDP http_anti_virus Type=TCP DestinationPorts=80 ALG=anti_virus
```

最後に、新しいサービスを使用するために NAT ルールを編集する :

```
DFL-xxxx:/> set IPRule NATHttp Service=http_anti_virus
```

Web Interface

A. まず、HTTP ALG オブジェクトを作成します。:

1. **Objects > ALG > Add > HTTP ALG** の順にメニューをクリックします。
2. ALG 名 (例 :「anti_virus」) を指定します。
3. Anti-Virus タブをクリックします。
4. Mode プルダウンメニューで「Protect」を選択します。
5. 「OK」ボタンをクリックします。

B. 次に、新しい HTTP ALG を使用した Service オブジェクトを作成する :

1. **Objects > Services > Add > TCP/UDP service** の順にメニューをクリックします。
2. 以下の情報を入力し、「OK」ボタンをクリックします。
3. Type プルダウンメニューで「TCP」を選択します。
4. 「Destination Port」テキストボックスに 80 を指定します。
5. ALG プルダウンメニューから先に作成した ALG を選択します。
6. 「OK」ボタンをクリックします。

C. 最後に、新しいサービスを使用するために NAT ルールを編集する :

1. **Policies> Firewalling > Main IP Rules** の順にメニューをクリックします。
2. 「lannet」と「all-nets」間のトラフィックを処理する NAT ルールをクリックします。
3. 「Service」のプルダウンメニューから定義済みの新しいサービス「http_anti_virus」を選択します。
4. 「OK」ボタンをクリックします。

アンチウィルススキャンが lannet から all-nets へのすべての Web トラフィックに有効になります。

6.4.4 ZoneDefense を使用したアンチウィルス

アンチウイルスがトリガとなる ZoneDefense は、ローカルネットワークにおいてウィルスに感染したホストとサーバを隔離するための機能です。内向きの感染ファイルがローカルネットワークに到達しないようにブロックするウィルススキャンをファイアウォールが行う間、ZoneDefense は、既に感染したローカルホストから他のローカルホストにウィルスが広まることを阻止するために使用されます。NetDefendOS のウィルススキャンエンジンがウィルスを検出すると、ファイアウォールは、ブロックの指示をローカルスイッチにアップロードし、感染したホストまたはサーバからすべてのトラフィックを防ぐように指示します。

スイッチにおける ZoneDefense のブロック状態は、制限のあるリソースであるため、管理者は、ウィルスが検出された場合にスイッチにブロックされるべきホストとサーバを設定しておくことができます。

例えば以下のようになります。
ローカルなクライアントは、インターネットにあるリモート FTP サーバから感染ファイルをダウンロードします。NetDefendOS はこれを検出して、ファイル転送を止めます。この時点では、NetDefendOS は、感染ファイルが内部ネットワークに到達するのを防いでいます。そのため、NetDefendOS が既にウィルスを止めたので、ローカルなスイッチでリモート FTP サーバをブロックする必要はありません。サーバの IP アドレスのブロックは、スイッチ内のブロックエントリを消費するだけです。

NetDefendOS がどのホストとサーバを妨げたらよいかを判断できるように、管理者は、ZoneDefense ブロックによって影響を受けるべきネットワーク範囲を指定することができます。この範囲内にあるすべてのホストとサーバがブロックされます。

本機能は、ALG のアンチウィルス設定を通じて制御されます。使用されるプロトコルによって、機能の使用方法について異なるシナリオが存在します。

本機能に関する詳細は、「7.9 ZoneDefense」を参照してください。

6.4.5 アンチウィルスキャッシュ

HTTP ALG で実行されるすべてのアンチウイルススキャンは、一般的なアンチウイルスキャッシュを使用します。このキャッシュは、アンチウイルスメカニズムがブロックした最近のスキャンファイルの URL を含む揮発性メモリの割り当てです。

キャッシュを使用してウィルスを検出すると、URL がブロックされた事を示す URLForbidden バナーファイルを表示します。これは、Web コンテンツフィルタリング（WCF）で使用するのと同じバナーファイルであり、管理者が変更できます。詳しくは、「6.2.5 WCF HTML ページのカスタム」を参照してください。大きいファイルで初めてウイルスが検出された際は、バナーファイルが表示されないことに注意してください。

キャッシュとログイベントの使用

キャッシュ操作に関連する追加のログメッセージはありません。アンチウイルススキャンが実際に行われる場合、または URL がキャッシュに見つかった場合、同じ virus_found ログメッセージを NetDefendOS は生成します。キャッシュ利用については生成されたログメッセージで示されません。

キャッシュエントリの生存時間

初期値では、エントリはグローバル設定の Anti-Virus Cache Lifetime が決定した期間キャッシュに残っています。生存時間の期限が切れると、キャッシュからエントリを削除します。そして、新しいダウンロードが要求されると、NetDefendOS はファイルの新しいアンチウイルススキャンを行います。ファイルに関する問題が、キャッシュに URL が入力されてからキャッシュから URL が削除される間（初期値ではキャッシュの生存時間は 20 分）に修正されていると、次の試行でファイルのダウンロードに成功します。

管理者は、ファイルがパブリックインターネットに位置している場合に修正されるファイル問題を制御できないかもしれません。しかし、ファイルが DMZ に位置するかもしれないローカルな Web サーバに位置していると、管理者は問題を解決できるかもしれません。

例題 6.47

アンチウィルスキャッシュ生存時間を変更する

この例題では、アンチウイルスキャッシュ内のエントリの生存時間を 15 分に変更します。

CLI

```
DFL-xxxx:/> set Settings MiscSettings AVCache_Lifetime=15
```

Web Interface

1. **System > Advanced Settings > Misc.Settings** の順にメニューをクリックします。
2. Anti-Virus Cache Lifetime に値 15 を入力します。
3. 「OK」ボタンをクリックします。

キャッシュを無効にする

管理者は、生存時間をゼロに設定することで、キャッシュを無効にすることができます。以下の CLI コマンドで行います。

```
DFL-xxxx:/> set Settings MiscSettings AVCache_Lifetime=0
```

アンチウイルスの性能を低下させ、ダウンロードがブロックされた際の HTTP トラフィックに関するブラウザの情報ページが表示されなくなるため、キャッシュを無効にすることは推奨されません。しかし、いくつかのシナリオで役に立つかもしれません。

キャッシュの統計

CLI の「avcache」コマンドはキャッシュを調べて、管理する方法を提供します。現在のキャッシュコンテンツのサイズを参照するには、パラメータなしでコマンドを使用します。

```
DFL-xxxx:/> avcache

Anti-virus cache size : 5 entries.
Cache hit count : 8 hits.
```

コマンドで表示される値は、以下の通りです。

項目	説明
Anti-virus cache size	キャッシュ内のユニークなファイル URL エントリの総数です。各エントリはアンチウイルスシグネチャのトリガーとなったためブロックされた要求ファイルのダウンロードに対応しています。
Cache hit count	実行に成功したキャッシュ検索の数です。言い換えれば、URL がキャッシュで検出された回数です。URL が初めてキャッシュに追加される場合、このカウンタは増加されません。 NetDefendOS の再起動後、カウンタはゼロになります。また、一度無効にした後、再度有効化することでもゼロにリセットされます。この動作は、AVCache_Lfetime の値をゼロに変更し、その後、正の値に戻すことで実施されます。

キャッシュのクリア

キャッシュをクリアするために、「avcache」コマンドを「-clear」オプションと共に使用できます。

```
DFL-xxxx:/> avcache -clear
```

注意 キャッシュはシグネチャアップデートの後にフラッシュされます。

アンチウイルスキャッシュは、アンチウイルスシグネチャデータベースのローカルコピーのアップデートの後にフラッシュされます。

6.5 ファイルコントロール

NetDefendOS のファイルコントロール機能により、ファイアウォールを通過するファイルの検査を行います。以下のいずれかのプロトコルを使用してファイル転送は行われます。

- HTTP
- FTP
- POP3
- SMTP
- IMAP

ファイルコントロールの設定

IP ポリシーオブジェクトをを使用してファイルコントロールを実装する方式が推奨されます。設定手順は以下の通りです。

- 新規のファイルコントロールプロファイルオブジェクトを作成し、必要に応じてプロパティを調整します。
- ターゲットにするトラフィックをフィルタする IP Policy オブジェクトに割り当てます。IP ポリシーで指定されるサービスのプロトコルプロパティには、対象のトラフィックタイプが設定されている必要があります。（例：HTTP）

ファイルコントロールポリシーは、IP ポリシーで有効化される他のタイプの処理と組み合わせて使用可能です。例えば、同じポリシー上でアンチウイルスを割り当てて有効化し、マルウェアに対するファイルのスキャンも実行するように設定できます。

ファイルコントロールプロファイルのプロパティ

ファイルコントロールプロファイルには以下のプロパティがあります。

項目	説明
Name	プロファイルに設定する適切な論理名。
File Type Action	Allow または Block（初期値）に設定し、File Types プロパティで指定する特定のファイルタイプをブロックまたは許可します。
File Type	ブロックまたは許可するファイルタイプの一覧です。ブロックまたは許可の処理は、Validate File Extension プロパティとは独立して実行されますが、「付録 C アンチウィルス MIME ファイルタイプ」に記載されている定義済みファイルタイプに基づいて実行されます。 i. Block: 指定されたファイルタイプはダウンロード時に破棄されます。リネームによりブロック処理が回避されないように、NetDefendOS は（MIME チェックと似た方法で）ファイルの中身を検索して確認します。 例えば、exe ファイルがブロック対象で、jpg ファイル（ブロック対象外）に exe データが含まれることが検出された場合、このファイルはブロックされます。ブロックが指定されてファイル一覧は指定されていない場合、ブロック処理は実行されません。 ii. Allow: 指定されたファイルのみがダウンロードを許可されて、他のファイルは破棄されます。ブロックの際、ファイルの中身が検査・確認が行われます。例えば、jpg ファイルが許可されている場合に、ファイルタイプ jpg で exe データを含むことが検出された場合、このファイルのダウンロードは破棄されます。このモードで何も指定されていない場合、すべてのファイルのダウンロードが許可されません。 デフォルトで含まれない追加のファイルタイプは「Allow/Block」リストに追加することができます。ただし、これらのエントリはコンテンツ検査の対象となりません。つまり、ファイルの中身の整合性はファイル拡張子によって信頼されます。
Validate File Extension	本オプションにより、ファイルダウンロードのファイルタイプ（ファイル名の拡張子）がファイルのコンテンツに適合するかをチェックする MIME 検証を有効化します。 NetDefendOS がチェックするすべてのファイルタイプが、「付録 C アンチウィルス MIME ファイルタイプ」に記載されています。有効な場合、MIME 検証に失敗するダウンロード（ファイルタイプがコンテンツに適合しないすべてのファイルダウンロード）は、セキュリティ上の脅威となる可能性によって破棄されます。

例題 6.48

IP ポリシーを使用したファイルコントロールのセットアップ

この例題では、内部の HTTP クライアントがインターネットからファイルをダウンロードする際にファイルコントロールポリシーによりファイルの検査が行われ、exe または msi のファイルタイプはブロックされます。また、すべてのファイルの MIME タイプについても検証が行われます。

CLI

A. 内向き HTTP トラフィック用にサービスオブジェクトを作成する :

```
DFL-xxxx:/> add Service ServiceTCPUDP my_http_service Type=TCP DestinationPorts=80 Protocol=HTTP
```

B. FileControlPolicy オブジェクトを作成する :

```
DFL-xxxx:/> add Policy FileControlPolicy my_fc_policy FileListType=Block File=exe,msi VerifyContentMimeType=Yes
```

C. HTTP トラフィック用に IP ポリシーを作成する :

```
DFL-xxxx:/> add IPPolicy Name=my_http_policy SourceInterface=lan SourceNetwork=lannet DestinationInterface=wan
            DestinationNetwork=all-nets Service=my_http_service Action=Allow SourceAddressTranslation=NAT NATS
            ourceAddressAction=OutgoingInterfaceIP FileControl=Yes FC_Mode=UsePolicy FC_Policy=my_fc_policy
```

Web Interface

A. 内向き HTTP トラフィック用にサービスオブジェクトを作成する :

1. **Objects > Services > Add > TCP/UDP Service** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_http__service
   - Type: TCP
   - Destination: 80
   - Protocol: HTTP

3. 「OK」ボタンをクリックします。

B. FileControlPolicy オブジェクトを作成する :

1. **Policies > Firewalling > File Control > Add > File Control Profile** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_fc_profile
   - File Type Action: Block
   - File Types: exe.msi
   - Validate File Extension: Enabled

3. 「OK」ボタンをクリックします。

C. HTTP トラフィック用に IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_http_policy
   - Action: Allow

3. Filter で以下の情報を入力します。
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: wan
   - Destination Network: all-nets
   - Service: my_http_service

4. Source Translation で以下の設定を行います。
   - Address Translation: NAT
   - Address Action: Outgoing Interface IP

5. VoIP タブを選択し、以下の設定を行います。
   - Enable VoIP: ON
   - VoIP Profile: my_h323_profile

6. 「OK」ボタンをクリックします。

ゲートウェイから lannet 状の内部電話に送信されるトラフィックに適用対し、IP ポリシーを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: gw_to_lan
   - Action: Allow

3. File Control で以下の情報を入力します。
   - Enable File Control: ON
   - File Control Profile: my_fc_profile

4. 「OK」ボタンをクリックします。

第 7 章 脅威防御

この章では、NetDefendOS セキュリティ機能について記述します。

- 「7.1 アクセスルール」
- 「7.2. IP レピュテーション」
- 「7.3 Botnet Protection」
- 「7.4 Denial-Of-Service Attacks（DoS）保護」
- 「7.5 Scanner Protection」
- 「7.6 侵入検知と防御」
- 「7.7 しきい値ルール」
- 「7.8 ホストとネットワークのブラックリスト化」
- 「7.9 ZoneDefense」

7.1 アクセスルール

7.1.1 概要

NetDefendOS の主要な機能の一つに認可した接続だけに保護データリソースへのアクセスを許可するという機能があります。アクセスコントロールは、NetDefendOS の IP ルールセットによって行われます。これは、保護されている LAN アドレス範囲をトラストホストとして扱い、信頼できない送信元から信頼されるエリアへのトラフィックフローの入力を制限します。

新しい接続を IP ルールセットでチェックする前に、NetDefendOS は接続ソースをアクセスルールでチェックします。アクセスルールは、指定したインタフェースで予想されるトラフィックソースの指定、また、特定のソースから送信されるトラフィックを自動的に破棄するための指定ができます。アクセスルールは新しい接続の試みに関して効果的で対象を絞った初期フィルタを提供します。

デフォルトアクセスルール

管理者がカスタムアクセスルールを明確に指定しなくても、デフォルトアクセスルールとして知られている基本アクセスルールが常に置かれています。

このデフォルトルールは、実は本当のルールではありませんが、NetDefendOS のルーティングテーブルにおいてリバース検索を実行することによって、入力トラフィックの有効性をチェックします。この探索によって、ルーティングテーブルが示すソースから到来する入力トラフィックが、トラフィックが到着したインタフェース経由でアクセスできるかどうかを検証します。このリバース検索が失敗すると、接続は破棄され、「デフォルトアクセスルール」ログメッセージが生成されます。

破棄された接続について障害調査する場合、管理者はログ内の「デフォルトアクセスルール」メッセージに注意する必要があります。問題の解決方法は、接続が到着するインタフェースに対してルートを作成し、ルートの宛先ネットワークが incomming 接続の送信元 IP と同じまたは同じ範囲となるようにします。

カスタムアクセスルールはオプションです

多くの設定では、デフォルトアクセスルールで充分であり、管理者は他のルールを明示的に指定する必要はありません。例えば、デフォルトルールは、次のセクションで説明する IP スプーフィングから防御します。カスタムアクセスルールが明確に指定されていても、新しい接続が指定ルールのいずれにも適合しないなら、デフォルトアクセスルールが適用されます。

最初にカスタムアクセスルールなしで NetDefendOS を構成して、新しい接続をより厳しくチェックする必要がある場合に追加していくことをお勧めします。

7.1.2 IP spoofing

ファイアウォールのセキュリティメカニズムを通過しようと試みる、トラストホストから到来するかのようにふるまうトラフィックが攻撃者から送信されます。このような攻撃は一般的に Spoofing として知られています。

IP Spoofing は最もよく知られた Spoofing 攻撃のひとつです。フィルタを迂回するために信頼された IP アドレスが使用されます。パケットの送信元アドレスを示す IP パケットのヘッダが、攻撃者によってローカルなホストアドレスに書き換えられます。パケットがはじめの送信元に対して正しく応答されることはありませんが、不必要なネットワークの混雑と DoS（denial of service）攻撃の可能性があります。たとえファイアウォールが DoS 攻撃を検出できても、Spoofing（なりすまし）のため、それを追跡したり、止めることは困難です。

セキュリティメカニズムの VPN は、Spoofing（なりすまし）を回避する 1 つの手段を提供しますが、VPN が適切なソリューションでないところでは、アクセスルールは、送信元アドレス検証に特別なフィルタを提供することによって、anti-spoofing 機能を提供します。アクセスルールにより、指定したインタフェースで受信したパケットが他のインタフェースのネットワークに紐づく送信元アドレスを持っていないことを検証することができます。つまり、以下のような動作となります。

- ローカルのトラストホストに所属する送信元 IP アドレスを持つ incoming トラフィックは許可されない。
- 外部の信頼できないネットワークに所属している送信元 IP アドレスを持つ outgoing トラフィックは許可されない。

最初のポイントは、部外者がローカルホストのアドレスを送信元アドレスとして使用することを防ぎます。二つ目のポイントはあらゆるローカルホストが Spoofing を起動することを防ぎます。
DOS 攻撃については、「7.4.3 DoS 攻撃の例」で詳しく記載します。

7.1.3 アクセスルール設定

アクセスルールの設定は通常のルールと類似しており、フィルタリングフィールドとアクションを含みます。トラフィックがすべてのフィールドに一致する場合、ルールが起動して、NetDefendOS により指定されたアクションが実行されます。

アクセスルールフィルタリングフィールド

ルールを起動するアクセスルールのフィルタリングフィールドには以下の項目があります。

項目	説明
インタフェース	パケットが到達するインタフェース。
ネットワーク	送信者アドレスが属する必要がある IP スパン。

アクセスルールアクション

指定できるアクセスルールのアクションは、以下の通りです。

項目	説明
Drop	定義済みのフィールドに合致するパケットを破棄する。
Accept	ルールセット内におけるより詳細な検査のために、定義したフィールドに一致するパケットを許可する。
Expect	パケットの送信元アドレスがこのルールセットに指定されたネットワークに一致する場合、受信するインタフェースは指定したインタフェースと比較されます。インタフェースが一致する場合、パケットは Accept アクションと同様に許可されます。インタフェースが一致しない場合、Drop アクションと同様に破棄されます。

注意 ログへの出力機能の有効化

ログへの出力機能は、必要に応じてこれらのアクションに対して有効にすることができます。

デフォルトアクセスルールメッセージを止める

「デフォルトアクセスルール」ログメッセージが、何らかの理由のために送信元に絶え間なく生成されていて、止める必要がある場合、その送信元に対するアクセスルールをアクション「Drop」に指定します。

アクセスルールに関連する問題のトラブルシューティング

アクセスルールは、他の NetDefendOS モジュールが参照する前の最初のトラフィックフィルタとなることに注意する必要があります。このためにVPN トンネルの設定のような問題が時々起こります。ルールが VPN トンネル確立などの他の機能の正常な動作を妨げるような問題を調査する際には、アクセスルールをチェックすることをお勧めします。

例題 7.1

アクセスルールを設定する

lannet ネットワーク以外の送信元アドレスを持つトラフィックが LAN インタフェースで受信されないようにするルールを定義します。

CLI

```
DFL-xxxx:/> add Access Name=lan_Access Interface=lan Network=InterfaceAddresses/lannet Action=Expect
```

Web Interface

1. **Thereat Prevention > Access Rules > Add > Access** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。

General

- Name : lan_access
- Action : Expect
- Interface : lan
- Network : lannet

7.2. IP レピュテーション

概要

NetDefendOS には、通信の送信元 / 送信先 IPv4 アドレスを検証し、それらの IP に対して IP レピュテーションの値を決定する機能があります。IPv4 のみに対応しています。また、本機能はサブスクリプションベースの機能であり、適切な NetDefendOS のサポート契約を必要とします。

IP レピュテーションによる決定は、IP レピュテーションデータベースの IP を検索することにより行われます。高い脅威の IP については、一部が NetDefendOS ファイアウォールのローカルに保存されます。データベースの残りの部分は外部サーバに保存されます。データベースには、脅威となり得る IP アドレス及び IP アドレス範囲が含まれています。データベースの検索により潜在的な脅威となり得る各 IP や IP 範囲が決定されます。これには脅威の種類を定義する Threat Category および脅威の重大性を定義する Threat Level が含まれます。

レピュテーションデータベースは、IP レピュテーションの品質と幅の広さで知られる Webroot 社によって提供され、常に更新されます。このデータベースには D-Link サーバを経由して接続されるため、NetDefendOS によるインターネット接続が必要となります。

IP レピュテーションには有効なサブスクリプションが必要

IP レピュテーションはサブスクリプションベースの機能であり、アプリケーションコントロールが動作するにはサブスクリプションを購入する必要があります。詳細およびサブスクリプションの期限が切れた場合の動作については「付録 A セキュリティ更新サービス」を参照してください。

IP レピュテーションの脅威レベル

IP レピュテーションシステムにより、IP アドレスに対して 1 から 100 の脅威レベルが割り当てられます。以下の表では 1-100 の脅威の分類を示しています。

範囲	脅威レベル	情報
1-20	High risk	ローカルデータベース内の 600-12,000,000IP アドレス。
21-40	Suspicious	未分類の IP のスコアは 40 です。
41-60	Moderate risk	
61-80	Low risk	
81-100	Trustworthy	

NetDefendOS による高速なアクセスのために、IP データベースの High Risk 部分についてはローカルに保存されています。

脅威のカテゴリ

IP レピュテーションシステムによって IP アドレスにスコアが割り当てられ、レベルが決定すると、下記リストの 1 つ以上のカテゴリに置かれることになります。IP がカテゴリに関連付けられない場合、その IP は脅威ではないとみなされます。IP に対応するカテゴリは通信時に生成されるログメッセージに出力されます。

カテゴリ	ケース	説明
Spam sources	インバウンド	プロキシを介したスパムメッセージのトンネリング、異常な SMTP アクティビティフォーラムスパムアクティビティ。
Windows Exploits	インバウンド	マルウェア、シェルコード、ルートキットを提供または配布するアクティブ IP アドレス、ワームまたはウイルス。
Web Attacks	インバウンド	クロスサイトスクリプティング、iFrame インジェクション、SQL インジェクション、クロスドメインインジェクション、またはドメインパスワードブルートフォース。
BotNets	インバウンド アウトバウンド	ボットネット C & C チャネルとボットによって制御される感染したゾンビマシンマスター。
Scanners	インバウンド	プローブ、ホストスキャン、ドメインスキャン、パスワードのブルートフォースなどのすべての偵察。
Denial of Service	インバウンド	DOS、DDOS、異常な SYN フラッド、異常なトラフィック検出。
Reputation	インバウンド	現在マルウェアに感染していることが知られている IP アドレス。このカテゴリには、一貫して低い評価スコアを持つ URL をホストする IP も含まれます。
Phishing	インバウンド	フィッシングサイトおよび広告クリック詐欺やゲーム詐欺などのその他の種類の詐欺行為をホストする IP アドレス。
Proxy	インバウンド	プロキシおよびアノニマイザーサービスを提供する IP アドレス。このカテゴリには、TOR アノニマイザーの IP アドレスも含まれます。
Mobile Threats	インバウンド	悪意のある、不要なモバイルアプリケーションの IP アドレス。
Package	インバウンド	このタイプには、他のすべてのタイプが含まれます。
TOR Proxy	インバウンド	TOR ネットワークの出口ノードとして機能する IP アドレス。出口ノードは、プロキシチェーンに沿った最後のポイントであり、発信者の目的の宛先に直接接続します。

IP レピュテーションの特徴

IP レピュテーションサブシステムに関する次の特徴に注意する必要があります。

- IP レピュテーションのログ機能は 1 つのグローバル設定で制御され、初期値で有効化されています。設定方法は「IP レピュテーションログの有効化」で説明しています。
- 本機能が有効化されると、すべてのインタフェースにおける、すべてのパブリック（グローバルユニキャスト）の送信元 / 送信先 IPv4 アドレスが IP レピュテーションデータベースに対してチェックされます。NetDefendOS インタフェースの信頼されるパブリック IP については例外となります。
- データベースの検索毎に、1 つのパブリック IP アドレスに対して 1 つのログメッセージが生成されます。このメッセージには、IP アドレスがスコア計算に使用した IP のレピュテーションスコアとカテゴリが含まれます。
- 送信元 / 送信先 IP アドレスは、NetDefendOS のステートテーブルにより追跡された通信毎に 1 度だけ検索されます。FwdFast IP ルールまたは Stateless IP ポリシーの対象となるデータパケットは、NetDefendOS のステートテーブルで追跡されず、IP レピュテーションサブシステムによる評価は行われません。

除外 IP アドレス

次の IPv4 アドレスは IP レピュテーションサブシステムによって検索されません。

- NetDefendOS インタフェースに割り当てられたパブリック IP アドレス（既に述べた通りです）
- すべてのプライベート IP アドレスとローカルホストの IP（127.0.0.1）
- すべてのブロードキャストまたはマルチキャストアドレス

データベースの更新

IP レピュテーションデータベース全体に対し、D-Link サーバ経由でインターネットから接続が行われます。このデータベースにはすべての脅威レベルの IP とネットワークが含まれており、終日、常に更新されています。

データベースの一部は、クラウド検索時の遅延を避けるためにローカルの NetDefendOS ディスクでミラーされています。ローカルデータベースに保存された部分には、脅威レベルが「High Risk」の IP とネットワークが含まれ、レピュテーションスコアは 1 から 20 となっています。ローカルデータベースのデータは 24 時間毎に全体が更新されます。

NetDefendOS は、検索のパフォーマンスを向上するために、最も直近の IP レピュテーション検索の小さなキャッシュを高速メモリに保持しています。さらに、24 時間毎の完全な更新の間に、D-Link サーバによる部分的なローカルデータベースの更新が発生する場合もあります。全体の High Risk ローカルデータベースが更新されるまで、この部分的な更新についてもキャッシュに保持されます。

要約すると、IP レピュテーションデータベースには 3 つのレベルが存在します。
・外部のクラウド上に存在するデータベース全体
・NetDefendOS のローカルに保存される、高リスクの IP のみのデータベースコピー
・高速メモリに保存され、直近の検索と部分的なデータベース更新を含む、NetDefendOS キャッシュ

IP レピュテーションのログメッセージ

IP レピュテーションのログが有効化されると、IP_Reputation ログメッセージが IP 検索毎に生成されます。典型的なメッセージは以下の通りです。

```
CONN prio=Info id=00600120 rev=1 event=ip_reputation action=none
ip=203.0.113.4 score=10 categories="Spam Sources, Windows Exploits,
Web Attacks" connipproto=ICMP connrecvif=core connsrcip=203.0.113.4
connsrcid=27507 conndestif=wan conndestip=192.168.98.14 conndestid=27507
```

Web インタフェースにおけるログメッセージの表示

IP レピュテーションのログは、NetDefendOS の Web インタフェースで **Status > IP Reputation Logging** から見ることもできます。ただし、このステータス画面では IP レピュテーションのスコアが 40 以下（1 番目と 2 番目に高い脅威レベル）のログメッセージしか表示されません。

IP レピュテーションの検索遅延

高レベルの脅威の IP のみ、ローカルの IP レピュテーションデータベースに保存されるため、IP がローカルで見つからない場合は遅延が発生する可能性があります。この場合、クラウド上のデータベースに対してクエリの送信が行われる必要があります。つまり、接続がオープンした後、それから（ICMP ping 交換など）一時的な接続オープンの場合は接続がクローズした後に IP レピュテーションのログメッセージが生成される可能性があります。

データベースの更新を強制する

次の CLI コマンドを使用して、ローカルに保存された IP レピュテーションのデータベースの更新を強制することができます。

```
DFL-xxxx:/> updatecenter -update ipreputation
```

データベースの更新は、Web インタフェースの **Status > Maintenance > Update Center** で、IP Reputation の「Update」ボタンをクリックして実行することもできます。

更新が手動で実行されると、キャッシュが部分的に削除されます。最近検出された高リスクのキャッシュエントリ（脅威レベル 20 以下）が削除されます（すべてのキャッシュエントリは最大 60 時間保存される）。これにより、頻繁に接続がある無害な IP に対し、高速な検索を行うことができます。

しかしながら、強制的な更新では、キャッシュに保存されたローカルの部分的なデータベース更新すべてがディスク上のローカルの IP レピュテーションデータベースに読み込まれる訳ではありません。これは、ローカルデータベースの完全な更新が実施される 24 時間に 1 度だけ行われます。ただし、NetDefendOS が D-Link サーバに一定期間接続できず、部分的な更新が行われていない可能性がある場合などに、強制的な更新を行うことができます。

起動時にダウンロードと更新が自動的に行われる

NetDefendOS システムが起動すると、過去にデータベースがダウンロードされていない、もしくは 24 時間毎の更新がまだ行われていない場合には、直近 24 時間分の完全なローカルデータベース更新が行われます。また、NetDefendOS 起動時には、前回の 24 時間毎の更新で更新されていなかった部分をダウンロードし、IP レピュテーションキャッシュに保存します。

IP レピュテーションのログ機能が有効化されているかどうかにかかわらず、データベースの自動的なダウンロードは実行されます。本機能の有効なサブスクリプションが存在する限り、ローカルに保存された部分的な IP レピュテーションデータベースは自動的にダウンロードされます。

再起動時にはローカルデータベースが保持される

NetDefendOS の再構成が実行された場合でも、IP レピュテーションのローカルデータベースとキャッシュには影響がありません。一方で、NetDefendOS の再起動ではキャッシュがすべて削除されます。ただし、ローカルデータベースはそのまま保持されます。先に述べた通り、システム起動後、高レベルの脅威に関する部分的な更新が D-Link サーバから自動的にダウンロードされ、キャッシュに保存されます。

CLI コマンド ipreputation

CLI コマンド ipreputation を実行することにより、IP レピュテーションに直接対話し、IP クエリを行ってサブシステムの状態を検査することができます。

IP アドレスの問い合わせを行うには、-query オプションを使用します。

```
DFL-xxxx:/> ipreputation -query 203.0.113.6
Result of query
----------------------
Address            : 203.0.113.6
Response IP        : 203.0.113.6
Reputation         : 10
Categories         : Spam_Sources Windows_Exploits Web_Attacks
In IP Threat List  : 1
Found in           : Local Database
```

-category オプションを使用すると、特定のカテゴリを検索します。

上記の例における「Found in」行は、検索で一致が見つかったことを示しています。以下の値が表示されます。

項目	説明
Cloud lookup	IP が外部データベースサーバで検出されました。
Local Database	IP が NetDefendOS のローカルに保存された IP レピュテーションデータベースの高リスク部分で検出されました。
Cache	IP がローカルの NetDefendOS キャッシュで検出されました。既に最近検出されたか、部分的なデータベース更新に含まれていた（前述の通り、高リスクエントリが含まれるローカルデータベースに対する更新は最初にキャッシュに保存される）ことを意味します。

-query オプションを使用するためにレピュテーションのログを有効化する必要はありません。

-show -verbose オプションでは、最後の再起動以降または有効化後の、IP レピュテーションエンジンに関する統計と、直近の更新に関する詳細を表示します。

```
DFL-xxxx:/> ipreputation -show
IP Reputation Engine Status
---------------------
Database Entries

IP Addresses        : 1489822
IP Ranges           : 16783
Offline DB total    : 1506605
In latest partial   : 1
Cache Entries       : 9

Database updates

Database date       : 2017-02-07 12:56:00
Partial update date : 2017-02-07 12:56:00
Last update check   : 2017-03-16 13:11:49
Last update         : 2017-03-16 13:11:49
Server              : 203.0.113.1
Status              : Connected
```

eputation -updates
Valid options: -update, -verbose オプションを使用すると、IP レピュテーションエンジンを使用する NetDefendOS のサブシステムが表示されます。

```
DFL-xxxx:/> ipreputation -subsystems
Name
-------------
State Engine
CLI
```

「State Engine」という値はログが有効化されていることを意味します。「CLI」は、CLI 検索でエンジンが使用されていることを意味します。想定される他の値には、IP レピュテーション検索を実行する Thereat Prevention オブジェクト（DoS Protection オブジェクトなど）があります。Threat Prevention オブジェクトの説明で後述しますが、異なるサブシステムによるエンジンの利用は、お互いに独立したものとなっています。

ipreputation コマンドのすべてのオプションについては別紙「NetDefendOS CLI Preference Guide」を参照してください。

例題 7.2

IP レピュテーションログの有効化

この例では、すべてのインタフェースに対して IP レピュテーションの検査とログを有効化します。

CLI

```
DFL-xxxx:/> set Settings StateSettings IPReputationLogs=Yes
```

Web Interface

1. **System > Advanced Settings > State Settings** の順にメニューをクリックします。
2. Log IP Reputation にチェックを入れ、「OK」ボタンをクリックします。
3. 「OK」ボタンをクリックします。

Threat Prevention オブジェクトで IP レピュテーションを利用する

接続を破棄すべきかどうか判断するために、以下の NetDefendOS コンフィグレーションオブジェクトで IP レピュテーションサブシステムが使用されます。

- **DoS Protection**

DoS Protection オブジェクトでは、サーバに対する Denial of service attack（DoS 攻撃）から保護することができます。このオブジェクトの詳細は「7.4 Denial-Of-Service Attacks（DoS）保護」に記載しています。

- **Scanner Protection**

Scanner Protection オブジェクトでは、サーバのポートをスキャンして脆弱性を探す外部ホストから保護します。オブジェクトの詳細は「7.5 Scanner Protection」に記載しています。

- **Botnet Protection**

Botnet Protection オブジェクトでは、内部及び外部のクライアント、botnet の一部となったサーバから保護します。オブジェクトの詳細は「7.3 Botnet Protection」に記載しています。

Threat Protection オブジェクトは IP レピュテーションデータベースのローカル部分を使用する

Botnet Protection などの Threat Prevention オブジェクトによって IP レピュテーションサブシステムが使用される場合、IP レピュテーションデータベースのローカル部分のみ参照されます。従って、以下の動作となります。

- IP レピュテーションスコアは遅延なしに決定されます。ローカルの IP レピュテーションデータベースキャッシュにより、検索時間が最小限に抑えられます。
- ローカルに保存された部分的なデータベースには、最も重大な脅威を示す IP のみが含まれているため、誤検知の可能性は最小限に抑えられます。

IP レピュテーションのログは Thereat Prevention オブジェクトに依存しない

IP レピュテーションのログ機能と Threat Prevention オブジェクトはそれぞれ独立して動作しますが、IP レピュテーション検索の重複は発生しません。IP レピュテーションのログが有効化され、DoS Prootection などの Threat Prevention オブジェクトが 1 つ以上有効化されると、新しい接続に対する処理は以下のようになります。

1. 有効化された Threat Prevention オブジェクトが最初に適用されます。起動した最初のオブジェクトにより接続が破棄され、IP がブラックリストへ追加されます。そして、ブラックリストのログメッセージが生成されます。
2. Threat Prevention オブジェクトにより接続が破棄されなかった場合、IP レピュテーションログのサブシステムによって検索ログメッセージが生成されます（ログが有効化されている場合）。

7.3 Botnet Protection

Botnet は、悪意のある攻撃を起動するために第三者によって制御されたリモートのホストから構成されています。NetDefendOS は IP レピュテーションのサブシステムを使用することで、Botnet 攻撃発信元の IP やネットワークを認識し、関連する接続を破棄します。NetDefendOS コンフィグレーションには、定義済みの Botnet Protection オブジェクトが存在します。このオブジェクトを有効化するだけで、この種類の保護を有効化することができます。

Botnet 保護は、サーバに対して攻撃する他のタイプの保護と異なります。Botnet では、サーバ同様に個別のクライアントも攻撃の送信元や対象になり得ます。従って、本機能を有効化されると、新しい接続の送信元と送信先両方の IP アドレスが検査されます。

Botnet 保護は以下の手順で設定することができます。

- コンフィグレーションに事前定義された 1 つの Botnet Protection オブジェクトを有効化します。
- オプションとして、Botnet Protection オブジェクトの Zone Defense 機能を有効化します。この場合、ZoneDefense が起動するための IP 範囲を指定する必要があります（IP 範囲は all-nets に設定することもできます）。
- ZoneDefense オプションが有効化されている場合、少なくとも 1 つ以上の ZoneDefense Switch オブジェクトが定義されている必要があります。IP によって Botnet 保護が起動すると、NetDefendOS はすべての定義済みスイッチにメッセージを送信します。そして、該当 IP が送信元アドレスであった場合はその IP がブロックされます。

有効化されると、Botnet Protection サブシステムは次のように動作します。

1. インタフェース上で通信が開始されると、送信元と送信先の IP がそれぞれ個別にブラックリストで検索されます。ブラックリストでどちらかが検出された場合、接続は破棄されます。
2. ブラックリストに含まれない場合、送信元および送信先 IP は IP レピュテーションデータベースで検索されます。どちらかの IP が Botnet として分類されると、接続は暗黙的に破棄され IP はブラックリストに追加されます。その IP が送信元または送信先となる機能は、次から破棄されるようになります。

接続の送信元と送信先 IP の両方が Botnet として分類される可能性もあります。この場合、ブラックリストではそれぞれに対してエントリが作成されます。

3. Botnet Protection で ZoneDefense が有効化された場合、トリガとなった IP が破棄されるように、該当 IP のメッセージがすべての定義済み Zone Defense スイッチに送信されます。IP は指定した IP 範囲に含まれている必要があります。

IP レピュテーションの検索メカニズムの詳細については「7.2. IP レピュテーション」で説明しています。また、ZoneDefense については「7.9 ZoneDefense」で説明しています。

生成されるログメッセージ

Botnet Protection オブジェクトは、起動した際に以下の 3 つのログイベントメッセージを生成します。以下のメッセージは機能全体が起動した際に表示されるものです。

```
BLACKLIST: prio=2 id=04600006 rev=4 event=host_blacklisted
reason="Botnet Protection" proto=all srcnet=0.0.0.0/0
dstnet=192.168.114.1 port=all
```

送信元アドレスがブラックリストに含まれる場合、以下のメッセージが表示されます。

```
BLACKLIST: prio=2 id=04600006 rev=4 event=host_blacklisted:
reason="Botnet Protection" proto=all srcnet=192.168.114.1
dstnet=0.0.0.0/0 port=all
```

送信先アドレスがブラックリストに含まれる場合、以下のメッセージが表示されます。

```
BLACKLIST: prio=2 id=04600010 rev=1 event=botnet_src_detected
action=blacklist rule=BotnetProtection recvif=VMnet3 srcip=192.168.114.1
destip=192.168.114.100 ipproto=ICMP ipdatalen=40 icmptype=ECHO_REQUEST
echoid=1 echoseq=74 ipaddr=192.168.114.1 reputation=3
```

例題 7.3

Botnet 保護を有効化する

この例題では、Botnet 保護と ZoneDefese を有効化します。IP が 203.0.113.0/24 の範囲に含まれる場合のみ、IP が破棄されます。

少なくとも 1 台の ZoneDefese Switch オブジェクトが定義されており、どのスイッチが NetDefendOS からの ZonseDefense メッセージを受信できるかが設定されているものします。

CLI

```
DFL-xxxx:/> set BotnetProtection EnableBotnetBlacklist=Yes ZDEnabled=Yes ZDNetwork=203.0.113.0/24
```

Web Interface

1. **Threat Prevention > Botnet Protection** の順にメニューをクリックします。
2. Enable Botnet Blacklist を ON に設定します。
3. ZoneDefense を有効化します。
4. Block Range を 203.0.113.0/24 に設定します。
5. 「OK」ボタンをクリックします。

7.4 Denial-Of-Service Attacks（DoS）保護

7.4.1 概要

よくある攻撃の手法は、インターネットの分散トポロジを利用して Denial of Service (DoS) 攻撃を開始し、Web サーバの動作を麻痺させて正当な接続要求への応答ができなくさせてしまうものです。

DoS 攻撃を受ける側になることは、どんなネットワーク管理者も経験したくないことでしょう。攻撃はどこからともなく現れ、サーバーのクラッシュ、インターネット接続の妨害、ビジネスクリティカルなシステムの過負荷により壊滅的な結果をもたらす可能性があります。

DoS 攻撃について

DoS の攻撃は多くの方法で実行されますが、3 つの攻撃の基本タイプがあります。

- 帯域幅、ディスクスペース、または CPU 時間のようなコンピュータリソースの消費。
- ルーティング情報などの設定情報の中断
- 物理的ネットワークコンポーネントの中断

最も一般的に使用される方法の 1 つは、コンピュータリソースの消費で、これは DoS の攻撃がネットワークをフラッドさせ、ビジネスに重要なアプリケーション動作用の重要なリソースを停止させてしまいます。場合によっては、UNIX や Windows™ のオペレーティングシステムの脆弱性が故意にシステムをクラッシュさせるために利用されます。一方、一見したところ不正ではない大容量トラフィックがシステムが過負荷になり、クラッシュに至るという場合もあります。

NetDefendOS の DoS 保護機能は以下のいずれかまたは両方の方式で実行されます。

- 指定したインタフェースで開始された通信の送信元 IP を検査し、IP レプリケーションサブシステムを使用することで、IP が既知の DoS 攻撃送信元であるかどうか判断します。既知の送信元であった場合、接続は破棄され該当の IP はブラックリストに追加されます。
- 指定したインタフェースで開始された通信の送信元 IP の地域を検査し、管理者により定義されたブロック対象の国のリストを使用することにより、IP が DoS 攻撃送信元である可能性があるかどうか判断します。これに当てはまった場合、接続は破棄され該当の IP はブラックリストに追加されます。

この機能は、NetDefendOS のレート制限機能と一緒に使用することができます。レート制限については「7.7 しきい値ルール」で説明しています。

7.4.2 DoS 保護の設定

DoS 保護は次の手順で設定します。

- コンフィグレーションに事前定義された DoS Protection オブジェクトを有効化します。Enable DoS Blacklist または Enable Region Blacklist のどちらかまたは両方を有効化することができます。
- Enable Region Blacklist を有効化した場合、ブラックリストに追加する国を選択します。
- 保護するインタフェースを選択します。通常、インターネットに接続されたインタフェースのみ選択します。

Enable DoS Blacklist を有効化した場合、DoS 保護サブシステムが以下の通り動作します。

1. 一覧のいずれかのインタフェースで通信が開始された場合、ブラックリストで送信元 IP が検索され接続が破棄されます。
2. ブラックリストに IP が含まれない場合は、送信元 IP が IP レピュテーションデータベースで検索されます。IP が DoS であると分類されると、接続は暗黙的に破棄され IP がブラックリストに追加されます。当該 IP からの接続は破棄されるようになります。

IP レピュテーション検索のメカニズムは「7.2. IP レピュテーション」で詳しく説明しています。

Enable Region Blacklist を有効化した場合、DoS 保護サブシステムが以下の通り動作します。

1. 一覧のいずれかのインタフェースで通信が開始された場合、ブラックリストで送信元 IP が検索され接続が破棄されます。
2. ブラックリストに IP が含まれない場合は、送信元 IP がブラックリスト対象の国に対して検索されます。IP がブラックリスト対象の国に属していると、接続は暗黙的に破棄され IP がブラックリストに追加されます。当該 IP からの接続は破棄されるようになります。

生成されるログメッセージ

Threat Prevention オブジェクトと同様に、Dos Protection オブジェクトが起動してブラックリストに追加された場合にのみログイベントメッセージを生成されます。典型的なメッセージは以下の形式です。

```
BLACKLIST prio=2 id=04600006 rev=4 event=host_blacklisted
reason="DoS Protection" proto=all srcnet=203.0.113.5
dstnet=0.0.0.0/0 port=all
```

例題 7.4

DoS 保護を有効化する

この例題では、DoS 保護を wan インタフェースで有効化します。

CLI

```
DFL-xxxx:/> set DoSProtection EnableDoSBlacklist=Yes Interfaces=wan
```

Web Interface

1. **Threat Prevention > DoS Protection** の順にメニューをクリックします。
2. Enable DoS Blacklist を有効化します。
3. インタフェース wan を選択して「Include」をクリックし、Available から Selected に移動します。
4. 「OK」ボタンをクリックします。

7.4.3 DoS 攻撃の例

インターネットの短い歴史の中で最もよく知られた DoS 攻撃のいくつかの例を下記に挙げます。

- Ping of Death attacks
- Fragmentation overlap attacks
- Land and LaTierra attacks
- The WinNuke attack
- Amplification attacks
- TCP SYN flood attacks

これら古典的な攻撃例の性質について次のセクションで詳しく説明します。このセクションでは最もよく知られたDoS攻撃のいくつか種類について、その技術を紹介します。

7.4.3.1 Ping of Death 攻撃

これは、最も初期の OSI レイヤ 3/4 攻撃のひとつです。最もシンプルな実行方法は、コンソールコマンド「ping -l 65510 o.p.q.r」実行する方法です。「o.p.q.r」は攻撃先のオペレーティングシステムの IP アドレスです。「Jolt」は ping コマンドが特大のパケットを生成すること拒否するオペレーティングシステム上にそのようなパケットを生成するようにわざと書かれたプログラムの 1 つです。このタイプの攻撃の別名は Ping of Death です。

最後のフラグメントが総パケットサイズ 65535 バイトを超過させることによって起動します。65535 は 16 ビットの整数が保存できる最も大きな数字です。値がオーバフローすると、非常に小さい数に戻ります。そうなった場合、攻撃先の IP スタックが実行されてしまう事態が発生します。

NetDefendOSは、フラグメントに65535バイトを超過する合計サイズを決して許可しません。さらにNetDefendOSの「Advanced Settings」でIPパケットサイズの制限値を設定することができます。

この攻撃タイプは、IP ルールセットのエントリ名「LogOversizedPackets」で破棄アクションとして NetDefendOS のイベントログに表示されます。送信元 IP は偽装されている可能性があります。

7.4.3.2 Fragmentation overlap 攻撃

Teardrop とその派生（Bonk、Boink、Nestea を含む）はオーバーラッピングフラグメント攻撃です。多くの IP スタックは、オーバラップフラグメントにさらされた場合、不正なふるまい（過度のリソース消費やクラッシュ）をします。

NetDefendOS は、フラグメンテーションオーバラップ攻撃を完全に防御します。フラグメントが重複すると、システムの通過を許可されません。

Teardrop とそれに続く攻撃は、NetDefendOS ログ内で「IllegalFrags」という名前で破棄されたことを記載されます。
送信元 IP アドレスは偽装されている可能性があります。

7.4.3.3 Land and LaTierra 攻撃

Land and LaTierra 攻撃は、攻撃対象にパケットを送信してそこからレスポンスを返させます。そこからさらに別のレスポンスを生成させていきます。これは、犠牲となすマシンをダウンさせるか、クラッシュさせます。

この攻撃は、IP パケットに含まれる送信元 / 送信先 IP アドレスフィールドの攻撃対象者の IP アドレスを使用することで実行されます。

NetDefendOSは、すべてのパケットにIP snooping防御を適用することでこの攻撃から守ります。デフォルト設定では、到着するパケットとルーティングテーブルを比較します。システムがその送信元を予想するインタフェースとは異なるインタフェースにパケットが到着する場合、パケットは破棄されます。

これらの攻撃タイプは、IP ルールなどの NetDefendOS イベントのログ内で、デフォルトでは「AutoAccess」というルール名で破棄されたことを示します。コンフィグレーションにカスタムアクセスルールオブジェクトが含まれる場合は、そのアクセスルール名でパケットは破棄されます。送信元の IP アドレスは送信先 IP アドレスと常に同じであるため、重要ではありません。

7.4.3.4 WinNuke 攻撃

WinNuke 攻撃は、「outof-band」データ（URG ビットで設定された TCP セグメント）を処理しないものの、そのようなデータを許可する TCP サービスに接続することによって動作します。これにより、通常サービスはタイトループに陥り、全ての利用可能な CPU 時間が消費されます。

そのようなサービスは、Windows™ マシンの TCP/IP サービス上の NetBIOS に存在しており、これが攻撃者の名前となっています。

NetDefendOS は 2 つの方法でこれを防御します。

- 慎重な内向きポリシーを使用すると、攻撃が大幅に減少します。危険にさらされたサービスだけが攻撃の犠牲になる可能性があり、パブリックサービスは、ローカルネットワークを提供するためだけに想定されていたサービスよりも良く記述されている傾向があります。
- システムを横断するすべての TCP セグメントからデフォルトで URG ビットを削除します。（Web インタフェースで **System > Advanced Settings > TCP Settings** の順にメニューをクリックし、TCP URG を設定します。）

WinNuke 攻撃は、接続の試みを許可しない IP ルールセットのエントリと一緒に、通常の破棄アクションとして NetDefendOS 内のログに表示されます。システム経由で許可された接続には、（TCPUrg 設定に従う）「TCP」または「DROP」カテゴリエントリは「TCPUrg」というルール名で現れます。送信元 IP アドレスは偽装されていない可能性があります。out-of-band セグメントが送信される前に、3 ウェイハンドシェイクが完了していなければなりません。

7.4.3.5 Amplification 攻撃

このカテゴリの攻撃すべてが、「amplifiers」（パケットストリームを増幅させ最終的なターゲットに送信する不完全な構成のネットワーク）を使用します。この歴史的な例には Smurf、Papasmurf、および Fraggle があります。

これらの攻撃の目標は、過度の帯域幅消費です。つまり、犠牲者のインターネット接続能力のすべてを消費することです。十分な帯域を持つ攻撃者は、amplification の全段階を実行せずに、単純に、ターゲットに対して膨大なデータを送信します。しかし、これらの攻撃では、ターゲットより少ない帯域を持つ攻撃者であっても、データを増幅させて被害者の帯域を逼迫させることができます。

- 「Smurf」と「Papasmurf」は、多くのマシンを持つオープンなネットワークのブローキャストアドレスに ICMP エコーパケットを送信し、送信元の IP アドレスを攻撃ターゲットのものにするように偽造します。その後オープンなネットワークにあるすべてのマシンは、そのターゲットに応答します。
- 「Fraggle」は、同じ概念を使用しますが、UDP エコー（ポート 7）を使用する点が異なります。インターネット上で UDP エコーサービスを有効にしているホストは少ないため、「Fraggle」では通常、データを増幅させる要素も少なくなります。

Smurf 攻撃は、NetDefendOS イベントログに多数の破棄された ICMP Echo Reply パケットとして出力されます。
送信元 IP アドレスは、使用される amplifier ネットワークのものとなります。Fraggle 攻撃は、大量の破棄された（またはポリシーによっては許可された）パケットとして NetDefendOS ログ内に出力されます。

amplifier になることを回避する

最大の帯域ストリームが攻撃ターゲット側にあったとしても、amplifier ネットワークとして選択されることによっても多大なリソースを消費することになります。初期設定では、NetDefendOS は直接接続しているネットワークのブロードキャストアドレスに送信されるパケットを破棄します。（**System > Advanced Settings > IP Settings > Directed Broadcasts** で「ダイレクトブロードキャスト」を設定することが可能です。）しかし、正当な内向きポリシーを使用した何の防御も行われていないネットワークは、smurf amplifier になることについて危惧する必要があります。

Victim 側における保護

Smurf とそれに続く攻撃は、インターネット接続能力までリソースを使い果たす攻撃です。一般的な場合、ファイアウォールはこのクラスの攻撃に対して大きな防御を提供するために、インターネット接続のボトルネックの「悪い」方のサイドに設置されます。パケットがファイアウォールに到達する時には既に被害が発生しています。

しかし、NetDefendOS は内部サーバの負荷がかからないようにして、内部サービスまたは攻撃のターゲットにされないセカンダリインターネットを経由したサービスを利用可能にします。

- Smurf and Papasmurf floods は、犠牲者側には ICMP Echo Response として見えます。「FwdFast」ルールが使用されていない限り、トラフィックを許可するルールがあるかどうかに関わらず、そのようなパケットは、新しい接続を開始することを決して許可されません。
- Fraggle パケットは、攻撃者からターゲットにされ得るどの UDP 送信先ポートにも到達する可能性があります。強化した内向きのルールセットが有効です。

NetDefendOS 内に実装されているトラフィックシェーピング機能は、防御されたサーバに到達する前に多少のフラッドを緩和することに役立ちます。

7.4.3.6 TCP SYN Flood 攻撃

TCP SYN Flood 攻撃は、指定のポートに大容量の TCP SYN パケットを送信し、その応答として返された SYN ACK に応答しないことで行われます。これにより、多くの SYN パケットに応答できなくなり、既存のハーフオープン状態の接続がタイムアウトになるまで犠牲マシンの Web サーバでローカルな TCP スタックリソースを停止します。

NetDefendOS は、Syn Flood Protection オプションがトラフィック上で起動する IP ルールセット内のエントリに関連付けられているサービスオブジェクトで有効にされると、TCP SYN Flood 攻撃を防御します。また、これは時々 SYN Relay オプションとも呼ばれます。

Flood Protection は、事前定義済みのサービス「http-in」、「https-in」、「smtp-in」および「ssh-in」で自動的に有効となります。新しいカスタムサービスオブジェクトが管理者によって定義されると、「Syn Flood Protection」は必要に応じて有効または無効にすることができます。

SYN Flood Defense メカニズム

「SYN Flood」防御は、ターゲットのサービスと 2 個目のハンドシェイクを行う前に、クライアントと 3-way ハンドシェイクを完了させることで行われます。NetDefendOS においては、優れたリソース管理と、通常他のオペレーティングシステムに設定されているような制限がないことにより、過負荷状態ははほとんど起こりません。他のオペレーティングシステムでは、わずかな 5 つの outstanding ハーフオープン通信によって問題となり得ますが、NetDefendOS では通常とは異なる問題が発生しないうちに、全ステートテーブルを一杯にすることができます。ステートテーブルが満たされると、古い未解決の SYN 接続ははじめに破棄され、新しい接続用に空きが準備されます。

SYN Flood の検出

TCP SYN Flood 攻撃は、NetDefendOS ログ内に大量の新しい接続（または、攻撃がクローズポートを対象にした場合、破棄）として出力されます。送信元 IP アドレスは殆ど変わることなく偽装されます。

ALG は自動的にプライベートフラッド防御を提供する

Syn Flood Protection は、ALG が関連するサービスで明示的に有効にする必要がないことにご注意ください。ALG は、自動的に SYN フラッド防御を提供します。

7.4.3.7 Jolt2 攻撃

Jolt2 タイプの攻撃は、攻撃対象マシンに同一のフラグメントの一定したストリームを送信することによって行われます。ストリームが終了するまで 1 秒間に 200 ～ 300 のパケットが送信され、脆弱なマシンを完全にフリーズさせます。

NetDefendOS は、この攻撃を完全に防御します。順番に通過するために、初めのフラグメントはそれより前のフラグメントを待機しますが、これが発生せず、最初のフラグメントでさえも通過することができません。後に続くフラグメントは、はじめのフラグメントに同一であるために廃棄されます。

攻撃者が NetDefendOS 内の **System > Advanced Settings > Length Limit Settings** によって設定された制限よりも高いフラグメントオフセットを選択した場合、パケットは直ちに廃棄されます。
Jolt2 攻撃は、NetDefendOS ログ内に表示または未表示となります。攻撃者が攻撃に非常に高いフラグメントオフセットを選択すると、LogOversizedPackets に設定されたルールによって破棄アクションとして出力されます。
フラグメントオフセットが十分低い場合、ログへの出力は行われません。送信元 IP は偽装されているかもしれません。

7.4.3.8 Distributed Denial of Service（DDoS）攻撃

DoS のより洗練された形態が、Distributed Denial of Service(DDoS) 攻撃です。これらの攻撃は、数百または数千に細かく分けられて、インターネットに存在する個々のコンピュータに DDoS ソフトウェアをインストールしていきます。これにより、ハッカーは、犠牲となるターゲットサイトで組織的攻撃を開始するために、乗っ取ったマシンを直接制御できます。これらの攻撃は、攻撃ターゲットへのネットワークの接続を止めて、帯域、ルータ処理能力、またはネットワークスタックリソースを枯渇させます。

最近の DDoS 攻撃は、プライベートコーポレートと公共の組織的なシステムの両方から開始されていますが、ハッカーは、オープンで分散された性質を持つ大学や公共機関のネットワークを好む傾向があります。
DDoS 攻撃を開始するために使用されるツールには Trin00、TribeFlood Network（TFN）、TFN2K および Stacheldraht があります。

7.5 Scanner Protection

「Scanner」という用語は、偵察のアクティビティを実行する外部ホスト上のソフトウェアを指します。プローブやドメインスキャン、パスワードブルートフォースアタックなどが含まれます。NetDefendOS では、そのようなアクティビティで知られる IP やネットワークを識別して接続を破棄し、関連する IP をブラックリストに追加してそれ以降の接続の試みを破棄するように設定することができます。

スキャナー保護は以下の手順で設定します。
- NetDefendOS の定義済みコンフィグレーションである Scanner Protection オブジェクトを有効化します。
- 保護するインタフェースを指定します。

本機能が有効化された場合、スキャナー保護機能が以下のように動作します。
1. 指定したインタフェースで通信が開始されると、ブラックリストで送信元 IP が検索されます。ブラックリストに含まれる場合、接続は破棄されます。
2. ブラックリストに含まれない場合、送信元 IP は IP レピュテーションデータベースで検索されます。IP がスキャナー IP として分類され、レピュテーションスコア 10 以下である場合、通信は暗黙的に破棄されブラックリストに IP が追加されます。それ以降の該当 IP の接続は破棄されるようになります。

IP レピュテーション検索のメカニズムは「7.2. IP レピュテーション」で詳しく説明しています。

生成されるログメッセージ

Threat Prevention オブジェクトと同様に、Scanner Protection オブジェクトが起動してブラックリストに追加された場合にのみログイベントメッセージを生成されます。典型的なメッセージは以下の形式です。

```
BLACKLIST prio=2 id=04600006 rev=4 event=host_blacklisted
reason="Scanner Protection" proto=all srcnet=203.0.113.5
dstnet=0.0.0.0/0 port=all
```

例題 7.5

スキャナー保護を有効化する

この例題では、スキャナー保護を wan インタフェースで有効化します。

CLI

```
DFL-xxxx:/> set ScannerProtection EnableScannerBlacklist=Yes Interfaces=wan
```

Web Interface

1. **Threat Prevention** > **Scanner Protection** の順にメニューをクリックします。
2. Enable Scanner Blacklist を有効化します。
3. インタフェース wan を選択して「Include」をクリックし、Available から Selected に移動します。
4. 「OK」ボタンをクリックします。

7.6 侵入検知と防御

7.6.1 概要

コンピュータサーバは、ネットワークトラフィックに運ばれる攻撃に時々さらされるという弱点があります。ワーム、トロイの木馬、およびバックドアエクスプロイトはそのような攻撃の例で、攻撃に成功すると、潜在的に危険にさらし、サーバの制御を奪います。これらのサーバが脅威にさらされることを説明するために使用される一般的な用語は、「intrusion」（侵入）です。

侵入検知

「intrusion」は、通常 1 つのファイルダウンロード内にウィルスが含まれており、クライアントシステムにこれがダウンロードされるという点で通常のウィルスと異なっています。サーバセキュリティメカニズムを迂回することを目的としたインターネットデータの悪意のあるパターンとして、「intrusion」は現れます。「intrusion」は珍しくなく、攻撃者が作成を自動化するなどそれらは常に発展しています。NetDefendOS の IDP は、これらの脅威を食い止める重要なラインアップを提供します。

Intrusion Detection and Prevention（IDP）は、これらの侵入の試みから保護するために設計されている NetDefendOS サブシステムです。IDP は、D-Link ファイアウォールを通過するネットワークを監視して、侵入の試みを示すパターンを検索します。一度検出されると、NetDefendOS IDP は、侵入の試みやそのソースの両方を無効にするように処理を行います。

IDP、IPS および IDS

「Intrusion Detection と Prevention」（IDP）、「Intrusion Prevention System」（IPS）、および「Intrusion Detection System」（IDS）は D-Link のドキュメントに互換性を持って使用されることにご注意ください。それらはすべて、NetDefendOS 内の IDP で IDP として知られる同じ機能について言及しています。

IDP 設定の課題

効果的で信頼できる IDP システムのためには、以下の検討すべき課題があります。

・ どんな種類のトラフィックを分析するのか？

IDP Rule で指定する送信元 / 送信先のネットワーク / インタフェースとサービスの組み合わせを決定します。

・ そのトラフィック内で検索するものは何か？

IDP Rule に追加される IDP Rule Action オブジェクトで指定するシグネチャ（セット）を決定します。シグネチャグループまたはサブグループのすべてのシグネチャが必要か？スループット改善のために特定の IDP シグネチャを除外すべきか？少数の現在の既知の脅威から保護する場合、個別の少数の IDP シグネチャを指定するだけで問題ないでしょう。

・ 侵入を見つけた場合、どのようなアクションを行うか？

各 IDP Rule Action には Action プロパティが存在し、シグネチャが起動した際のアクションを決定することができます。接続を破棄するべきか？転送を許可してログを出力するべきか？

また、トリガとなったトラフィックの送信元 IP は今後も破棄されるようにブラックリストに追加するべきか？ブラックリストに追加されている期間はいつまでとするか？トリガとなったプロトコルのみをブラックリストに含めるべきか？ブラックリストの IP からの既存の通信は破棄するべきか？

IDP セットアップ手順とプロセス

IDP のセットアップ手順とそれに続く処理は以下の通りです。

- 管理者により、IDP Rule が設定されます。IDP Rule では、送信元 / 送信先ネットワーク / インタフェースとサービスの組み合わせによって対象トラフィックを指定します。
- 各ルールには 1 つ以上の IP Rule Action オブジェクトが含まれ、対象トラフィックに適用する IDP シグネチャと、シグネチャで起動されるアクションを指定します。
- その後、対象トラフィックがファイアウォールを通過する際にシグネチャとの照合が行われます。
- 設定した IDP シグネチャのいずれかが起動すると、それらに指定したアクションが適用されます。複数の IDP Rule Action オブジェクトで同じシグネチャが繰り返される場合、最初に起動した IDP Rule Action のアクションのみが適用されます。

IDP トラフィックシェーピング

IDP は、ファイアウォールを経由する様々なタイプのトラフィックフローおよびそれらの動因であるアプリケーションを識別する優れた方法を提供します。この機能は識別した特定のフローに帯域幅と優先度制限を定義できる IDP トラフィックシェーピングを提供する NetDefendOS のトラフィック管理機能と組み合わされます。

IDP トラフィックシェーピング機能に関する詳細は「11.2 IDP トラフィックシェーピング」を参照してください。

IDP は ZoneDefense のトリガーとなる

Protect Action には、IDP ルールを起動した特定のスイッチを、D-Link ZoneDefense 機能を通じて、非アクティブ化できるというオプションがあります。本機能に関する詳細は、「7.9 ZoneDefense」を参照してください。この機能は、D-Link が製造したスイッチだけで利用可能であることに注意してください。

7.6.2 IDP コンフィグレーションコンポーネント

IDP ルール

IDP ルールは分析を行うトラフィックまたはサービスの種類を定義します。IDP ルールは、NetDefendOS における IP ルールセットエントリなどの他のセキュリティポリシーと似た構造をしています。IDP ルールには送信元 / 送信先ネットワーク / インタフェースとサービスから成るトラフィックフィルタの設定があります。

IDP ルールのアクション

各 IDP Rule オブジェクトには、1 つ以上の IDP Rule Action オブジェクトが含まれます。さらに、各 IDP Rule Action オブジェクトで IDP シグネチャを指定し、起動時のアクションが設定されます。

IDIP Rule 配下の各 IDP Rule Action オブジェクトのプロパティでは以下の値を設定することができます。

項目	説明
Protect	接続を破棄して、イベントをログに出力します。追加オプションでは、以下で説明されるように、接続の送信元をブラックリストにのせる、または NetDefendOS ZoneDefense 機能を有効化することができます。
Pipe	IDP パイプアクションをトリガするホストに対して帯域制限を行います。本オプションについては「11.2 IDP トラフィックシェーピング」で説明しています。
Audit	接続はオープンのまま許可しますが、イベントをログに取得します。
Ignore	侵入が検出された場合に何もせず、接続をオープンしたままにします。ルールアクションリストで指定されたシグネチャグループから個別のシグネチャを除外する場合に有効であるかもしれません。

IDP ルールに IDP シグネチャを関連付ける

IDP Rule オブジェクトの子オブジェクトである、IDP Rule Action オブジェクトの中で IDP シグネチャを設定します。Web インタフェースの IDP Rule Action 画面におけるシグネチャの選択画面は以下の通りです。

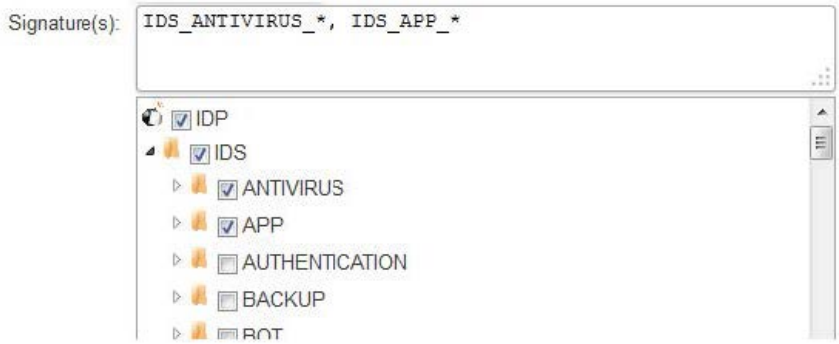


図 7-12 IDP シグネチャ選択

上側のテキストボックスにシグネチャを入力するか、または下側のツリーで選択することでシグネチャを選択することができます。ツリーでは、グループ毎に個別のシグネチャをまとめています。ツリーでグループが選択されている場合、同等のワイルドカード定義は上のボックスに自動的に表示されます。個々のシグネチャをツリー経由で選択することはできないため、テキストボックスに入力します。

上のテキストボックスで指定する内容は、IDP ルールの定義に CLI を使用する際にシグネチャを指定する方法と同じです。

現在のすべての IDP シグネチャが、タイプのメンバシップおよび分類とともに表示されます。
http://security.dlink.com.tw

アドバイザリは「NetDefend Live」メニューの「NetDefend IPS」オプションで確認することができます。
IDP シグネチャ階層構成は「7.6.3 IDP シグネチャとシグネチャグループ」で「7.6.3 IDP シグネチャとシグネチャグループ」で説明しています。

HTTP ノーマライゼーション

各 IDP ルールには、HTTP ノーマライゼーション用の設定セクションがあります。これにより、管理者は、IDP が到来する HTTP リクエストに埋め込まれた URI における矛盾性を見つけた場合に行うアクションを選択することができます。いくつかのサーバ攻撃は、HTTP サーバ製品の弱点を利用するシーケンスで URI を作成することをベースにしています。

IDP が検出できる URI 条件は、以下の通りです。

- **Invalid UTF8**
  URI の無効な UTF8 キャラクタを検索します。
- **Invalid hex encoding**
  有効な 16 進数のシーケンスは、1 バイトのデータを表すために % 符号の後に 2 つの 16 進数値が続きます。無効な 16 進数のシーケンスは、% 符号の後に不正な 16 進数値が続きます。
- **Double encoding**
  これは他の 16 進数のエスケープシーケンスを使用することで、それ自体がコード化される 16 進数のシーケンスを検索します。例えば、オリジナルのシーケンスが %2526 の場合、%25 は HTTP サーバによって '%' に復号化されて、結果としてシーケンス '%26' になります。そして、これは最終的に '&' に復号化されます。

初期パケット処理

IDP でパケット処理の開始手順は以下の通りです。

1. ファイアウォールにパケットが到着し、NetDefendOS は通常の検証を行います。パケットが、新しい接続の一部である場合、パケットが IDP サブシステムを通過する前に、IP ルール設定に対してチェックされます。パケットが既存の接続の一部である場合、IDP システム上を通過します。パケットが既存の接続の一部でない場合、または IP ルールセットによって拒否された場合、パケットは破棄されます。

2. パケットの送信元および送信先情報は、管理者に定義された IDP ルールと比較されます。一致が見つかると、パケットは下の手順 3 に記載した次の IDS 処理レベルのパターン照合に渡されます。一致が見つからない場合、IDP ルール設定に定義されているアクション（例えばアドレス変換、ログ機能など）が適用されますが、パケットは許可され、IDP システムはそれ以上のアクションは行いません。

7.6.3 IDP シグネチャとシグネチャグループ

IDP シグネチャ

IDP が攻撃を正しく識別するためには、異なる攻撃のタイプに関連する指示のプロファイルまたは「パターン」を使用します。攻撃パターンに対してトラフィックを分析するためには、これらの「シグネチャ」と呼ばれる事前に定義したパターンをローカルな NetDefendOS データベースに保存し、IDP サブシステムで使用します。各 IDP シグネチャは固有の番号によって指定されます。

FTP サーバとのやり取りを伴う以下のシンプルな攻撃例を考えてみます。不正ユーザは FTP コマンドの RETR passwd を使用している FTP サーバからパスワードファイル "passwd" を引き出そうとします。ASCII 文字列「RETR」と「passwd」を検索するシグネチャは、この場合、攻撃の可能性がある一致を見つけます。この例では、プレーンテキストでパターンを見つけますが、同様に純粋なバイナリデータでパターン照合をします。

未知の脅威を認識する

新しい侵入を作る攻撃者は、多くの場合より古いコードを再使用します。これは、新しい攻撃がすぐに出回って表れることを意味します。これを無効にするために、D-Link IDP では、NetDefendOS により、完全なプログラムよりむしろビルディングブロックを検索するパターン照合で再利用可能なコンポーネントをスキャンするアプローチを使用します。これは、同じ再利用可能なコンポーネントから成る、以前は未知であった新しい脅威および、「既知の」脅威から守ることができることを意味します。

シグネチャアドバイザリはオンラインで検索可能

アドバイザリはシグネチャの説明している原文の記述です。シグネチャのアドバイザリは、シグネチャが検索する管理者への説明になります。シグネチャデータベースは更新される性質のため、アドバイザリは、D-Link ドキュメンテーションには含められていませんが、代わりに以下の D-Link Web サイトで利用可能です。
現在のすべての IDP シグネチャが、タイプのメンバシップおよび分類とともに表示されます。

http://security.dlink.com.tw

「NetDefend Live」メニューにおける「NetDefend IPS」オプションでアドバイザリを見つけることができます。
シグネチャグループとサブグループ、シグネチャの階層については以下に説明します。

シグネチャグループ

通常、いくつかの攻撃が特定のプロトコルに存在し、ネットワークトラフィックを分析する際、同時にそれらのすべてに検索を行うことが最も効率がいいと言えます。これを実施するためには、同じプロトコルを参照するシグネチャがともにグループ化されます。例えば、FTP プロトコルを参照するすべてのシグネチャは 1 つのグループを形成します。個別のシグネチャについて考慮するよりも検索されるトラフィックに関連するグループを指定することが最も適切です。パフォーマンス向上のために、可能な限り最小の数のシグネチャを使用して NetDefendOS がデータを検索することが大切です。

シグネチャグループを指定する

IDP シグネチャグループは 3 つのレベルの階層構造になっています。階層構造は次の形式の名前で表されます。

```
Type_Group_Subgroup
```

この階層の最上位がシグネチャタイプ、第 2 レベルがカテゴリ、第 3 レベルがサブカテゴリです。このような例として、POLICY_DB_MSSQL と呼ばれるシグネチャグループは、ポリシーが Type、DB が Category、MSSQL が Sub-Category となっています。これらの 3 つのシグネチャコンポーネントを以下で説明します。

1. シグネチャグループ
   - IPS
     Intrusion Protection Signatures (IPS) は非常に正確であり、一致するとほぼ確実に脅威の指標となります。Protect アクションを使用することが推奨されます。これらのシグネチャにより管理アクションとセキュリティスキャナを検出する場合があります。
   - IDS
     Intrusion Detection Signatures (IDS) では侵入が疑われるイベントを検知します。IPS よりも正確性は低く、誤検知が発生することもあります。そのため、常に Audit アクションを使用することが推奨されます。Protect アクションで使用する場合、通常のトラフィックを遮断してしまう可能性があります。
   - Policy
     Policy Signatures では、異なる種類のアプリケーショントラフィックを検出します。ファイル共有アプリケーションやインスタントメッセージのような特定のアプリケーションをブロックするために使用することができます。

2. シグネチャグループカテゴリ
   この第 2 レベルの命名はアプリケーションかプロトコルのタイプについて説明しています。例として、以下のようなグループが存在します。
   - ICMP
   - DNS
   - FTP
   - HTTP
   - SMTP
   - P2P

3. シグネチャサブグループ
   第 3 レベルの命名は、グループのターゲットのより詳細な指定であり、MYSQL のようなアプリケーションそのものを指定することも多くあります。シグネチャのセットを指定するにあたって Type と Group で十分な場合（例：APP_ITUNES）は、サブグループは不要かもしれません。

IDP グループのリスト

IDP グループのリストは「付録 B IDP シグネチャグループ」で確認できます。付録のリストには Group メイトそれに続く Subgroup 名を使用したすべてのシグネチャグループが記載されています。Type は IDS、IPS または POLICY のいずれかであるため、リストには含まれていません。

複数アクションを処理する

IDP Rule オブジェクトに対しては、IDP Rule の子オブジェクトとして 1 つ以上の IDP Rule Action を追加することができます。対象トラフィックに対し、各 IDP Rule Action のシグネチャが上から下へ順番に全て適用されます。一致したエントリがあると、IDP Rule Action オブジェクトのアクションが適用されます。

IDP Rule Action のリストの一番上のシグネチャは、同じシグネチャでリスト内の順番が低いものよりも優先されます。つまり、IDP Rule Action リストで最初に出てくるシグネチャに関連するアクションのみが実行されます。したがって、グループからの個別シグネチャの除外は、Action が ignore に設定されている高い優先度の Rule Action 内で指定することにより実現できます。「例題 7.6 メールサーバに IDP を設定する」でこの設定について説明しています。

IDP シグネチャワイルドカード

IDP シグネチャグループを選択する場合、1 個以上を選択するためにワイルドカードを使用することができます。「?」は、グループ名の 1 文字を任意の文字にする場合に使用されます。「*」は、グループ名に含まれるどんな長さの文字列に対しても任意の文字列にする場合に使用されます。

注意 必要な最小の IDP シグネチャを使用します。

必要最小限の IDP シグネチャと（もしくは）グループのみを使用してください。グループには多くのシグネチャが含まれる場合があるため注意が必要です。現在の多くの重大な脅威に対して保護を行うには、特定の少数のシグネチャのみで十分であるかもしれません。

IDP トラフィックスキャンは、ファイアウォールで追加の処理負荷を引き起こします。ベースとなっているハードウェアによっては、パフォーマンスを著しく低下させるものではありません。スキャン中、あまりにも多くのシグネチャを使用すると、スループットに悪影響を与えることになります。一度にすべての IDP シグネチャを使用しないようにしてください。

7.6.4 Insertion/Evasion（挿入 / 回避）攻撃防止

概要

IDP Rule オブジェクトを定義する場合、管理者は「Protect against insertion/evasion attacks」オプションを有効または無効にします。Insertion/Evasion 攻撃は、特に IDP メカニズムを避けることを狙った攻撃の形です。TCP/IP データ転送で、各データの断片が間違った順序で到着するか、または何らかの方法で断片化されるため、データストリームをしばしばより小さいデータから組み立て直さなければならないという事実を利用します。Insertion または Evasion は、この再組み立てプロセスを利用するように設計されています。

Insertion 攻撃

Insertion 攻撃は、データストリームへの挿入データから成り立つため、結果として生じるデータパケットのシーケンスは IDP サブシステムで許容されますが、ターゲットのアプリケーションには拒否されます。この処理結果は、2 つの異なるストリームデータです。

例えば、4 つのパケットへの壊れたデータストリームを考えてみます。: p1、p2、p3、および p4。攻撃者は最初に、パケットの p1 と p4 をターゲットアプリケーションに送信する可能性があります。パケットの p2 と p3 が到着し、再組み立てされるまで、これらは IDP サブシステムとアプリケーションの両方に保持されます。攻撃者は、故意に 2 つのパケット「p2」と「p3」を送信し、これはアプリケーションに拒否されますが、IDP システムには許容されます。ここで IDP システムは、パケットの再組み立てを完了でき、完全なデータストリームを持つと認識します。攻撃者は 2 つの追加パケット「p2」および「p3」を送信します。これは、再組み立てを完了するアプリケーションに許容されますが、IDP サブシステムで参照されたものと異なるデータストリームをもたらします。

Evasion 攻撃

Evasion 攻撃は、IDP サブシステムが参照する、およびターゲットアプリケーションが参照するという 2 つの異なるデータストリームを生成する点で、Insertion 攻撃に結果が似ていますが、逆の方法で実行されます。Evasion 攻撃は、IDP システムで拒絶される一方でターゲットアプリケーションで許容されるデータパケットを送信することから成り立ちます。

検出アクション

Insertion/Evasion 攻撃は、Insertion/Evasion 防御オプションが有効である場合に検出されると、NetDefendOS は、攻撃に関連している不正なデータを除去することによって、自動的にデータストリームを修正します。

Insertion/Evasion ログイベント

NetDefendOS における Insertion/Evasion 攻撃のサブシステムは、2 つのタイプのログメッセージを生成します。:

- 攻撃が特定されて防御されたことを示す Attack Detected ログメッセージ。
- TCP/IP ストリームの再組み立て時に NetDefendOS が潜在的な攻撃を確認できないものの、そのような攻撃が存在している可能性があることを示す Unable toDetect ログメッセージ。この条件はストリーム内のデータのまれで複雑なパターンによって発生します。

Insertion/Evasion の保護が推奨される

初期値では、Insertion/Evasion 保護はすべての IDP ルールに対して有効とされます。これは多くの構成に推奨される設定です。オプションを無効にするケースとしては、以下の 2 つの理由が考えられます。

- スループットを向上させる - 可能な範囲で最も高いスループットが望まれる場合にオプションをオフにすると、処理速度がわずかに増加します。
- 過度の誤検知 - 異常に高いレベルの Insertion/Evasion の誤検知に関する証拠がある場合にその原因が調査される間、オプションを無効にするのが賢明です。

7.6.5 IDP の設定

IDP を設定する手順は以下の通りです。

- 処理されるトラフィックを特定する IDP Rule オブジェクトを作成します。
- ルールに 1 つ以上の IDP Rule Action オブジェクトを追加します。:

  i. ルールがターゲットとするトラフィックをスキャンする時に使用される IDP シグネチャ。 1 つ以上のシグネチャと（または）グループから構成されます。
  ii. シグネチャがトリガーとなった場合に行うアクション。接続の破棄とログ出力、ログ出力のみ、アクション起動の無視、といった動作を指定することができます（後者は、アクションリストの優先度の低いアクションからシグネチャを除外する場合に役に立ちます。）
  iii . IDP を起動するブラックリストの送信元 IP。これは次のセクションで説明します。

IDP ブラックリスト

IP Rule Action オブジェクトの「Protect」オプションには、IDP Rule Action を起動する送信元 IP アドレスをファイアウォールのブラックリストに追加する追加のオプションが含まれます。これは、ブラックリストに含まれる送信元 IP から送信されるその後のすべてのトラフィック（オプションで同じプロトコルのみを対象とすることも可能）が NetDefendOS によって自動的に破棄されることを意味します。

ブラックリストが有効化されている場合、動的なブラックリストを制御するために、IDP Rule Action オブジェクトには次のプロパティが用意されています。

- **Block duration**

ブロックする期間（秒）を指定します。指定されない（初期値）の場合、期限なしまたは次のシステムの再起動までとなります。

- **Block service only**

送信元 IP アドレスのブロックは、IDP を起動したプロトコルのアドレスから送信されたトラフィックのみに適用されます。異なるプロトコルのトラフィックには適用されません。初期値では無効化されています。

- **Ignore established**

送信元 IP アドレスによってブロックが起動された場合でも、その IP アドレスからの既存の通信には影響ありません。初期値では無効化されています。

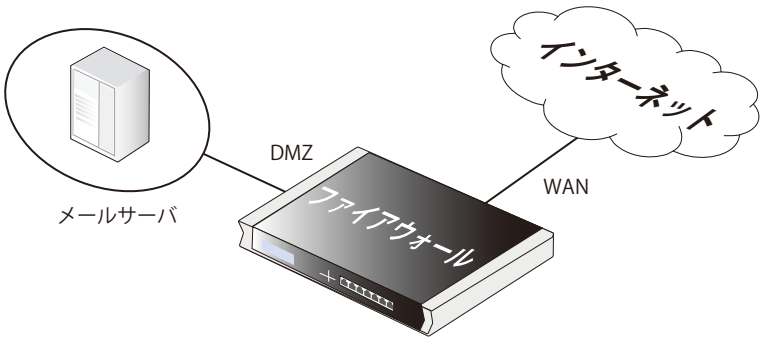
管理 IP アドレスをホワイトリストに追加する

NetDefendOS のホワイトリストに存在する IP アドレスはすべてブラックリストにのせることができません。
このため、IDP を使用する場合、管理者用ワークステーションと NetDefend Firewall 自体の IP アドレスをホワイトリストに追加することをお勧めします。

例題 7.6

メールサーバに IDP を設定する

以下の例題は、メールサーバがパブリック IP アドレスを持つ DMZ ネットワーク上でインターネットに接しているが、以下のように IDS に保護されているというシンプルなシナリオを設定するために必要な手順を示しています。インターネットには、WAN インタフェース上のファイアウォールを経由して到達することができます。



IDPMailSrvRule という名前の IDS ルールを作成し、サービスオブジェクトとして SMTP サービスを適用します。送信元インタフェースと送信元ネットワークはトラフィックを送信する場所を定義します。この例題では外部ネットワークです。送信先インタフェースと送信先ネットワークはトラフィックの送信先を定義します。ここではメールサーバです。そのため、送信先ネットワークはメールサーバを定義しているオブジェクトに設定されます。
また、ここでは IDP シグネチャグループ「IPS_SMTP_*」を使用しますが、SMTP オーバーフローエクスプロイト（72828、72829、58183、52543）に対する特定のシグネチャは、個別に IDP Rule Action を追加することで最初にグループから除外します。

新しい接続により Protect アクションが起動すると、送信元アドレスがブラックリストに追加されます。ブロックされる時間は 3600 秒です。

CLI

IDP ルールを作成する。

```
DFL-xxxx:/> add IDPRule SourceInterface=wan SourceNetwork=wannet DestinationInterface=dmz
            DestinationNetwork=ip_mailserver Service=smtp Name=IDPMailSrvRule
```

CLI コンテキストを IDPRule に変更します。

```
DFL-xxxx:/> cc IDPRule IDPMailSrvRule
```

IPS_SMTP グループから除外するシグネチャを設定します。

```
DFL-xxxx:/IDPMailSrvRule> add IDPRuleAction Action=Ignore Signatures=72828,72829,58183,52543
```

IPS_SMTP グループシグネチャを含むスキャン設定を追加します。

```
DFL-xxxx:/IDPMailSrvRule> add IDPRuleAction Action=Protect Signatures=IPS_SMTP_* Blacklist=Yes
BlackListTimeToBlock=36000
```

Web Interface

IDP ルールを作成する

1. **Threat Prevention** > **Intrusion Prevention** > **Add** > **IDP Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: IDPMailSrvRule
   - Service: smtp
   - Source Interface: wan
   - Source Network: wannet
   - Destination Interface: dmz
   - Destination Network: ip_mailserver

IPS_SMTP グループから除外するシグネチャを追加する

1. IDP ルールで Rule Actions タブを選択します。

2. **Add** > **IDP Rule Action** の順にクリックします。

3. 以下の情報を入力します。
   - Action: Ignore
   - Signatures: 72828,72829,58183,52543

4. 「OK」ボタンをクリックします。

IPS_SMTP グループシグネチャのスキャン設定を追加する

1. 同様に、**Add** > **IDP Rule Action** の順にクリックします。

2. 以下の情報を入力します。
   - Action: Protect
   - Signatures: IPS_SMTP_*
   - Dynamic Blacklisting: Enable
   - Block duration: 3600

3. 「OK」ボタンをクリックします。

7.6.6 IDP イベントに対する SMTP ログレシーバ

E-mail を通して IDP イベントに関する通知を受け取るためには、SMTP ログレシーバを設定します。この E-mail にはユーザが設定した時間に発生した IDP イベントの要約が含まれています。

IDP イベントが発生した場合、NetDefendOS は E-mail 通知の送信前に Keep collecting before sending（保持時間）秒待機します。しかし、この時間内に発生したイベント数が Event count threshold（ログのしきい値）に一致するか、またはそれよりも多くなると E-mail は送信されます。この E-mail が送信されると、NetDefendOS は、新しい E-mail を送信する前に Minimum time between emails（最小繰り返し時間）秒待機します。

SMTP ログレシーバの IP アドレスが必要とされます。

SMTP ログレシーバを指定する場合、レシーバの IP アドレスを指定する必要があります。dns:smtp.example.com などのドメイン名を使用した指定はできません。

例題 7.7

SMTP ログレシーバを設定する

この例題では、既存の IDP Rule「examplerule」が SMTP2c ログレシーバに設定されます。IDS イベントが一度発生すると、IDP ルールが始動します。少なくとも 1 つの新しいイベントが Keep collecting before sending（120 秒）内で発生し、Event count threshold レベル（少なくとも 2 つのイベントが発生する）に到達します。この結果、IDP イベントのサマリが E-mail で送信されます。追加の IDS イベントがこのあとに発生する可能性がありますが、メールサーバのフラッドを防ぐために、NetDefendOS は新しいメールを送信する前に 600 秒（10 分）待機します。SNMP2c サーバがアドレス帳に「smtp-server」という名前で既に設定されているものとします。

CLI

SMTP2c ログレシーバを追加する

```
DFL-xxxx:/> add LogReceiver LogReceiverSMTP smt4IDP2 IPAddress=smtp-server Recipient=youremail@example.com
            Sender=hostmaster@example.com Subject=LogMessage_NetDefendOS Port=25 KeepCollectingPeriod=2 MinT-
            imeBetweenEmail=10 EventCountThreshold=2
```

次に、IDPRule になるように CLI コンテキストを変更します。

```
DFL-xxxx:/> cc IDPRule <index>
```

今度は、最初の IDPRuleAction のプロパティを設定します。

```
DFL-xxxx:/examplerule> set IDPRuleAction 1 LogEnabled=Yes
```

初期値の CLI コンテキストに戻します。:

```
DFL-xxxx:/> cc
```

Web Interface

SMTP2c ログレシーバを追加する :

1. **System > Device > Mail Alerting > Add > Mail Alerting** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: smtp4IDP
   - SMTP Server: smtp-server
   - Server Port: 25
   - ログを受信する E-mail アドレスを指定します。（最大 3 個）
   - Subject: Log event from NetDefendOS
   - Minimum Repeat Delay: 600
   - Minimum time between emails:10（分）
   - Keep collecting before sending:2（分）
   - Log Threshold: 2
3. 「OK」ボタンをクリックします。

IDP ルール :

1. **Policies > Intrusion Prevention > IDP Rules > Add > IDP Rule** の順にメニューをクリックします。
2. ルール examplerule を選択します。
3. Rule Actions の設定で Logging を有効にします。
4. 「OK」ボタンをクリックします。

7.6.7 最適な設定

推奨する IDP の設定

推奨される IDP の設定は以下の通りです。

- 許可されるトラフィック用の IDP シグネチャだけを有効にします。例えば、IP ルールセットで HTTP トラフィックのみを許可している場合、FTP シグネチャを有効にする意味がありません。
- IDP 処理で関連するシグネチャが選択された後、IDP システムはまずは常に Audit モードで実行されるべきです。
- ライブトラフィックを使用してサンプル期間に Audit モードで IDP を実行した後に、生成されたログメッセージを調査します。以下の項目に対してチェックを行います。:

  i. IDP がトリガーとなる場合、どんな種類のトラフィックに起こるのか？
  ii. 正しいトラフィックが識別されているか？
  iii. 選択されたシグネチャに誤検知はあるか？

- シグネチャ選択を調整し、再度ログを調査します。期待された効果が得られていることをログが証明するまでに、いくつかの調整が行われる可能性があります。

  あるシグネチャが繰り返しトリガーを起こすのであれば、サーバは攻撃されているかどうかをチェックするために、より詳細に注視するべき理由があるかもしれません。

- 何日か Audit モードで動作させて、満足できる結果がログに見られたら、トリガーとなる接続が NetDefendOS によって破棄されるように、IDP を Protect モードに変更してください。しかし、誤検知によって正常なトラフィックフローが阻害されることもあり得るため、IDS シグネチャを Audit モードのままにするのが最善です。
- 必要に応じて、トリガーとなるトラフィックの送信元 IP がブロックされるように IDP のブラックリスト機能を有効にしてください。これは、BitTorrent のようなアプリケーションに対処する時に IDP の強力な機能となり、役に立ちます。

IDP データベース更新

自動的に IDP シグネチャデータベースをアップデートできます。既存のシグネチャは破棄または更新され、新しいシグネチャが導入されます。更新後の影響を観察するために、手動で強制的にデータベース更新を行うことが望ましい場合もあります。

自動更新は、ライブトラフィックの中断がないこと確認するのに必要なチェックをしないで行われる可能性があります。

7.7 しきい値ルール

概要

Threshold Rule（しきい値ルール）コンフィグレーションオブジェクトは、異常な接続動作を検知し、これに対処する手段を備えることを目的としています。こうした異常な動作を引き起こす例として、内部ホストがコンピュータウィルスに感染し、外部 IP アドレスへの接続を繰り返すことなどが挙げられます。また、外部の発信元が、膨大な数の接続を開こうとする場合もあります。（ここで「接続」とは、TCP、UDP や ICMP など、NetDefendOS のステートエンジンで追跡できるあらゆるタイプの接続を指します）。

しきい値のポリシー

しきい値ルールは、NetDefendOS で参照されるポリシーベースのルールに似ています。HTTP などのサービスと同様に送信元 / 送信先 ネットワーク / インタフェースのフィルタリング組み合わせを指定できます。各ルールは、子供として追加された 1 つ以上の Threshold Action オブジェクトを持ち、これらのアクションではトリガーとなるしきい値と、しきい値を超過した場合のアクションを指定します。

Threshold Action オブジェクトは以下の主要なプロパティを持っています。

項目	説明
Action	制限を超過した場合のルールの応答となります。Audit または Protect のいずれかを選択できます。これらのオプションについては下で詳しく説明します。
Group By	ホストベースまたはネットワークベース。これらのオプションについては下で詳しく説明します。
Threshold	アクションを始動するために超えなければならない制限数値。
Threshold Type	1 秒あたりの接続を制限するかまたは同時接続の総数を制限。 接続レート制限（Connections/Second）によって、管理者は 1 秒あたりに開かれる新しい接続の数を制限できます。 総接続数制限（Connecting）によって、管理者は開かれる総接続数を制限できます。本機能は、peer-to-peer のアプリケーションが大量の接続を必要とするため、NAT プールを使用する場合に非常に役に立つます。

グループ化設定

このプロパティに許可される 2 つのグループ化を以下に示します。

項目	説明
Host Based	異なる IP アドレスからの接続に対し、個々にしきい値が適用されます。
Network Based	ルールに一致するすべての接続をグループとしてしきい値が適用されます。

ルールアクション

しきい値ルールが始動される時、2 つの応答のうち 1 つが適用されます。

項目	説明
Audit	接続に対する処置は行いませんが、イベントのログを取得します。
Protect	ルールのトリガーとなった接続を破棄します。

適切な始動値をあらかじめ決められない場合は、ログへの出力を選択することをお勧めします。あるしきい値には「Audit」を指定し、よりしきい値が高い場合は「Protect」に指定するというように、1 つのルールに複数のアクションを指定することができます。

複数の始動アクション

ルールが始動される時、NetDefendOS は、発生した条件に一致する、ルールに関連するアクションを実行します。複数のアクションが条件に一致した場合、ユーザインタフェースで表示される順で、一致するアクションが適用されます。

「Type」と「Grouping」（用語の定義については上記を参照してください。）の組み合わせが等しい複数のアクションが同時に始動される場合は、最も高いしきい値を持つアクションだけがログに出力されます。

適用外の接続

「Before Rules」設定といういくつかの拡張設定を用いて、リモート管理に用いる一部のタイプの接続について、NetDefendOS ルールセットによる検査を免除できます。これらの設定で、接続をしきい値ルールから免除することもできます。

しきい値ルールと ZoneDefense

過剰な接続試行をする送信元を内部ホストから遮断するため、D-Link ZoneDefense 機能の中でしきい値ルールが使用されます。この機能に関する詳細は、「7.9 ZoneDefense」を参照してください。

しきい値ルールブラックリスト化

「Protect」オプションが使用される場合、しきい値ルールは、これを始動した送信元が IP アドレスまたはネットワークのブラックリストに自動的に追加されるよう設定できます。ブラックリスト化が有効にされている複数の「Protect」アクションが同時に始動される場合、最初に始動したブラックリスト化アクションだけが NetDefendOS で実行されます。

ブラックリスト化が有効にされているホストベースのアクションは、始動された時に単一のホストをブラックリスト化します。ブラックリスト化が有効にされているネットワークベースのアクションは、ルールに関連する送信元のネットワークをブラックリスト化します。しきい値ルールがサービスに関連付けられている場合、このサービスだけを遮断することができます。

ブラックリストを有効化する場合、NetDefendOS は、トリガーとなる送信元からの既存の接続を、そのままにしておくか破棄するかを選択できます。送信元がブラックリスト化される時間を秒単位で設定することもできます。

例題 7.8

しきい値ルールの作成

この例題では、wan インタフェース経由で内部 Web サーバに送信される HTTP 通信を想定します。1 つの送信元 IP アドレスから毎秒 100 を超える接続を破棄する Threshold Rule オブジェクトを作成します。インターネットからの HTTP 接続が wan インタフェースに到着するようにルールを適用します。

さらに、しきい値が超過すると、送信元 IP からのすべての HTTP トラフィックが 5 分間（300 秒）ブラックリストに載せられ、しきい値ルールが始動すると、その IP からの既存の接続の全てが破棄されます。また、送信先アドレス wan_ip を、保護された Web サーバの IP アドレスへ変換する SAT ルールも設定されているものとします。SAT ルールの定義はこの例題では記載しません。

CLI

まず、しきい値ルールを作成します。

```
DFL-xxxx:/> add ThresholdRule SourceInterface=wan SourceNetwork=all-nets DestinationInterface=core
            DestinationNetwork=wan_ip Service=http-all Name=limit_dmz
```

次に、コンテキストを新しいルールに変更して、しきい値アクションを追加します。

```
DFL-xxxx:/> cc ThresholdRule limit_dmz
DFL-xxxx:/1(limit_dmz)> add ThresholdAction Threshold=100 ThresholdUnit=Conns Action=Protect GroupBy=SourceIP
            BlackList=Yes BlackListBlockOnlyService=Yes BlackListTimeToBlock=300 BlackListIgnoreEstablished=No
```

Web Interface

まず、しきい値ルールを作成します。

1. **Threat Prevention > Threshold Rules> Add > Threshold Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: limit_dmz
   - Service: http-all
   - Source Interface: wan
   - Source Network: all_nets
   - Destination Interface: core
   - Destination Network: wan_ip

次に、しきい値アクションをルールに追加します。

3. Threshold Action タブを選択します。

4. **Add > Threshold Action** の順にメニューをクリックします。

5. 以下の情報を入力し、「OK」ボタンをクリックします。:
   - Action: Protect
   - Group by: Host based
   - Threshold: 100/Connections
   - 「BlackList」を有効にします。
   - Time to block: 300
   - 「Block only service」を有効にします。
   - 「Ignore Established」を無効にします。

6. 「OK」ボタンをクリックします。

7.8 ホストとネットワークのブラックリスト化

概要

NetDefendOS は、特定のインターネットリソースから到着するトラフィックを防御するために、ホストまたはネットワーク IPv4 アドレスのブラックリストを提供します。
ブラックリストに記載された IPv4 アドレスから通信をオープンする試みを NetDefendOS 上で受信した場合、接続は破棄されログイベントメッセージが生成されます。さらに、NetDefendOS ではホワイトリストで IPv4 アドレスを指定することでブラックリストから除外することができます。

IDP などにより自動的にブラックリストに追加されたエントリについては、ブラックリストに対して、受信した通信の送信元 IP アドレスのみがチェックされます。CLI の blacklist コマンドにより手動でエントリを追加することも可能です。これは送信先の IP アドレスをチェックします。

注意 NetDefendOS の再起動はブラックリスト / ホワイトリストに大きく影響することはありません。

ファイアウォールが再起動した場合でも、ブラックリスト及びホワイトリストの多くのコンテンツは失われません。ファイアウォールの CPU に不要な負荷がかからないように、NetDefendOS は非揮発性メモリに 2 時間毎に両方のリストをコピーします。したがって、最大で過去 2 時間の変更は失われる可能性があります。

HA（高可用性）クラスタにおける同期

HA クラスタのピア間で、NetDefendOS のブラックリストは同期されません。つまり、HA フェイルオーバー後、ブラックリストの以前の内容は利用不可となります。例外として、ブラックリストの古いエントリを追加するトリガとなった外部の IP アドレスは、継続して IDP やしきい値ルールなどの関連する機能を起動している場合、再度実行されます。

一方で、ホワイトリストでは異なる動作となります。ホワイトリストはスタティックなリストであるため、HA クラスタのデバイス間で同期が行われます。コンテンツはフェイルオーバー後にも保持されます。

ブラックリスト追加の方式

NetDefendOS のいくつかのサブシステムでは、特定の条件下でホストまたはネットワークをブラックリストに追加するオプションを備えています。ブラックリストのエントリは手動で追加または削除できます。関連するサブシステム及びブラックリストへの追加方式は以下の通りです。

- 侵入検知と防御（IDP）ルールが起動した場合に追加する。
- しきい値ルールが起動した場合に追加する。（特定の NetDefendOS モデルのみで利用可能です。詳細は「7.7 しきい値ルール」を参照してください。）
- Botnet Protection、DoS Protection、または Scanner Protection が起動した場合に追加する。
- CLI コマンド「balcklist」を使用して手動で追加する。
- REST API を使用してリモートコンピュータから追加する。この方式については「付録 I REAT API の使用方法」を参照してください。

ブラックリストエントリのデータフィールド

各ブラックリストエントリにおける重要なデータフィールドは以下の通りです。

項目	説明
Host	ブロックされる送信元 IP アドレスです。
Destination	（オプション）新しい接続が破棄されるには、送信先アドレスがこの値に一致する必要があります。
Service	エントリに追加された Service オブジェクトです。複数のエントリで同じブラックリスト IPv4 アドレスを持つことが可能ですが、それに紐づくサービスはそれぞれ異なる必要があります。この内容については別途説明します。
Port	（オプション）Service プロパティの代わりに指定して、Host アドレスの特定のポート番号への接続を破棄します。
Time to Live	この指定期間、ブラックリストにエントリが追加された状態となります。
Alert Type	エントリを作成した NetDefendOS のサブシステム、または CLI や REST API による手動追加を示します。すべての Alert Type は別紙「CLI Reference Guide」の blacklist のセクションに記載されています。
Rule Name	ブラックリストエントリに追加された、コンフィグレーションのルールオブジェクト名です。CLI や REST API によって手動で追加された場合、任意のテキスト文字列となり、オブジェクト名を表しません。

エントリには一意の IP アドレスとサービスの組み合わせが含まれる

各ブラックリストエントリには対応する Service オブジェクトのリファレンスが含まれており、それぞれのエントリで固有の IPv4 アドレス /Service の組み合わせを持っています。サービスは、エントリを作成したトリガーのルールの Service プロパティによって指定されています。

例えば、IPv4 アドレス 203.0.113.1 のブラックリストエントリとサービス http-all の組み合わせは、IPv4 アドレス 203.0.113.1 とサービス ftp-inbound の組み合わせとは異なります。これらは別々に作成され、削除されます。エントリのサービスが all_services の場合、サービスの種類にかかわらず、該当の IP アドレスから送信される通信は破棄されます。

手動でブラックリストエントリを追加する場合、サービスの代わりにポート番号を IP アドレスと一緒に指定することも可能です。

IDP ルールとしきい値ルールのブラックリストオプション

ホストまたはネットワークを自動的にブラックリストに追加する機能は、ルールがトリガされる際の Protect アクションを指定することによって IDP と Threshold Rules で有効にすることができます。有効にした場合、3 つのブラックリストのオプションがあります。

- **Time to Block Host/Network（秒）**
  トラフィックの送信元であるホストまたはネットワークは、指定した時間ブラックリストにとどまり、その後削除されます。同じ送信元が、ブラックリストに対して別のエントリを開始する場合、防御時間がそのオリジナルの値に更新されます。（つまり、累積されません。）

- **Block Only Service**
  初期値では、ブラックリストは起動するホストへのすべてのサービスを防御します。

- **Ignore Established**
  この新しいブラックリストエントリと同様の送信元を持つ確立された接続がある場合、このオプションが設定されている場合、破棄されません。

使用方法に関する詳しい内容は、「7.6.5 IDP の設定」および「7.7 しきい値ルール」を参照してください。

「blacklist」CLI コマンド

blacklist コマンドは、ブラックリストの現在の内容の参照と処理を行うために使用されます。現在のブラックリストを参照します。また、ホワイトリストの参照のみに使用することもできます。

```
DFL-xxxx:/> blacklist -show -black
```

同様に、以下のコマンドでホワイトリストの内容を参照します。

```
DFL-xxxx:/> blacklist -show -white
```

ブラックリストからホストを削除するには「-unblock」オプションを使用します。ホストを追加するには「-block」オプションを使用します。

```
DFL-xxxx:/> blacklist -block 203.0.113.1
```

「-unblock」オプションでホストを削除します。

```
DFL-xxxx:/> blacklist -unblock 203.0.113.1
```

例題 7.9

ブラックリストに IP ネットワークを追加する

この例題では、IP4 ネットワーク 203.0.113.0/24 をブラックリストに追加して、このネットワークから送信される HTTP または HTTPS 通信（サービス「http-all」に一致）が破棄されるように設定します。ブラックリストのエントリは 86,400 秒（1 日）ブラックリストに残ります。

CLI

```
DFL-xxxx:/> blacklist -block 203.0.113.0/24 -serv=http-all -time=86400
```

ブラックリストと Web インタフェース

Web インタフェースではブラックリストのエントリを追加・削除することはできませんが、エントリを閲覧することはできます。（**Status > Blacklist**）

ホワイトリスト

どのような環境下でもブラックリストに追加されないように管理ステーションなどの信頼するソースから送られてくるインターネットトラフィックを保証するために、NetDefendOS はホワイトリストも保持しています。あらゆる IP アドレスオブジェクトをこのホワイトリストに追加できます。

注意 重要な IP アドレスは、ホワイトリストに追加するべきです。

すべての管理ワークステーションの IP アドレスと同様に、ホワイトリストに D-Link ファイアウォール自身も追加することをお勧めします。それらの IP アドレスがブラックリスト追加された場合、ネットワーク制御に重大な結果を招く恐れがあります。

ホワイトリストは、ネットワークトラフィックの送信元がブラックリストに載せられることを防ぐことはできますが、送信元からの接続を破棄または拒否するしきい値ルールなどのメカニズムを防ぐことは難しいことを理解することが重要です。ホワイトリストに追加した場合、ルールのアクションで送信元がブラックリストに追加されるように設定されていても、それを回避することができます。

ホワイトリストに追加する

ホワイトリストへの追加は blacklist コマンドでは行うことができません。代わりに、特別な Whitelist host（CLI では BlacklistWhiteHost）をコンフィグレーションに追加することができます。

例題 7.10

ホストをホワイトリストに追加する

Whitelist Host という IP アドレスオブジェクトをホワイトリストに追加します。これは、この IP アドレスを決してブラックリストに載せることができないことを意味します。

CLI

```
DFL-xxxx:/> add BlacklistWhiteHost Addresses=white_ip Service=all_tcp
```

Web Interface

1. **Threat Prevention** > **Whitelist** > **Add** > **Whitelist host** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。
   - Addresses : white_ip を選択し、「Selected」リストに追加します。
   - Service : このホワイトリストエントリに関連付けるサービス all_tcp を選択します。

7.9 ZoneDefense

ZoneDefense は、スイッチを使用することでホストまたはネットワークをブロックする

ZoneDefense は、ウィルスに侵された他のコンピュータからローカルネットワークのコンピュータにウィルス感染するのを防ぐために使用される機能です。

ネットワーク上のホストまたはクライアントが、ウィルスまたは別の脅威の形式に感染した場合、外部ホストに大量の新しい接続をオープンさせることなど異常な動作により明らかになります。ZoneDefense 機能を使用することで、NetDefendOS は、そのような異常な振る舞いを検出すると、自動的にホストまたはネットワークへのアクセスをブロックするように D-Link スイッチに指示できます。

ZoneDefense 機能は、D-Link 製のスイッチを使用した場合にだけ動作します。サポートするスイッチのリストは、本セクションの後で記載されます。

ZoneDefense は SNMP を利用する

SNMP（Simple Network Management Protocol）は複雑なネットワーク管理を行うためのアプリケーション層のプロトコルです。SNMP では、ネットワーク内のマネージャと管理デバイスは、お互いに通信することを許可します。

ZoneDefense では、NetDefendOS は、スイッチの動作を制御するのに SNMP を使用します。NetDefendOS は、書き込みアクセスに設定されている SNMP Community String を使用してスイッチへの管理の権限を取得します。そして、どのようにコマンドをスイッチに送信するかを決定するために、適切な Management Information Base（MIB）ファイルを使用します。

すべての関連 MIB ファイルが既に NetDefendOS にロードされていますが、ZoneDefense を設定する場合に、NetDefendOS は、使用するべき MIB を伝える必要があります。古い D-Link スイッチについては、正確なスイッチ製品名を指定することで、これが行われます。しかし、新しい D-Link スイッチは、一般的な Universal MIB を使用するので、正確なスイッチタイプを指定する必要はありません。

しきい値ルールは ZoneDefense のトリガーとなる

しきい値ルールを設定することにより定義したしきい値を越えたホストやネットワークは、ZoneDefense 機能を使用して動的に遮断されます。しきい値は、 1 秒あたりの新しい接続数、または接続の総数に基づいて設定します。

これらの接続は特定の CIDR ネットワーク範囲のホストによるものか、すべてのホストによるものかを定義できます（IP アドレスの範囲は IP アドレスとネットワークで指定できます）。これらのルールは、「7.7 しきい値ルール」で、より詳しく記載されています。

Botnet Protection は Zone Defense のトリガーとなる

NetDefendOS の Botnet Protection は、いずれかのインタフェースで通信の送信元または送信先の IP が IP レピュテーションサブシステムによって Botnet と関連付けられているとフラグが付いた場合、ZoneDefese を起動させることができます。本機能は「7.3 Botnet Protection」で詳しく説明しています。

ACL のアップロードをブロックする

NetDefendOS が、ホストまたはネットワークが指定したしきい値に到達したのを感知すると、スイッチに ACL（Access Control List）ルールをアップロードし、通常とは異なる動作を見せるホストまたはネットワークのすべてのトラフィックをブロックします。ブロックされたホストやネットワークは、システム管理者が手動でファイアウォールの Web GUI またはコマンドラインインタフェースでブロックを解除するまで、ブロックされ続けます。

サポートする ZoneDefense スイッチ

ファイアウォールに制御されるすべてのスイッチは、NetDefendOS コンフィグレーションに手動で設定される必要があります。

スイッチを制御するために、コンフィグレーション設定に指定されるべき情報は以下の通りです。

- スイッチの管理用インタフェースの IP アドレス。
- スイッチのモデルタイプ（または、より新しいスイッチでは Universal MIB）。
- スイッチへの書き込みアクセスのための SNMP コミュニティ名。

ZoneDefense は、Universal MIB を使用するすべての新しい D-Link スイッチをサポートします。

注意 スイッチのファームウェアバージョンは最新のものとします。

ZoneDefense を使用する時、すべてのスイッチに最新のファームウェアバージョンがインストールされていることを確認することをお勧めします。

しきい値ルールの使用

しきい値ルールは ZoneDefense により、しきい値ルールに指定された接続の限界を超えた場合に、特定のホストやネットワークに対するブロックを発動させます。トリガーとなる制限は以下の 2 つのうちのいずれかとなります。

- 接続レート制限（Connections/Second）- ファイアウォールに対する 1 秒あたりの新しい接続のレートが指定のしきい値を超えた場合に発動されます。
- 接続総数による制限（Connections）- ファイアウォールとの接続総数が指定のしきい値を超えた場合に発動されます。

しきい値ルールには、IP ルール同様、設定値があります。これらの設定値でしきい値ルールを適用するトラフィックのタイプを指定します。

しきい値ルールオブジェクトには以下のようなプロパティがあります。

- 送信側インタフェースと送信側ネットワーク
- 受信側インタフェースと受信側ネットワーク
- サービス
- しきい値の種類 : ホストベースと（または）ネットワークベース

上の基準に合い、かつホストまたはネットワークにしきい値を越えさせたトラフィックにより、ZoneDefense 機能が起動されます。これにより、ホストまたはネットワークからスイッチへの接続は遮断されます。しきい値によるすべての遮断は、スイッチ上でホストまたはネットワークの IP アドレスを基準に行われます。ネットワークベースのしきい値が超過すると、攻撃しているホストだけでなくすべての発信側ネットワークが遮断されます。
しきい値ルールの設定方法と機能については、「7.7 しきい値ルール」を参照してください。

手動の遮断リストと除外リスト

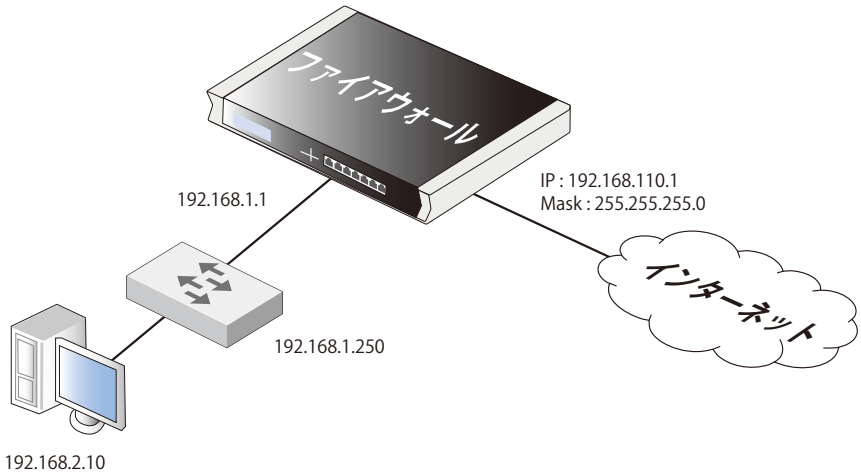
しきい値ルールに加え、手動で遮断もしくは遮断対象から除外するホストやネットワークを定義することができます。手動でのホストやネットワークの遮断は、常にまたはスケジュールで指定できます。プロトコルやプロトコルポート番号の指定による遮断も可能です。

除外リストは、しきい値ルールの制限に到達しても遮断対象から除外するホストを指定するために作成します。ZoneDefense スイッチに接続しているファイアウォールのインタフェースの IP か MAC アドレスは除外リストに加えます。これにより、ファイアウォールが遮断されるのを防ぎます。

例題 7.11

ZoneDefense の設定

この例題では、HTTP トラフィックのしきい値ルールによって起動される、スイッチ上のホストをブロックする ZoneDefense 設定を説明します。D-Link ファイアウォールのインタフェースは以下に示すとおりすべて正しく設定されているものとします。



1 秒当たり 10 接続という HTTP しきい値がトラフィックに対して適用されるものとします。接続レートが制限を超えると、NetDefendOS は、そのホストからスイッチへの接続をブロックするように指示します。（ネットワーク範囲は 192.168.2.0/24）

D-Link スイッチのモデルは DES-3226S を想定し、アドレスが 192.168.1.250 の管理用インタフェースを持ち、アドレスが 192.168.1.1 のファイアウォールのインタフェースに接続しているものとします。インタフェースは、スイッチによって偶発的にブロックされてしまうのを防止するために、除外リストに追加されます。

Web Interface

Zone Defense セクションに新しいスイッチを追加する :

1. **Threat Prevention > ZoneDefense > Switches** の順にメニューをクリックします。
2. **Add > ZoneDefense Switch** を選択します。
3. 以下のとおり情報を入力します。
   - Name: switch1
   - Switch model: DES-3226S
   - IP Address: 192.168.1.250
4. SNMP Community にスイッチに設定されている Write コミュニティ文字列を入力します。
5. ファイアウォールがスイッチと通信し、コミュニティ文字列が正しいことを確認するために「Check Switch 」をクリックします。
6. 「OK」ボタンをクリックします。

除外リストにファイアウォール管理インタフェースを追加する :

1. **Threat Prevention > ZoneDefense > Exclude List** の順にメニューをクリックします。
2. 除外リストに追加するために、「Available」リストからファイアウォールのオブジェクト名（ここでは、lan1_ip）を選択し、「Selected」リストに移動します。
3. 「OK」ボタンをクリックします。

HTTP しきい値に 10 接続 / 秒を設定する :

1. **Threat Prevention > Threshold Rules > Add > Threshold Rule** の順にメニューをクリックします。

2. Threshold Rule を入力します。
   - Name : HTTP-Threshold
   - Service : http

3. Address Filter を入力します。
   - Source Interface : ファイアウォールの管理インタフェースを指定します。（例 : management-int）
   - Destination Interface : any
   - Source Network : 192.168.10.0/24（またはオブジェクト名）
   - Destination Network : all-nets

4. 「OK」ボタンをクリックします。

しきい値、しきい値のタイプ、およびしきい値を超えた場合のアクションを指定します

1. 作成した Threshold Rule を選択し、**Add > Threshold Action** の順にクリックします。

2. Threshold Action を以下のとおり設定し、「OK」ボタンをクリックします。
   - Action: Protect
   - Group By: Host-based
   - Threshold: 10
   - しきい値の単位を「Connections/Second」に設定します。
   - 「Use ZoneDefense」をチェックします。

3. 「OK」ボタンをクリックします。

アンチウィルススキャンを使用した ZoneDefense

ZoneDefense では、NetDefendOS アンチウィルススキャン機能と共に使用することもできます。NetDefendOS は、最初に、アンチウィルススキャンを通じてウィルス発生元を特定して、次に、ZoneDefense と共に動作するように設定されたスイッチと通信することによって、その発生元をブロックします。本機能は以下の ALG を通じてアクティブ化されます。

- HTTP - ZoneDefense はウィルスの発生元である HTTP サーバをブロックすることができます。
- FTP - ZoneDefense はウィルスをアップロードしているローカルな FTP クライアントをブロックすることができます。
- SMTP - ZoneDefense はメールでウィルスを送るローカルな SMTP クライアントをブロックすることができます。

アンチウィルススキャンについては「6.4.4 ZoneDefense を使用したアンチウィルス」および個別の ALG 機能を説明したセクションに記述されています。ポリシーでアンチウイルスプロファイルオブジェクトを有効化し、ZoneDefense をアンチウイルススキャンと一緒に設定することが可能になります。

ZoneDefense の制限

スイッチの種類によって、ZoneDefense にはいくつかの違いがあります。一つ目は遮断ルールに達した瞬間から実際に遮断を開始するまでの遅延です。すべてのスイッチモデルでは、ルールが適用されてブロッキングを実行するまでわずかに遅延が生じます。1 秒未満でルールが有効になるモデルもあれば、1 分以上かかるものもあります。

二つめの違いはスイッチでサポートするルールの最大数です。あるスイッチは最大 50 のルールをサポートしますが、最大 800 のルールをサポートするものもあります。これは、ホストやネットワークをブロックするために、スイッチのポートごとにルールを設定することが必要なこともよくあるからです。この制限に到達すると、それ以降はホストやネットワークを遮断することができません。

注意 スイッチの ACL ルールセットをクリアします。

ZoneDefense はスイッチの ACL ルールセットの一部を使います。これらのルールの潜在的な衝突の可能性を防ぎ、ファイアウォールのアクセス制御を保証するには、管理者が ZoneDefense を設定する前にスイッチの ACL ルールを明確に把握することを強くお勧めします。

第 8 章 アドレス変換

この章では、NetDefendOS のアドレス変換機能について説明します。

- 「8.1 概要」
- 「8.2 NAT（ダイナミックアドレス変換）」
- 「8.3 NAT プール」
- 「8.4 SAT（スタティックアドレス変換）」
- 「8.5 自動変換」

8.1 概要

NetDefendOS には、D-Link ファイアウォールを通り抜けるパケットの IP アドレスを変換するアドレス変換機能があります。

ある IP アドレスを別のアドレスに変換する機能には多くの利点があります。重要な利点として次の 2 つがあります。:

- 保護されたホストがインターネットに接続する必要がある保護されたネットワークで、プライベート IPv4 アドレスを使用することができます。パブリックインターネットから接続可能にする必要があるプライベート IPv4 アドレスを持つサーバを設定できます。
- 保護されたネットワークのトポロジが、侵入者によって把握されることが難しくなるように、セキュリティが強化されています。アドレス変換によって内部の IP アドレスを隠すので、外部からの攻撃はさらに難しくなるわけです。

アドレス変換のタイプ

NetDefendOS はダイナミックアドレス変換（NAT）とスタティックアドレス変換（SAT）の 2 つのタイプのアドレス変換をサポートしています。両方の変換タイプに対するアプリケーションは、指定したセキュリティポリシーに依存します。つまり、サービスなど送信元 / 送信先のネットワーク / インタフェースの組み合わせを定義するフィルタリングルールに基づいて特定のトラフィックに適用されます。

ここでは、「NAT」と「SAT」ルールの設定について例題をあげて説明します。

8.2 NAT（ダイナミックアドレス変換）

ダイナミックアドレス変換（NAT: Dynamic Network Address Translation。以下、NAT と言う）は、オリジナルの送信元 IP アドレスを異なるアドレスに変換する方法を提供します。この機能によって、外向きパケットが異なる IP アドレスから送信されているように見え、そのアドレスに戻る内向きパケットはアドレスが元の IP アドレスに変換して戻されます。

NetDefendOS で NAT を設定する方式

NetDefendOS の IP ルールセットで NAT を設定す方式は以下の 2 通りあります。

• IP ポリシーを使用する

IP Policy オブジェクトを IP ルールセットに追加して、その Source Address Translation プロパティを NAT に指定します。これは NAT を設定する推奨方法であり、同じ IP ルールセットのエントリで他のセキュリティメカニズムを追加することを簡単にします。

IP ポリシーの Source Address Translation を NAT に指定する代わりに、初期値の Auto に設定することもできます。Auto に指定した場合、送信元 IP アドレスがプライベート IP アドレスかつ送信元の IP アドレスがパブリック IP アドレスであった場合に、自動的に NAT 変換が行われます。このセクションでは Auto オプションについて詳しく述べませんが、「8.5 自動変換」で説明しています。

• IP ルールを使用する

IP Rule オブジェクトを IP ルールセットに追加して、その Action プロパティを NAT に指定します。古い NetDefendOS バージョンとの互換性を保つ場合にはこの方式が有効ですが、IP ポリシーを使用する場合と比べて利点はありません。

これら両方の方式の例題は、本セクション内で説明します。

NAT の利点

NAT には次の重要な利点があります。

- 各クライアントの IP アドレスとホストをファイアウォールの IP アドレスに隠すことができます。
- パブリックインターネットに接続するためのパブリック IPv4 アドレスが必要なのは、ファイアウォールだけです。ホストおよびネットワークは、ファイアウォールの背後でプライベート IPv4 アドレスの割り当てを行うことができますが、同時にパブリック IPv4 アドレスを使用してパブリックインターネットに接続することも可能です。
- NAT を使用すると、利用可能なパブリック IPv4 アドレスが少ないインターネット環境で、1 つの IPv4 アドレスでマルチプレックスによる複数の接続を提供します。これは、エンタープライズレベルで重要となるほか、Carrier Grade NAT (CG-NAT) を有効化するために 2 レベルの NAT が使用される ISP レベルにおいても有用です。

NAT の「多対 1」IP アドレス変換

NAT は「多対 1」変換を提供しています。これは、NAT を行う各 IP ルールセットのエントリは、いくつかの送信元 IP アドレスを一つの送信元 IP アドレスに変換することを意味します。

セッション状況の情報を維持するためには、ダイナミックに変換されたアドレスからの各接続は、送信者として固有のポート番号と IP アドレスの組み合わせを使用する必要があります。そのため、NetDefendOS は IP アドレスと同様に送信元ポート番号の自動変換を行います。つまり、接続するための送信元 IP アドレスはすべて同じ IP アドレスに変換されるので、各接続に固有のポート番号を割り当てることによって個々の接続を区別します。

以下の図は NAT の概要を示しています。

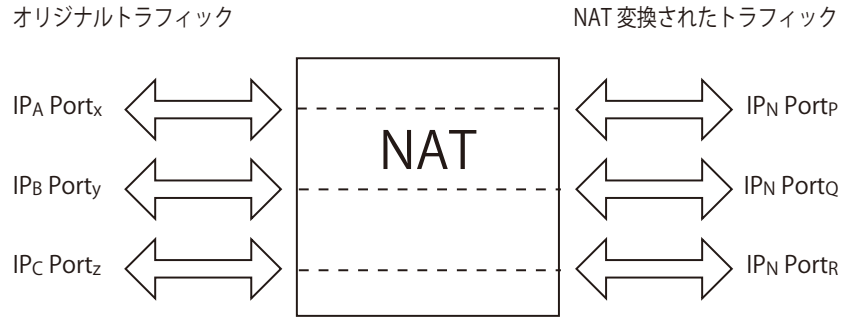


図 8-1　NAT IP アドレス変換

上の図では、IP アドレス A、B、および C からの 3 つの接続が 1 つの送信元 IP アドレス N を経由して NAT 変換されています。元のポート番号も変換されています。

新しい NAT 接続のために割り当てられる次のソースポート番号は、NetDefendOS がランダムに選択した最初のフリーなポートです。セキュリティを向上するためにポートをランダムに割り当てます。

NAT 接続数の制限

接続がユニークな IP アドレスのペアであり、別々のポート番号が使用されていないか、または同じ送信先ポートが使用されている場合、約 64,500 個の NAT 接続が同時に可能です。

しかし、送信元および送信先ポートはそれぞれ想定され得る範囲が 64,400 であるため、すべてのポートを使用すると、2 つの IP アドレス間には 40 億以上の接続を持つことが理論的には可能です。

NAT プールを使用すると、接続をさらに増やすことができる

D-Link ファイアウォールと特定の外部ホスト IP の間に存在できる NAT 接続の数を増やすために、（ファイアウォールで自動的に追加 IP アドレスを利用できる）NetDefendOS NAT プール機能を使用できます。

これはリモートサーバが、すべての接続を単一のポート番号に対して行う必要がある場合に役立ちます。そのような場合、ユニークな IP アドレスのペアに 64,500 の制限が適用されます。

詳しくは、「8.3 NAT プール」を参照してください。

変換に使用する送信元 IP アドレス

NetDefendOS が NAT 変換に使用する送信元 IP アドレスを決定する際、以下の 3 つのオプションがあります。:

項目	説明
インタフェース用 IP アドレスの使用	新しい接続が確立すると、その接続のアウトバウンドインタフェースを解決するためにルーティングテーブルを参照します。解決されたインタフェースの IP アドレスは、その後 NetDefendOS がアドレス変換を実行する場合に、新しい送信元 IP アドレスとして使用されます。これが IP アドレスを決定するデフォルトの方法です。
特定 IP アドレスの指定	特定の IP アドレスを新しい送信元 IP アドレスとして指定します。指定された IP アドレスには、アウトバウンドインタフェースと一致する ARP パブリッシュエントリを設定する必要があります。そうでない場合、リターントラフィックを D-Link ファイアウォールは受信することができません。このテクニックは、トラフィックの送信元に応じて送信元 IP を異なるものにする場合に使用することができます。例えば、NAT を使用しているインターネットサービスプロバイダで、異なる顧客には異なる IP アドレスを使用するということが可能になります。
NAT プールの IP アドレスの使用	管理者が定義する「NAT Pool」という IP アドレスセットを使用することができます。「NAT Pool」で次に利用可能なアドレスを、NAT に使用する IP アドレスとして使用することが可能です。1 つ以上の NAT プールを設定することが可能であり、1 つのプールを複数の NAT ルールで使用することもできます。詳しくは「8.3 NAT プール」を参照してください。

NAT 変換のプロセス

単純な例で NAT 処理を説明するために、プライベート IP アドレス 192.168.1.5 が設定された、ファイアウォール配下の保護されたクライアントを想定します。パブリック IP アドレス 203.0.113.10 のサーバ上のポート 80 で HTTP 通信ができるようにします。

インターネットに接続する NetDefendOS のイーサネットインタフェースのパブリック IP は、203.0.113.5 です（つまり、このインタフェースとサーバは同じネットワーク上に存在します）。クライアントからサーバへの通信を許可する NAT 変換の IP ルールセットエントリを設定することにより、このインタフェースから送信される通信に NAT 変換が適用されます。

NAT 処理で発生するイベントについて以下に説明しています。

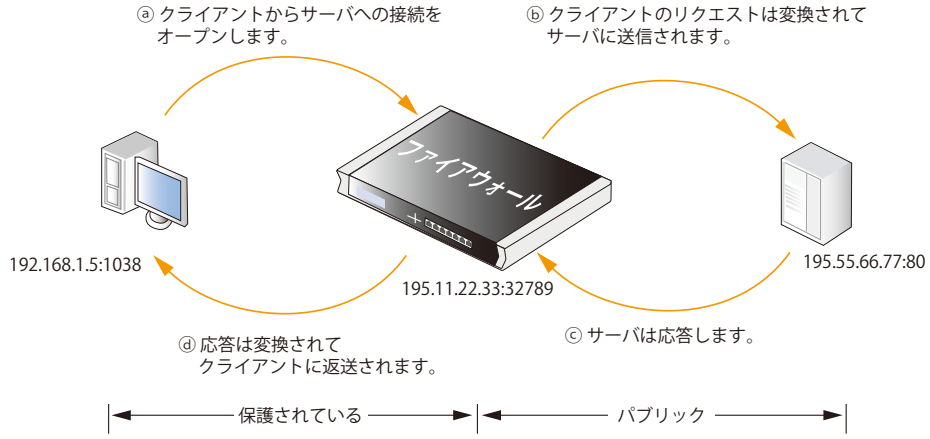


図 8-2　NAT の例

1. 送信元（192.168.1.5）は、ダイナミックに割り当てられたポート（例 : ポート 1038）からサーバ（例 : 203.0.113.10、ポート 80）にパケットを送信します。
   192.168.1.5:1038 => 203.0.113.10:80

2. IP ポリシーの NAT で Outgoing Interface IP オプションが使用されることを想定します。NetDefendOS によって送信元ポートがそのインタフェース上のランダムな未使用ポートに変更されます（ポート 1024 より上の番号）。ここでは、ポート 32789 を選択するものとします。パケットはその後インターフェースのこの送信元ポートと送信元 IP を持つ送信先 IP に送信されます。
   203.0.113.5:32789 => 203.0.113.10:80

3. その後受信サーバがパケットを処理し、送信元 IP/ ポートにレスポンスを送信します。
   203.0.113.10:80 => 203.0.113.5:32789

4. NetDefendOS はパケットを受信し、オープンな接続のリスト内の送信先 IP ポートについてパケットを照合します。接続を検出すると、元の送信元 IP アドレスとポートをリストアし、パケットを転送します。
   203.0.113.5:32789 => 192.168.1.5:1038

5. 元の送信者は自身パブリック IP アドレスを使用することなく、レスポンスを受信します。

例題 8.1

IP ポリシーを使用して NAT を設定する

wan インタフェースのパブリックインターネットに送信されるように、内部ネットワーク lan から生成されるすべての HTTP トラフィックにアドレス変換を実行する NAT IP ポリシーを追加します。wan インタフェースの IP アドレスはすべての接続に対して NAT を行うアドレスとして使用されます。

CLI

```
DFL-xxxx:/> add IPPolicy Name=nat_http SourceInterface=lan SourceNetwork=lannet DestinationInterface=wan
            DestinationNetwork=all-nets Service=http-all Action=Allow SourceAddressTranslation=NAT NATSourceAd
            dressAction=OutgoingInterfaceIP
```

初期値でインタフェースアドレスを使用するため、NATSourceAddressAction オプションを省くことができます。代わりに、特定のアドレスを使用する SingleIP や NATPool を指定することもできます。また、送信側アドレスが、明示的にインタフェースに ARP パブリッシュされる必要があります。

Web Interface

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。
2. 適切なルール名を入力します。例 : nat-http
3. 以下の情報を入力します。
   - Action: Allow
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: wan
   - Destination Network: all-nets
   - Service: http-all
4. SOURCE TRANSLATION で以下の指定を行います。
   - Address Translation: NAT
   - Address Action: Outgoing Interface IP
5. 「OK」ボタンをクリックします。

ログ機能は初期値で有効です。

例題 8.2

IP ルールを使用して NAT を設定する

この例題は、「例題 8.1 IP ポリシーで NAT を設定する」と基本的には同じ設定ですが、IP ルールオブジェクトを使用する点が異なっています。IP Policy ではより多くのオプションが直接設定できるため、IP Policy を使用することが推奨されます。

CLI

```
DFL-xxxx:/> add IPRule Action=NAT SourceInterface=lan SourceNetwork=lannet DestinationInterface=wan
            DestinationNetwork=all-nets Service=http-all NATAction=UseInterfaceAddress Name=NAT_HTTP
```

初期値ではインタフェースアドレスを使用するため、NAT Action オプションを省略することができます。代わりに、SpecifySenderAddress オプションを指定し、NATSenderAddress オプションを使用して、IP アドレスを指定できます。明示的に送信者のアドレスをインタフェース上に ARP パブリッシュする必要があります。

Web Interface

1. **Policies > Firewalling >Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 適切なルール名を入力します。例 : NAT_HTTP
3. 以下の情報を入力します。
   - Action: NAT
   - Service: http-all
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: wan
   - Destination Network: all-nets
4. NAT action で、Use Interface Address オプションが選択されているのを確認します。
5. 「OK」ボタンをクリックします。

ログ機能は初期値で有効です。

NAT が扱うプロトコル

NAT は、アルゴリズムにより TCP、UDP および ICMP がそれぞれ固有となるように値を調整するため、適した機能レベルでそれらのプロトコルを処理することができます。他の IP レベルのプロトコルについては、固有の接続は送信者のアドレス、送信先アドレスとプロトコル番号によって識別されます。

これは以下の通り識別することを意味します。

- 一つの内部のマシンは、同じ IP プロトコルを使用して多くの外部サーバと通信できます。
- 一つの内部のマシンは、異なる IP プロトコルを使用して多くの外部サーバと通信できます。
- 複数の内部のマシンは、同じ IP プロトコルを使用して異なる外部サーバと通信できます。
- 複数の内部のマシンは、異なる IP プロトコルを使用して同じサーバと通信できます。
- 複数の内部のマシンは、同じ IP プロトコルを使用して同じ外部サーバと**通信できません**。

注意 制限は IP レベルプロトコルにのみ適用されます

これらの制限は、TCP、UDP および ICMP 以外の IP レベルプロトコル（例 :OSPF、L2TP）にだけ適用されます。telnet、FTP、HTTP、SMTP などの TCP、UDP および ICMP によって変換されるプロトコルには適用されません。NetDefendOS は、通信が同じ IP に変換された送信元アドレスを持っていたとしても、各接続を固有にするために、TCP と UDP 内のポート番号情報を変更することができます。

使用される送信方法にかかわらず、アドレス変換中に問題が発生するプロトコルもあります。

NAT によるインターネットトラフィックの匿名化

NetDefendOS の NAT 機能で役に立つ利用法の 1 つは、匿名サービスプロバイダ向けに、パブリックインターネットを経由するクライアントとサーバ間のトラフィックを匿名化することです。そうすることで、クライアントのパブリック IP アドレスはサーバへの接続要求時やピアツーピアトラフィックに表示されないようになります。

ここでは、D-Link ファイアウォールが PPTP サーバとして機能し、PPTP クライアントのための PPTP トンネルを遮断する典型的なケースを検討します。匿名を希望するクライアントは、PPTP を使用しているローカルの ISP を使用して通信します。トラフィックは、匿名化を行うサービスプロバイダに直接接続しますが、そこではファイアウォールがインストールされクライアントに対し PPTP サーバとして機能しており、PPTP トンネルを遮断しています。以下の図はこの仕組みについて説明しています。

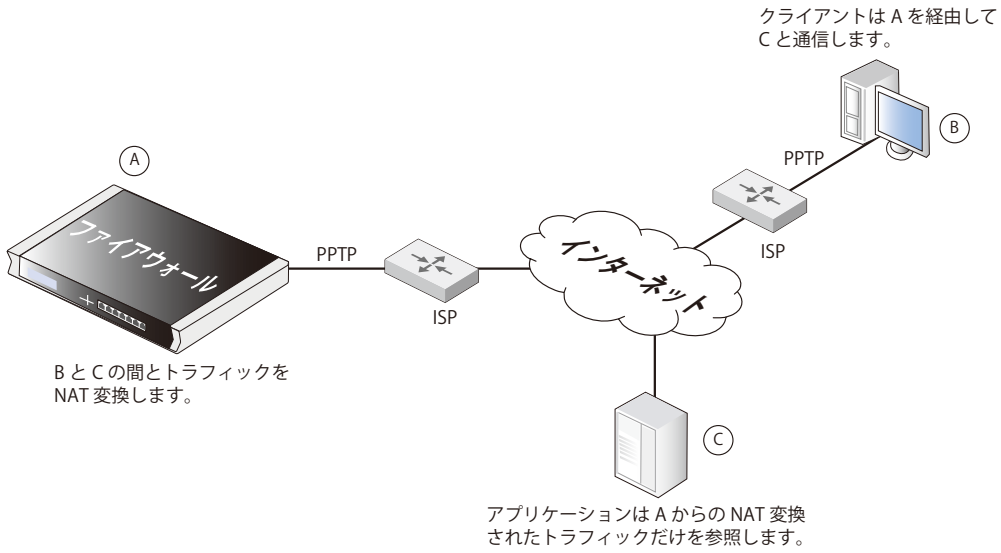


図 8-3　NAT による匿名化

NetDefendOS は IP ルールセットの中の「NAT」ルールを使用して設定されているので、クライアントから送信されてくる通信トラフィックを受け取り、NAT がインターネットに送り返します。クライアントとの通信は、PPTP プロトコルで行いますが、クライアントからの PPTP トンネルはファイアウォールで遮断されます。このトラフィックがファイアウォールとインターネットの間でリレーされる時には、PPTP によるカプセル化は行われていない状態になります。

Web サーバのようなアプリケーションがクライアントから要求を受信した場合、それは、クライアントの IP からではなく、あたかも匿名化を行うサービスプロバイダの外部 IP アドレスから送信されたかのように見えます。そこで、アプリケーションはレスポンスをファイアウォールに送り返し、ファイアウォールが PPTP トンネルを経由してそのトラフィックをリレーしてクライアントに戻します。クライアントのオリジナルの IP アドレスは、NetDefendOS で PPTP トンネルの遮断の後にリレーされるので、トラフィック内では明らかにされません。

通常、すべてのトラフィックは、ただ 1 つのパブリック IPv4 アドレスしか持たない同じ物理インタフェースを通過します。複数のパブリック IP アドレスが利用可能な場合は、複数のインタフェースを使用することができます。トラフィックの匿名化には、明らかにわずかな処理の付加が伴いますが、匿名化を行うのに十分なハードウェアリソースが使用されるのであれば、大した問題にはなりません。

また、PPTP 接続の代わりに L2TP を使用する場合にも同様のテクニックを使用することができます。これらプロトコルに関する詳細は、「10.4.4 PPTP/L2TP クライアント」を参照してください。

8.3 NAT プール

概要

「8.2 NAT（ダイナミックアドレス変換）」で述べた通り、NAT は、一意のプライベートな内部 IP アドレスを持つ複数の内部クライアントとホストを、1 つの外部パブリック IPv4 アドレスを介してリモートホストと通信させる方法です。複数のパブリック外部 IP アドレスが利用できる時、「NAT プール」オブジェクトを用いて、これらのパブリック IPv4 アドレスを介する新しい接続を割り当てることができます。

単一ポートで非常に多くの接続が必要となるケースにおいて、一般的に NAT プールが使用されます。NetDefendOS Port Manager では、送信元と送信先 IP アドレスの 1 つの組み合わせについて、接続数を約 65,000 までに制限しています。多数の内部クライアントが、ファイル共有ソフトウェアなどのアプリケーションを使用している場合、膨大な数のポートが各クライアントに必要となります。多数のクライアントがプロキシサーバを介してインターネットにアクセスしている場合も同様です。ポート数の制約は、インターネットアクセス用の外部 IP アドレスを余分に割り当て、NAT プールを用いてこれらを介する新しい接続を割り当てることによって解決できます。

NAT プールの種類

NAT プールは、3 つのタイプの中からいずれかを使用でき、それぞれ異なる方法で新しい接続を割り当てます。

- ステートフル
- ステートレス
- 固定

これら 3 つのタイプについて、以下に説明します。

ステートフル NAT プール

「Stateful」オプションを選択すると、NetDefendOS は、最近ルートされた接続数が最も少なく、最もロードが少ないと思われる外部 IP アドレスに新しい接続を割り当てます。NetDefendOS は、こうした接続すべての記録をメモリに保持します。同じ内部クライアントホストを含む接続が後に続く場合は、同じ外部 IP アドレスを使用します。

ステートフルの利点は、複数の外部 ISP リンクを介する接続間でバランスを取れることです。また、外部ホストが必ず同じ IP アドレスに通信し返すことは、HTTP などのプロトコルにおいてクッキーが含まれる時には不可欠です。欠点は、NetDefendOS がステートテーブルで使用状況を追跡することと新しい接続の処理にかかるわずかな処理オーバヘッドにより、余分なメモリが必要になることです。

アクティブではなくなった無通信のエントリがステートテーブルに含まれないようにするには、「State Keepalive」時間を設定します。非アクティブ状態がこの秒数続いた後、ステートテーブルからステートが消去されます。この期間の後、NetDefendOS は、関連する内部ホストから通信がこれ以上発生しないと推定します。ステートが消去された後に、そのホストから通信が続くと、新しいステートがテーブルにエントリされ、異なる外部 IP アドレスが NAT プールから割り当てられます。

ステートテーブル自体がメモリを消費するため、「NAT プール」オブジェクトの「Max States」値を用いてテーブルのサイズを制限できます。ステートテーブルは、すぐにすべてが割り当てられるわけではありませんが、必要に応じてサイズが増加されます。ステートテーブルの 1 つのエントリは、D-LInk ファイアウォール背後の 1 つのホストについて、接続が外部ホストに関わるか否かに関わらず、すべての接続を追跡します。「Max States」に達すると、最も空き時間の長い既存ステートが置き換えられます。テーブル内のすべてのステートがアクティブである場合、ランダムなエントリが置き換えられます。最大値に達したことを示す max_states_reached ログメッセージが生成されます。概算として、「Max States」値は、プールを使用して接続すると想定されるローカルのホスト数またはクライアント数以上に設定する必要があります。

ステートレス NAT プール

「Stateless」オプションでは、ステートテーブルは保持されず、既に割り当てられていて最も接続の少ない外部 IP アドレスが新しい接続にそれぞれ選択されます。この場合、1 つの内部ホストが、2 つの異なる外部 IP アドレスを用いて、同じ外部ホストに対する接続を 2 つ持つ可能性があります。

ステートレス NAT プールの利点は、メモリをステートレステーブルに割り当てなくとも、外部 IP アドレス間に新しい接続を効果的に広げられることと、新しい接続をそれぞれ確立する際に要する処理時間が少ないことです。欠点は、一定の外部 IP アドレスが必要な通信には向かないことです。

固定 NAT プール

「Fixed」オプションでは、各内部クライアントまたはホストに、外部 IP アドレスの 1 つがハッシュアルゴリズムで割り当てられます。管理者は使用される外部接続を制御しませんが、この方式では、特定の内部クライアントまたはホストは必ず同じ外部 IP アドレスを介して通信します。

「Fixed」オプションは、ステートテーブルに用いるメモリを必要とせず、新しい接続を非常に速く確立できるという利点があります。このオプションでロードバランシングは明示的に含まれていませんが、割り当てアルゴリズムのランダムな性質により、外部接続の負荷分散は行われます。

IP プールの使用

外部 IP アドレスを NAT プールに割り当てる時、これらを明示的に指定する必要はありません。代わりに、NetDefendOS「IP Pool」オブジェクトを選択できます。IP プールは、DHCP を通して自動的に IP アドレスをまとめて収集し、外部 IP アドレスを NAT プールに自動的に提供することができます。このトピックの詳細については、「5.5 IP プール」を参照してください。

プロキシ ARP の使用

外部ルータが、NAT プールに含まれる外部 IP アドレスを解決するよう、D-Link ファイアウォールに ARP クエリを送信した場合、NetDefendOS は、これをプロキシ ARP メカニズムで解決する正しい ARP 応答を送信するため、外部ルータは正しくルーティングテーブルを構築できます。

デフォルトでは、管理者は NAT プールで使用されるインタフェースの「NAT プール」設定の中で指定する必要があります。すべてのインタフェースに対して NAT プールのプロキシ ARP を有効にするオプションがありますが、パケットが到着すべきではないインタフェースに向けた経路を作成してしまう可能性があることから、問題が発生するおそれがあります。従って、NAT プールプロキシ ARP メカニズムに使用するインタフェースを明示的に指定することをお勧めします。

NAT プールを使用する

NAT プールは、通常の NAT IP ルールとともに使用されます。NAT ルールを定義する時、ルールで使用する NAT プールを選択するオプションが用意されています。この連携によって、NAT プールが使用できるようになります。

例題 8.3

NAT プールを使用する

この例題は、外部 IP アドレス範囲 10.6.13.10-10.16.13.15 に適用されるステートフルな NAT プールを作成します。これは、lan_net から wan インタフェースに来る HTTP トラフィックの用の NAT IP ルールで使用されます。

10.6.13.0/24 などのネットワークが NAT プールの IP 範囲に使用されると、0 と 255 のアドレス (10.6.13.0 と 10.6.13.255) が自動的に範囲から除外されることにご注意ください。

CLI

A. はじめに、アドレス帳に対象アドレス範囲のオブジェクトを作成します。

```
DFL-xxxx:/> add Address IP4Address nat_pool_range Address=10.6.13.10-10.16.13.15
```

B. 次に my_stateful_natpool と呼ばれるステートフル NAT Pool オブジェクトを作成します。

```
DFL-xxxx:/> add NatPool my_stateful_natpool IPRange=nat_pool_range Type=Stateful ProxyARPInterfaces=wan
```

C. 最後に、IP ルールセットに NAT ルールを定義します。:

```
DFL-xxxx:/> add IPRule Action=NAT SourceInterface=lan SourceNetwork=lannet DestinationInterface=wan
            DestinationNetwork=all-nets Service=http-all NATAction=UseNATPool NATPool=my_stateful_natpool
            Name=NAT_HTTP
```

Web Interface

A. はじめに、アドレス帳に対象アドレス範囲のオブジェクトを作成します。

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。
2. Name に適切な名前を指定します。例：nat_pool_range
3. Address テキストボックスに「10.6.13.10-10.16.13.15」を入力します。
4. 「OK」ボタンをクリックします。

B. 次に my_stateful_natpool と呼ばれるステートフル NAT Pool オブジェクトを作成します。

1. **Objects > NAT Pools > Add > NAT Pool** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_stateful_natpool
   - Pool type: stateful
   - IP Range: nat_pool_range
3. Proxy ARP タブを選択し、WAN インタフェースを追加します。
4. 「OK」ボタンをクリックします。

C. 最後に、IP ルールセットに NAT ルールを定義します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 「General」の下を入力します。
   - Name: nat_pool_rule などの適切な名前を入力します。
   - Action: NAT

3. 「Address Filter」の項目を入力します。
   - Source Interface: lan
   - Source Network: lan-net
   - Destination Interface: wan
   - Destination Network: all-nets
   - Service: http-all

4. 「Network Address Translation」の項目を入力します。:
   - 「Use NAT Pool」オプションを選択します。
   - プルダウンメニューから my_stateful_natpool を選択します。

5. 「OK」ボタンをクリックします。

8.4 SAT（スタティックアドレス変換）

8.4.1 はじめに

NetDefendOS の Static Address Translation（SAT）機能は、IP アドレス、そして / またはポート番号の範囲を他の定義済みのスタティックな値に変換できます。変換は 1 つのアドレスおよび / またはポートに行われますが、範囲内の各アドレスおよび / またはポート、またはネットワークが新しい範囲やネットワーク内の対応する値にマップされるように置き換えることもできます。

注意 SAT はポートフォワーディングと同じです

ネットワーク機器ベンダの中には、「SAT」に言及する場合、「port forwarding」という用語を使用するところもあります。どちらの用語も同じ機能を示しています。

NetDefendOS で SAT を設定する方式

NetDefendOS の IP ルールセットで SAT を設定する方式は以下の 2 通りあります。

- **IP ポリシーを使用する**

IP Policy オブジェクトを IP ルールセットに追加して、その Destination Address Translation プロパティを SAT に指定します。これは SAT を設定する推奨方法であり、同じ IP ルールセットのエントリで他のセキュリティメカニズムを追加することを簡単にします。

- **IP ルールを使用する**

IP Rule オブジェクトを IP ルールセットに追加して、その Action プロパティを SAT に指定します。古い NetDefendOS バージョンとの互換性を保つ場合にはこの方式が有効ですが、IP ポリシーを使用する場合と比べて利点はありません。

本セクションにおける多くの説明や例題は、SAT を設定するために P ポリシーが使用されることを想定しています。IP ルールを使用した SAT の設定については「8.4.9 IP ルールを使用した SAT ルールの設定」で説明しています。

SAT 変換のタイプ

SAT 変換は一般的に以下の 3 つのタイプに分けられます。

- **One-to-one** - 1 つの IP アドレスが 1 つの新しいアドレスに変換されます。
- **Many-to-one** - 複数の IP アドレスが複数の新しいアドレスに置き換えられます。
- **Many-to-one** - 複数の IP アドレスが 1 つのの新しいアドレスに変化されます。

変換される値は、NetDefendOS が設定した新しい接続のソースまたは宛先のいずれかの IP アドレスおよび / またはポート番号であるかもしれません。後述の通り、many-to-one 変換はポート番号には利用できません。

IP アドレスマッピングのタイプを指定する

NetDefendOS は以下のルールを使用して SAT IP アドレスマッピングのタイプを認識します。

- **One-to-One**
  オリジナルのアドレスが 1 つの IP アドレスであれば、one-to-one マッピングが常に実行されます。新しい IP アドレスも 1 つのアドレスであるべきです。これは SAT の最も一般的な用法です。詳細は「8.4.2 One-to-One IP 変換」さらに詳しく説明します。

- **Many-to-Many**
  オリジナルのアドレスが IP 範囲またはネットワークの場合、変換プロパティが有効である場合、常に many-to-many マッピングが実行されます。
  many-to-many マッピングを使用すると、1 つの新しい IP アドレスが指定され、マッピングはそのアドレスから開始して増加するように行われます。全体のネットワークを別のネットワークに変換する場合は、新しい IP アドレスは新しいネットワークの最初のアドレスであるべきです。
  例 :192.168.1.0

- **Many-to-One**
  Many-to-One マッピングが実行されると、元の送信元 IP アドレスは IP 範囲またはネットワークとなり、新しい送信先 IP アドレスは単一の IP アドレスになります。Transposotion は有効にすべきではありません。
  送信元アドレスが all-nets である場合、Many-to-One の SAT マッピングが常に使用されます。
  この変換タイプは「8.4.4 Many-to-One IP 変換」でさらに詳しく説明します。

SAT に IP ポリシーを使用する

SAT IP ポリシーを作成する場合、送信元および送信先の変換を指定することができます。アドレスの変換方式は以下のオプションの両方またはいずれか指定します。

- **Address Action**
  これは、IP アドレスが変換される方法を決定します。以下のいずれかに指定します。
  i. Single IP - 1 つのオリジナルの IP または範囲 / ネットワークのどちらかが、指定した 1 つの新しいアドレスに変換されます。これは 1 対 1 または多対 1 の IP 変換をもたらします。
  ii. Transposed - これは、変換用のベースアドレスとして指定の新しい IP アドレスを使用して、オリジナルの範囲 / ネットワーク内の各アドレスが新しい範囲 / ネットワークに変換される many-to-many 変換をもたらします。

- **Port Action**
  これは、IP アドレスが変換される方法を決定します。以下のいずれかに指定します。
  i. None - ポート変換は行われません。
  ii. Single Port - これは指定した新しいポートへの 1 対 1 変換に使用されます。
  iii. Transposed - これは、変換のベースポート番号を使用して、ポート番号の範囲を新しい範囲に置き換えます。これは many-to-many 変換のためのものです。

  ポート変換の詳細については「8.4.7 ポート変換」で説明します。

自動設定を使用した送信元変換

IP ポリシーの送信元変換プロパティの初期値は Auto です。
このセクションの例では、送信元変換が None または Transpose に設定されているため、実行されているアクションが明確になります。
送信元変換の自動設定については、「8.5 自動変換」で説明します。

8.4.2 One-to-One IP 変換

SAT の最も簡単な形は、1 つの IP アドレスを別の 1 つの固定 IP アドレスにする変換です。最も一般的なシナリオでは、外部ユーザがプライベート IP アドレスを持ち、DMZ に位置する保護されたサーバへの接続を行うことです。これは、仮想 IP または仮想サーバの実装とも言います。また、よく DMZ と共に使用されます。

DMZ の役割

SAT ルールはしばしば DMZ アクセスを許可するために使用されるため、現時点では Demilitarized Zone (DMZ) として知られるネットワークの役割について論じる意味があります。

DMZ の目的は、外部の信頼されていないクライアントからアクセス可能なリソースを置くネットワークを持つことであり、通常このアクセスはパブリックインターネットをまたいで行われます。DMZ 内のサーバは外的脅威に大きくさらされるため、秘密が漏洩する大きなリスクを持っています。

DMZ に位置するこれらのサーバを隔離することによって、より機密なローカルな内部ネットワークとは分けられます。これにより、NetDefendOS は DMZ と内部ネットワーク間を流れるトラフィックを制御して、DMZ サーバで起こるどんなセキュリティ違反からも隔離することができます。

注意 DMZ ポートはどのポートでも可能です。

D-Link NetDefend ハードウェアのいくつかのモデルには、DMZ ネットワーク用として示されている特定のイーサネットインタフェースがあります。これを他の目的に使用し、他のイーサネットインタフェースを DMZ の代わりに使用することもできます。

例題 8.4

IP ポリシーを使用した One-to-One IP 変換

この例題では、インターネットから DMZ 内への HTTP および HTTPS 通信について、変換及び許可するために SAT を使用します。ファイアウォールは、IP アドレスとしてアドレスオブジェクト wan_ip を持つ wan インタフェースを経由してインターネットに接続します。Web サーバは、IPv4 アドレス 10.0.0.5 を持ち、dmz インタフェース経由で到達可能です。このポート番号は変換されません。

CLI

SAT IP ポリシーを作成します。

```
DFL-xxxx:/> add IPPolicy Name=sat_http_to_dmz SourceInterface=wan SourceNetwork=all-nets
            DestinationInterface=core DestinationNetwork=wan_ip Service=http-all Action=Allow
            SourceAddressTranslation=None DestAddressTranslation=SAT DestAddressAction=SingleIP Dest-
            NewIP=10.0.0.5
```

Web Interface

SAT IP ポリシーを作成します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name : sat_http_to_dmz
   - Action : ALLOW
3. FILTER セクションで以下の情報を入力します。
   - Source Interface:any
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip
   - Service : http-all
4. SOURCE TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: None
5. DESTINATION TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Single IP
   - New IP Address: 10.0.0.5
6. 「OK」をクリックします。

SAT IP ポリシーを内部クライアントに適用する

この上の例題によって、ルールセット main に以下の 2 つのルールセットが追加されます。

#	アクション	送信元 インタフェース	送信元 ネットワーク	送信先 インタフェース	送信先 ネットワーク	サービス	SAT アクション
1	Allow/SAT	wan	all-nets	core	wan_ip	http-all	Destination IP: 10.0.0.5

インタフェースの IP が通常 core に送信されるため、SAT ルールの送信先インタフェースは、core（NetDefendOS 自身）である必要があります。
以下の図で示されるシナリオのように、DMZ の Web サーバにアクセス可能な lan_net 上内部クライアントを想定します。

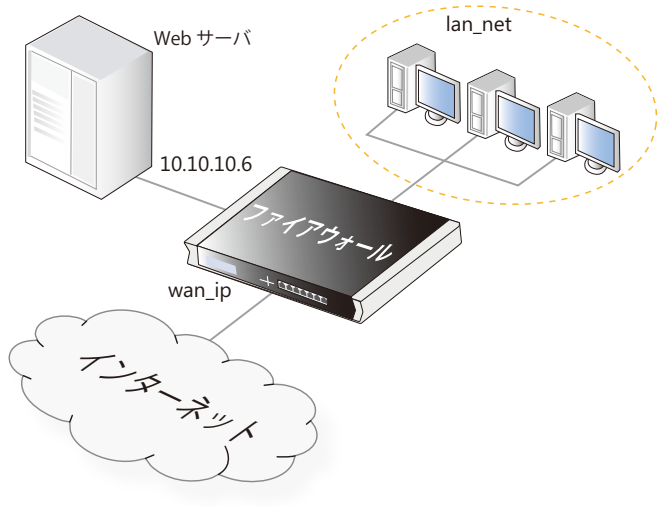


図 8-4　SAT アドレス変換

内部のクライアントがインターネットへのアクセスを必要とする場合 NAT IP ルールセットのエントリも必要となります。しかし、SAT IP ポリシーのソースインタフェースには lan インタフェースが含まれないため、Web サーバへのアクセスが許可されません。この問題に対しては、以下のいずれかの設定で対応することができます。

・ ソースインタフェースの値を変更する

SAT IP ルールの Souce Interface の値を All に設定します。IP ルールセットのエントリは以下のようになります。

#	アクション	送信元 インタフェース	送信元 ネットワーク	送信先 インタフェース	送信先 ネットワーク	サービス	SAT アクション
1	Allow/SAT	any	all-nets	core	wan_ip	http-all	Destination IP:10.0.0.5
2	Allow/NAT	lan	lan-net	any	all-nets	http-all	

・ インタフェースグループを使用する

wan および lan インタフェースが含まれる Intaface Group を作成し、これを Source Interface プロパティに割り当てます。限定的な指定方法であり、セキュリティの観点でより推奨されるソリューションです。

・ IP ポリシーの自動変換機能を使用する

最もシンプルなソリューションとして、IP ポリシーの自動変換機能を使用することができます。この機能については「8.5 自動変換」を参照してください。「IP ポリシーを使用した自動 SAT/NAT 変換」で説明する通り、内部クライアントに対して必要となる SAT 変換と NAT 変換の両方を実行する単一の IP ポリシーを作成することができます。

Web サーバがクライアントと同じネットワークにある場合は、アプローチが必要です。これについては「8.4.6 NAT を使用した SAT」で説明されます。

8.4.3 Many-to-Many IP 変換

1 つの SAT ルールは、IP アドレスの範囲全部とネットワークを別の範囲またはネットワークに変換するために使用されます。これは、最初のオリジナルの IP アドレスが新しい範囲またはネットワークにおける最初の IP アドレスに変換され、次に 2 番から 2 番目というように変換される many-to-many 変換です。

このタイプの変換を実行するように NetDefendOS に伝えるために、オリジナルの IP アドレスが範囲またはネットワークである必要があります。また、IP ポリシーの Address Action プロパティを Transposed に指定する必要があります。新しい範囲またはネットワークは、変換用の開始アドレスである 1 つの IP アドレスを使用して指定されます。例えば、置き換えがネットワーク 192.168.1.0/24 に行われ、そのネットワークの最初のアドレスから始まるとすると、192.168.1.0 が新しいアドレスとして指定されます。

別の例では、SAT IP ルールセットのエントリは、194.1.2.16/29 ネットワークへの接続が 192.168.0.50 に変換されることを指定します。これの IP ポリシーは以下の通りです。

#	アクション	送信元 インタフェース	送信元 ネットワーク	送信先 インタフェース	送信先 ネットワーク	サービス	SAT アクション
1	Allow/SAT	any	all-nets	core	194.1.2.16/29	all_services	Destination IP:192.168.0.50

これらの IP ポリシーは以下の変換をもたらします。

オリジナルアドレス	変換アドレス
194.1.2.16	192.168.0.50
194.1.2.17	192.168.0.51
194.1.2.18	192.168.0.52
194.1.2.19	192.168.0.53
194.1.2.20	192.168.0.54
194.1.2.21	192.168.0.55
194.1.2.22	192.168.0.56
194.1.2.23	192.168.0.57

これらの IP ルールは以下の変換を行います。

- 194.1.2.16 と通信を試みることは、192.168.0.50 に接続する結果になります。
- 194.1.2.22 と通信を試みることは、192.168.0.56 に接続する結果になります。

この機能の適用例は、DMZ 内にいくつかの保護されたサーバを持つ場合です。そこでは、各サーバは固有のパブリック IP アドレスを使用してアクセスすることができます。

Many-to-Many SAT 変換の設定

Many-to-Many SAT 変換を設定するには以下の手順を実施する必要があります。

- パブリック IPv4 アドレスの範囲を含むアドレスオブジェクトを定義する
- Web サーバ IP アドレスのベースアドレスに対して別のアドレスオブジェクトを定義する
- インターネットに接続するインタフェースでパブリック IPv4 アドレスを ARP パブリッシュする
- SAT 変換を実行する IP Policy オブジェクトを作成する

例題 8.5

IP ポリシーを使用した Many-to-Many SAT アドレス変換

この例題では、IP ポリシーを使用して DMZ に位置する 5 個のパブリック IPv4 アドレスを 5 個の Web サーバに変換します。ファイアウォールは、wan インタフェースを使用してインターネットに接続され、そのパブリック IPv4 アドレスの範囲は 195.55.66.77 ～ 195.55.66.81 です。Web サーバが 10.0.0.5-10.0.0.9 の範囲に IPv4 アドレスを持っている場合、それらは dmz インタフェースに接続するネットワーク上にあります。

パブリック IPv4 アドレスは手動で ARP パブリッシュされ、これらのアドレスは core 上でルーティングされないため、SAT の送信先インタフェースは core ではなく wan となることに注意してください。

CLI

パブリック IPv4 アドレスに対するアドレスオブジェクトを作成する :

```
DFL-xxxx:/> add Address IP4Address wwwsrv_pub Address=203.0.113.1-205.0.113.5
```

Web サーバ IP アドレスを基に別のアドレスオブジェクトを作成する :

```
DFL-xxxx:/> add Address IP4Address wwwsrv_priv_base 10.0.0.5
```

ARP パブリッシュを使用し、wan インタフェース内のパブリック IPv4 アドレスをパブリッシュする :

1 個の ARP オブジェクトが各 IP アドレスに必要です。

```
DFL-xxxx:/> add ARPND Interface=wan IP=203.0.113.1 mode=Publish
```

5 個のパブリック IPv4 アドレスすべてに繰り返します。

変換に対する IP ポリシーを作成する :

```
DFL-xxxx:/> add IPPolicy Name=sat_http_to_dmz SourceInterface=any SourceNetwork=all-nets
            DestinationInterface=wan DestinationNetwork=wwwsrv_pub Service=http-all Action=Allow
            SourceAddressTranslation=None DestAddressTranslation=SAT DestAddressAction=TransposedRange
            DestBaseIP=wwwsrv_priv_base
```

Web Interface

パブリック IPv4 アドレスに対するアドレスオブジェクトを作成する :

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General

- Name : wwwsrv_pub
- IP Address : 203.0.113.1-205.0.113.5

Web サーバ IP アドレスをベースに別のアドレスオブジェクトを作成する :

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General

- Name : wwwsrv_priv_base
- IP Address : 10.0.0.5

ARP パブリッシュを使用して、wan インタフェース内のパブリックアドレスをパブリッシュする :

1 つの ARP アイテムが各 IP アドレスに必要とされます。

1. **Network > Interfaces and VPN > ARP/Neighbor Discovery > Add > ARP/Neighbor Discovery** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General

- Mode : Publish
- Interface : wan
- IP address : 203.0.113.1

3. 5 個のパブリック IPv4 アドレスすべてに繰り返し設定します。

変換に対する SAT ルールを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name : sat_http_to_dmz
   - Action : SAT

3. FILTER セクションで以下の情報を入力します。
   - Source Interface:any
   - Source Network: all-nets
   - Destination Interface: wan
   - Destination Network: wwwsrv_pub
   - Service : http-all

4. SOURCE TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: None

5. DESTINATION TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Transposed
   - Base IP Address: wwwsrv_priv

6. 「OK」をクリックします。

8.4.4 Many-to-One IP 変換

NetDefendOS は、範囲またはネットワークを 1 つの IP アドレスに変換するために使用されます。194.1.2.16-194.1.2.20 と 194.1.2.30 の宛先 IPv4 アドレスの範囲を 1 つの IPv4 アドレス 102.168.0.50 に変換するという要件を想定します。ポート番号は変更されません。

変換を実行する SAT IP ルールは以下の通りです。

#	アクション	送信元 インタフェース	送信元 ネットワーク	送信先 インタフェース	送信先 ネットワーク	サービス	SAT アクション
1	Allow/SAT	any	all-nets	wan	194.1.2.16- 194.1.2.20、 194.1.2.30	http-all	Destination IP:192.168.0.50

このルールセットのエントリによって実行される変換の例は以下の通りです。

- IPv4 アドレス 194.1.2.16 と通信する試みは、192.168.0.50 に接続する結果になります。
- IPv4 アドレス 194.1.2.30 と通信する試みは、192.168.0.50 に接続する結果になります。

例題 8.6

IP ポリシーを使用した Many-to-One SAT 変換

この例題は、前の many-to-many の例題に似ていますが、今回は SAT IP が 5 つのパブリック IPv4 アドレスを DMZ に位置する単一の Web サーバに変換します。

NetDefendOS ファイアウォールは、wan インタフェース経由でインターネットに接続され、そのパブリック IPv4 アドレスは 203.0.113.6-203.0.113.9 の範囲にあります。サーバはプライベート IPv4 アドレス 10.0.0.5 を持ち、dmz インタフェースに接続するネットワーク上にあります。

実行するためには、以下の手順を実行します。

- パブリック IPv4 アドレスの範囲を含むアドレスオブジェクトを定義する
- Web サーバの IPv4 アドレスとなる別のアドレスオブジェクトを定義する
- インターネットに接続するインタフェースでパブリック IPv4 アドレスを ARP をパブリッシュする
- SAT 変換を実行す IP Policy オブジェクトを作成する

パブリック IPv4 アドレスは手動で ARP パブリッシュされます。これらのアドレスは core 上でルーティングされないため、SAT の送信先インタフェースは core ではなく wan となることに注意してください。

CLI

パブリック IPv4 アドレスに対するアドレスオブジェクトを作成する :

```
DFL-xxxx:/> add Address IP4Address wwwsrv_pub Address=203.0.113.6-203.0.113.9
```

Web サーバのプライベート IP アドレス用の別のオブジェクトを作成する :

```
DFL-xxxx:/> add Address IP4Address wwwsrv_priv Address=10.0.0.5
```

ARP パブリッシュを使用し、wan インタフェースに 5 つのパブリック IPv4 アドレスをパブリッシュする。以下のような CLI コマンドが各 IP アドレスに必要です :

```
DFL-xxxx:/> add ARPND Interface=wan IP=203.0.113.6 mode=Publish
```

変換用の SAT IP ルールを作成する :

```
DFL-xxxx:/> add IPPolicy Name=sat_all_to_one SourceInterface=any SourceNetwork=all-nets
            DestinationInterface=wan DestinationNetwork=wwwsrv_pub Service=http-all Action=Allow
            SourceAddressTranslation=None DestAddressTranslation=SAT DestAddressAction=SingleIP
            DestNewIP=wwwsrv_priv
```

Web Interface

パブリック IPv4 アドレスに対するアドレスオブジェクトを作成する :

1. Objects > Address Book > Add > IP4 Address の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General

- Name : wwwsrv_pub
- IP Address : 203.0.113.6-205.0.113.9

Web サーバのプライベート IP アドレス用の別のオブジェクトを作成する :

1. Objects > Address Book > Add > IP4 Address の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General

- Name : wwwsrv_priv
- IP Address : 10.0.0.5

ARP パブリッシュを使用して、wan インタフェース内のパブリックアドレスをパブリッシュする :

1 つの ARP アイテムが各 IP アドレスに必要とされます。

1. **Network > Interfaces and VPN > ARP/Neighbor Discovery > Add > ARP/Neighbor Discovery** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General

- Mode : Publish
- Interface : wan
- IP address : 203.0.113.6

3. 5 個のパブリック IPv4 アドレスすべてに繰り返し設定します。

変換用の SAT IP ルールを作成する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name : sat_all_to_one
   - Action : Allow

3. FILTER セクションで以下の情報を入力します。
   - Source Interface:any
   - Source Network: all-nets
   - Destination Interface: wan
   - Destination Network: wwwsrv_pub
   - Service : http-all

4. SOURCE TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: None

5. DESTINATION TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Single IP
   - New IP Address: wwwsrv_priv

6. 「OK」をクリックします。

8.4.5 ステートレス IP ルールセットのエントリで SAT を設定する

「ステートレス」な IP ルールセットのエントリで SAT を設定することが可能です。これはつまり、通信の一部として、送信元から送信先の間のパケットフローを追跡しないエントリということです。したがって、トラフィックフローの各方向に対して 2 つのエントリが必要になります。2 つ目のエントリにより、リターントラフィックを明示的に変換する必要もあります。

IP Policy オブジェクトを使用する代わりに、Stateless Policy を使用するべきです。

以下の表では、dmz インタフェースに配置されたプライベート IP アドレス wwwsrv を持つ Web サーバへの通信のために、SAT Stateless Policy オブジェクトの正しい設定が IP ルールセットに追加されています。

#	アクション	送信元 インタフェース	送信元 ネットワーク	送信先 インタフェース	送信先 ネットワーク	サービス	SAT アクション
1	Allow/SAT	any	all-nets	core	wan_ip	http-all	Destination IP: wwwsrv
2	Allow/SAT	dmz	wwwsrv	any	all-nets	http-all	Source IP: wan_ip

2 番目のエントリはリターントラフィックとなるため、送信先 IP ではなく送信元 IP が変換されています。

例題 8.7

ステートレスポリシーを使用したステートレスな One-to-One SAT 変換

この例題では、「IP ルールを使用した One-to-One IP 変換」と似た設定を行いますが、IP ポリシーの代わりにステートレスポリシーを使用します。トラフィックフローの各方向に対してそれぞれ設定が必要となります。

CLI

インバウンドトラフィックに対して SAT ステートレスポリシーを作成します :

```
DFL-xxxx:/> add IPPolicy Name=stateless_sat_inbound_to_dmz SourceInterface=wan SourceNetwork=all-
            nets DestinationInterface=core DestinationNetwork=wan_ip Service=http-all Action=Allow
            SourceAddressTranslation=None DestAddressTranslation=SAT DestAddressAction=SingleIP Dest-
            NewIP=10.0.0.5
```

アウトバウンドトラフィックに対して SAT ステートレスポリシーを作成します :

```
DFL-xxxx:/> add IPPolicy Name=stateless_sat_outbound_to_dmz SourceInterface=dmz SourceNetwork=10.0.0.5
            DestinationInterface=any DestinationNetwork=all-nets Service=http-all Action=Allow
            SourceAddressTranslation=SAT SATSourceAddressAction=SingleIP SourceNewIP=wan_ip
```

Web Interface

インバウンドトラフィックに対して SAT ステートレスポリシーを作成します :

1. **Policies > Firewalling > Main IP Rules > Add > Stateless Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name : stateless_sat_inbound_to_dmz
   - Action : ALLOW

3. FILTER セクションで以下の情報を入力します。
   - Source Interface:wan
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip
   - Service : http-all

4. SOURCE TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: None

5. DESTINATION TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Single IP
   - New IP Address: 10.0.0.5

6. 「OK」をクリックします。

アウトバウンドトラフィックに対して SAT ステートレスポリシーを作成します :

1. **Policies > Firewalling > Main IP Rules > Add > Stateless Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name : stateless_sat_http_outbound_from_dmz
   - Action : ALLOW

3. FILTER セクションで以下の情報を入力します。
   - Source Interface:dmz
   - Source Network: 10.0.0.5
   - Destination Interface: wan
   - Destination Network: all-nets
   - Service : http-all

4. SOURCE TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Single IP
   - New IP Address: wan_ip

5. DESTINATION TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: None

6. 「OK」をクリックします。

8.4.6 NAT を使用した SAT

送信先 IP アドレスを SAT で変換し、送信元 IP アドレスを NAT で変換する必要がある場合に、1 つの IP ポリシーの中で SAT ルールと NAT ルールを使用する場合があります。これにより、トラフィックの送信先から送信元へトラフィックを送り返すことが可能となります。

「8.4.2 One-to-One IP 変換」の最後で述べた問題として、HTTP/HTTPS 通信を Web サーバへ送信するクライアントが、サーバと同じ内部ネットワークにあるケースが想定されます。クライアントとサーバが同じネットワーク内に配置することは推奨されませんが、そのようなケースも存在します。

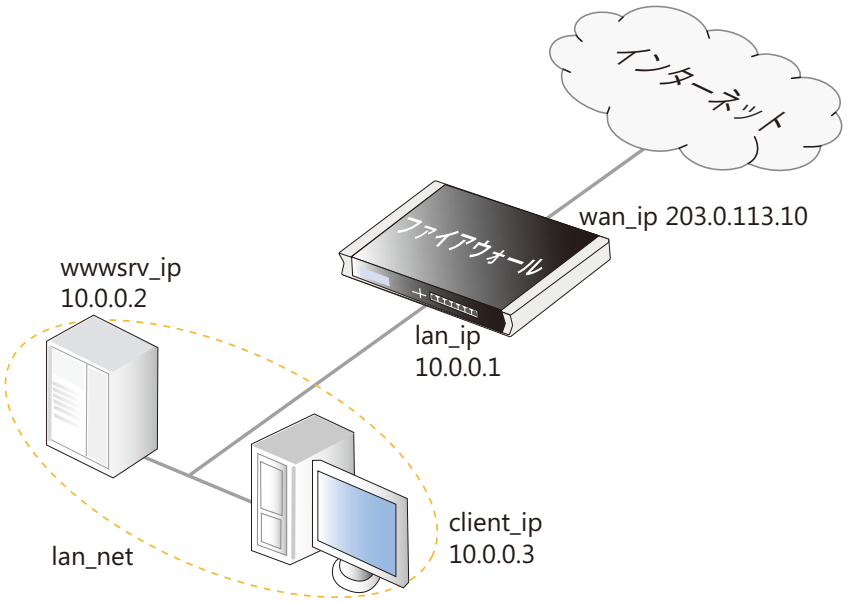


図 8-5　SAT と NAT

以下の IPv4 アドレスを想定します。

- wan_ip（203.0.113.10）: ファイアウォールのパブリック IPv4 アドレス
- lan_ip（10.0.0.1）: ローカルネットワークのプライベート IPv4 アドレス
- wwwsrv_ip（10.0.0.2）: Web サーバのプライベート IPv4 アドレス
- client_ip（10.0.0.3）: ローカルクライアントのプライベート IPv4 アドレス

パブリックアドレス wan_ip に到達し、Web サーバのプライベートアドレス wwwsrv_ip へ向かう SAT トラフィックに対し、以下の IP ポリシーが存在することを想定します。

#	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス	SAT アクション
1	Allow/SAT	any	all-nets	core	wan_ip	http-all	Destination IP: wwwsrv_ip

しかし、これは Web サーバと同じネットワークのクライアントでは正常に動作しません。そのようなクライアントが応答を受信する時、送信元アドレスが要求を送信した IP アドレスに一致しないためです。これはクライアントが応答を無視する結果となります。このような結果となるのは以下に示す一連のイベントのためです。

1. ローカルクライアントは、Web サーバ IP のためにパブリック DNS 検索を実行して、Web サーバに到達するように HTTP リクエストを wan_ip に送信します。

   10.0.0.3:1038 = > 203.0.113.10:80

2. SAT IP ポリシー 1 に従ってトラフィックが許可され、送信先アドレスを wwwsrv_ip に変換します。

   10.0.0.3:1038 = > 10.0.0.2:80

3. wwwsrv_ip のサーバはパケットと応答を処理します。

   10.0.0.2:80 = > 10.0.0.3:1038

   応答は、ファイアウォールを通過することで、ローカルネットワークを経由して直接クライアントに送信されます。

4. クライアントは 10.0.0.2:80 ではなく、203.0.113.10:80 からの応答を予想します。そのため、リプライは廃棄され、クライアントは決して到着しない 203.0.113.10:80 からのレスポンスを待ち続けます。

この問題に対するソリューションの 1 つとして、同じネットワークにあるクライアントとサーバが直接通信できるようにすることが考えられます。しかし、そのような動作を実現するには、Web サーバのプライベート IP アドレスを検出するために内部 DNS サーバが必要となります。より適切なソリューションは、クライアントのトラフィックに NAT を適用して送信元を wan_ip とし、送信先を wwwsrv_ip とする SAT を適用する 2 つ目の IP ポリシーを作成することです。この IP ポリシーは次の表のようになります。

#	アクション	送信元 インタフェース	送信元 ネットワーク	送信先 インタフェース	送信先 ネットワーク	サービス	SAT アクション
1	Allow/SAT	any	all-nets	core	wan_ip	http-all	Destination IP: wwwsrv_ip
2	Allow NAT/SAT	lan	lan_net	core	wan_ip	http-all	Destination IP: wwwsrv_ip (SAT) Source IP: wan_ip (NAT)

イベントの順序は、以下の通りになります。

1. クライアントは、Web サーバに到達するために wan_ip にトラフィックを送信します。
   10.0.0.3:1038 = > 203.0.113.10:80

2. NetDefendOS は、ルール 2 に従って接続を変換します。
   10.0.0.1:32789 = > 10.0.0.2:80

3. wwwsrv_ip のサーバはパケットと応答を処理します。
   10.0.0.2:80 = > 10.0.0.1:32789

4. 応答は、変換ルールが逆順で適用されるように、NetDefendOS によって処理されて、想定される送信元アドレスと共にクライアントに到着します。
   203.0.113.10:80 = > 10.0.0.3:1038

以下の例題では新しい NAT/SAT ポリシーの作成方法を詳細に説明します。

例題 8.8

IP ポリシーを使用して SAT/NAT を設定する

この例題では、SAT/NAT の IP ポリシーを作成し、クライアントが同じネットワーク内に配置されている Web サーバへの HTTP 接続を行えるように設定します。

「図 8-5 SAT と NAT」で示されているネットワーク設定を想定し、クライアントとサーバが lan_net ネットワークに存在しているものとします。

CLI

SAT IP ポリシーを作成する :

```
DFL-xxxx:/> add IPPolicy Name=sat_nat_http SourceInterface=lan SourceNetwork=lan_net DestinationInterface=core
            DestinationNetwork=wan_ip Service=http-all Action=Allow SourceAddressTranslation=NAT NATSourceAdd
            ressAction=OutgoingInterfaceIP DestinationAddressTranslation=SAT DestinationAddressAction=SingleIP
            DestNewIP=wwwsrv_ip
```

Web Interface

SAT IP ポリシーを作成する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name : sat_nat_http
   - Action : Allow

3. FILTER セクションで以下の情報を入力します。
   - Source Interface : wan
   - Source Network : lan_nets
   - Destination Interface : core
   - Destination Network : wan_ip
   - Service : http-all

4. SOURCE TRANSLATION セクションで以下の情報を入力します。
   - Address Translation : NAT
   - Address Action : Outgoing Interface IP

5. DESTINATION TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Single IP
   - New IP Address: wwwsrv_priv

6. 「OK」をクリックします。

自動変換オプションを使用した NAT/SAT

1 つの IP ポリシーの中で NAT と SAT を一緒に設定し、IP ポリシーの送信元変換で Auto オプションを指定することで内部クライアントの問題を解消することも可能です。詳細は「8.5 自動変換」で説明します。保護されたクライアントから保護された Webs サーバへの接続について、それぞれ同じネットワークであってもそうでなくても、通信を許可するように設定することも可能です。

8.4.7 ポート変換

ポート変換（PAT: Port Address Translation）は、接続の送信元または送信先ポートを編集するために使用されます。前の SAT の例題では、新しいポート番号が指定されておらず、オリジナルのポート番号が初期値で使用されました。ポート番号が指定されると、IP アドレスとポート番号の両方が変換されます。

ポートマッピングを有効化する

ポートマッピングを有効化するには、SAT IP ポリシーの Port Action プロパティを Single Port または Transposed のいずれかに指定します。いずれの場合でも、ポート番号を指定する必要があります（one-to-one 変換の場合は新しいポート番号、many-to-many 変換の場合はベースポート番号）。

Service 設定に使用されるポートマッピングのルール

SAT 変換を行う IP ポリシーに割り当てる Service オブジェクトに対しては、以下のルールに従ってポートマッピング機能が動作します。

- IP ルールセットのエントリで使用される Service オブジェクトにポートプロパティとして 1 つの値または単純な範囲が指定されていない場合、ポート変換は実行されません。

  「単純な範囲」とは最小値最大値のみが含まれる 1 つの範囲、または 1 つの値を示します。（例：50-60）

- Port Action で Single Port を指定して New Port の番号を指定し、使用される Service オブジェクトのポートプロパティで 1 つの番号が指定されている場合、すべての通信は新しいポート番号に変換されます。

- Port Action で Transposed を指定して Base Port 値を指定し、使用される Service オブジェクトのポートプロパティで単純な番号の範囲が指定されている場合、すべての通信はベースポート番号から始まる新しいポート番号に変換されます。

ポート変換の例

例えば、関連する Service オブジェクトが単純なポート範囲 80-85 を持っている以下の SAT IP ポリシーを考えます。エントリは宛先アドレス wwwsrv_pub が wwwsrv_priv に変換されるように指定します。また、ポートアクションを Transosed、Base Port を 1080 に指定することで、該当のポートのみが many-to-many 変換の対象となるようにします。

#	アクション	送信元 インタフェース	送信元 ネットワーク	送信先 インタフェース	送信先 ネットワーク	サービス	SAT アクション
1	Allow/SAT	any	all-nets	wan	wwwsrv_pub	TCP 80-85	Destination IP: wwwsrv_priv Action: Transposed Base Port:1080

このルールセットエントリでは、80-85 の範囲にあるすべてのポートに対して Many-to-Many 変換を実行します。例として、以下のような処理が実行されます。

- Web サーバのパブリックアドレス、ポート 80 と通信する場合、Web サーバのプライベートアドレス、ポート 1080 と通信する結果になります。
- Web サーバのパブリックアドレス、ポート 84 と通信する場合、Web サーバのプライベートアドレス、ポート 1084 と通信する結果になります。

Port プロパティに単一の値 80 を指定するように Service を変更した場合、ポート 80 に対してのみ IP ルールセットのエントリがトリガーされ、常に新しいポート 1080（one-to-one 関係）に変換されます。

例題 8.9

IP ポリシーを使用したポート変換

この例題では、「IP ポリシーを使用した One-to-One IP 変換」と同様の設定を行いますが、ポート 80 ～ 85 で接続するプロトコルを指定したカスタムサービスを使用します。また、many-to-many 変換を実行して 80 ～ 85 の送信先ポート範囲が 1080 ～ 1085 となるようにします。
IP ポリシーと一緒に ALG を使用する場合、サービスオブジェクトに対してプロトコルを割り当てる必要があります。

CLI

カスタムサービスを作成する：

```
DFL-xxxx:/> add Service ServiceTCPUDP my_sat_service Type=TCP DestinationPorts=80-85
```

SAT IP ポリシーを作成する：

```
DFL-xxxx:/> add IPPolicy Name=sat_port_translate SourceInterface=wan SourceNetwork=all-nets
            DestinationInterface=core DestinationNetwork=wan_ip Service=my_sat_service Action=Allow
            SourceAddressTranslation=None DestAddressTranslation=SAT DestAddressAction=SingleIP Dest-
            NewIP=10.0.0.5 DestPortAction=TransposedRange DestBasePort=1080
```

Web Interface

カスタムサービスを作成する

1. **Objects > Services > Add > TCP/UDP service** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。
   - Name : my_sat_service
   - Type：TCP
   - Destination port: 80-85

SAT IP ポリシーを作成する

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name : sat_port_translate
   - Action : ALLOW

3. FILTER セクションで以下の情報を入力します。
   - Source Interface:wan
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip
   - Service : my_sat_service

4. SOURCE TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: None

5. DESTINATION TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Single IP
   - New IP Address: 10.0.0.5
   - Port Action: Transpose
   - Base Port: 1080

6. 「OK」をクリックします。

8.4.8「SAT」が処理するプロトコル

一般的に、SAT はアドレス変換を実行できるすべてのプロトコルを処理できます。しかし、特別な場合にだけ変換できるプロトコルや、まったく変換されないプロトコルもあります。

SAT を使用した変換ができないプロトコルは、NAT を使用して変換することもおそらく不可能です。その理由は以下の通りです :

- 暗号化プロトコルはアドレスが変更されないことが必要です。これは、多くの VPN プロトコルにも言えます。
- プロトコルは TCP または UDP レベルデータ内部に IP アドレスを埋め込み、IP レベルで見えるアドレスが、データ埋め込みのものと同じである必要があります。例えば FTP などが該当します。
- どちらかのパーティが、そのパーティに対して見えるアドレスに新しいダイナミック接続をオープンしようとします。これはアプリケーションまたはファイアウォール設定を編集することで解決できる場合もあります。

どのプロトコルがアドレス変換できる、またはできないかを定義したリストはありません。 一般的なルールでは VPN プロトコルは通常変換されません。さらに、初期接続に加え、セカンダリ接続をオープンするプロトコルは変換するのが困難です。

アドレス変換が難しいプロトコルの中には、アプリケーションデータの読み取りと（または）変換用に特別に記述されたアルゴリズムによって処理されるものもあります。これは一般的に「Application Layer Gateways」または「Application Layer Filters」と呼ばれるものです。NetDefendOS ではそのような Application Layer Gateway を多数サポートしています。詳細は「6.1 アプリケーションレイヤゲートウェイ」を参照してください。

8.4.9 IP ルールを使用した SAT ルールの設定

複数の IP ルールが必要な SAT

NATとは異なり、SATでは複数のIPルールの設定が必要です。必要とされる変換を指定するために、ターゲットトラフィックのトリガーとなるSATルールを最初に作成する必要があります。しかし、NetDefendOSは、一致するSATルールの検索完了後もルールセット検索を終了しません。代わりに、ルールセットは一致する「Allow」、「NAT」または「FwdFast」ルールの検索を続けます。NetDefendOS がそのような 2 番目のマッチングを検出する場合のみ、SAT ルールがトラフィックに適用されます。IP ポリシーの場合、1 つの IP Policy オブジェクトのみが必要となります。

「SAT」ルールは、実行されるべき変換のみを定義します。2 番目（関連付けられた IP ルール）が、実際にトラフィックフローを許可します。

第 2 ルールが変換されていない IP アドレスで始動する

「SAT」の IP ルールを作成する際に覚えておくべき重要な原則は、第 2 のルール、例えば「Allow」ルールは、変換されていない古い IP アドレス（SAT ルールのタイプに依存するソースまたは宛先 IP のいずれか）上で始動する必要があるということです。 一般的な誤りは、新しく変換された IP アドレスで始動するべきだと想定して、2 番目の IP ルールを作成することです。

例えば、「SAT」ルールが宛先の IPv4 アドレスを「192.168.0.1」から「172.16.0.1」に変換した場合、第 2 の関連ルールでは、必ずトラフィックが宛先アドレス「172.16.0.1」ではなく「192.168.0.1」を通過するように許可すべきです。

第 2 のルールがトリガーしてトラフィックを許可した後にだけ、NetDefendOS が変換後の宛先アドレスに対しルートを検索して、そのトラフィックを送り出すべきインタフェースを決定します。

SAT IP ルールのプロパティ

SAT IP ルールは、送信元ネットワーク / インタフェース + 宛先ネットワーク / インタフェース + サービスの組み合わせで起動するという点で IP ルールの他のタイプに似ています。SAT IP ルールには、以下の追加のプロパティがあります。

項目	説明
SAT Translate	変更されるアドレスを指定します。 **i.** Destination IP - オリジナルの宛先 IP が変換されます。 **ii.** Source IP - オリジナルのソース IP が変換されます。
New IP Address	変換用の新しいアドレス。
New Port	変換に使用される新しいポート番号。以下で説明されるように、ポート変換はアドレス変換の如何にかかわらず起こり、わずかに異なるルールに従います。
All-to-One Mapping	複数の IP アドレスを 1 つの IP アドレスにマッピングする場合に有効とします。all-to-one ポート変換はできないため、ポート変換には使用されません。

例題 8.10

IP ルールを使用した One-to-One IP 変換

この例題は「8.4 IP ポリシーを使用した One-to-One IP 変換」と同じ設定を行いますが、IP ポリシーの代わりに IP ルールを使用しています。

CLI

SAT IP ルールを作成します。:

```
DFL-xxxx:/> add IPRule Action=SAT Service=http-all SourceInterface=wan SourceNetwork=all-nets
            DestinationInterface=core DestinationNetwork=wan_ip SATTranslate=DestinationIP
            SATTranslateToIP=10.10.10.5 Name=SAT_HTTP_To_DMZ
```

次に、対応する Allow ルールを作成する :

```
DFL-xxxx:/> add IPRule Action=Allow Service=http-all SourceInterface=wan SourceNetwork=all-nets
            DestinationInterface=core DestinationNetwork=wan_ip Name=Allow_HTTP_To_DMZ
```

Web Interface

最初に SAT ルールを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 適切なルール名を指定します。例 : SAT_HTTP_To_DMZ
3. 以下の情報を入力します。
   - Action: SAT
   - Service: http-all
   - Source Interface: wan
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip
   - SAT Translate: Destination IP
   - New IP Address: 10.10.10.5
4. 「OK」ボタンをクリックします。

次に、対応する Allow ルールを作成する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 適切なルール名を指定します。例 : Allow_HTTP_To_DMZ
3. 以下の情報を入力します。
   - Action: Allow
   - Service: http-all
   - Source Interface: wan
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip
4. 「OK」ボタンをクリックします。

例題 8.11

IP ルールを使用した Many-to-Many IP アドレス変換

この例題は「8.5 IP ポリシーを使用した One-to-One SAT 変換」と同じ設定を行いますが、IP ポリシーの代わりに IP ルールを使用しています。

CLI

パブリック IPv4 アドレスに対するアドレスオブジェクトを作成する :

```
DFL-xxxx:/> add Address IP4Address wwwsrv_pub Address=203.0.113.1-205.0.113.5
```

Web サーバ IP アドレスを基に別のアドレスオブジェクトを作成する :

```
DFL-xxxx:/> add Address IP4Address wwwsrv_priv_base Address=10.0.0.5
```

ARP パブリッシュを使用し、wan インタフェース内のパブリック IPv4 アドレスをパブリッシュする。:

1 個の ARP アイテムが各 IP アドレスに必要です。

```
DFL-xxxx:/> add ARPND Interface=wan IP=195.55.66.77 mode=Publish
```

5 個のパブリック IPv4 アドレスすべてに繰り返します。

変換に対する SAT ルールを作成する :

```
DFL-xxxx:/> add IPRule Action=SAT Service=http-all SourceInterface=any SourceNetwork=all-nets
            DestinationInterface=wan DestinationNetwork=wwwsrv_pub SATTranslateToIP=wwwsrv_priv_base
            SATTranslate=DestinationIP
```

最後に、対応する Allow ルールを作成する :

```
DFL-xxxx:/> add IPRule Action=Allow Service=http-all SourceInterface=any SourceNetwork=all-nets
            DestinationInterface=wan DestinationNetwork=wwwsrv_pub
```

Web Interface

パブリック IPv4 アドレスに対するアドレスオブジェクトを作成する :

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General

- Name : wwwsrv_pub
- IP Address : 203.0.113.1-205.0.113.5

Web サーバ IP アドレスをベースに別のアドレスオブジェクトを作成する :

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General

- Name : wwwsrv_priv_base
- IP Address : 10.10.10.5

ARP パブリッシュを使用して、wan インタフェース内のパブリックアドレスをパブリッシュする :

1 つの ARP アイテムが各 IP アドレスに必要とされます。

1. **Network > Interfaces and VPN > ARP/Neighbor Discovery > Add > ARP/Neighbor Discovery** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General

- Mode : Publish
- Interface : wan
- IP address : 203.0.113.1

3. 5 個のパブリック IPv4 アドレスすべてに繰り返し設定します。

変換に対する SAT ルールを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。
   - Name : SAT_HTTP_To_DMZ

- Action : SAT
- Service : http-all
- Source Interface:any
- Source Network: all-nets
- Destination Interface: wan
- Destination Network: wwwsrv_pub
- SAT Translate: Destination IP
- New IP Address: wwwsrv_priv_base

最後に、対応する Allow ルールを作成する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。
- Name : Allow_HTTP_To_DMZ
- Action: Allow
- Service: http-all
- Source Interface: any
- Source Network: all-nets
- Destination Interface: wan
- Destination Network: wwwsrv_pub

例題 8.12

IP ルールを使用した All-to-One IP 変換

この例題は「8.6 IP ポリシーを使用した Many-to-One SAT 変換」と同じ設定を行いますが、IP ポリシーの代わりに IP ルールを使用しています。

CLI

パブリック IPv4 アドレスに対するアドレスオブジェクトを作成する :

```
DFL-xxxx:/> add Address IP4Address wwwsrv_pub Address=203.0.113.6-203.0.113.9
```

Web サーバ IP アドレスを基に別のアドレスオブジェクトを作成する :

```
DFL-xxxx:/> add Address IP4Address wwwsrv_priv Address=10.10.10.5
```

ARP パブリッシュを使用し、wan インタフェースに 5 つのパブリック IPv4 アドレスをパブリッシュする。以下のような CLI コマンドが各 IP アドレスに必要です。:

```
DFL-xxxx:/> add ARPND Interface=wan IP=203.0.113.6 mode=Publish
```

変換用の SAT IP ルールを作成する :

```
DFL-xxxx:/> add IPRule Action=SAT Service=http-all SourceInterface=any SourceNetwork=all-nets
            DestinationInterface=wan DestinationNetwork=wwwsrv_pub SATTranslateToIP=wwwsrv_priv
            SATTranslate=DestinationIP SATAllToOne=Yes
```

最後に、対応する Allow ルールを作成する :

```
DFL-xxxx:/> add IPRule Action=Allow Service=http-all SourceInterface=any SourceNetwork=all-nets
            DestinationInterface=wan DestinationNetwork=wwwsrv_pub
```

Web Interface

パブリック IPv4 アドレスに対するアドレスオブジェクトを作成する :

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General
- Name : wwwsrv_pub
- IP Address : 203.0.113.6-205.0.113.9

Web サーバ IP アドレスをベースに別のアドレスオブジェクトを作成する :

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General

- Name : wwwsrv_priv_base
- IP Address : 10.10.10.5

ARP パブリッシュを使用して、wan インタフェース内のパブリックアドレスをパブリッシュする :

1 つの ARP アイテムが各 IP アドレスに必要とされます。

1. **Network > Interfaces and VPN > ARP/Neighbor Discovery > Add > ARP/Neighbor Discovery** の順にメニューをクリックします。

2. 以下の通り情報を入力し、「OK」ボタンをクリックします。

< 入力例 >

General

- Mode : Publish
- Interface : wan
- IP address : 203.0.113.6

3. 5 個のパブリック IPv4 アドレスすべてに繰り返し設定します。

変換用の SAT IP ルールを作成する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 適切なルール名を指定します。例 :SAT_HTTP_To_DMZ

3. 以下の情報を入力します。

- Action: SAT
- Service: http-all
- Source Interface: any
- Source Network: all-nets
- Destination Interface: wan
- Destination Network: wwwsrv_pub
- SAT Translate: Destination IP
- New IP Address: wwwsrv_priv
- オプションを有効にします。: All-to-One Mapping

4. 「OK」ボタンをクリックします。

最後に、対応する Allow ルールを作成する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。

2. 適切なルール名を指定します。例 :Allow_HTTP_To_DMZ

3. 以下の情報を入力します。

- Action: Allow
- Service: http-all
- Source Interface: any
- Source Network: all-nets
- Destination Interface: wan
- Destination Network: wwwsrv_pub

4. 「OK」ボタンをクリックします。

8.5 自動変換

概要

IP Policy オブジェクトは、送信元アドレスに対して Automatic Address Translation を適用するオプションを提供します（IP ルールでは利用不可）。IP ポリシーの Souce Translation プロパティ設定を Auto にすることにより、本機能を有効化することができます（初期値）。

自動変換オプションは、以下のようなシナリオで簡単に設定を行う場合に役に立ちます。

- プライベート IPv4 アドレスを持つ内部クライアントがインターネットへ接続する必要がある。この設定手順については「8.5.1 NAT のみの変換」で説明しています。
- 保護されたローカル Web サーバに対して SAT 変換が必要であり、プライベート IPv4 アドレスを持つ内部クライアントから接続する必要もある。設定手順については「8.5.2 NAT/SAT 変換」で説明しています。

自動変換で処理される内容

自動変換は、送信元のアドレス変換に Auto オプションを選択することで有効になります。これは IP Policy オブジェクトの初期値で選択されています。そして、NetDefendOS は、以下のテーブルにまとめられたルールを適用することで、実行する変換を決定します。

#	送信元 IP のタイプ	送信先 IP のタイプ	実施される IP アクション
1	Public	Private または Public	変換なしで許可する。
2	Private	Public	送信先インタフェースを使用した NAT。
3	Private	以下のすべての条件に当てはまるタイプ ・Private ・Destination Translation = SAT ・Source Network に SAT IP が含まれる	送信先インタフェースを使用した NAT。
4	Private	以下のすべての条件に当てはまるタイプ ・Private ・前のアクションがトリガされていない	変換なしで許可する。

上にまとめられた自動変換ルールに関するさらに詳しい説明は以下の通りです。

- **接続の送信元 IP アドレスがパブリックアドレスの場合：**
  NetDefendOS は送信元アドレスから宛先アドレスまでのトラフィックを許可します。

- **接続の送信元 IP アドレスがプライベートアドレスの場合：**
  i. 宛先アドレスがパブリック IP アドレスであれば、NetDefendOS は送信元アドレスを宛先インタフェースの IP アドレスを通じて NAT 変換します。
  ii. Destination Translation が SAT するように設定されていて、Source Network が SAT Destination IP アドレスを含んでいると、NetDefendOS はプライベートな送信元アドレスを宛先インタフェースの IP アドレスを通じて NAT 変換します。（これは、例えば保護された Web サーバが内部のクライアントによってアクセスされるのを許可します。）

  または、上記とは異なり宛先アドレスがプライベート IP アドレスである場合、NetDefendOS はプライベートな送信元アドレスからプライベート宛先アドレスまでのトラフィックを許可します。

以下は自動変換を利用する IP ポリシーに関する注意事項です。

- Source Network と Destination Network はプライベートとパブリック IP アドレスの混合から構成されることが可能です。

- 上で説明された 1 つ以上のアクションを 1 つの IP ポリシーにより、異なる接続に適用できます。各接続の送信元および宛先アドレスに従って、違うアクションが適用されます。

自動変換は拒否されたトラフィックに影響しない

トラフィックを拒否する設定の IP ポリシーでは、トリガーとなるトラフィックは常に破棄され変換は実行されないため、Source Translation プロパティ設定は関連しません。
したがって、拒否のポリシーでは Source Translation を Auto のままとしておくことができます。そのようなポリシーについては「「Drop All」IP ルールセットエントリの作成」で説明しています。

自動変換の詳細を確認する

IP Policy オブジェクトで Auto オプションを指定した場合、IP ポリシーを実装するためにバックグラウンドで IP Rule オブジェクトのセットが作成されます。これらの IP ルールは Web インタフェースでは表示されませんが、詳細を確認する必要がある場合、CLI コマンド「rules」を使用して作成されたすべての IP ルールを見ることができます。

8.5.1 NAT のみの変換

以下の図では自動 NAT 変換が使用される典型的なシナリオを示しています。

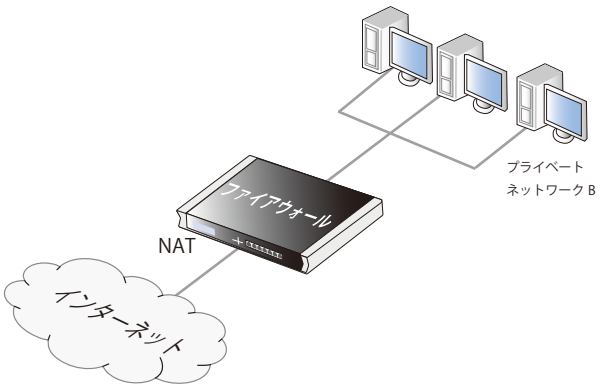


図 8-6　自動 NAT 変換

上記の図では、以下の種類のトラフィックフローが許可される必要があります。

- IPv4 ネットワーク B 上の内部クライアントから他の異なるプライベート IP アドレスへの接続。自動変換により、プライベート IPv4 アドレス間のトラフィックは常に変換なしで許可されます。
- IPv4 ネットワーク B 上の内部クライアントからインターネットへの接続。この通信では、プライベート IPv4 アドレスを、インターネットに接続されたファイアウォールのインタフェースのパブリック IPv4 アドレスに変換する必要があります。プライベート IPv4 アドレスがパブリック IPv4 アドレスに接続しようとする場合、自動変換で常に NAT 変換が行われます。

上記のすべての要件またはいずれかの要件は、自動変換を有効化した 1 つの IP ポリシーによって実現できます。設定方法は以下の例題の通りです。

例題 8.13

IP ポリシーを使用した自動 NAT 変換

この例題では、自動変換オプションを有効化した 1 つの IP ポリシーを作成して、プライベート IP アドレスを持つ lan-net 上の HTTP/HTTPS クライアントが、自動 NAT 変換を使用して 1 つの IP アドレス wan_ip によりインターネットに接続できるように設定します。
Source Translation の初期値は Auto ですが、分かりやすくするためこの例題では明示的に記載しています。

CLI

自動変換オプションを使用して IP ポリシーを作成する：

```
DFL-xxxx:/> add IPPolicy Name=http_auto_nat_policy SourceInterface=lan SourceNetwork=lan-net
            DestinationInterface=wan DestinationNetwork=all-nets Service=http-all Action=Allow
            SourceAddressTranslation=Auto
```

Web Interface

自動変換オプションを使用して IP ポリシーを作成する：

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name : http_auto_nat_policy
   - Action : ALLOW
3. FILTER セクションで以下の情報を入力します。
   - Source Interface:lan
   - Source Network: lan_net
   - Destination Interface: wan
   - Destination Network: all-nets
   - Service : http-all
4. SOURCE TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: Auto
5. 「OK」をクリックします。

8.5.2 NAT/SAT 変換

以下の図では、自動 NAT/SAT 変換が行われる典型的なシナリオを表しています。前のセクション「8.5.1 NAT のみの変換」で説明したシナリオを拡張し、インターネットからファイアウォールのパブリック IP アドレスへの通信において、送信先アドレスから Web サーバのプライベート IP アドレスへの SAT 変換を必要としています。

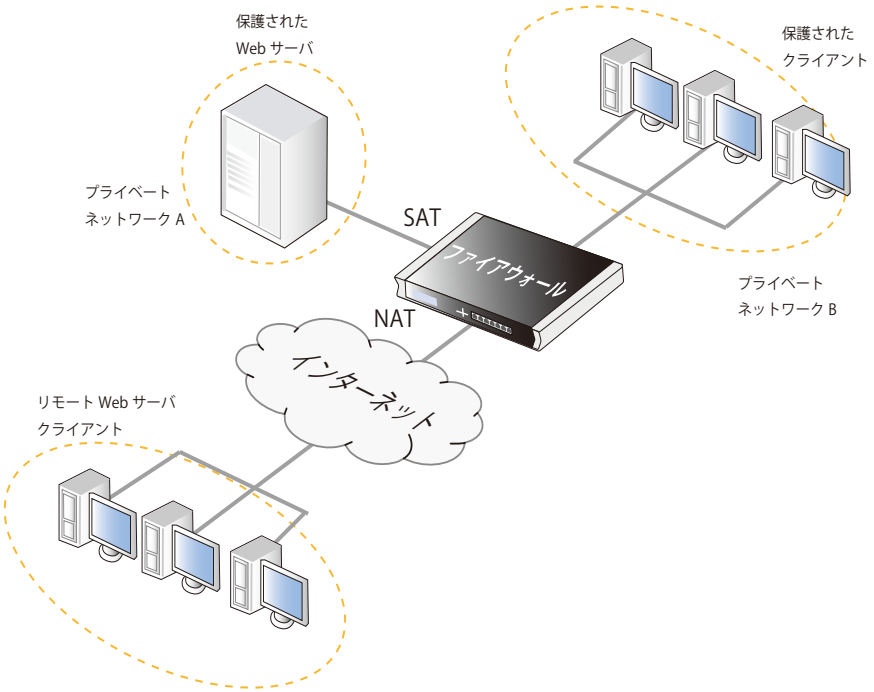


図 8-7　自動 NAT/SAT 変換

上記の図では、以下の種類のトラフィックフローが許可される必要があります。

- IPv4 ネットワーク B 上の内部クライアントから他の異なるプライベート IP アドレスへの接続。変換を行わずに、自動変換によって常にプライベート IPv4 アドレス間のトラフィックが許可されます。
- IPv4 ネットワーク B 上の内部クライアントからインターネットへの接続。この通信では、プライベート IPv4 アドレスを、インターネットに接続されたファイアウォールのインタフェースのパブリック IPv4 アドレスに NAT 変換する必要があります。プライベート IPv4 アドレスがパブリック IPv4 アドレスに接続しようとする場合、自動変換で常に NAT 変換が行われます。
- IPv4 ネットワーク B 上の内部クライアントからパブリック IP アドレス経由での Web サーバへの接続。上記 2 つ目で説明した NAT の自動変換により、この接続が許可されます。

上記のすべての要件またはいずれかの要件は、自動変換を有効化した 1 つの IP ポリシーによって実現できます。設定方法は以下の例題の通りです。

例題 8.14

IP ポリシーを使用した自動 SAT/NAT 変換

この例題では、自動変換オプションを有効化した 1 つの IP ポリシーを作成して、インターネットおよび lan-net 上の HTTP/HTTPS クライアントが、プライベート IP アドレス 10.0.0.5 を持つ DMZ 上の保護された Web サーバへ接続できるように設定します。サーバへの接続は、パブリック IP アドレス wan_ip が割り当てられた wan インタフェースを介して行われます。さらに、サーバへの通信に SAT 変換を適用します。
また、lan_net 上のクライアントは wan インタフェース経由でインターネットに接続する必要があります。
この例では分かりやすくするために、インタフェースの設定を any や all-nets に指定していますが、セキュリティの観点では、適切な Interface Group や IP4 Address オブジェクトを作成して限定することが推奨されます。

CLI

```
DFL-xxxx:/> add IPPolicy Name=http_auto_satnat_policy SourceInterface=any SourceNetwork=all-
            nets DestinationInterface=any DestinationNetwork=wan_ip Service=http-all Action=Allow
            SourceAddressTranslation=Auto DestAddressTranslation=SAT DestAddressAction=SingleIP Dest-
            NewIP=10.0.0.5
```

Web Interface

自動変換オプションを使用して IP ポリシーを作成する。

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name : http_auto_satnat_policy
   - Action : ALLOW

3. FILTER セクションで以下の情報を入力します。
   - Source Interface: any
   - Source Network: all-nets
   - Destination Interface: any
   - Destination Network: wan_ip
   - Service : http-all

4. SOURCE TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: Auto

5. DESTINATION TRANSLATION セクションで以下の情報を入力します。
   - Address Translation: SAT
   - Address Action: Single IP
   - New IP Address: 10.0.0.5

6. 「OK」をクリックします。

注意 クライアントとサーバは同じネットワーク

上記の例では、DMZ 上のクライアントからパブリック IP アドレス経由での Web サーバへの接続を許可しているだけではなく、Web サーバと同じネットワークのクライアントに対しても接続が許可されます。

第 9 章 ユーザ認証

この章では NetDefendOS がユーザ認証を実行する方法について記載します。

- 「9.1 概要」
- 「9.2 認証設定」
- 「9.3 認証 HTML ページのカスタマイズ」
- 「9.4 認証を必要とする IP ポリシー」
- 「9.5 Brute Force 保護」
- 「9.6 User Identity Awareness」
- 「9.7 多要素認証」
- 「9.8 RADIUS リレー」
- 「9.9 RADIUS アカウンティング」

9.1 概要

D-Link ファイアウォールを通して個々のユーザが保護されたソースに接続する場合、アクセスを許可する前に管理者は各ユーザが認証プロセスを通るよう要求します。本章は NetDefendOS の認証設定を扱いますが、最初に、認証にかかわる一般的な問題を検証します。

アイデンティティの立証

認証の目的は、ユーザに自身のアイデンティティを証明させ、そのアイデンティティに基づいてネットワーク管理者がリソースへのアクセスを許容したり、または拒絶することです。立証の方法には以下のようなものがあります。

A. ユーザが誰であるのか。指紋などの各人の異なるユーザの固有の特性。
B. X.509 デジタル証明書、パスカードまたは公開鍵 / 秘密鍵などのユーザが持っているもの。
C. パスワードなどのユーザが知っているもの。

方式 A では特別な生体認証装置が必要です。また、データを失った場合にその特別な機能の代替がないという別の問題もあります。そのため、方式 B と C がネットワークセキュリティで最も一般的な識別の方法です。しかしながら、これらには欠点があります。
例えば、鍵は傍受され、カードは盗まれ、人々は推測しやすい弱いパスワードを選択するため、秘密を保持するためには不適当であると言えるかもしれません。そのため、パスワードやピンコードを要求するパスカードのように B と C はしばしば組み合わせられます。

ユーザ名 / パスワードの組み合わせを利用する

この章では特に、ユーザがリソースにアクセスを試みる場合に、手動で入力するユーザ名とパスワードの組み合わせにより実行されるユーザ認証について記載します。HTTP プロトコルを使用している内部クライアントが D-Link ファイアウォールを通じて外部のパブリックインターネットにアクセスする場合がその一例です。

この方法を使う場合、推測による検索や系統的に自動化された検索によって、ユーザ名 / パスワードのペアはしばしば攻撃を受けやすくなります。攻撃に対抗するためには、パスワードを注意深く選択する必要があります。理想的なものは以下の通りです。

- 循環性を持たず 8 文字以上であること。より長い文字列が推奨されます。
- 一般的に使用されるフレーズでないランダムな文字列を使用すること。
- 小文字と大文字の文字を含むこと。
- 数字と特殊文字を含むこと。

さらにセキュリティのためにパスワードに行うべきことは以下の通りです。
- どこにも記録してはいけない。
- 決して誰にも漏らしてはいけない。
- 3 カ月毎など定期的に変更する。

認証処理

以下のリストでは、NetDefendOS 内のユーザ名 / パスワード認証の処理フローについて説明します。

1. あるユーザが D-Link ファイアウォールに新しい接続を確立したとします。

2. NetDefendOS は、インタフェース上の新しいユーザ接続を認識すると、認証ルールセットをチェックして、このネットワークから送信されたトラフィックに照合するルールがこのインタフェース上にあるかどうか、データが次のどのタイプであるかを確認します。

   - HTTP トラフィック
   - HTTPS トラフィック
   - IPsec トンネルトラフィック
   - L2TP トンネルトラフィック
   - PPTP トンネルトラフィック
   - SSL VPN トンネルトラフィック

3. 照合する認証ルールがない場合は、IP ルールセットで許可されている限りは接続を許可し、認証プロセスは終了します。

4. 最初に一致した認証ルールの設定に基づき、NetDefendOS はユーザ名 / パスワードのペアの入力を要求する認証リクエストをユーザに知らせます。

5. NetDefendOS は認証ルールが指定した認証ソースに照らしてユーザの資格を確認します。この認証ソースは、NetDefendOS 内のローカルデータベース、または外部の RADIUS データベースサーバのいずれかになります。

6. NetDefendOS は、認証が成功している限りこの接続のトラフィックを許可し、要求されるサービスは IP ルールセットのルールに従って許可されます。そのルールの送信元ネットワークオブジェクトは、使用可能な「定義証明書なし」のオプションが有効であるか、あるいはグループと関連付けられていて、ユーザもそのグループのメンバとなっています。

7. 認証ルールでタイムアウト制限を指定した場合、認証ユーザは、規定時間アクセスがない時には自動的にログアウトされます。

認証に失敗した IP アドレスからのパケットはすべて廃棄されます（別のルールに従っている場合は除く）。

9.2 認証設定

9.2.1 設定の概要

以下のリストは NetDefendOS におけるユーザ認証設定の手順をまとめたものです。

- それぞれ 1 つのユーザ名 / パスワードの組み合わせを持つユーザのデータベースから成る認証ソースを設定します。以下のいずれかが認証ソースになることができます。
  - NetDefendOS 内のローカルユーザデータベース。
  - D-Link ファイアウォール外部の RADIUS サーバ。
  - ファイアウォール外部の LDAP サーバ。

- ファイアウォールを通過するどのトラフィックが認証されるか、またどの認証ソースが認証を実行するのに使用されるか、を記載した認証ルールを定義します。「9.2.5 認証ルール」を参照してください。

- 必要に応じて、認証するクライアントの IP アドレスを IP オブジェクトに定義付けします。これを、Originator IP として直接認証ルールに関連付けるか、または認証グループに関連付けることができます。

- 前述の手順で設定した IP オブジェクトに属するクライアントが、認証を受け、リソースにアクセスするのを許可する IP ルールを設定します。

以下のセクションでは、詳しくこれらの手順の構成要素について記述します。

- 「9.2.2 ローカルデータベース」
- 「9.2.3 外部 RADIUS サーバの設定」
- 「9.2.4 外部 LDAP サーバ」
- 「9.2.5 認証ルール」

9.2.2 ローカルデータベース

ローカルユーザデータベースは NetDefendOS に実装されたレジストリで、認可ユーザとユーザグループのプロファイルを含んでいます。セキュリティに可逆暗号を使用して、パスワードが保存されている状態で、ユーザ名 / パスワードの組み合わせをこれらに入力することができます。初期値では、AdminUsers と呼ばれる 1 つのローカルユーザデータベースが存在しています。管理者は必要に応じて追加のデータベースを作成することができます。

ユーザ名 / パスワードの長さの制限

ローカルユーザデータベースの各ユーザにはそれぞれユーザ名 / パスワードが設定され、その長さには以下の制限があります。

- ユーザ名の最大文字数：31 文字
- パスワードの最大文字サイズ：72Bytes

パスワードの最大文字サイズは文字数ではなくバイトで示されていることに注意してください。特殊記号は 72 Bytes 中、2Bytes まで使用可能であるためです。

例題 9.1

ローカルユーザデータベースを作成します。

この例題では、新しいユーザデータベース lan_users を作成する方法を示しています。

CLI

```
DFL-xxxx:/> add LocalUserDatabase lan_users
```

Web Interface

1. **System > Device > Local User Databases > Add > LocalUserDatabase** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: lan_users
   - Comments: lan auth group
3. 「OK」ボタンをクリックします。

グループメンバシップ

ローカルデータベースに追加された各 User オブジェクトは、オプションで、1 つ以上の認証グループのメンバになるように指定されます。User オブジェクトの Group プロパティに 1 つ以上のグループ名を指定することによって、認証グループのメンバになるように設定します。

2 つのグループだけが NetDefendOS で既に定義されおり、グループ名 administrators と auditors を持っています。これらのグループに与えられた特権は、後のセクションで説明されます。新しいグループは個別のオブジェクトとして明示的には作成されません。代わりに、グループ名がユーザに関連付けられる時に、暗黙的に作成されます。管理者が作成したグループ名には、以下の制限があります。

- グループ名は、大文字と小文字を区別する文字列として入力され、最大 128 文字の長さを持つことができます。
- グループ名に使用できない文字はスペースとカンマです。
- グループ名の番号における唯一の制限は、128 文字から作成されるユニークな組み合わせの番号であることです。
- ユーザが複数のグループのメンバである場合、グループ名はカンマで区切って入力します。例 : group1,group2,group3

例題 9.2

グループメンバシップにユーザを追加する

この例題では、新しいユーザをローカルデータベース lan_users に追加する方法を示しています。ユーザ名は myusername でパスワード myuserpassword、2 つのグループ groups lan_group と employees のメンバシップを持つようにします。

CLI

ローカルデータベースになるように CLI コンテキストを変更します。

```
DFL-xxxx:/> cc LocalUserDatabase lan_users
```

今度は、このデータベースにユーザを追加します。

```
DFL-xxxx:/lan_users> add User myusername Password=myuserpassword Groups=lan_group,employees
```

ユーザを追加した後は必ず、コンテキストをデフォルトに変更します。

```
DFL-xxxx:/lan_users> cc
DFL-xxxx:/>
```

Web Interface

1. **System > Device > Local User Databases** の順にメニューをクリックします。
2. lan_users を選択します。
3. Users を選択し、**Add > User** をクリックします。
4. 以下の情報を入力します。
   - Name: myusername
   - Password: myuserpassword
   - Confirm Password: myuserpassword
   - Groups: lan_group,employees
5. 「OK」ボタンをクリックします。

Administrators と Auditors グループメンバシップ

新しいユーザを定義する時、オプションで以下のデフォルトグループの 1 つにメンバシップを付与することができます。

- **Administrators グループ**
  このグループのメンバは、Web インタフェースおよびリモート CLI を通じて NetDefendOS にログインし、NetDefendOS のコンフィグレーションを編集できます。管理者権限では 1 度に 1 つのユーザしかログインすることはできません。（1 人の管理者が 1 つ以上の同時セッションにログインすることはできます。）
- **Auditors グループ**
  これは、Administrators グループに似ていますが、メンバはコンフィグレーションデータを参照できるだけで、それを変更することはできません。複数の audit ユーザは同時にログインすることができます。

IP ルールセットと共にグループを使用する

認証グループは、Authentication Rule オブジェクトと一緒に直接は使用されませんが、代わりに接続を許可する IP ルールセットのエントリに使用される送信元ネットワークまたは送信先ネットワーク IP オブジェクトに関連付けることができます。

IP ルールセットのエントリに送信元ネットワークを指定する場合、ユーザ定義の IP オブジェクトを使用し、その IP オブジェクトに Authentication Group プロパティを関連付けることができます。これは、IP ルールセットのエントリが、送信元ネットワークに関連するグループに所属するログイン中のクライアントにだけ適用されることを意味します。

あるいは、認証サーバだけがクライアントに利用可能となるように、送信先ネットワークを使用することも可能です。サーバの認証は、まるでサーバがクライアントであるかのように一度 NetDefendOS に単独で接続をオープンすることで行われます。

いずれの場合も、特定のグループのメンバにのみ適用される IP ルールセットのエントリを設定することで、指定ネットワークへのアクセスを制限することができます。リソースへのアクセスを得るために、それを許可する IP ルールセットのエントリが存在する必要があります。また、クライアントは Source Network または Destination Network address オブジェクトに指定したのと同じグループに所属する必要があります。

グループメンバシップを使用したユーザ認証の設定例については、本セクションで後述する「Web アクセスのためのユーザ認証設定」を参照してください。

PPTP/L2TP 構成

クライアントが PPTP/L2TP を使用して D-Link ファイアウォールに接続している場合、以下の 3 つのオプションを、ローカルの NetDefendOS ユーザデータベースに指定することができます。

- **Static Client IP Address**
  これは、クライアントが認証される場合に持つ必要があるIPアドレスです。指定しないと、ユーザはどんなIPも持つことができます。このオプションは固定 IP アドレスを持つユーザのために特別なセキュリティを提供します。
- **Networks behind user**
  ネットワークがこのユーザに指定されると、そのユーザが接続する場合に、そのルートは自動的に NetDefendOS の「main」ルーティングテーブルに追加されます。この追加されたルートの存在は、指定したネットワークに向かうどんなトラフィックも、ユーザの PPTP/L2TP トンネルを通じて正しく送信されることを意味します。

  ユーザへの接続の終了時に、このルートは NetDefendOS によって自動的に削除されます。

注意 慎重にネットワークオプションを使用してください。

管理者は、このオプションを使用した結果がどうなるかを慎重に考える必要があります。例えば、このオプションを「all-nets」に設定すると、すべてのインターネットトラフィックが場合によってはトンネル経由でこのユーザに送られます。

- **Metric for networks**
  ユーザオプションの背後にあるネットワークが指定される場合、これは、NetDefendOS によって自動的に追加されるルートに使用されるメトリックです。同じネットワークに一致する 2 つのルートがあると、このメトリックが、どれを使用すべきであるかを決定します。

注意 他の認証ソースは PPTP/L2TP オプションを持っていません。

SSH 公開鍵の指定

PPTP/L2TP クライアントで、ユーザ名とパスワードを指定する代替手段として、しばしば鍵を使用します。以前にアップロードされた NetDefendOS SSH Client Key オブジェクトを選択することによって、ローカルデータベースユーザに秘密鍵を指定できます。

ユーザが接続する場合、ユーザの識別子を検証するためにクライアントによって使用された鍵の自動チェックがあります。一度が確認されると、ユーザがユーザ名とパスワードを入力する必要はなくなります。

この機能を使用するためには、最初に、関連する SSH Client Key オブジェクトを NetDefendOS に個別に定義する必要があります。クライアントキーは Web インタフェースの Key リング内でオブジェクトタイプとして検出されます。定義にはクライアンが使用するキーのペアのためにパブリックキーファイルのアップロードが必要です。

9.2.3 外部 RADIUS サーバの設定

外部サーバを使用する理由

管理作業負担がより大きくなる大規模なネットワークトポロジにおいては、専用サーバに 1 つの中央データベースがあることが望ましいと思われます。ネットワーク内に 1 つ以上の D-Link ファイアウォールと何千ものユーザがいる場合、個々のデバイスの認証データベースを別々に管理することは問題が多くなります。その代わりに、外部の認証サーバは、NetDefendOS からの要求に応じることでユーザネーム / パスワード組み合わせを検証することができます。この方法を提供するため、NetDefendOS は、RADIUS プロトコルをサポートします。

NetDefendOS を使用した RADIUS の使用

RADIUS クライアントとして動作する NetDefendOS は、指定した RADIUS サーバに RADIUS メッセージとしてユーザ証明書と接続パラメータ情報を送信します。サーバは、リクエストを処理して RADIUS メッセージレスポンスを返信し、許可または拒否します。一つ以上の外部サーバがファイアウォール内に定義できます。

RADIUS セキュリティ

RADIUS メッセージにセキュリティを提供するために、一般の共有シークレットは、RADIUS クライアントとサーバ両方に設定されます。共有シークレットは、RADIUS メッセージが RADIUS クライアントからサーバまで転送される際のユーザのパスワードの暗号化を可能にし、通常長い文字列として設定されます。（128 文字以内で、大文字と小文字を区別します。）

RADIUS は、RADIUS クライアントとサーバの間でユーザ名 / パスワードメッセージを交換するために PPP や、PAP、CHAP のような PPP 認証スキームを使用します。RADIUS 認証メッセージは、UDP ポート 1812 を経由して UDP メッセージとして送信されます。

Primary Retry Interval

認証ルールの Primary Retry Interval プロパティでは、プライマリ RADIUS サーバが無応答で、セカンダリサーバが代わりに使用された後の動作を指定します。Primary Retry Interval をゼロに設定すると、選択されたセカンダリサーバは、プライマリサーバが後で利用可能になっても、継続して使用されます。

ゼロ以外を設定すると、Primary Retry Interval プロパティは、NetDefendOS が再びプライマリサーバに接続を試みる前の待機する時間（秒）として設定されます。これらの再試行は無期限に続きます。プライマリサーバが利用可能になると、NetDefendOS は直ちにセカンダリからプライマリに戻します。

ソース IP の設定

初期値では、Source IP プロパティは自動に設定されており、ファイアウォールの送信側インタフェースの IP アドレスが、RADIUS サーバに送信されるトラフィックの送信元アドレスとして使用されます。このプロパティを Manual に設定すると、特定の送信元 IP アドレスをサーバに送信されるトラフィックに使用できます。

送信元 IP アドレスが指定される場合、管理者は、送信側インタフェースに IP アドレスを ARP パブリッシュするように手動で NetDefendOS を設定する必要があります。設定方法については「3.5.3 ARP パブリッシュ」で説明しています。

グループのサポート

RADIUS 認証はユーザ用にグループの指定をサポートしています。これは、ユーザが Administrators または Auditors グループに所属するように指定できることを意味します。

注意 RADIUS Vendor ID をグループメンバシップに設定してください。

サーバを設定する場合、RADIUS サーバがグループメンバシップを送信するのに必要であるなら、ユーザグループのベンダの特定の属性ベンダを使用することが必要です。NetDefendOS Vendor ID は 5089 で、ユーザグループは vendor-type 1 として文字列タイプの値で定義されます。

IPv4 と IPv6 のサポート

NetDefendOS で設定する RADIUS サーバの IP アドレスは、IPv4 と IPv6 どちらでも設定可能です。

自動 IP アドレス割り当て

ローミングクライアント用の IPsec、L2TP、および PPTP トンネルでは、NetDefendOS が RADIUS 認証プロセスの一部分として自動的に IP アドレスを割り当てることができます。

設定方法によってはオプションで、クライアントを認証する時、RADIUS サーバは、Access-Accept メッセージに IP アドレス情報を入れて NetDefendOS に返すことができます。
NetDefendOS は RADIUS の Accept-Access メッセージで自動的に以下のパラメータを認識して、使用します。

項目	説明
Framed-IP-Address	トンネルネゴシエーションの一部分として NetDefendOS が接続クライアントに自動的に送信する、クライアントに割り当てる IP アドレスです。
Framed-IP-Netmask	場合によっては、クライアントは、ネットワークを背後に持つ別のファイアウォールなどのネットワークデバイスかもしれません。Framed-IP-Netmask パラメータでは、Framed-IP-Address も Access-Accept メッセージに存在する必要があります。トンネルネゴシエーションの中でクライアントに送信されるルートを形成するために、クライアント後方のネットワークの定義として、IP アドレスと一緒にネットマスクが組み合わされます。
Framed-Route	RADIUS サーバは Framed-IP-Address と Framed-IP-Netmask の代わりにこれを送信することができます。クライアント後方のネットワークの定義として、トンネルネゴシエーションの中でルートがクライアントに送信されます。

この IP アドレス情報は自動的に以下の方法のどちらかでクライアントに送信されます。
- IPsec トンネルの IKE ネゴシエーションフェーズ
- L2TP か PPTP トンネルを設定する場合の PPP 上

さらに、NetDefendOS は、Framed-IP-Netmask パラメータと共に Framed-IP-Address、Framed-Route または Framed-IP-Address のどれかを受信する場合、自動的にルートをコンフィグレーションに追加します。このルートの自動追加は、ルートの自動追加用のトンネルオブジェクトに関連するプロパティを設定することで通常の方法で制御されます。

例題 9.3

RADIUS サーバを設定する

以下の手順は RADIUS サーバが設定される方法を例証します。NetDefendOS オブジェクトが、rs_users という名前と、アドレス帳に定義済みの radius_ip という IPv4 アドレスを持つように設定します。

接続ポートは 1812（初期値）で、共有秘密キー mysecretcode がセキュリティに使用されます。

リトライタイムアウト値の 2 は、無応答が 2 秒以上であると、NetDefendOS が認証要求を再送することを意味します。最大 3 回再試行します。

CLI

```
DFL-xxxx:/> add RadiusServer rs_users IPAddress=radius_ip SharedSecret=mysecretcode Port=1812 RetryTimeout=2
```

Web Interface

1. **Policies > User Authentication > User Directories > RADIUS > Add > RADIUS Server** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: rs_users
   - IP Address: radius_ip
   - Port: 1812
   - Retry Timeout: 2
   - Shared Secret: mysecretcode
   - Confirm Secret: mysecretcode
3. 「OK」ボタンをクリックします。

9.2.4 外部 LDAP サーバ

Lightweight Directory Access Protocol（LDAP）は、NetDefendOS で認証ソースとして使用されます。これは、D-Link ファイアウォールが 1 つのクライアントとして、1 つまたは複数の LDAP サーバに対し実行します。いずれかのサーバがダウンした場合でも冗長性を供給できるように複数のサーバを設定することができます。

LDAP 認証の設定

LDAP サーバによるユーザ認証の設定には次の 2 つのステップがあります。

- NetDefendOS 内に、1 つまたは複数のユーザ認証 LDAP サーバオブジェクトを定義します。

- これらの LDAP サーバオブジェクトのリストをユーザ認証ルール内に指定します。
  複数の LDAP サーバを、ユーザ認証ルール内のリストに関連付けることが可能です。リストの順番によって、サーバ接続を試みる順番が決まります。リストの 1 番目のサーバは最も高い優先度を持っており、最初に使用されます。

  認証に失敗するか、またはサーバが未到達状態であると、リストの 2 番目が使用されるというようになります。

LDAP 問題

残念ながら、LDAP 認証の設定は、RADIUS セットアップほど簡単でないかもしれません。LDAP サーバを NetDefendOS に定義する際に使用されるパラメータの慎重な検討が必要とされます。以下のような問題を引き起こす多くの問題があります。

- LDAP サーバはそれぞれ実装方式が異なります。NetDefendOS は、LDAP サーバ設定において柔軟な方法を提供しており、LDAP サーバソフトウェアの種類によっては、LDAP サーバといくつかの設定オプションを変更する必要があるかもしれません。

- PPTP または L2TP クライアントの認証には、LDAP サーバに対していくつかの管理用の変更が必要かもしれません。これについては後で説明します。

LDAP サーバとしてのマイクロソフトの Active Directory

LDAP サーバとして NetDefendOS にマイクロソフトの Active Directory を設定することができます。Active Directory を使用する場合に、特別に配慮すべきこととして、NetDefendOS LDAP サーバ設定のオプション（Name Attribute）を「SAMAccountName」に設定する必要があります。

LDAP プロトコル制限のため、NetDefendOS は、Microsoft LDAP サーバからプライマリに設定された LDAP ユーザグループを受信して、セキュリティポリシーに使用することはできません。

LDAP サーバの定義

NetDefendOS 内には、複数の名前付き LDAP サーバオブジェクトを定義することができます。このオブジェクトにより、NetDefendOS はどの LDAP サーバが利用可能であるか、どのようにアクセスするかを識別することができます。

LDAP サーバによっては LDAP の仕様に正確に従っていない可能性もあるため、LDAP サーバを NetDefendOS に定義するのは簡単ではない場合もあります。また、LDAP 属性の名前が変更されるように、管理者がサーバの LDAP スキーマを変更することが可能です。

LDAP 属性

LDAP 設定を完全に理解するために、いくつかの設定値が属性であることに注意することが重要です。属性は以下の通りです。

- Name 属性
- Membership 属性
- Password 属性

LDAP 属性は属性名（本マニュアルでは、混乱を避けるために属性 ID と呼びます）と属性値から成るタプル（1 組のデータ値）です。例 : ユーザ名の ID と「Smith」の値を持っているユーザ名属性のタプル。

これらの属性は様々な場面で利用することがありますが、LDAP サーバに対するそれらの意味は、通常、サーバのデータベーススキーマによって定義されます。サーバ管理者は、通常、属性を変更するためにデータベースのスキーマを変更することができます。

一般的な設定

各サーバの設定には、以下の一般的な項目を使用します。

項目	説明
Name	NetDefendOS 内で表示するためにサーバオブジェクトにつけられる名前。例えば、NetDefendOS 認証ルールが定義され、この名前を参照するかもしれません。 この値は以下で説明する Name Attribute とは関係ありません。本項目は、LDAP サーバではなく、NetDefendOS による使用のためだけのものです。
IP Address	LDAP サーバの IP アドレス。
Port	TCP/IP を使用して送信されるクライアントの要求を受信する LDAP サーバのポート番号。初期値は 389 です。
Source IP Selection	初期値（Automatic）では、ファイアウォールの送信側インタフェースの IP アドレスは、LDAP サーバに送信されるトラフィックの送信元アドレスとして使用されます。このプロパティを Manual に設定すると、特定の送信元 IP アドレスが使用されます。 特定の送信元 IP アドレスが指定されると、管理者は、送信側インタフェースに IP アドレスを ARP パブリッシュするように手動で NetDefendOS を設定する必要があります。設定方法については「3.5.3 ARP パブリッシュ」で説明しています。 初期値は Automatic です。
Timeout	ユーザ認証を行う LDAP サーバのタイムアウト（秒）。この時間を過ぎても、要求に対しサーバから何の返答もない場合、そのサーバは切断されていると見なされます。初期値は 5（秒）です。
Name Attribute	ユーザ名を含む LDAP サーバのデータフィールドの ID。これの NetDefendOS 初期値は、多くの UNIX ベースサーバにとって正しい「uid」です。マイクロソフト Active Directory を使用する場合、必ず「SAMAccountName」に設定してください。（大文字と小文字を区別なし） Active Directory におけるユーザの詳細を参照する場合、ユーザログイン名は「Account」タブの「SAMAccountName」フィールドに定義されます。 **注意** LDAP サーバデータベースは正しい値を決定します。 これは属性のタプルであり、LDAP サーバのデータベーススキーマ定義により使用する正しい ID が決定されます。
Retrieve Group Membership	ユーザが所属するグループを LDAP サーバから検索するかどうか指定します。グループ名は、ログイン成功後、ユーザがサービスへのアクセス権を許可された場合に、しばしば使用されます。 また、本オプションを有効にした後、次に説明する Membership Attribute オプションを有効にすることができます。
Membership Attribute	Membership Attribute は、ユーザがどのグループのメンバであるかを定義します。これは、ユーザが NetDefendOS の admin または audit データベースグループに所属する方法と同じです。これはサーバのデータベーススキーマによって定義された別のタプルであり、その ID の初期値は「MemberOf」です。 マイクロソフト Active Directory では、「MemberOf」タブでユーザの詳細情報を参照することによって、ユーザが所属するグループを見つけることができます。
Use Domain Name	サーバには、認証を成功させるためにユーザ名とドメイン名の組み合わせを要求するものがあります。以下の項目から選択します。 • Do Not Use - ユーザ名の変更はありません。例 : testuser • Username Prefix - 認証時に、ユーザ名の前に「<domain name>/」を付けます。例 : myldapserver/testuser • Username Postfix - 認証時に、ユーザ名の後ろに「@<domain name>」を付け加えます。例 : testuser@myldapserver 「Do Not Use」以外を選択した場合は、後で説明する「Domain Name」パラメータオプションを必ず指定してください。 LDAP サーバの種類ごとにドメインの扱いが異なる可能性があるため、サーバ要求をチェックする必要があります。Windows Active Directory の多くのバージョンでは、Postfix オプションの使用が必要です。 OpenLDAP サーバや、多くのマイクロソフト以外の LDAP サーバを使用するとき、このプロパティを「Do not use」に設定し、次のプロパティ Combined User Name は有効とするべきです。
Combined User Name	OpenLDAP サーバを使用する場合、Use Domain Name プロパティを「Do not use」に設定し、このプロパティを有効にします。また、他のマイクロソフト以外の LDAP サーバでは、おそらく本オプションを有効にすることが必要となります。

項目	説明

Optional Attribute	Combined User Name プロパティが有効であると、サーバに送信されるオプションのテキスト属性を指定するのにこのプロパティを使用することも可能です。
	
	例えば、このプロパティを以下のように設定します。
	`ou=people`
	
	これは名前と基本のオブジェクトの間に挿入されます。例えば、属性は結果的に以下の通りとなります。
	`uid=someuser,ou=people,dc=somedomain,dc=com`

Routing Table	サーバの IP アドレスをルートに解決するためにルート検索が実行される NetDefendOS のルーティングテーブル。初期値は「main」ルーティングテーブルです。

データベース設定

データベース設定は以下の通りです。

項目	説明
Base Object	LDAP サーバ内のどこでユーザアカウントのツリー検索を開始するかを定義します。 LDAP サーバデータベースで定義されたユーザは、ツリー構造に体系付けされます。Base オブジェクトは、関連ユーザがこのツリーのどこに位置しているかを指定します。Base オブジェクトを指定すると、Base オブジェクト下のユーザだけが検証されるため、LDAP ツリーの検索を早くするという効果があります。 **注意** Base オブジェクトは正しく指定される必要があります。 Base オブジェクトが不正に指定される場合、Base オブジェクト配下のツリーの部分にユーザがいないと、ユーザは見つけられずに、認証されないことを意味します。そのため、最初にツリーのルートとして Base オブジェクトを指定することをお勧めします。 カンマで区切られた domainComponent（DC）のセットとして、Base オブジェクトを指定します。完全なドメイン名が「myldapserver.local.eu.com」であり、Base オブジェクトである場合、以下のように指定されます。 `DC=myldapserver,DC=local,DC=eu,DC=com` これで、ユーザ名検索は、「myldapserver」ツリーのルートで開始します。
Administrator Account	LDAP サーバは、検索するために接続を確立するユーザが、管理者特権を持っていることを要求します。管理者アカウントには administrator ユーザ名を指定します。このユーザ名は、前述の「Use Domain Name」と同じく、サーバによっては特別な形式を要求されるかもしれません。
Password/Confirm Password	上で指定された管理者アカウント用のパスワード。
Domain Name	LDAP サーバを動作するコンピュータのドメイン名。ドメイン名は、ユーザ名のフォーマットを構成する場合に使用されます。これは完全なドメイン名の最初の部分です。上記の例では、「myldapserver」です。完全なドメイン名は「.」（ドット）でラベルを分けて設定します。（例 : myldapserver.local.eu.com） 本オプションは、「Server Type」が「Other」以外に設定されている場合にのみ利用可能です。 本項目を空白のままとすることができますが、LDAP サーバのバインド要求時にドメイン名を要求する場合に必要となります。

オプションの設定

1 個のオプションの設定があります。

項目	説明
Password Attribute	ユーザのパスワードを含む LDAP サーバのタプルの ID を指定します。ID の初期値は「userPassword」です。 HAP や MS-CHAPv1、MS-CHAPv2 を使用した PPP 経由、または SSL VPN を使用して接続しているユーザの認証に LDAP サーバが使用されていない限り、本オプションは空白のままにします。 これらの認証に LDAP サーバが使用されている場合、本オプションによって、LDAP サーバデータベースにおける、プレーンテキストのユーザパスワードを含むデータフィールドの ID が決定されます。LDAP サーバ管理者は、このフィールドが実際にパスワードを含むことを確認する必要があります。詳しくは、後で説明します。 SSL VPN と共に LDAP を使用する場合、ユーザ認証オブジェクトの Agent オプション設定に基づいた userPassword または Description として、Password Attribute を指定する必要があります。

バインドリクエスト認証

LDAP サーバ認証は、LDAP のバインドリクエスト認証を使用して動作するように自動的に設定されます。これは、LDAP サーバへの接続が成功すれば、認証も成功するということを意味しています。個々のクライアントが他のクライアントから識別されることはありません。

LDAP サーバの照会は、バインド要求認証では起きないものですが、もし起きたとしても、照会を送信するサーバは返答されなかったものと見なされます。

LDAP サーバ応答

LDAP サーバが NetDefendOS からユーザ認証要求をクエリされると、次のような処理が発生します。

- サーバがポジティブレスポンスを返答して、そのユーザを認証する。

  CHAP、MS-CHAPv1 または MS-CHAPv2 による PPP を使用するクライアントは特別なケースであり、後ほど説明するように、認証は実際には NetDefendOS によって行われます。

- サーバがネガティブレスポンスを返答し、そのユーザを認証しない。

- サーバがサーバに指定された「Timeout」時間内に返答しない。サーバが 1 つだけ指定されている場合には認証は失敗したと考えられます。ユーザ認証ルールに定義されている別のサーバがある場合には、次のサーバにクエリを送信します。

ユーザ名はドメインを必要とする

特定の LDAP サーバでは、ユーザがユーザ名 / パスワードの組み合わせで認証を試みようとする時には、ドメイン名をユーザ名と組み合わせる必要があります。

そのドメインが「mydomain.com」であれば、「myuser」のためのユーザ名は、myuser@mydomain.com として指定される必要があります。LDAP サーバによっては、これは、myuser@domain、mydomain.com\myuser または mydomain\myuser となるかもしれません。この形式は、LDAP サーバ及びその要求に完全に依存します。

統計のリアルタイムモニタリング

ユーザ認証を行う LDAP サーバ接続のリアルタイムモニタリングでは、以下の統計情報の利用が可能です。

- 秒単位の認証数。
- 認証要求の総数。
- 認証に成功した要求の総数。
- 認証に失敗した要求の総数。
- 無効のユーザ名の総数。
- 無効のパスワードの総数。

LDAP 認証の CLI コマンド

認証に使用される LDAP サーバに対応する CLI オブジェクトは、「LDAPDatabase」オブジェクトと呼ばれます。CLI で、証明書の検索に使用する LDAP サーバは、「LDAPServer」オブジェクトと呼ばれます。

認証を行うために NetDefendOS で定義された特定の LDAP サーバを次のコマンドで表示することができます。

```
DFL-xxxx:/> show LDAPDatabase <object_name>
```

データベースのすべてのコンテンツは次のコマンドで表示することができます。

```
DFL-xxxx:/> show LDAPDatabase
```

LDAP 認証と PPP

PPTP または L2TP 接続を行うために PPP ベースのクライアントを使用する場合、CHAP、MS-CHAPv1 または MS-CHAPv2 で LDAP 認証が成功するかどうかについて、特別な配慮をする必要があります。(A) 通常の PPP 認証と (B) 暗号化を使用した PPP の 2 つの場合について、次に検証します。

A. 通常の LDAP 認証

次の図は、Webauth 認証、XAuth 認証、または PPP の PAP 認証に対する通常の LDAP 認証を示しています。ユーザ名とパスワードの「bind request」による認証が LDAP サーバに送信された後、サーバは認証を行い、「bind response」を返します。

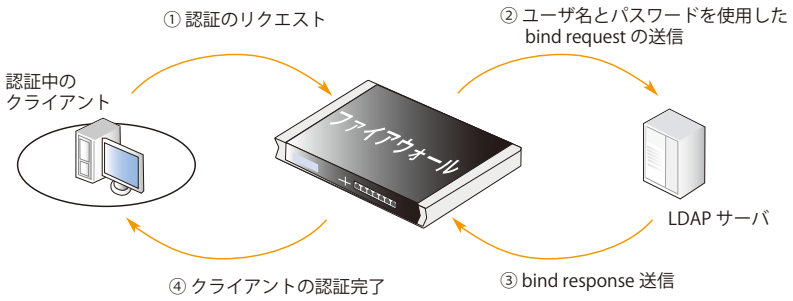


図 9-1　通常の LDAP 認証

グループメンバシップが取得される場合は、メンバシップを検索するために要求が LDAP サーバに送信された後、グループメンバシップが応答として送り返されるため、処理が異なります。

B. CHAP、MS-CHAPv1 または MS-CHAPv2 暗号化を使用した PPP 認証

認証に CHAP、MS-CHAPv1 または MS-CHAPv2 による PPP 認証が使用されている場合、クライアントは、ユーザのパスワードダイジェストを NetDefendOS に送信します。NetDefendOS はこのダイジェストを識別できないため、LDAP サーバに転送できません。これに対するソリューションは、NetDefendOS が LDAP サーバからプレーンテキストのパスワードを取得し、ダイジェスト自体を作成し、次に、クライアントのダイジェストと作成済みのダイジェストを比較することです。2 つが同じ場合は認証は成功となりますが、認証決定をするのは、LDAP サーバではなく NetDefendOS です。LDAP サーバからパスワードを検索するために、以下の 2 つが必要です。

- Password Attribute パラメータが、サーバを NetDefendOS に定義する場合に指定される必要があります。これは、返送される際、パスワードを含む LDAP サーバのフィールドの ID となります。

  この ID は、初期パスワード属性（通常、多くの LDAP データベースの「userPassword」）とは別にする必要があります。LDAP データベースの description フィールドの使用をお勧めします。

- ID が指定されているデータベースフィールドにサーバがパスワードを返すためには、LDAP 管理者は、プレーンテキストパスワードがそこで見つけられることを確認する必要があります。LDAP サーバは、暗号化されたダイジェスト形式でパスワードを保存します。これを行う自動メカニズムを提供していないため、管理者は手動で新しいユーザを追加し、既存のユーザパスワードを変更する必要があります。

  LDAP サーバ上でプレーンテキスト形式としてパスワードを危険にさらされるのと同様に、この点も、明らかに管理者による何らかの努力が明確に必要となります。これらは、LDAP が有効な CHAP、MS-CHAPv1 または MS-CHAPv2 による PPP 認証ソリューションとしては参照されない理由の 1 つです。

NetDefendOS は、クライアントからパスワードダイジェストを受け取ると、LDAP サーバへ「Search Request」の送信を開始します。サーバは、ユーザのパスワードやグループメンバシップを含む「Search Response」を返答します。すると、NetDefendOS は、ダイジェストを比較することができます。以下の図にこの処理を示します。

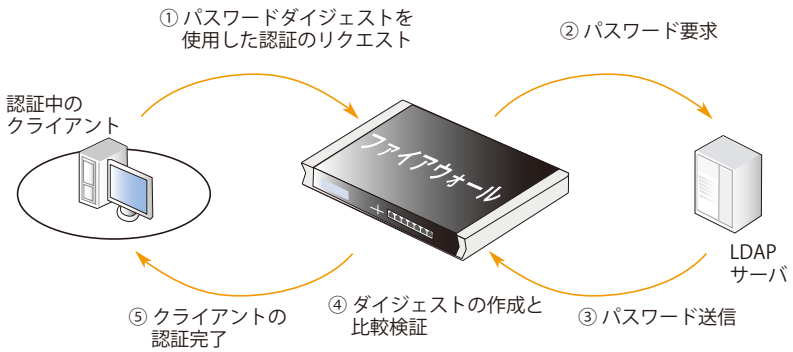


図 9-2　CHAP、MS-CHAPv1 または MS-CHAPv2 による PPP 認証と LDAP

注意 LDAP サーバとのリンクを保護する必要があります。

LDAP サーバがプレーンテキストのパスワードを NetDefendOS に返送するので、D-Link ファイアウォールとサーバとのリンクを保護する必要があります。2 つの間のリンクがローカルでないなら、VPN リンクを使用すべきです。

また、プレーンテキストにパスワードを保存する場合、LDAP サーバ自体へのアクセスを制限する必要があります。

9.2.5 認証ルール

D-Link ファイアウォールを介して接続を確立しているユーザがユーザ名 / パスワードでログインを試みる場合には、「User Authentication Rule」を必ず定義する必要があります。

認証ルールは、NetDefendOS の他のセキュリティポリシーと似た方法で設定され、ルールの対象となるトラフィックを指定することで設定されます。これは、認証されたクライアントのネットワークやインタフェースの送信先にではなく送信元に注目する他のポリシーとは異なっています。

認証ルールプロパティ

認証ルールオブジェクトには以下のような設定値があります。

項目	説明
Authentication Agent（認証エージェント）	認証されるトラフィックのタイプを指定します。 • ARPCache - クライアントのインタフェースの MAC アドレスを認証用に RADIUS サーバに送信します。どのトラフィックタイプにも適用できます。 本オプションの詳細は、「9.2.7 MAC 認証」を参照してください。 • HTTP - Web 事前定義、またはカスタムの Web ページ経由で認証される HTTP Web 接続（詳細は「HTTP 認証」を参照）。また、クライアントに core へのアクセスを許可する IP ルールがこのエージェントタイプで必要とされます。ARP 認証はこのオプションを使用して行われます。詳しくは、「9.2.7 MAC 認証」を参照してください。 • HTTPS - Web 事前定義、またはカスタムの Web ページ経由で認証される HTTPS Web 接続（詳細は以下の「HTTP 認証」を参照）。また、クライアントに core へのアクセスを許可する IP ルールがこのエージェントタイプで必要とされます。 • XAuth - IPsec を使用した VPN トンネルの確立の一部として使用される IKE 認証方式です。これは、通常の IKE を拡張したものであり、通常の IPsec セキュリティを強化します。VPN にアクセスするクライアントはログインに際しユーザ名とパスワードを提供する必要があります。 エージェントとして XAuth 認証を使用したルールは、すべての IPsec トンネルに使用されるので、インタフェース値は XAuth 認証ルールを使用して入力されないことにご注意ください。しかし、このアプローチでは、すべてのトンネルにはただ 1 つの認証ソースを使用するものと仮定しています。クライアントに core へのアクセスを許可する IP ルールを必要としません。 • L2TP/PPTP/SSL VPN - L2TP、PPP、または SSL VPN 認証に特に使用されます。クライアントに core へのアクセスを許可する IP ルールセットのエントリを必要としません。また、このエージェントタイプでは認証ルールの PPP Agent オプションを変更することができます。初期値では、PAP、CHAP、MS-CHAP、MS-CHAPv2 オプションが有効化され、Allow no authentication オプションは無効化されています。SSL VPN では PAP オプションのみを有効とするべきです。 • EAP - IPsec トンネル確立の際に使用される IKEv2 認証方式です。IPv4 または IPv6 のクライアント IP アドレスを認証します。Originator IP および Terminator IP は、既に関連する IPsec Tunnel オブジェクトで Local Endpoint/Remote Endpoint として定義済みであるため、この方式では設定しません。クライアントに core インタフェースへのアクセスを許可する IP ルールセットのエントリが必要です。
Authentication Source	認証ソースを指定します。 • LDAP - ユーザは外部の LDAP サーバデータベースで検索されます。 • RADIUS - 外部の RADIUS サーバが検索に使用されます。 • Disallow - このルールを始動するすべての接続を明示的に禁止します。 本ルールは、認証ルールセットの最後に設定するのがよいとされます。 • Local - NetDefendOS に定義されたローカルデータベースがユーザ証明書の検索に使用されます。 • Allow - このルールを始動するすべての接続が自動的に認証されます。データベース索引は起こりません。
Interface	認証される通信が到達する送信元インタフェース。このプロパティは必須であり、ルールとインタフェースの対応付けを行います。XAuth または EAP ソースでは、インタフェースが IPsec トンネル名となります。ルールをすべてのインタフェースに紐づけるために any を指定することも可能です。
Originator IP	新しい接続が到達する送信元 IP またはネットワーク。PPP の場合、これは Originator IP になります。XAuth または EAP のルールでは、IPsec トンネルの Local Endpoint となるため指定されません。
Terminator IP	新しい接続が到達する送信先ネットワーク。Authencation Agent が PPP（L2TP/PPTP/SSL VPN）の場合のみ指定します。XAuth または EAP のルールでは、IPsec トンネルの Remote Endpoint となるため指定されません。

接続タイムアウト

認証ルールはユーザセッションに関連する以下のタイムアウトを指定することができます。

項目	説明
アイドルタイムアウト	自動的にタイムアウトになるまで、アイドル状態になる時間（初期値は 1800 秒）。
セッションタイムアウト	最大接続時間（初期値は設定なし）。

認証サーバを使用する場合、サーバから値をセットするように Use timeouts received from the authentication server を有効化することができます。

複数のログイン

認証ルールでは、異なる送信元 IP アドレスから複数のユーザが同じユーザ名でログインしようとした場合、どのようにその複数ログインを処理するかを指定できます。可能なオプション項目は以下の通りです。

- Allow multiple logins per username - 1 ユーザあたり複数のログオンを許可する。
- Allow one login per username, disallow the rest. - 1 ユーザあたり 1 つのログオンだけを許可する。
- Allow one login per username, disallow the rest without any exception. (strict) -
  IKE Rekey 処理を実行する IKEv1 IPsec クライアントの特定シナリオに対応したオプションです。クライアントソフトウェアによっては、Rekey によってクライアントがログアウトされず、NetDefendOS は同じユーザ名による 2 つ目の認証が実行されたと認識します。1 つ前のオプションでは、これが許可されます。本オプションでは、クライアントがログアウトしない限り、同じ認証情報による IKE Rekey 後の認証を許可しません。
- Allow one login per username, Replace existing user if idle for more than: 10 seconds -
  ユーザ毎に 1 つのログオンを許可する。同じユーザ名による 2 つ目オンログイン試行は、1 つ目のユーザがログアウトすると成功します。これは、指定期間アイドル状態であると発生します。アイドル時間の初期値は 10 秒であり、変更することも可能です。

9.2.6 HTTP 認証

このドキュメントにおける HTTP Authentication という用語は HTTP/HTTPS プロトコル両方に関連する認証を指しています。ユーザが HTTP または HTTPS プロトコルを使って Web ブラウザで接続している場合は、NetDefendOS はユーザに HTML 形式のページを示し、必要なユーザ情報を入力させて認証を行います。これは WebAuth とも呼ばれます。HTTP/HTTPS 認証の設定には他にもいくつかの検討事項があり、それらについて本セクションで説明します。

管理 Web インタフェースポートの変更の必要性

HTTP 認証は、同じく初期値で TCP ポート 80（HTTP）、TCP ポート 443（HTTPS）を使用する Web インタフェースのリモート管理サービスと衝突します。この問題を避けるため、認証を設定する前に Web インタフェースポート番号を変更する必要があります。WebUI のメニューで **System > Remote Management > Advanced settings** の順にクリックして、WebUI HTTP ポートと WebUI HTTPS ポートの設定を変更してください。例えば、HTTP ポートを 81 に変更することが可能です。

HTTP と HTTPS エージェントオプション

HTTP および HTTPS 認証について、認証ルール内にはエージェントオプションと呼ばれる一連のオプションがあります。これらは以下の通りです。

- ログインタイプ - 以下のいずれかに設定できます。
  - HTML form - ユーザにデータを記入する認証用の HTML 形式のページを提示し、そのデータをポストと共に NetDefendOS に返信します。NetDefendOS で事前定義されている HTML を使用できますが、後で説明するようにカスタマイズすることもできます。

  - BASIC authentication - 401 認証要求メッセージをブラウザに送り返し、組み込みのダイアログによりユーザにユーザ名 / パスワードの組み合わせを要求します。ブラウザのダイアログに示す領域の文字列は任意に指定することができます。

    ブラウザがログオンデータをキャッシュに保持してしまうことがあるので、いくつかの場合では、BASICAUTH より HTML form を使うことをお薦めします。

  - MAC authentication - 認証はログイン画面なしで HTTP と HTTPS クライアントに対して実行されます。代わりに、接続クライアントの MAC アドレスがユーザ名として使用されます。パスワードは、MAC アドレスまたは特定の文字列です。

    MAC 認証については「9.2.7 MAC 認証」で詳しく説明します。

- Agent が HTTPS に設定されている場合、既に NetDefendOS にロードされている証明書リストからホスト証明書とルート証明書を選択する必要があります。証明書チェーンはルート証明書のためにサポートされます。

IP ルールの必要性

認証の実行を明白に許可するルールを IP ルールセットに追加しておかないと、HTTP 認証は作動しません。これは HTTPS の場合も同様です。ローカルネットワーク lannet の多数のクライアントが、wan インタフェース上の外部のインターネットに頻繁にアクセスする場合を想定しているならば、IP ルールセットには以下のルールが必要です。

#	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
1	Allow	lan	lannet	core	lan_ip	http-all
2	Allow/NAT	lan	trusted_users	wan	all-nets	http-all
3	Allow/NAT	lan	lannet	wan	all-nets	dns-all

最初のルールでは、認証プロセスの実行を許可し、ローカルネットワークが接続する D-Link ファイアウォール上のインタフェースの IP アドレスである lan_ip IP アドレスに、クライアントがアクセスしようとしていると想定しています。

2 番目のルールでは、通常のネットサーフィンは許可されますが、lannet からの認証されていないクライアントにはすべてルールが適用されるので、lannet をソースネットワークとして使用することはできません。代わりに、送信元ネットワークは、trusted_users と呼ばれる、管理者が定義した IP オブジェクトであり、これは lannet と同じネットワークですが、さらに認証オプション「定義証明書なし」が有効になっているか、または、認証グループ（ユーザに割り当てられたグループと同じグループ）が割り当てられています。

3 番目のルールでは、DNS に URL の検索を許可します。

注意 上の IP ルールにおけるデフォルト http-all サービスを変更しないでください。認証の失敗を引き起こす可能性があります。

ユーザをログインページに誘導する

この設定では、認証されていないユーザが lan_ip 以外の IP にネットサーフィンを試みた場合、ルールによって認証が失敗し、パケットは破棄されます。これらのユーザに常に認証ページを表示するには、SAT ルールと関連した Allow ルールを追加しなければなりません。ルールセットは以下のようになります。

#	アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
1	Allow	lan	lannet	core	lan_ip	http-all
2	Allow/NAT	lan	trusted_users	wan	all-nets	http-all
3	Allow/NAT	lan	lannet	wan	all-nets	dns-all
4	Allow/SAT	lan	lannet	wan	all-nets all-to-one 127.0.0.1	http-all

SAT ルールでは、認証されていないリクエストをすべて捉えますが、そのリクエストを core（NetDefendOS 自身）に相当するアドレス 127.0.0.1 に導くよう、オールツーワンアドレスマッピングの設定が必要です。

例題 9.4

Web アクセスのためのユーザ認証設定

以下のコンフィグレーションファイルでは、lannet のユーザグループの lan_group に対して HTTP ユーザ認証を有効にする方法を示しています。IP ルールに定義されている場合、グループユーザに所属するユーザだけが、認証後に Web 検索サービスを得ることができます。
lannet、users、lan_ip、ローカルのユーザデータベースフォルダ「lannet_auth_users」、および認証アドレスオブジェクト「lannet_users」が指定されているものとします。

認証 IPv4 アドレスオブジェクト lan_users_net が定義されて、lan_group に設定された Groups プロパティを持っているものとします。グループ lan_group は、lan_users データベース内の個人ユーザの Groups プロパティとして使用されています。

CLI

手順 A 認証を許可する IP ポリシーを設定する：

```
DFL-xxxx:/> add IPPolicy Name=http_auth SourceInterface=lan SourceNetwork=lannet DestinationInterface=core
            DestinationNetwork=lan_ip Service=http-all Action=Allow
```

手順 B 認証ルールを設定する：

```
DFL-xxxx:/> add UserAuthRule Name=http_auth AuthSource=Local Interface=lan OriginatorIP=lannet LocalUserDB=lan_
            users LoginType=HTMLForm
```

手順 C 認証ユーザがインターネットを閲覧できるように IP ポリシーを設定する：

```
DFL-xxxx:/> add IPPolicy Name=allow_http_auth SourceInterface=lan SourceNetwork=lan_users_
            net DestinationInterface=wan DestinationNetwork=all-nets Service=http-all Action=Allow
            SourceAddressTranslation=NAT NATSourceAddressAction=OutgoingInterfaceIP
```

Web Interface

手順 A 認証を許可する IP ポリシーを設定する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。
- Name: http_auth
- Action: Allow
- Service: http-all
- Source Interface: lan
- Source Network: lannet
- Destination Interface core
- Destination Network lan_ip

手順 B 認証ルールを設定する :

1. **Policies > User Authentication > Authentication Rules > Add > User Authentication Rule** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。
- Name: HTTPLogin
- Authentication Agent: HTTP
- Authentication Source: Local
- Interface: lan
- Originator IP: lannet
- Local User DB : lannet_auth_users
- Login Type : HTML form

手順 C 認証ユーザがインターネットを閲覧できるように IP ポリシーを設定する :

1. **Policies > Firewalling >Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: allow_http_auth
- Action: ALLOW
- Source Interface: lan
- Source Network: lan_users_net
- Destination Interface :wan
- Destination Network :all-nets
- Service: http-all

3. Source Translation で以下の情報を入力します。
- Address Translation: NAT
- Address Action: Outgoing Interface IP

4. 「OK」ボタンをクリックします。

9.2.7 MAC 認証

ARP 認証（MAC 認証とも呼ばれる）は接続クライアントのイーサネットインタフェースの MAC アドレスに基づく認証です。管理者が特定デバイスに対してアクセスを簡単にしたい場合にこれは便利であり、ユーザは証明書を入力する必要がなくなります。NetDefendOS は、接続クライアントの MAC アドレスを RADIUS または LDAP サーバに送信します。RADIUS または LDAP サーバは、データベースを検索してクライアントが認証済みであるか否かを NetDefendOS に伝えます。（ARP 認証にローカルのデータベースを使用することはサポートしていません。）

2 つの方法のいずれかで ARP 認証を設定できます。

- **HTTP または HTTPS トラフィックのみ**
  HTTP または HTTPS に設定された Authentication エージェントを持つ認証ルールでは、Agent Options 下の Login タイプを MAC authentication に設定します。

- **ARP Cache を使用する任意のトラフィックタイプ**
  認証ルールの Authentication agent を ARPCache に設定し、Authentication Source を RADIUS または LDAP に設定します。

  前の方式と異なり、これは、どんなトラフィックにも使用できますが、次に説明される更なる手順を必要とする欠点を持っています。

  Authentication Source が Allow に設定されると、すべてのユーザがデータベースの参照なしで自動的に認証されることに注意してください。これを行う唯一の利点は、Web インタフェースで **Status > Run-time Information > User Authentication** の順にメニューをクリックすることで管理やユーザのログインリストを簡単に参照できることです。

ARP キャッシュ方式を使用した他の手順

ARP キャッシュ方式を使用している場合、認証成功のために必要とされるデータを NetDefendOS ARP キャッシュが持つように、管理者が行う別のコンフィグレーションの手順があります。

- Reject 機能を持つ Allow または NAT IP ルールの下に 2 番目の IP ルールを持つ必要があります。これは、まだ認証されていないクライアントが ARP キャッシュに MAC アドレスをおくのを確実にします。2 番目のルールが存在しないと、認証は正常に動作しません。

- 例えば、ARP キャッシュ更新の間隔は、低い値で調整されるべきです。そうすることで、アイドルタイムアウトによって一時的に接続が切断された際に、キャッシュが妥当な時間内に更新されるようになります。ARP の高度な設定の ARP Expire を小さくすることで行います。

  接続にアイドルタイムアウトが起こると、キャッシュが更新されるまで、影響を受けるクライアントは再びログインできません。ARP Expire 設定の許容値はネットワークのサイズに基づいて決定する必要があります。大規模なネットワークほど高い値を必要とする可能性があります。ARP Expire 設定は接続タイムアウト設定より低くする必要があります。

サーバに MAC アドレスを送信する

上記の ARP 認証の両方の方式では、NetDefendOS は、クライアントを認証するのに RADIUS または LDAP サーバを使用します。サーバと通信する時、NetDefendOS はユーザ名として常に MAC アドレス自体を送信します。

初期値では、サーバに送信されるパスワードは、クライアントの MAC アドレスです。しかし、これは、認証ルールオブジェクトの MAC Auth Secret プロパティを設定することによって、特定のパスワードに変更することができます。

サーバに MAC アドレスを指定する

認証サーバのデータベースに MAC アドレスをテキストで入力します。このテキストは、NetDefendOS が送信する形式に従う必要があります。これは 16 進数の小文字 2 文字ごとにハイフン「-」文字で区切られたものが 6 個連続するものです。例題は以下の通りです。

```
00-0c-19-f9-14-6f
```

コピーした MAC アドレスに対処する

ファイアウォールと接続するクライアントの間にルータがあると、NetDefendOS はオリジナルのクライアント MAC アドレスの代わりにルータから同じ MAC アドレスを受信します。初期値では、NetDefendOS は、クライアントが MAC アドレスをコピーすることを許可しないように設定されるため、問題となります。

この問題は、関連する認証ルール用のプロパティ「Allow clients behind router to connect」を有効にすることで解決されます。

9.3 認証 HTML ページのカスタマイズ

ユーザ認証では、HTML ファイルセットを使用して認証プロセスの間ユーザに情報を表示することができます。HTTP 認証処理には以下のオプションが利用可能です。

- ユーザがブラウザを使用して Web ページを開こうとすると、ログインページ（「FormLogin」ページ）に接続します。ログインに成功した後、ユーザは元々要求したページに接続されます。

- ログインに成功した後、ユーザを指定した Web ページに接続させることができます。

- ログインに成功した後、ユーザは、特定の Web ページ（「LoginSuccess」ページ）に接続され、その後自動的に元々要求したページに再接続されます。

HTTP バナーファイル

「HTTP banner files」と呼ばれる Web ページファイルは、NetDefendOS 起動時に初期状態で NetDefendOS 内に既に保存、格納されています。これらのファイルは、Web インタフェース内で直接編集を行うか、SCP クライアント経由でダウンロードして再度アップロードを行い、特定のインストールの要望に合うようカスタマイズすることができます。

NetDefendOS のバナーファイルには以下の 2 つのタイプがあります。
- WebAuth を使用した認証ルールのためのバナー（HTTP および HTTPS ログイン）。これらは以下に説明します。
- HTTP ALG のバナーファイル。詳しくは、「6.2.5 WCF HTML ページのカスタム」を参照してください。

Web 認証用のバナーファイル

Web 認証で編集可能なファイルは次の通りです。
- FormLogin
- LoginSuccess
- LoginFailure
- LoginAlreadyDone
- LoginChallenge
- LoginChallengeTimeout
- LoginSuccess
- LoginSuccessBasicAuth
- LogoutFailure
- FileNotFound

バナーファイルのカスタマイズ

Web インタフェースでは、ファイルをダウンロードして編集した後、NetDefendOS に編集した HTML をアップロードする簡単な方法を提供しています。以下に説明するこの方法の詳細は、「6.2.5 WCF HTML ページのカスタム」で詳しく記述されています。

カスタマイズを行うには、まず新しい名前で「Auth Banner Files」オブジェクトを作成する必要があります。この新しいオブジェクトは自動的に「Default」の「Auth Banner Files」内のすべてのファイルを含みます。その後これらの新しいファイルを編集して NetDefendOS にアップロードして戻すことができます。元々の「Default」オブジェクトを編集することはできません。以下の例題はカスタマイズの手順です。

HTML ページパラメータ

WebAuth の HTML ページには、以下の通り多くのパラメータがあります。

項目	説明
%CHALLENGE_MESSAGE%	問われた質問。
%IPADDR%	ブラウズを行った IP アドレス。
%ERRORMSG%	接続が拒否された理由。
%USER%	入力したユーザ名。
%REDIRHOST%	要求されたホストの IP。
%REDIRURL%	要求されたホストのパス。
%REDIRURLENC%	URL の暗号化パス。
%IPADDR%	クライアントの IP。
%DEVICENAME%	認証ファイアウォール名。

ARP 認証を使用した LoginFailure ページ

ARP 認証（MAC 認証）による認証に失敗すると、%USER% パラメータには要求側クライアント（または、最もファイアウォールに近いルータの MAC アドレス）の MAC アドレスが含まれます。

ARP アドレス認証を使用する場合、「LoginFailure」ページの典型的なパラメータセットは以下の通りです。

```
USER: 00-0c-19-f9-14-6f
REDIRHOST: 10.234.56.71
REDIRURL: /testing?user=user&pass=pass
REDIRURLENC: %2ftesting%3fuser%3duser%26pass%3dpass
IPADDR: 10.1.6.1
DEVICENAME: MyGateway
```

「%REDIRURL%」パラメータは削除されない

バナー Web ページには必ず「%REDIRURL%」パラメータが表示されます。これは、元々要求された URL のプレースホルダで、その後、認証されていないユーザにユーザログイン画面を表示します。認証が成功すると、ユーザはこのパラメータによって保持されていた URL に再接続されることになります。

「%REDIRURL%」パラメータだけがこの内部的な目的を持っているので、このパラメータは Web ページから削除すべきではなく、また使用されている場合は必ず「FormLogin」ページに表示されます。

例題 9.5

コンテンツフィルタリング HTTP バナーファイルを編集する

この例題では、「URLforbidden」HTML ページのコンテンツを編集する方法を示します。

Web Interface

1. **System > Advanced Settings > HTTP Banner Files > Add > Auth Banner Files** の順にメニューをクリックします。

2. 名前を入力し、「OK」ボタンをクリックします。
   - Name : new_forbidden

3. 新しいバナーファイル設定用タブで、以下の情報を入力し、「Save」ボタンをクリックします。

◇ **Edit & Preview タブ**

< 入力例 >

Edit
- Page : FormLogin
- FormLogin ページのテキストボックスに表示される HTML ソースを編集します。
- 「Save」ボタンをクリックすると、変更が保存されます。

Preview
- 「Preview」ボタンをクリックすると、レイアウトをチェックすることができます。

4. 「OK」ボタンをクリックし、編集を終了します。

バナーファイルの登録

1. **Policies > User Authentication > Authentication Rules** の順にメニューをクリックし、関連する認証ポリシー を選択します。

2. Agent Option タブを選択します。

3. HTTP Banners オプションに my_banner を設定します。

4. 「OK」ボタンをクリックします。

5. **Configuration > Save and Activate** をクリックし、新しいファイルをアクティブ化します。

6. 「OK」ボタンをクリックします

新しいファイルが NetDefendOS にアップロードされます。

注意 HTML ファイルの変更を保存する必要があります。

上記の例では、1 回のセッションで複数の HTML ファイルを編集することが可能ですが、別のファイルの編集を始める前には、必ず「Save」ボタンを押して編集箇所を保存してください。

SCP を使用したアップロード

SCP を使用して新しい HTTP バナーファイルをアップロードすることが可能です。以下の手順で行います。

1. SCP を使用してオリジナルのデフォルト HTML をダウンロードすることはできないので、必ず最初にソースコードを WebUI からローカルのテキストファイルにコピー & ペーストしてから、適当なエディタを使用して編集を行ってください。

2. 編集したファイルをアップロードする新しい「Auth Banner Files」オブジェクトが必要です。オブジェクト名を「ua_html」とする場合、このオブジェクトを作成するコマンドは次のようになります。

```
DFL-xxxx:/> add HTTPAuthBanners ua_html
```

   このコマンドは、すべての「Default」の「user auth banner files」のコピーを含むオブジェクトを作成します。

3. それから SCP を使用して変更したファイルをアップロードします。オブジェクトタイプ「HTTPAuthBanner」、「FormLogin」属性の「ua_html」オブジェクトにアップロードされます。編集した「Formlogon」ローカルファイルを「my.html」としている場合、Open SSH SCP クライアントを使用したアップロードコマンドは次のようになります。

```
scp my.html admin@10.5.62.11:HTTPAuthBanners/ua_html/FormLogin
```

   SCP クライアントの使用については、「2.1.8 セキュアコピー」に詳しく説明しています。

4. 次に CLI を使用して、必ず関連するユーザ認証ルールが「ua_html」を使用できるように設定してください。ルールを「my_auth_rule」とした場合、コマンドは次のようになります。

```
DFL-xxxx:/> set UserAuthRule my_auth_rule HTTPBanners=ua_html
```

5. 通常通り、CLI コマンドの「activate」と「commit」を使用して、ファイアウォール内の変更箇所を有効にします。

9.4 認証を必要とする IP ポリシー

ユーザが NetDefendOS に認証されている場合、あるリソースにアクセスする前にユーザ認証を要求するセキュリティポリシーを IP ルールまたは IP ポリシーの形態で作成することができます。

さらに、以下のいずれかを指定することができます。

1. ユーザは、特定のユーザ名を持ちます。
2. ユーザは特定のユーザグループに所属します。
3. ユーザは認証されるだけで、ユーザ名またはグループは関連していません。

これらのオプションのいずれかを設定するのに以下を必要とします。

1. 接続するユーザの IP アドレスを含む IP アドレスオブジェクトを作成します。
2. 特定のユーザまたはグループを要求する、またはユーザが認証されるように、この IP アドレスオブジェクトに認証プロパティを設定します。
3. クライアントによるリソースへのアクセスを許可する IP ルールセットのエントリを作成し、IP ルールセットのエントリの Source Network または Destination Network プロパティに上で作成した IP アドレスオブジェクトを使用します。送信元と送信先は以下の方法で使用されます。
   - Source Network プロパティは、通常、認証クライアントからサーバ等の特定のリソースへのアクセスのみを許可するように指定されます。
   - Destination Network プロパティは、クライアントが認証サーバへのアクセスのみを許可するように通常設定されます。サーバの認証は、サーバがたとえクライアントであっても、NetDefendOS への接続を 1 度オープンすることで行われます。

例題 8.6

認証を必要とする IP ポリシー

この例題では、グループ client_group のメンバであれば、If1 インタフェースを通じて接続するクライアントが If2 インタフェースのネットワークにアクセスすることを許可する、IP ポリシーを作成する方法を示します。

CLI

認証グループ client_group の一員として接続するクライアントの IP 範囲を指定する IP4Address オブジェクトを作成します :

```
DFL-xxxx:/> add Address IP4Address client_net Address=192.168.10.10-192.168.10.255 UserAuthGroups=client_group
```

送信元ネットワークとして上で作成済みのアドレスオブジェクトを使用して、インタフェース If2 のネットワークにアクセスを許可する IP ポリシーオブジェクトを作成します。

```
DFL-xxxx:/> add IPPolicy Name=client_access_policy SourceInterface=If1 SourceNetwork=client_net
            DestinationInterface=If2 DestinationNetwork=all-nets Service=all_services Action=Allow
```

Web Interface

認証グループ client_group の一員として接続するクライアントの IP 範囲を指定する IP4Address オブジェクトを作成します :

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: client_net
   - IP Address: 192.168.10.10-192.168.10.255
   - User Authentication: client_group

3. 「OK」ボタンをクリックします。

送信元ネットワークとして上で作成済みのアドレスオブジェクトを使用して、インタフェース If2 のネットワークにアクセスを許可する IP ポリシーオブジェクトを作成します :

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: client_access_policy
   - Action: Allow
   - Service: all_services
   - Source Interface: If1
   - Source Network: client_net
   - Destination Interface: If2
   - Destination Network: all-nets

3. 「OK」ボタンをクリックします。

注意 認証アドレスオブジェクトは 1 つの使用目的だけ持っています。

認証プロパティセットと共に認証に使用される IP アドレスオブジェクトは、IP ルールセットのエントリの送信元ネットワークまたは送信先ネットワークとして使用されます。他の目的にそれらを使用できません。これは Web インタフェースによって提示される IP アドレスリストと CLI によって提供される Tab 補完の選択に反映されます。

9.5 Brute Force 保護

概要

初期値では、NetDefendOS はローカルユーザデータベースに対してユーザ名 / パスワード資格証明書の確認にかかわるどんな認証にも brute force 保護を適用します。（データベースは外部データベースではなく、NetDefendOS の中で定義される。）これは、Web インタフェースまたは SSH 経由で行う管理ログインは、この機能によって保護されることを意味します。

管理者はこの機能をオフにすることができません。また、このメカニズムを調整できるプロパティは何もありません。しかし、管理者には、機能のアクティビティをモニタできる方法があり、そのような攻撃が行われているか、または行われたかを参照することができます。

Brute Force 攻撃に対する保護

Brute Force 攻撃は、外部コンピュータが、次々と異なるユーザ名 / パスワードのペアを繰り返し試すことでネットワーク上の認証デバイスに接続するという特徴があります。このタイプの攻撃は短時間に多くの組み合わせを試みることができるということに依存します。NetDefendOS は、連続的な攻撃の間に次第に長い待ち時間を行使することでこのアプローチを無効にします。

ユーザ名 / パスワードの検証は、最初の失敗の段階では短い待機時間で次の試行を行うことができます。続けて何回か失敗すると、次に試行可能になるまでに、より長い待機時間を必要とします。待機時間を増やすことで、有効なユーザ名 / パスワードを見つけるために十分な資格証明書の組み合わせを試すことを実行不可能にします。しかし、単に一度以上資格認証を間違って入力した有効なユーザは、ある程度の時間内に再び認証が可能な状態となるべきです。

Blocked User List

ユーザ名 / パスワード確認が所定の回数失敗すると、NetDefendOS は「blocked user list」にユーザを追加し、NetDefendOS が再構成または再起動するまでそのままにします。このリストのユーザには、Blocked remaining と呼ばれる整数のプロパティがあります。これは減少していく時間（秒）です。Blocked remaining がゼロより大きい間は、接続試行に対して認証を行いません。この数値は、次に認証が失敗した場合に新しい整数にリセットされます。

Blocked remaining 値がゼロに達すると、ユーザは 24 時間リストから削除されません。これにより、管理者は、後でそのようなブロックされたユーザを参照できます。しかし、Blocked remaining 値のゼロは、ユーザが、NetDefendOS が無視しない別の認証の試みを行えることを意味します。

手動による Brute Force 設定

Brute Force 保護機能は Automatic（初期値）または Manual Settings を指定することにより有効化することができます。Manual Settings に指定した場合、管理者は次の値を設定することができます。

- Failed Attempts - 指定回数失敗すると、ユーザはブロックリストに追加されます。
- Lockout Time - ユーザがブロックリストに留まる時間を指定します。

手動設定を使用すると、失敗回数とロックされる期間が固定となり、失敗の試行回数に到達する毎に自動的に増加しません。

Brute Force 保護でブロックされるとユーザ側からどう見えるか

ユーザはブロックリストにあったとしても、何も変更が行われていないかのように、さらに認証の試行を行うことができます。言い換えれば、それらの資格認証が正しくても、Blocked remaining 値がゼロに達するまで、NetDefendOS は認証エラーとしてそれらの試みを扱います。ブロックリストにいるユーザには、ユーザがそれらのリストに載っていることや、どの程度待機する必要があるかということは示されません。同様に、悪意がある攻撃者に対して、試みが失敗した理由に関して NetDefendOS からの通知は行われません。

Blocked List のモニタ

NetDefendOS は、ブロックユーザリストに含まれるユーザの検証のために以下の方式を提供します。

- **CLI**

  ブロックされたユーザに関する情報を表示するには CLI コマンド「userauth」を使用します。

```
userauth -list -verbose -blocked

Blocked users:
User           Local Database  Blocked since        Blocked remaining
-------------- -------------- ------------------- --------------------
clavu          sslvpn          2016-06-10 12:09:18   17s
```

  Blocked remaining メッセージは、ユーザの認証を再度受け付けるまでに待機しなければいけない時間を示します。

- **Web インタフェース**

  上で示した CLI の情報は、**Status > Run-time Information > User Authentication** の順にメニューを選択することで、NetDefendOS Web インタフェースでも確認することが可能です。

- **ログイベントメッセージ**

  NetDefendOS は、brute force 保護メカニズムがブロックリストにユーザ名を追加するときには必ずログイベントメッセージを生成します。以下は代表的なメッセージです。

```
SYSTEM prio=Notice id=03200802 rev=1
event=user_blocked database=AdminUsers username=admin
blockedremaining=10s blockedsince="2016-06-10 09:42:12"
```

複数要素の認証は追加のセキュリティを提供します。

Brute Force 攻撃を無効にできる別の手法は、複数要素認証を使用することであり、この方式では、通常の認証情報に加えて追加のコードを入力する必要があります。詳しくは、「9.7 多要素認証」を参照してください。

9.6 User Identity Awareness

9.6.1 概要

特定のリソースにアクセスを希望する度にユーザ名とパスワード資格証明を入力するように促されるのではなく、自動的に NetDefend OS への認証が完了できれば、クライアントユーザにはより便利になる場合があります。NetDefendOS の User Identity Awareness（UIA）機能は、Windows™ ドメインサーバからユーザの認証情報を受信することで行われます。

identity awareness 機能にかかわる 2 つの異なるコンポーネントがあります。

- Identity Awareness Agent（IDA）は、D-Link ソフトウェアとは別のコンポーネントであり、アクティブディレクトリとして動作する 1 つ以上の Windows™ ドメインサーバ上で動作し、NetDefendOS に認証クライアントの情報を送信します。IDA は、ドメインコントローラまたはドメインメンバのどちらかで動作します。IDA ソフトウェアの複数サーバへのインストールは冗長度を提供します。

  Windows™ サーバ上で動作する IDA ソフトウェアのインストールと管理については、「付録 H Identity Awareness Agent (IDA) のインストールと管理」で説明しています。

- クライアントがファイアウォール経由でリソースにアクセスを試みる際に、認証プロセスが発生します。このプロセスは Identity Awareness Agent によって送信された情報を使用します。

クライアント、サーバおよび D-Link ファイアウォール間の全体の関係は以下の図に示されています。

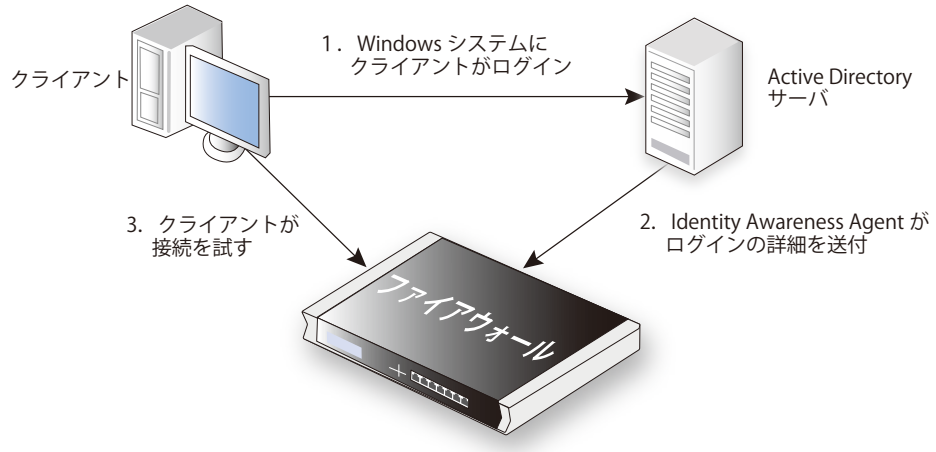


図 9-3　User Identity Awareness

認証間のイベントフロー

identity awareness 機能を持つイベントのフローは以下の通りです。

- Windows™ ベースのクライアントコンピュータのユーザがログインします。
- ユーザは Windows Active Directory サーバに対して認証されます。
- D-Link Identity Awareness Agent(IDA) はそのドメインの少なくとも 1 サーバで動作します。このソフトウェアは成功したクライアント認証をリッスンします。クライアントが認証されると、エージェントは、設定している D-Link ファイアウォールに以下を送信します。
  - i. ユーザ名。
  - ii. ユーザのグループ。
  - iii. ユーザの IP。
- IP ルールセットのエントリが、ユーザの IP アドレスを許可するために定義されていると、その IP アドレスは NetDefendOS に認証され、その IP との接続が、ファイアウォールを通して許可されます。
- クライアントは、NetDefendOS を通じた接続のオープンを試みます。
- NetDefendOS の IP ルールセットエントリが起動し、この接続の許可を行います。
- 起動したエントリに含まれる送信元ネットワークアドレスオブジェクトには、関連付けられている許可ユーザ名とグループの認証リストがあります。クライアントがこのリストにあると、接続を確立することができます。

認証のために作成される IP ルールセットエントリは、認証プロセスのトリガーだけでなく接続を特定して許可する 2 つの目的を持っています。また、NAT はルールまたはポリシーに含まれる機能になることもできます。

注意 IDA では NetDefendOS の認証は認識されません。

IDA サービスの目的は NetDefendOS に認証イベントの詳細を送信することです。通信は一方向であり、IDA サービスは NetDefendOS によって送信される認証を認識せず、インタフェースに情報を表示しません。

9.6.2 Identity Awareness の設定

Identity Awareness をセットアップするために、以下の手順が必要です。

- 1 つ以上のドメインサーバに Identity Awareness Agent（IDA）ソフトウェアをインストールして、設定します。サーバは、ドメインコントローラまたはドメインメンバのどちらかとします。IDA ソフトウェアについては本セクションの終わりでさらに詳しく説明します。シングルサーバへのインストールでも十分ですが、複数サーバへの設置は冗長性を提供します。

  IDA ソフトウェアのインストールと管理の詳細については、「付録 H Identity Awareness Agent (IDA) のインストールと管理」で説明しています。IDA ソフトウェアは NetDefendOS では提供していませんが、D-Link Web サイトで個別にソフトウェアパッケージをダウンロードすることができます。ソフトウェアには固有のバージョン番号が割り振られており、随時更新される可能性があります。

- ドメインサーバにインストールされたエージェントが使用するものに対応する IP アドレスと事前共有鍵を持つ Authentication Agent オブジェクトを NetDefendOS に設定します。IDA ソフトウェアがインストールされているドメインの各サーバに個別の Authentication Agent オブジェクトを作成するべきです。

  Pre-shared Key プロパティを指定しないと、定義済みの PSK オブジェクト auth_agent_psk の値を初期値とします。また、これは、D-Link Identity Awareness Agent によって使用されるデフォルトキーの値です。しかし、デフォルトキーは、すべての NetDefendOS システムにおいて同じであり、テスト目的だけに使用されるべきです。

  エージェントから来るトラフィックを許可するために、NetDefendOS は IP ルールセットのエントリを必要としません。

- クライアントの認証の際に取得する IP アドレス、IP 範囲またはネットワークを定義するアドレス帳 IP4 Address オブジェクトを設定します。

  このアドレスオブジェクトの Authentication プロパティには、接続を許可されるユーザ名、そして / または、グループを指定してください。username@domain 形式でユーザ名を指定しなければなりません。例えば、myusername@example.com です。@ シンボルを持つこの形式が使用されず、簡単な文字列（例 myusername）が使用されると、これはグループとして扱われます。

重要 グループ名にスペースではなくアンダースコアを使用する

NetDefendOS ではグループ名にスペース記号を含むことはできません。ドメインコントローラサーバのグループ名にはスペースを含むことができますが、NetDefendOS でグループ名を指定する際にはアンダースコア "_" に置き変える必要があります。

- クライアント接続における認証のトリガとなって接続がオープンできるように、NetDefendOS の IP ルールセットにエントリを指定します。このルールまたはポリシーのための送信元ネットワークは前の手順で指定した IPv4 アドレスオブジェクトである必要があります。

  この IP ルールセットエントリのトリガーが、認証プロセスのトリガーとなります。

例題 9.7

User Identity Awareness を有効にする

この例題では、If1 インタフェースに接続するネットワーク client_net に外部クライアントがいるものと仮定します。これらのクライアントは、If2 インタフェースでネットワーク server_net のホストへの HTTP アクセスを希望しています。

クライアント接続は、identity awareness 機能を使用することで認証されます。許可されるユーザ名は、ser1@mydomain と user2@mydomain です。

また、D-Link Authentication エージェントソフトウェアは既に 1 つの外部 Windows™ ドメインサーバにインストールされ、アドレス帳オブジェクト aa_server_ip で定義された IPv4 アドレスと aa_server_key PSK オブジェクトで定義された事前共有鍵で設定されているものとします。

ドメインには 1 つのサーバしかないものとします。

CLI

外部サーバを示す Authentication Agent オブジェクトを定義します。

```
DFL-xxxx:/> add AuthAgent IPAddress=aa_server_ip PSK=aa_server_key Name=my_auth_agent
```

クライアント IP のネットワークオブジェクトに許可されるユーザ名を割り当てます。

```
DFL-xxxx:/> set Address IP4Address client_net UserAuthGroups=user1@mydomain,user2@mydomain
```

ソースネットワークとして client_net を許可および使用する IP ポリシーを作成します。

```
DFL-xxxx:/main> add IPPolicy SourceInterface=If1 SourceNetwork=client_net DestinationInterface=If2
            DestinationNetwork=server_net Service=http-all Name=client_to_server Action=Allow
```

Web Interface

外部サーバを示す Authentication Agent オブジェクトを定義します。

1. **Policies > User Authentication > Rules > Authentication Agents > Add > Authentication Agent** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_auth_agent
   - IP Address: aa_server_ip
   - Pre-shared key: aa_server_key

3. 「OK」ボタンをクリックします。

クライアント IP のネットワークオブジェクトに許可されるユーザ名を割り当てます。

1. **Objects > Address Book > client_net** の順にメニューをクリックします。

2. User Authentication タブを選択します。

3. User Auth Groups に入力します。: user1@mydomain,user2@mydomain

4. 「OK」ボタンをクリックします。

クライアントがサーバにアクセスすることを許可し、ソースネットワークとして client_net を使用する IP ポリシーを作成します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: client_to_server
   - Action: Allow
   - Source Network: client_net
   - Source Interface: lf1
   - Destination Network: server_net
   - Destination Interface: lf2
   - Service: http-all

3. 「OK」ボタンをクリックします。

この例題では、どのユーザが認証されるかを指定するために、各ユーザ名がアドレスオブジェクトに使用されることに注意してください。このセクションの前に説明したとおり、グループ名を代わりまたは追加で使用することができます。

9.6.3 Identity Awareness のアクティビティをモニタする

管理者は、identity awareness アクティビティの詳細を示すように NetDefendOS にリクエストすることができます。

Web インタフェースでは、管理者は **Status > Run-time Information > Authentication Agents** を開き、IDA サービスが NetDefendOS に接続されていることを参照することができます。CLI では、以下のコマンドで同様に実行できます。

```
DFL-xxxx:/> authagent
```

ユーザが認証されている時、Web インタフェースで **Status > Run-time Information > User Authentication** を開いて、それらを参照できます。CLI では、以下のコマンドで同様に実行できます。

```
DFL-xxxx:/> userauth -list
```

NetDefendOS とドメインサーバ上の IDA サービス間の通信についてコンソールモニタを行うには、以下のコマンドを使用します。

```
DFL-xxxx:/> authagentsnoop <agent-name>
```

すべてのスヌーピングを終了するには以下のコマンドを実行します。

```
DFL-xxxx:/> authagentsnoop none
```

上のすべての CLI コマンドのオプションは個別の「NetDefendOS CLI Reference Guide」に示されています。

9.7 多要素認証

NetDefend Firewall の背後に位置するリソースへのアクセスが資格証明に基づいている時、Multi Factor Authentication（多要素認証）を使用することによって、セキュリティをさらに強化できます。これは、二要素認証または二段階認証とも呼ばれます。通常、最初の要素はユーザ名 / パスワードの組み合わせです。また、2 番目の要素は、ログイン時点で SMS またはメールでユーザに送信されるかもしれないワンタイムコード、または、ユーザによって何らかの方法（例 : コードボックス）で生成されるかもしれないワンタイムコードです。

多要素のサポートは自動である

初期値では、NetDefendOS は、RADIUS Access-Challenge メッセージを認識し、追加コードを要求する特別な Web ページを表示することで多要素認証のサポートを提供します。この Web ページには、LoginChallenge という名の NetDefendOS Banner File があります。

また、以下の認証方法を使用する時、モバイル VPN IPsec クライアントは多要素認証によってサポートされます。

- XAuth と IKEv1
- EAP と IKEv2

多要素処理の順序

NetDefendOS における多要素認証の処理の順序は以下の通りです。

1. 認証は、認証ルールおよび IP ルールセットのエントリ を使用して通常通り設定されます。
2. 認証ソースは多要素認証を実行するために設定された外部の RADIUS サーバになります。
3. ユーザは NetDefend Firewall を通してリソースにアクセスしようとします。標準の NetDefendOS ログインページを使用して表示され、自分の資格証明を入力します。
4. NetDefendOS は、RADIUS Access-Request メッセージでの認証用の RADIUS サーバにこれらの資格証明を送信します。
5. 多要素認証では、RADIUS サーバは以下の 2 つのことを行います。
   i. RADIUS Access-Challenge メッセージを返送することによって多要素認証を使用しなければならないことを NetDefendOS に知らせます。
   ii. 追加のチャレンジのタイプ次第で、サーバはワンタイムコードをユーザに送信するかもしれません。例えば、モバイルデバイスではこれは SMS メッセージに含まれるかもしれません。あるいはまた、コードは、ユーザによって例えばコードボックスを使用することで自分たちで生成されるかもしれません。

以下の図では、このポイントに関してすべての手順を示しています。ここでは、RADIUS サーバによって SMS メッセージに含まれる形でコードがユーザのスマートフォンに送信されます。通常、SMS メッセージを生成するために、RADIUS サーバが他の専用サーバに対してメッセージを送信します。

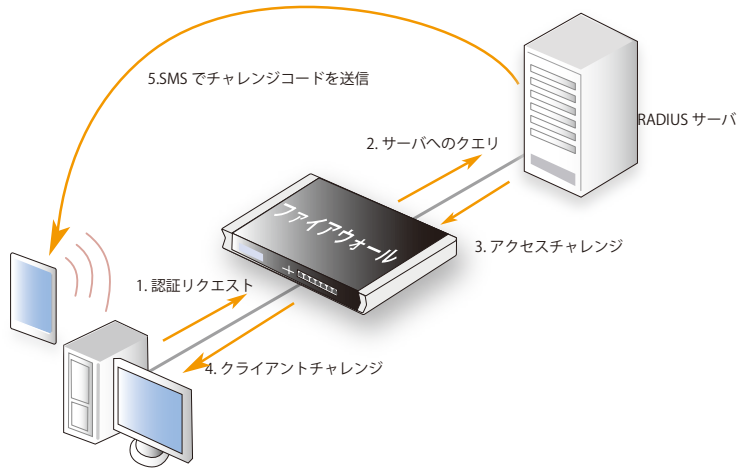


図 9-4　多要素認証

その後、以下の手順によって処理が完了します。

6. ユーザは受信または生成したコードを入力すると、NetDefendOS は、別の Access-Request メッセージで RADIUS サーバに入力されたコードをリレーします。
7. RADIUS サーバはコードについて検証します。ユーザを認証する場合は、NetDefendOS に Access-Accept に送り返します。そして、保護リソースへのアクセス権をクライアントに与えます。認証されない場合、サーバは Access-Reject メッセージを NetDefendOS に返送するため、アクセスは拒否されます。

多要素認証に関する注意

NetDefendOS との多要素認証を設定することに関して注意するポイントは以下の通りです。

- Challenge コードが RSA SecureID(TM) 製品などのローカルのコード生成デバイスによって生成されるか、または RADIUS サーバでユーザにそれを送信するのであれば、同じ NetDefendOS 設定が使用されています。
- この他のコンフィグレーションは NetDefendOS で必要ではありません。しかし、バナーファイル LoginChallenge を Challenge プロセスで使用するのであれば、適切なテキストを表示するために編集する必要があるかもしれません。詳しくは、「9.3 認証 HTML ページのカスタマイズ」を参照してください。
- 管理者は適切に RADIUS サーバをする必要があります。この方法についてはサーバのドキュメントを参照するべきです。
- RADIUS サーバがユーザにコードを送信する場合、これは NetDefendOS から独立しています。様々なサードパーティのソリューションを、このコードを生成するために利用可能です。

9.8 RADIUS リレー

概要

NetDefendOS の機能の RADIUS Relay は、Mobile Data Offloading（MDO）などの通信技術のシナリオのために設計されており、スマートフォンなどの User Equipment (UE) でオペレータの無線ネットワークから Access Point (AP) ポイントを経由する Wi-Fi を使用した通信に切り換えます。AP は、このアクセスを制御するファイアウォール機能を持った D-LInk ファイアウォールを経由して UE をパブリックインターネットなどのリソースに接続させます。

ファイアウォールの背後にあるリソースへのアクセス権を得るために、UE は RADIUS サーバを使用して AP 経由で自身を認証しなければなりません。RADIUS の認証要求は、RADIUS サーバに要求をリレーする AP によって NetDefendOS に送信されます。サーバの応答は AP にリレーして戻され、認証されたユーザは、次に、NetDefendOS セキュリティポリシーに基づいてリソースへのアクセスを認可されるように、NetDefendOS ユーザリストに入力されます。

RADIUS リレー認証の間のイベントシーケンス

以下のイベントのシーケンスは radius リレーで起こります。

- UE は AP からネットワークアクセスを要求します。
- AP は RADIUS Access-Request を NetDefendOS に送信します。NetDefendOS RADIUS リレー機能を設定している場合、定義済みの RADIUS サーバにこの要求を転送します。
- RADIUS Access-Accept または Access-Reject メッセージを NetDefendOS に返送することによって、RADIUS サーバは UE を認証、または UE を認証しません。これらが AP にリレーして戻されると、これらのメッセージのコンテンツを NetDefendOS が検証します。
- RADIUS サーバが認証すると、UE は DHCP 要求を出します。そして、設定された NetDefendOS DHCP サーバから DHCP IP リースを UE に返送します。（LeasesRequireAuth オプションが有効である）認証されたクライアントにだけリースを配布するように DHCP サーバを設定します。
- 認証成功により、NetDefendOS はログインしているユーザのリスト（CLI userauth コマンドと Web インタフェースを通して参照が可能）の UE のユーザ名を含んでおり、これは、定義済みの NetDefendOS セキュリティポリシーによって決定しているリソースへの UE のアクセスを許可します。

グループメンバシップを使用する

NetDefendOS セキュリティポリシーは、グループにおける UE のメンバシップがアクセスを許可するどうかを決定するグループメンバシップに基づくことができます。この場合、認証の間、ユーザのグループ名を返送するために RADIUS サーバを設定しなければなりません。さらに、NetDefendOS と通信する RADIUS サーバで、正しく Vendor ID を設定しなければなりません。これの実行については、本セクションの終わりで詳しく説明します。

また、UE によるアクセスを許可する IP ルールまたは IP ポリシーが、RADIUS サーバが返送するのと同じグループ名に設定された User Auth Groups プロパティ（CLI では UserAuthGroups プロパティ）を持つ IP アドレスオブジェクトを Source Network に使用しなければならないことも重要です。詳しくは、「9.4 認証を必要とする IP ポリシー」を参照してください。

グループメンバシップによる検証が必要ない場合、Source Network に使用される IP アドレスオブジェクトに使用される IP アドレスオブジェクトの No defined credentials プロパティは有効であるべきです。

グループ名が Source Network アドレスオブジェクトに指定されない場合、RADIUS Relay オブジェクトの Idle Timeout 期限が経過した後に、その時トラフィックが流れていたとしても、その接続はドロップされます。

重要 DHCP サーバの LeasesRequireAuth オプションを有効にします。

RADIUS リレーが NetDefendOS コンフィグレーションに使用されている場合、設定されたクライアントにのみリースを配布するように、すべての DHCP サーバを設定する必要があります。これは、CLI の LeasesRequireAuth プロパティ、Web インタフェースの「Leases Require Authentication」オプションを有効化することで設定することができます。

すべての DHCP サーバでこの設定をしないと、RADIUS リレーで使用されるかどうかに関係なく、セキュリティの脆弱性が発生し、未認証のクライアントが保護されたリソースにアクセスすることを許可してしまう可能性があります。

Radius Relay オブジェクトプロパティ

Radius Relay オブジェクトの重要なプロパティは以下の通りです。

項目	説明
Name	コンフィグレーションで使用されるオブジェクトの記述名。
DHCP Server	UE が認証された後に IP アドレスリースを与えるのに使用される DHCP サーバ。
Source Interface	NetDefendOS が AP のリクエストをリッスンする NetDefendOS インタフェース。これは、以下のいずれかです。 **i.** イーサネットインタフェース。 **ii.** VLAN インタフェース。 **iii.** インタフェースグループ。 プロパティ Override User Data Interface がセットされると、このインタフェースは、AP からの初期接続のみをリッスンし、認証トラフィックを送信します。Override User Data Interface に割り当てられたインタフェースは、データトラフィックを運びます。これは以下で詳しく説明します。
Client IP Filter	アクセスポイントが所属する送信元 IP 範囲を指定します。これは通常ネットワーク範囲です。これを NetDefendOS アドレス帳オブジェクトとして指定することをお勧めします。
Listening IP	アクセスポイントがソースインタフェースで接続する IP アドレスです。リッスンするインタフェースがイーサネットインタフェースまたは VLAN であると、これはオプションとなります。指定しない場合、インタフェースの IP アドレスは初期値となります。 ソースインタフェースがインタフェースグループであれば、リッスンする IP を指定しなければなりません。
Listening Port	これは、リッスンするインタフェースのためのリッスンポート番号であり、初期値は 1812 です。
Override User Data Interface	初期値では、ユーザは、データトラフィックの転送に使用される上記の Source Interface プロパティに設定された値と同じインタフェースを使用して認証されます。これはセキュリティリスクを引き起こす可能性があるため、これらの 2 つの機能に異なるインタフェースを使用することをお勧めします。Override User Data Interface プロパティは、インタフェースがデータにだけ使用されるように設定されます。通常、Source Interface と Override User Data Interface は、AP に接続する物理インタフェースで動作する 2 つの異なる VLAN になります。 以下でさらにこれについて説明します。
Routing Table	UE が認証されて、IP アドレスを受信すると、IP へのルートは自動的にこのルーティングテーブルに追加されます。通常、デフォルトの main ルーティングテーブルが使用されます。
Remote Server IP	UE 認証を実行する RADIUS サーバの IP アドレスです。
Remote Server Port	UE 認証を実行する RADIUS サーバのポート番号です。初期値は 1812 で、これは RADIUS の標準です。
Sending IP	RADIUS サーバに送信されるリクエストの送信側 IP として、このオプションの IP アドレスは使用されます。設定されないと、送信側インタフェースの IP アドレスが使用されます。送信側インタフェースは RADIUS サーバの IP アドレスのルート検索により決定されます。
Idle Timeout	認証されたユーザからのトラフィックのない時間（秒）で、これが経過すると、ユーザは自動的にログアウトされます。
Session Timeout	使用済みセッションが認証状態を許可される絶対的な時間（秒）です。ゼロに設定されると、無限のセッションを意味します。
Use timeouts received from the authentication server.	このプロパティが有効であり、RADIUS サーバが正しく設定されると、Idle Timeout と Session Timeout プロパティは RADIUS サーバが送信した値を取り入れます。

個別の認証とデータトラフィック

認証トラフィックの Source Interface に割り当てられたインタフェースとは別になるように、データトラフィックのみに使用されるインタフェースに対して、Override User Data Interface プロパティを設定することを強く推奨します。通常、同じ物理イーサネットインタフェースで動作し、AP に接続する 2 つの異なる VLAN インタフェースに設定します。これは、バックボーンネットワークにフローするデータから RADIUS サーバに向かう認証データを完全に分けます。この設定をしないと、セキュリティリスクが引き起こされます。

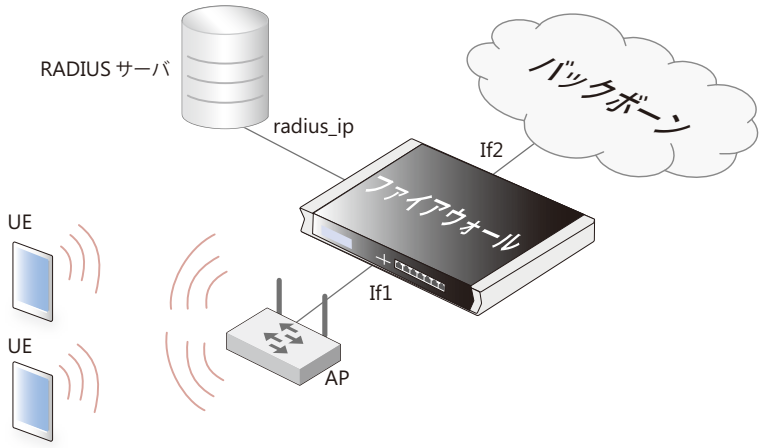
Override User Data Interface プロパティを使用する場合、以下の項目について注意するべきです。

- 管理者は AP が認証を送信し、データトラフィックが正しい VLAN に送信されることを保証します。
- IP アドレスを配布する DHCP サーバオブジェクトに使用されるインタフェースは、データに使用されるインタフェース（Override User Data Interface）であり、認証に使用されるインタフェース（Source Interface）ではありません。
- これ以外の IP ルールセットエントリは DNS トラフィックまたは認証トラフィックのどちらにも必要ありません。データがクライアントからバックボーンまでフローする IP ルールセットエントリは、1 つだけ必要です。

例題 9.8

Radius リレー

この例題では、以下で例証されるシナリオのために Radius Relay オブジェクトを設定する方法を示しています。ここでは、クライアントデバイス (UE) は、アクセスポイント (AP) を経由してネットワークバックボーンからデータサービスにアクセスしなければなりません。まず、RADIUS サーバに認証され、次に、IP アドレスが割り当てられる必要があります。アクセスポイントは D-Link ファイアウォールの物理的な If1 イーサネットインタフェースに接続し、バックボーンネットワークは If2 インタフェースに接続します。



以下はその前提です。

- 2 つの VLAN が既に設定されており、これらの NetDefendOS オブジェクトは、クライアント認証トラフィック用の vlan_auth とバックボーンにフローするデータトラフィック用の vlan_data と呼びます。
- これらの VLAN の両方が物理イーサネットインタフェース If1 に流れるように既にセットアップされ、アクセスポイントは認証とデータのために適切な VLAN を使用するように正しく設定されています。
- 認証されるユーザはグループ ue_group に所属しなければなりません。
- vlan_auth インタフェースで認証要求をリッスンする Radius Relay オブジェクト（r_relay1 と呼ぶ）を作成し、IPv4 アドレス radius_ip を持つ RADIUS サーバにそれらをリレーします。以下の図はシナリオについて説明しています。
- 認証に成功すると、IP アドレスのリースは DHCP サーバオブジェクト rr_dhcp_server によって付与されます。IPv4 アドレスオブジェクト client_net で定義されるネットワーク 192.168.10.10-192.168.10.255 に所属するアドレスが UE に割り当てられるものとします。
- 認証に成功すると、IP ルール client_access_rule を使用して If2 インタフェース上のバックボーンネットワークへのアクセスが UE に許可されます。

CLI

A. UE 用のクライアント IP アドレスの範囲を定義する IP4Address オブジェクトを作成し、認証グループ ue_group にそれを割り当てます。

```
DFL-xxxx:/> add Address IP4Address client_net Address=192.168.10.10-192.168.10.255 UserAuthGroups=ue_group
```

B. DHCP サーバに IP アドレスプールを定義する IP4Address オブジェクトを作成します。同じ IP 範囲を使用しますが、これは別のオブジェクトとします。

```
DFL-xxxx:/> add Address IP4Address client_ip_range Address=192.168.10.10-192.168.10.255
```

C. これらのアドレスを配布する DHCPServer オブジェクトを作成します。

```
DFL-xxxx:/> add DHCPServer rr_dhcp_server Interface=vlan_data IPAddressPool=client_ip_range Netmask=255.255.255.0
            LeasesRequireAuth=Yes
```

D. インタフェース If2 に接続するバックボーンネットワークにフローするクライアントデータのアクセスを許可する IP Policy オブジェクトを作成します。

```
DFL-xxxx:/> add IPPolicy Name=client_access_rule SourceInterface=vlan_data SourceNetwork=client_net
            DestinationInterface=If2 DestinationNetwork=all-nets Service=all_services Action=Allow
```

E. RadiusRelay オブジェクトを作成します。

```
DFL-xxxx:/> add RadiusRelay r_relay1 SourceInterface=vlan_auth ClientIPFilter=client_ip_range
            RemoteServerIP=radius_ip DHCPServer=rr_dhcp_server OverrideUserDataInterface=vlan_data
```

Web Interface

A. UE 用のクライアント IP アドレスの範囲を定義する IP4Address オブジェクトを作成し、認証グループ ue_group にそれを割り当てます。

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: client_net
   - IP Address: 192.168.10.0/24
   - User Authentication: ue_group
3. 「OK」ボタンをクリックします。

B. DHCP サーバに IP アドレスプールを定義する IP4Address オブジェクトを作成します。同じ IP 範囲を使用しますが、これは別のオブジェクトとします。

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: client_ip_range
   - IP Address: 192.168.10.10-192.168.10.255
3. 「OK」ボタンをクリックします。

C. これらのアドレスを配布する DHCPServer オブジェクトを作成します。

1. **Network > Network Services > DHCP Servers > Add > DHCPServer** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: rr_dhcp_server
   - Interface Filter: vlan_data
   - IP Address Pool: client_ip_range
   - Netmask: 255.255.255.0
3. Options タブを選択し、以下のオプションを有効にします。
   - Leases Require Authentication
4. 「OK」ボタンをクリックします。

D. インタフェース If2 に接続するバックボーンネットワークにフローするクライアントデータのアクセスを許可する IP Policy オブジェクトを作成します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: client_access_rule
   - Action: Allow
   - Service: all_services
   - Source Interface: vlan_data
   - Source Network: client_net
   - Destination Interface: If2
   - Destination Network: all-nets
3. 「OK」ボタンをクリックします。

E. RadiusRelay オブジェクトを作成します。

1. **Network > Network Services > RADIUS Relays > Add > RADIUS Relay** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: r_relay1
   - DHCP Server: rr_dhcp_server
   - Source Interface: vlan_auth
   - Client IP Filter: client_ip_range
   - Remote Server IP: radius_ip
   - Override User Data Interface: vlan_data
3. 「OK」ボタンをクリックします。

注意 グループ名を送信するために RADIUS サーバを設定します。

上記の例題では、認証中、RADIUS サーバがグループ名 ue_group を返送するものとしています。これをするために RADIUS サーバを設定しなければなりません。

NetDefendOS にログインしているユーザにグループ情報を提供するように外部 RADIUS サーバを設定する場合、ユーザグループのベンダ指定の属性を使用する必要があります。NetDefendOS Vendor ID は 5089 で、ユーザグループは vendor-type 1 として文字列タイプの値で定義されます。

9.9 RADIUS アカウンティング

9.9.1 概要

中央データベースの設置

多数のユーザを抱えるネットワーク環境では、1 台またはクラスタ構成の中央サーバを置き、それらを用いてユーザのアカウンティング情報を保持し、認証および許可のタスクを行うことが有用です。専用サーバに置かれる中央データベースには、全ユーザの証明情報だけでなく、詳細な接続情報も含まれ、これにより運用の複雑性が大幅に軽減されます。リモート認証ダイアルインユーザサービス（RADIUS:Remote Authentication Dial-in User Service）は、こうした方法を実装するために広く使用されている、認証、認可、アカウンティング（AAA:Authentication、Authorization and Accounting）プロトコルであり、NetDefendOS ではこれを使用してユーザアカウンティングを行います。

RADIUS の構造

RADIUS プロトコルは、クライアント / サーバ構造を基本としています。D-Link ファイアウォールは、RADIUS サーバのクライアントとして動作し、専用サーバにリクエストを作成および送信します。RADIUS テクノロジーでは、ファイアウォールはネットワークアクセスサーバ（NAS : Network Access Server）として動作します。

ユーザ認証を行うため、RADIUS サーバは、リクエストを受け取り、データベースを参照してユーザ情報を確認し、「承認」または「拒否」の決定をリクエストしたクライアントに戻します。RFC 2866 規格では、アカウンティング情報の送受信を処理できるよう RADIUS が拡張され、NetDefendOS はこれをユーザアカウンティングの標準とします。これによって、中央サーバを持つ利点はユーザ接続アカウンティングにまで及びます。（RADIUS を用いた NetDefendOS 認証の詳細については、「9.2 認証設定」を参照してください。）

9.9.2 RADIUS アカウンティングメッセージ

メッセージ生成

送受信されるバイト数やパケット数などの統計情報は、RADIUS セッションを通して更新および保存されます。認証サーバに関わる接続が終了した時には必ず、その認証サーバについてのすべての統計情報が更新されます。

ユーザがファイアウォールを通じて新しい接続を確立したことにより、新しいクライアントセッションが開始される時、NetDefendOS は、指定された RADIUS サーバにアカウンティング要求 START メッセージを送信し、新しいセッションが開始されたことを記録します。
ユーザアカウント情報も RADIUS サーバに提供されます。サーバは、アカウンティング応答メッセージを NetDefendOS に返送して、メッセージを受信したことを知らせます。

ユーザがログアウトした後や、セッションが時間切れになった場合など、ユーザが認証されていない状態になると、関連するセッションの統計情報を含む NetDefendOS から、アカウンティング要求 STOP メッセージが送信されます。
これらの統計情報に含まれる情報は、ユーザが設定できます。START メッセージと STOP メッセージの内容を以下に詳しく記述します。

START メッセージパラメータ

NetDefendOS によって送信される START メッセージには、次のパラメータが含まれます。

パラメータ	説明
Type	サービス開始の合図としてこの AccountingRequest をマークします。（START）
ID	Acct-Status-Type が START に設定されている、以前に送信されたアカウンティング要求パケットをマッチングするための識別子。
User Name	認証サーバのユーザ名。
NAS IP Address	D-Link ファイアウォールの IP アドレス。
NAS Port	ユーザが認証された NAS のポート。（TCP ポートや UDP ポートではなく、物理的なポートです。）
User IP Address	認証サーバの IP アドレス。認証サーバで指定されている場合のみ送信されます。
How Authenticated	ユーザの認証方法。ユーザが RADIUS 経由で認証された場合は RADIUS、ローカルユーザ経由で認証された場合は LOCAL に設定されます。
Delay Time	アカウンティング要求パケットが送信されてから、認証確認応答が受信されるまでの遅延時間（秒）。サーバへの到着時間からこの値を引くと、このアカウンティング要求の生成にかかるおおよその時間が分かります。これには、ネットワークの遅延は反映されません。1 回目の試行では、このパラメータが 0 に設定されます。
Timestamp	1970-01-01 以降の秒数。このパケットが NetDefendOS から送信された時のタイムスタンプを設定するために使用されます。

STOP メッセージパラメータ

NetDefendOS によって送信される STOP メッセージには、次のパラメータが含まれます。

パラメータ	説明
Type	セッションの最後の合図として、本アカウンティングリクエストをマークします。（STOP）
ID	Acct-Status-Type が START に設定されている、以前に送信されたアカウンティング要求パケットをマッチングするための識別子。
User Name	認証サーバのユーザ名。
NAS IP Address	D-Link ファイアウォールの IP アドレス。
NAS Port	ユーザが認証された NAS 上のポート（TCP ポートや UDP ポートではなく、物理的なポートです。）
User IP Address	認証サーバの IP アドレス。認証サーバで指定されている場合のみ送信されます。
Input Bytes	ユーザが受信したバイト数（*）
Input Bytes	ユーザが送信したバイト数（*）
Input Packets	ユーザが受信したパケット数（*）
Output Packets	ユーザが送信したパケット数（*）
Session Time	このセッションが続いた秒数（*）
Termination Cause	セッションが終了した理由。
How Authenticated	ユーザの認証方法。ユーザが RADIUS 経由で認証された場合は RADIUS、ローカルユーザデータベース経由で認証された場合は LOCAL に設定されます。
Delay Time	本パラメータについては上記を参照してください。
Timestamp	1970-01-01 以降の秒数。このパケットがファイアウォールから送信された時のタイムスタンプを設定するために使用されます。
Input Gigawords	「Input Bytes」のカウンタが丸められた回数を示します。これは、インプットバイト数が丸められ、かつその「Input Bytes」属性が送信される場合にだけ送信されます。
Output Gigawords	「Output Bytes」のカウンタが丸められた回数を示します。これは、アウトプットバイト数が丸められ、かつ、その「Output Bytes」属性が送信される場合にだけ送信されます。

注意 リストの（*）の意味

上記のリストに記載されている（*）マークは、パラメータの送信がユーザ設定可能であることを意味します。

9.9.3 Interim Accounting メッセージ

「START」と「STOP」メッセージに加えて、NetDefendOS は、認証ユーザの現在のステータスを使用してアカウントサーバを更新するために Interim Accounting メッセージを定期的に送信するオプションを持っています。

メッセージはスナップショットである

Interim Accounting メッセージでは、認証ユーザが特定の時点まで使用していたネットワークリソースのスナップショットとして情報を見ることができます。この機能を用いて、RADIUS サーバは、最後のメッセージが送信された時点まで認証ユーザが送受信していたバイト数およびパケット数を追跡できます。

Interim Accounting メッセージには、認証ユーザに関する統計情報の現行値が含まれます。Acct-Terminate-Cause が含まれない（ユーザの接続が停止されていないため）ことを除いては、アカウンティング要求 Stop メッセージの内容とほぼ同じです。

メッセージの頻度

Interim Accounting メッセージの回数を認証サーバ上または NetDefendOS のいずれかで指定できます。NetDefendOS で設定を変更すると、アカウンティングサーバ上の設定が書き換えられます。

9.9.4 RADIUS アカウンティングの設定

RADIUS アカウンティングをアクティブにするには、以下のいくつかの手順に従う必要があります。

- RADIUS サーバを NetDefendOS に定義する必要があります。
- ユーザ認証オブジェクトが、RADIUS サーバが指定されている関連付けられたルールを持つ必要があります。
- 外部 RADIUS サーバ自体を正しく設定する必要があります。

ソース IP の設定

初期値では、Source IP プロパティは自動に設定されており、ファイアウォールの送信側インタフェースの IP アドレスは、RADIUS サーバに送信されるトラフィックの送信元アドレスとして使用されます。このプロパティを Manual に設定すると、特定の送信元 IP アドレスをサーバに送信されるトラフィックに使用できます。

送信元 IP アドレスが指定されると、管理者は、送信側インタフェースに IP アドレスを ARP パブリッシュするように手動で NetDefendOS を設定する必要があります。設定方法については「3.5.3 ARP パブリッシュ」で説明しています。

更なる RADIUS 問題

RADIUS のアクティブ化にあたっては次の重要なポイントに注意が必要です。

- IP ルールセットの FwdFast ルールの対象である接続では、RADIUS アカウンティングは機能しません。
- 認証とアカウンティングを同じ RADIUS サーバで処理する必要はありません。1 台のサーバで認証を行い、別のサーバでアカウンティングを行うことができます。
- プライマリサーバで実行不能なイベントを処理できるよう、NetDefendOS に複数の RADIUS サーバを構成することができます。

例題 9.9

RADIUS アカウンティングサーバの設定

IP アドレス 192.168.3.1 とポート 1813 を使用して、my-accounting という名のローカル RADIUS サーバを持つ NetDefendOS を設定する方法を示しています。共有秘密キーは 231562514098273 であるものとします。

CLI

```
DFL-xxxx:/> add RadiusAccounting my-accounting IPAddress=192.168.3.1 SharedSecret=231562514098273 Port=1813
            RetryTimeout=2 RoutingTable=main
```

Web Interface

1. **Policies > User Authentication > Accounting > RADIUS > Add > RADIUS Server** メニューをクリックします。
2. 以下の情報を入力します。
   - Name: my-accounting
   - IP Address: 192.168.3.1
   - Port: 1813
   - Retry Timeout: 2
   - Shared Secret: 231562514098273
   - Confirm Secret: 231562514098273
   - Routing Table: main
3. 「OK」ボタンをクリックします。

9.9.5 RADIUS アカウンティングセキュリティ

NetDefendOS と任意の RADIUS アカウンティングサーバ間の通信は、共有秘密鍵で保護されます。この秘密鍵がネットワーク上で送信されることはなく、代わりに、16 バイト長のオーセンティケータコードが一方向 MD5 ハッシュ関数を用いて算出され、アカウンティングメッセージの認証に使用されます。

共有秘密鍵は大文字小文字が区別され、最長 100 文字が含まれます。また、NetDefendOS と RADIUS サーバで正確に一致していることが必要です。

メッセージは UDP プロトコルを用いて送信され、ポート番号 1813 が初期値として使用されます（ユーザ設定可能）。

9.9.6 RADIUS アカウンティングと高可用性

HA クラスタでは、アクティブなファイアウォールとパッシブなファイアウォール間でアカウンティング情報を同期します。これは、接続が終了しているか否かに関わらず、両方のクラスタメンバでアカウンティング情報が自動的に更新されることを意味します。

特別なアカウンティングイベント

この他、2 つの特別なアカウンティングイベントがアクティブユニットで用いられ、パッシブユニットの同期が保たれます。

- アカウンティングサーバからレスポンスを受け取った時には必ず、HA 設定の非アクティブメンバに AccountingStart イベントが送信されます。これにより、特定の認証ユーザについてのアカウンティング情報が保存されるよう指示されます。

- アクティブユニットの認証ユーザに関わる接続が、非アクティブユニット上で同期される前にタイムアウトになった場合、アカウンティング情報の同期に問題が発生することがあります。この問題を回避するため、タイムアウトになったパッシブユニットに、接続に関する最近のアカウンティング情報が含まれる特別な AccountingUpdate イベントが送信されます。

9.9.7 無応答な RADIUS サーバに対処する

RADIUS サーバが応答しない AccountingRequestSTART パケットを RADIUS クライアントが送信するということが発生します。NetDefendOS は、これが発生すると、ユーザが指定した秒数後にリクエストを再送信します。ただしこれは、NetDefendOS がアカウンティングサーバに通信を試みる間もユーザがまだ認証アクセスを持っていることを意味します。

3 回の接続試行

NetDefendOS は、3 回通信を試みた後、アカウンティングサーバが通信不能であると見なします。管理者は、「Allow on error」という NetDefendOS 拡張設定を使用して、このような状況への対処方法を決定できます。この設定が有効になっている場合、既に認証されているユーザのセッションには影響が及びません。設定が有効でない場合、反映されるすべてのユーザは、既に認証されていても自動的にログアウトされます。

9.9.8 アカウンティングとシステムのシャットダウン

何らかの原因でクライアントが RADIUS アカウンティング要求 STOP パケットの送信に失敗した場合、アカウンティングサーバはそのユーザ統計情報を更新することができませんが、セッションがまだアクティブであると見なしてしまうことが予想されます。この状況を回避する必要があります。

認証ユーザのオンライン中にファイアウォール管理者がシャットダウンコマンドを発行した場合に、AccountingRequest STOP パケットがいつまでも送信されないことが考えられます。これを回避するためには、「Logout at shutdown」という拡張設定を使用して、NetDefendOS がシャットダウンを開始する前にまず、構成された任意の RADIUS サーバに任意の認証ユーザの STOP メッセージを送信するよう明示的に指定できます。

9.9.9 NAT での制約

NetDefendOS のユーザ認証モジュールは、ユーザの IP アドレスを基本としています。そのため、同じ IP アドレスを持つユーザに問題が発生する場合があります。

例えば、NAT を使用する同一のネットワーク内にいる複数のユーザが、1 つの外部 IP アドレスを介してネットワークアクセスを許可された場合などにこうした問題が発生します。すなわち、一人のユーザが認証された直後、NAT ゲートウェイ IP アドレスを通じて入ってくるトラフィックが、実際には同じネットワーク内の他のユーザからのものであっても、一人の認証ユーザからのものであると見なされる可能性があります。このため、NetDefendOS RADIUS アカウンティングは、複数個別のユーザではなく一人のユーザであっても、ネットワーク上のすべてのユーザの統計情報をまとめて収集します。

9.9.10 詳細な RADIUS 設定

RADIUS アカウンティングに以下の詳細な設定を行うことができます。

項目	説明
Allow on error	認証済みユーザのアカウンティングデータの送信時に設定した RADIUS アカウンティングサーバから応答がない場合でも、本設定を有効にするとユーザはログインしている状態が維持されます。 本設定を無効にすると、ユーザが認証済みであっても、RADIUS アカウンティングサーバに到達できない場合にはログアウトされます。 初期値 : Enabled（有効）
Logout at shutdown	管理者がファイアウォールの計画的なシャットダウンを行う場合、NetDefendOS は、設定されたすべての RADIUS サーバに RADIUS アカウンティング STOP メッセージを送信するまで、シャットダウンを遅らせます。 本オプションを有効にしないと、正しく終了されなかった RADIUS アカウンティングセッションがあっても、NetDefendOS はシャットダウンを行います。これは、RADIUS サーバは、セッションが終了してもユーザがまだログインしていると見なすという状況を引き起こします。 初期値 : Enabled（有効）
Vendor-Specific attribute at Accounting-Request messages	Accounting-Request メッセージで、RADIUS サーバに対してベンダー固有のアトリビュートを送信します。
Vendor-Specific attribute at Access-Request messages	Access-Request メッセージで、RADIUS サーバに対してベンダー固有のアトリビュートを送信します。
Log authenticated ALG user	認証ユーザ及び URL を ALG ログメッセージに出力します。
Log authenticated Conn user	認証ユーザ名を CONN ログメッセージ内に出力します。
MaxRADIUSContexts ID	RADIUS で許可するコンテキストの最大数。これはアカウンティングと認証の両方における RADIUS の使用に適用されます。 初期値 : 1024

第 10 章 VPN

この章では、NetDefendOS における仮想プライベートネットワーク（VPN）機能について説明します。

- 「10.1 概要」
- 「10.2 VPN クイックスタートガイド」
- 「10.3 IPsec」
- 「10.4 PPTP/L2TP」
- 「10.5 L2TP バージョン 3」
- 「10.6 SSL VPN」

10.1 概要

10.1.1 VPN の必要性

多くのネットワークは、インターネットによって相互に接続しています。インターネットが効率的で安価な通信を提供するため、ビジネスでの使用がますます増大しています。他人が読んだり、変更することなく、希望する受信者にインターネットを経由してデータを送信する手段を必要としています。

受信者は、(誰かのふりをしているなど)誰も情報を偽造していないことを確認することが、さらに重要です。Virtual Private Networks(VPN)はこのニーズを満たしており、安全な方法で情報を交換したいと思う相手と安全なリンクを確立する手段を提供します。

VPNはトンネルエンドポイントとして知られている2つのデバイス間のトンネルを設定することができます。トンネルを経由して流れるすべてのデータが安全です。トンネルセキュリティを提供するメカニズムは暗号化です。

VPN が使用されている 2 つの一般的なシナリオがあります。

LAN to LAN 接続

2 つの内部ネットワークがインターネットを経由して関連づけられる必要がある場合。この場合、各ネットワークはそれぞれの D-LInk ファイアウォールによって保護され、VPN トンネルはそれらの間で設定されます。

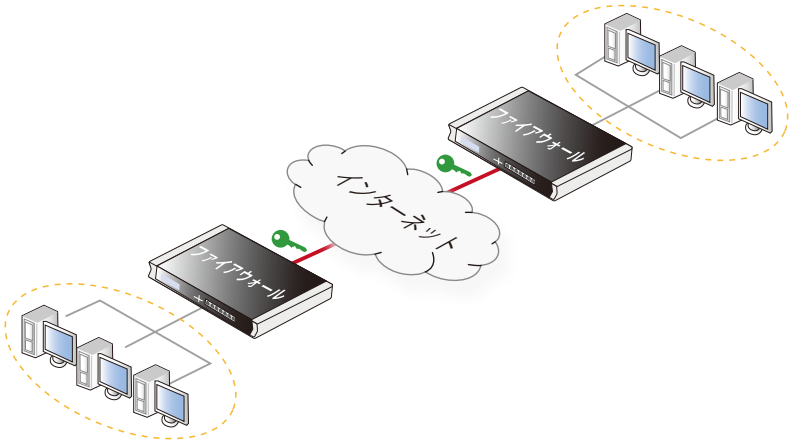


図 10-1　LAN to LAN VPN 接続図

Client to LAN 接続

多くのリモートクライアントがインターネットを経由して内部ネットワークに接続する必要がある場合。この場合、内部ネットワークはクライアントが接続するファイアウォールによって保護され、VPN トンネルはそれらの間で設定されます。

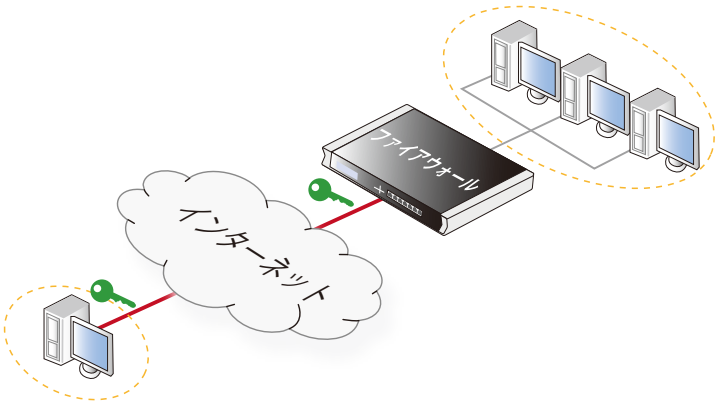


図 10-2　Client to LAN VPN 接続図

10.1.2 VPN 暗号化

VPN トラフィックの暗号化は暗号化の技術を使用して行われます。暗号は 3 つの基礎的な技術と利益をもたらします。

機密性

意図した受信者以外は通信を途中で受信し、解析することはできません。暗号化によって機密性が得られます。

認証と完全性

通信が本当に送信者からなされたか、そしてデータが転送中に改ざんされていないかを受信者に証明します。これは多くの場合、暗号鍵のハッシュによる認証によって行われます。

否認防止

実際にデータを送信した送信者は、後からそれを送ったことを否定することができません。否認防止は、認証の副次的なメリットとみなされます。

VPN は通常、機密性と認証に関係しているだけです。否認防止は通常ネットワークレベルで処理されるのではなく、むしろより高いトランザクションレベルで行われます。

10.1.3 VPN の計画

VPN 接続に対して攻撃をしようとしている者は、莫大な作業を必要とするので、一般的に VPN 暗号化を破るような方法は試みないと考えられます。むしろ、彼らは、その接続の端にこそ本当に脆弱で狙うべきものがあるということを、VPN トラフィックが示していると考える可能性があります。一般的に、モバイルクライアントと支社は、本社のネットワーク以上によく狙われます。一度そこに侵入してしまえば、社内ネットワークへの侵入は簡単になるためです。

VPN の設計においては、いつもは明らかにされないが提起すべき問題が多くあります。

- モバイルコンピュータと自宅用コンピュータを保護すること。
- モバイルコンピュータは脆弱なので、VPN を通した接続は必要なサービスに制限すること。
- VPN を通して他の会社で共用する必要があるサービスのために DMZ を作ること。
- ユーザのグループごとに VPN の接続ポリシーを適用すること。
- 鍵の配布ポリシーを決めること。

エンドポイントセキュリティ

VPN 接続はセキュリティの観点から内部のネットワークと同等であり、それ以上の警戒なしで直接接続してかまわないと誤解されることがよくあります。VPN 接続自体は安全かもしれませんが、全体でのセキュリティレベルは VPN トンネルの終端のセキュリティと同じものになるのです。

ユーザによるラップトップまたはタブレットから VPN 経由で会社ネットワークに直接接続するという流れは、ますます一般的になっています。しかし、クライアントの機器自体は保護されていないことが多いのです。別の言い方をすれば、侵入者は無防備のモバイルコンピュータと既に開かれた VPN 接続を通して、保護されたネットワークにアクセスすることができてしまうのです。

DMZ における位置決め

つまり、VPN 接続は決して保護されたネットワークの一部とみなすべきではありません。VPN ファイアウォールは、特別の DMZ か、VPN 専用のファイアウォールの外に置かれるべきなのです。こうすることによって、管理者は、VPN 経由の接続を受けるサービスを制限でき、侵入者に対してこれらのサービスがきちんと保護されているということを確認することができます。統合されている VPN 機能では、ファイアウォールはたいていの場合接続の種類によって許可を行うようにすることが可能です。NetDefendOS にも、もちろんこのような機能があります。

10.1.4 鍵の配布

はじめに鍵の配布方法を計画します。以下の点について決定します。

- どのような方法で鍵を配布するか。電子メールを使うのは良い考えではありません。電話による伝達は、十分に安全だと考えられます。
- 鍵の数をいくつにするか。ユーザごとに 1 つの鍵にするか。ユーザグループごとに 1 つの鍵にするか。接続する LAN ごとに 1 つの鍵にするか。すべてのユーザとすべての接続する LAN で 1 つの鍵にするか。将来的にユーザやグループの接続を調整することが簡単になるので、現在必要と思われるものよりも多くの鍵を使うようにする方がよいかもしれません。
- 鍵を変更するべきか。もしそうであれば、頻度はどれくらいにするか。鍵が複数のユーザによって共用される場合、新しい鍵が発行された時に古い鍵も短期間使えるように重複する方法を使用することを検討してください。
- 鍵を所有している従業員が会社をやめる時には、どうするか。複数のユーザが同じ鍵を使っているならば、変更する必要があります。
- VPN ファイアウォールのような直接鍵を扱うことができるネットワーク装置がない場合、鍵はどこに保管されるべきか。フロッピーディスクか。パスフレーズとして記憶するか。スマートカードか。物理的な媒体であれば、それはどのように保管するべきか。

10.1.5 VPN の TLS 代替策

HTTP を使用する、クライアントから Web サーバへの安全なアクセスを考慮しているシナリオであれば、TLS 終端に D-Link ファイアウォールを使用すると、簡単ですぐ実行できる代わりの「軽い」VPN の手法を実現できます。詳しくは、「6.1.11 TLS ALG」を参照してください。

10.2 VPN クイックスタートガイド

概要

本章の後のセクションで VPN コンポーネントについて詳しく説明します。後のセクションのために、このセクションでは VPN 設定の重要な手順を簡単に説明します。多くの場合、IKEv1 と IKEv2 の設定手順は同じであり、異なる点については明示的に説明しています。IKEv2 はより堅牢であり、built-in クライアントの多くは IKEv2 ベースであるため、通常は IKEv2 が推奨されます。ただし IKEv2 は L2TP では使用できません。

最も一般的な VPN シナリオを使用して VPN 設定の各手順を概説します。

- 事前共有鍵を使用した IPsec LAN to LAN
- 証明書を使用した IPsec LAN to LAN
- 事前共有鍵を使用した IPsec ローミングクライアント
- 証明書を使用した IPsec ローミングクライアント
- 事前共有鍵を使用した L2TP/IPsec ローミングクライアント
- 証明書を使用した L2TP/IPsec ローミングクライアント
- PPTP ローミングクライアント

IPsec トンネルの設定を簡単に行うことが可能

以下の IPsec トンネル設定手順は標準の IPsec Tunnel オブジェクトに基づいています。NetDefendOS では、LAN-to-LAN VPN やローミング VPN オブジェクトも提供しており、これらのオブジェクトにより NetDefendOS LAN-to-LAN そしてローミングクライアントの設定を簡単に行うことができます。
これらの IPsec プロファイルオブジェクトでは、シナリオに関連しない IPsec Tunnel オブジェクトプロパティが非表示となり、さらに、認証設定も簡易化されています。詳細は「10.3.15 IPsec プロファイルの使用」を参照してください。

一般的なトンネル設定の要件

各シナリオを参照する前に、タイプに関係なく VPN トンネル設定時の一般的な NetDefendOS の要件をまとめることが役に立ちます。

- トンネルを定義します。
  はじめに、トンネルを定義する必要があります。NetDefendOS には、IPsec トンネルオブジェクトなど、トンネルの定義に使用される様々なトンネルオブジェクトタイプがあります。
- ルートが必要です。
  どのトラフィックもトンネルに流れる前に、NetDefendOS ルーティングテーブルにルートを定義する必要があります。このルートが、トンネルの一端で見つけることができるネットワークを NetDefendOS に通知することで、どのトラフィックをトンネルに送ったらよいかがわかります。

  多くの場合、トンネルが定義される時、自動的にこのルートは作成され、これは、ルーティングテーブルを検証することでチェックされます。

  ルートが手動で定義されると、トンネルは、それが NetDefendOS の他の側面にあるので、ルートのプロパティではちょうど物理インタフェースのように扱われます。つまり、ルートは、あるネットワークがトンネルの別の一端で検出されることを NetDefendOS に伝えます。
- VPN トラフィックを許可する IIP ポリシーを定義します。
  トラフィックがネットワークとトンネル間を明確にフローできるように IP ポリシーを定義する必要があります。IP ポリシーを定義する場合、ルート定義と同様に、トンネルは物理インタフェースのように扱われます。

  トンネルオブジェクトの定義後に、IP ポリシーが自動的に作成されずに存在していないと、トラフィックは、トンネルを通って流れずに、破棄されます。

以下のセクションでは、以前に示した各 VPN シナリオの詳細な設定を記述します。

10.2.1 事前共有鍵を使用した IPsec LAN to LAN

目的は、以下の 2 つのネットワークを結合する安全な手段を作成することです。

- ローカルファイアウォールの保護された側となるローカルネットワーク
- リモートデバイスの向こう側にあり、インターネットなどの安全ではないネットワーク経由で配置された、リモートネットワーク

設定の手順は以下の通りです。

1. はじめに、事前共有鍵を作成します。

2. デフォルトのアルゴリズムのプロポーザルリストがトンネルのリモートエンドポイントにアクセスするアルゴリズムを提供していない場合、新しい IKE Algorithms オブジェクト、そして / または、IPsec Algorithms オブジェクトをオプションで作成します。これはトンネルの反対側にあるデバイスの機能によります。

3. アドレス帳に、以下の IP オブジェクトを作成します。
   - リモート VPN ゲートウェイは、トンネルのもう一方の端にあるネットワーク装置（このオブジェクトを remote_gw と呼ぶ）の IPv4 アドレスを持ちます。これは別の D-Link ファイアウォールであるかもしれません。
   - リモート VPN ゲートウェイ（このオブジェクトを remote_net と呼ぶ）の背後にあるリモートネットワーク。
   - ファイアウォールの配下のローカルネットワークは、トンネルを経由して通信します。ここでは、ローカルネットワークは定義済みアドレス「lannet」であり、ネットワークが IPv4 アドレス lan_ip を持つ NetDefendOS lan インタフェースに接続しているものと仮定します。

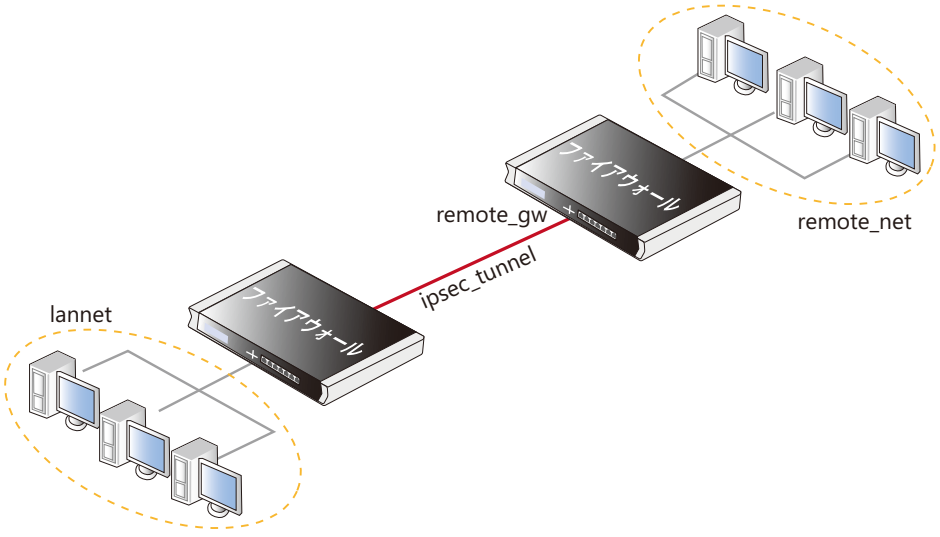


図 10-3　IPsec LAN to LAN 図

4. IPsec トンネルオブジェクトを作成します。（このオブジェクト ipsec_tunnel と呼びます。）以下のトンネルパラメータを指定します。
- IKE バージョンを選択します。最初に IKEv2 が試行される Auto オプションが推奨されます。
- ローカルネットワークに lannet を設定します。
- リモートネットワークに remote_net を設定します。
- リモートエンドポイントに remote_gw を設定します。
- IKEv1 の場合、Encapsulation Mode で Tunnel を指定します。IKEv2 の場合は常に Tunnel モードとなるため、指定する必要はありません。
- 使用する IKE と IPsec のアルゴリズムプロポーザルリストを選択します。
- 認証に関しては、上のステップ（1）で定義された事前共有鍵を選択します。
- IPsec トンネルプロパティの Add route statically は初期値で有効化されており、NetDefendOS コンフィギュレーションの main ルーティングテーブルに Remote Network へのルートを自動的に追加します。手動でルートを追加する必要はありません。

IPsec Tunnel オブジェクトは、次の手順で説明する NetDefendOS インタフェースオブジェクトと同じように扱われます。

5. IP ルールセットにおける 2 つの IP ルールをトンネルに設定します。
- 宛先インタフェースとして定義済みの ipsec_tunnel オブジェクトを持つ外向きトラフィックのための Allow ルール。ルールの宛先ネットワークはリモートネットワーク remote_net です。
- ソースインタフェースとして定義済みの ipsec_tunnel オブジェクトを持つ内向きトラフィックのための Allow ルール。ソースネットワークは remote_net です。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
Allow	lan	lannet	ipsec_tunnel	remote_net	all_services
Allow	ipsec_tunnel	remote_net	lan	lannet	all_services

これらのルールに使用されるサービスオブジェクトは、all_services ですが、定義済みまたはカスタムサービスとすることも可能です。

6. VPN トンネル ipsec_tunnel が、トンネルのもう一方の端でリモートネットワークに向かうルーティングパケットに対して使用するインタフェースであることを指定する新しい NetDefendOS Route を定義します。

インタフェース	ネットワーク	ゲートウェイ
ipsec_tunnel	remote_net	

実際のコンフィグレーションの手順を示す LAN-to-LAN の例については、「PSK ベースの LAN-to-LAN IPsec トンネルの設定」を参照してください。

10.2.2 証明書を使用した IPsec LAN to LAN

LAN to LAN セキュリティには、通常事前共有鍵を提供しますが、代わりに X.509 証明書を使用することが望ましい場合もあります。その場合、Certificate Authority（CA）が署名した証明書を使用します。これらは内部の CA サーバ、または、証明書の商業サプライヤから取得します。

証明書を使用した LAN to LAN トンネルの作成は、事前共有鍵を使用した前のセクションと同じ手順に従って行います。その違いは、証明書が認証用の事前共有鍵を交換することです。

2 つの CA 署名入り証明書のセット（エンド証明書、ルート証明書、およびゲートウェイ証明書のいずれか 2 つ）が LAN to LAN トンネル認証に必要です。

設定手順は以下の通りです。

1. トンネルの一端にある D-Link ファイアウォールの管理 Web インタフェースを開きます。

2. **Object > General > Key Ring > Add > Certificate** の順にメニューをクリックし、Root Certificate と Gateway Certificate を NetDefendOS にアップロードします。ルート証明書は公開鍵用に 1 つの証明書ファイルのみを必要とします。ゲートウェイ証明書には、次の 2 つの部分が必要です。公開鍵と秘密鍵のための証明書ファイル。また、ルートとゲートウェイ証明書間の証明書チェーンに必要な中間証明書についても、アップロードされる公開鍵キー用の証明書ファイルを持つ必要があります。

注意 Gateway Certificate は Host Certificate と呼ばれることもあります。

3. IPsec Tunnel オブジェクトを事前共有鍵に設定しますが、Authentication タブで使用する証明書を指定します。これを以下の手順で行います。
- X.509 認証オプションを有効にします。
- 追加するルート証明書を選択します。ゲートウェイ証明書への証明書チェーンがあると、ルート証明書としてすべての中間的証明書も追加する必要があります。
- ゲートウェイ証明書を選択します。

4. トンネルのもう一端にある D-Link ファイアウォール用の管理 Web インタフェースをオープンし、異なる証明書のセットに対して上記手順を繰り返します。

また、詳細は「3.9.4 CA サーバアクセス」を確認してください。証明書の有効性についての重要な事柄について説明しています。

CA 署名の代わりに自己署名証明書を LAN to LAN トンネルに使用できますが、Web インタフェースおよび他のインタフェースには、それらを生成する機能はありません。代わりに、それらを別のユーティリティで生成して、NetDefendOS にインポートします。つまり、NetDefendOS 制御外で生成されるため、本当は自己署名ではなく、それらの非公開鍵が固有であるという保証がないことを忘れるべきではありません。それでも、提供されるセキュリティが、シナリオによっては適切であると考えることもできます。

2 つの自己署名証明書が必要とされ、同じ 2 つの証明書がトンネルの他の端でも使用されますが、それらの用法は逆にします。つまり 1 通の証明書がルート証明書として片端（サイド A と呼ぶ）で使用され、もう一方の端（サイド B と呼ぶ）のホスト証明書として使用されます。2 番目の証明書は逆の方法（サイド A ではホスト証明書であり、サイド B ではルート証明書）で使用されます。

CRL の検索が行われないため、CA サーバの考慮は自己署名証明書には必要ではありません。

参照 D-Link VPN オブジェクトにより設定を簡単に行うことができる

上記の IPsec LAN-to-LAN 設定手順は標準の IPsec Tunnel オブジェクトに基づいています。NetDefendOS では、D-Link VPN オブジェクトも提供しており、これらのオブジェクトにより IKEv2 と（または）PSK、または証明書を使用した 2 つの D-Link ファイアウォール間の LAN-to-LAN IPsec 通信の設定を簡単に行うことができます。詳細は「10.3.15.1 LAN to LAN VPN」を参照してください。
IPsec Tunnel オブジェクトを使用して LAN-to-LAN トンネルを設定する例については「10.3.6 事前共有鍵を使用した LAN to LAN トンネル」を参照してください。

10.2.3 事前共有鍵を使用した IPsec ローミングクライアント

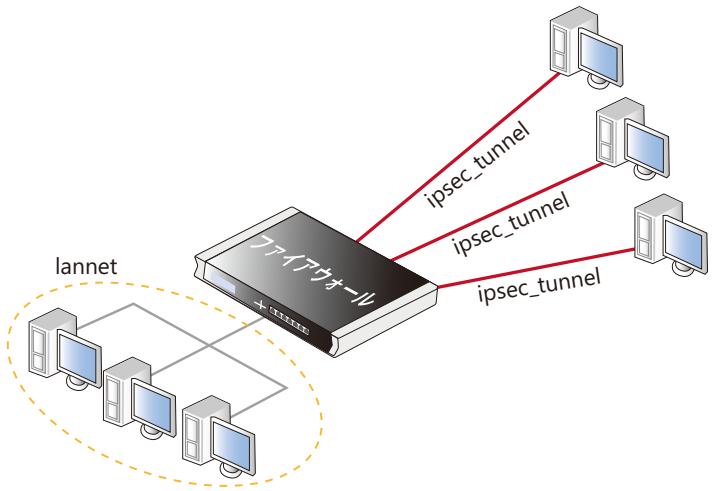


図 10-4　IPsec ローミングクライアント図

ここでは、事前共有鍵を使用した IPsec トンネルを経由して D-Link ファイアウォールの背後に位置する保護されたローカルネットワークに接続するローミングクライアントの設定について説明します。2 つのタイプのローミングクライアントがあります。

- A - クライアントの IPv4 アドレスを事前に割り当てます。
- B - クライアントが接続を試みる場合、クライアントの IPv4 アドレスを事前に知らないため NetDefendOS が与える必要があります。

A IP アドレスが割り当て済み

クライアントが接続する前に、事前に IPv4 アドレスを知り、ローミングクライアントに割り当てられている可能性があります。クライアントの IP アドレスは手動で VPN クライアントソフトウェアに入力されます。

1. IKE バージョンを選択します。iOS や Windows™ 上の in-built クライアントでは通常 IKEv2 を使用します。

2. ユーザ認証を設定します。IKEv1 ではトンネルオブジェクトで XAuth、IKEv2 では EAP を有効化する必要があります。認証ソースは以下のいずれかとなります。
   - NetDefendOS に内部であるローカルユーザ DB オブジェクト
   - 外部認証ユーザ

   内部のユーザデータベースは設定が簡単であり、ここではこの設定を想定しています。これを外部サーバに変更するのは後で簡単に行えます。

内部データベースでユーザ認証を実装する。
- ローカルユーザ DB オブジェクトを定義します。（このオブジェクトを TrustedUsers と呼びます。）
- 各ユーザを TrustedUsers に追加します。これは少なくともユーザ名とパスワードの組み合わせから構成されます。

グループのアクセスが、特定のソースネットワークに制限される場合、ユーザに対してグループ名を指定することができます。グループは IP オブジェクトの認証セクションに（同じテキスト名で）指定されます。次に、その IP オブジェクトが IP ルールセットのソースネットワークとして使用されると、そのルールは、ユーザのグループ名が IP オブジェクトのグループ名に一致する場合にだけユーザに適用されます。

注意 グループには、認証ルールは適用されません。

- TrustedUsers に設定した認証ソースで新しいユーザ認証ルールを作成します。ルールに対する他のパラメータは以下の通りです。

エージェント	認証ソース	送信元ネットワーク	インタフェース	クライアントソース IP
XAUTH (IKEv1) または EAP (IKEv2)	Local	all-nets	any	all-nets (0.0.0.0/0)

3. IPsec トンネルオブジェクト ipsec_tunnel には、以下のパラメータがあります。

- ローカルネットワークに lannnet を設定します。
- リモートネットワークに all-nets を設定します。
- リモートエンドポイントに all-nets を設定します。
- IKEv1 ではトンネルを Encapsulation モードに指定します。IKEv2 では常にトンネルを使用するため指定する必要はありません。
- IKE と IPsec プロポーザルリストをクライアントの機能に適合するように設定します。
- 1 つのルートも事前に定義できないので、Add route dynamically オプションをトンネルオブジェクトで有効にします。all-nets が送信先ネットワークであれば、Add route statically オプションを無効にします。（これは通常 LAN-to-LAN トンネルのみで使用されます）

注意 ダイナミックにルートを加えるオプションを LAN to LAN トンネルシナリオでは有効にするべきではありません。

- IKEv1 では、「Require IKE XAuth user authentication for inbound IPsec tunnels」を有効化します。IKEv2 では RAP プロパティを EAP Server に指定します。クライアント接続時、NetDefendOS は認証ルールで最初に一致する XAUTH ルールを検索します。

4. IP ルールセットはただ一つのルールを含むべきです。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
Allow	ipsec_tunnel	all-nets	lan	lannet	all_services

Allow ルールが、接続が設定されることを許可すると、双方向のトラフィックフローが許可されます。そのため、ここでは 1 つのルールだけが使用されています。上記で使用される all-nets の代わりに、あらかじめ割り当てられた IP アドレスの正確な範囲を指定するより安全な定義済みの IP オブジェクトを使用することもできます。

B NetDefendOS による IP アドレスの付与

クライアント IP アドレスを知らない場合、NetDefendOS はそれらを付与する必要があります。そのようにするには、以下の通り上記設定を変更する必要があります。

1. 特定の IP アドレス範囲がその時に利用可能なアドレスプールとして使用する場合 :
- （NetDefendOS インストール時に関連付けされている）Config Mode Pool オブジェクトを作成し、そこにアドレス範囲を指定します。
- IPsec トンネルオブジェクト ipsec_tunnel で IKE Config Mode Pool オプションを有効にします。

2. クライアント IP アドレスが DHCP を通じて取得される場合 :
- IP プールオブジェクトを作成し、そこに使用する DHCP サーバを指定します。DHCP サーバはシンプルな IP アドレスとして指定されるか、または、代わりに特定のインタフェースでアクセス可能であるとして指定できます。内部の DHCP サーバが使用される場合、DHCP サーバの IP アドレスとしてループバックアドレス 127.0.0.1 を指定します。
- （NetDefendOS インストール時に関連付けされている）Config Mode Pool オブジェクトを作成し、以前の手順で定義した IP Pool オブジェクトに割り当てます。
- 作成したプールが選択されるように IPsecTunnel オブジェクト ipsec_tunnel の IKE Config Mode オプションを設定します。

IKE コンフィグモードについては「10.3.11 コンフィグモード」を参照してください。

ローミングクライアント用の実際のコンフィグレーション手順については「ローミングクライアント用の PSK ベース IPsec トンネルの設定」と「10.3.7 IPSec ローミングクライアント」参照してください。

実際のコンフィグレーションの手順を示すローミングクライアントの例については、「ローミングクライアント用の PSK ベース IPsec トンネルの設定」を参照してください。

10.2.4 証明書を使用した IPsec ローミングクライアント

証明書が事前共有鍵の代わりに IPsec ローミングクライアントで使用される場合、事前共有鍵オブジェクトは必要ではなく、上で説明した設定における他の違いは以下の通りです。

1. ルート証明書とゲートウェイ証明書を NetDefendOS にアップロードします。ゲートウェイ証明書には、次の 2 つを追加する必要があります。証明書ファイル（通常、ファイルタイプ「.cer」または「.crt」）と秘密鍵ファイル（ファイルタイプ「.key」）ルート証明書には、証明書ファイルのみ追加が必要です。

   NetDefendOS に証明書をアップロードする手順については「3.9.2 証明書のアップロードと使用」を参照してください。

2. IPsec Tunnel オブジェクトを設定する場合、認証下で使用する証明書を指定します。以下の方法で行われます。
   - X.509 認証オプションを有効にします。
   - ゲートウェイ証明書を選択します。
   - ルート証明書を追加します。

3. IPsec クライアントソフトウェアは証明書とリモート IP アドレスが適切に設定される必要があります。既に上で言及した通り、多くのサードパーティの IPsec クライアント製品が入手可能であり、本マニュアルでは特定のクライアントについては記載しません。

認証ルールの設定は追加のセキュリティであり、オプションとなります。上記で説明した通り、XAuth は IKEv1 で使用され、EAP は IKEv2 で使用されます。いずれの場合もユーザ名とパスワードを入力する必要があり、ローカルユーザデータベースまたは外部の RADIUS サーバによって認証されます。

また、後述の「3.9.4 CA サーバアクセス」を見直してください。証明書の有効性についての重要な事柄について説明しています。

D-Link VPN オブジェクトにより設定を簡単に行うことができるローミング VPN オブジェクトにより IKEv2 設定を簡単に行うことができる

上記の IPsec ローミングクライアント設定は IPsec Tunnel オブジェクトに基づいています。NetDefendOS ではローミング VPN オブジェクトも提供しており、EAP 認証で証明書を使用する IKEv2 ローミングクライアントの設定を簡単に行うことができます。このオブジェクトについては「10.3.15.2 ローミング VPN」で説明します。

標準の IPsec Tunnel オブジェクトを使用した証明書による IKEv2 ローミングクライアントの設定については、「10.3.13 IKEv2 ローミングクライアントセットアップ」を参照してください。

IPsec のすべてのユースケースにおける証明書の使用に関しては「10.3.8 証明書を使用した IPSec」を参照してください。

10.2.5 事前共有鍵を使用した L2TP ローミングクライアント

Microsoft Windows™ には L2TP クライアントが組み込まれているため、L2TP はローミングクライアントの VPN シナリオにとって一般的な選択肢です。通常、L2TP は、IPsec にカプセル化され、トンネルモードの代わりにトランスポートモードで動作して、IPsec と共に暗号化を提供します。トンネル設定時、トランスポートモードでは IKEv2 を使用できないため IKEv1 を使用してください。

IPsec 上の L2TP 設定のための手順は以下の通りです。

1. クライアントに付与できる IP アドレスの範囲を定義する IP オブジェクト（それを l2tp_pool と呼ぶ）を作成します。選択範囲には 2 つのタイプがあります。
   - クライアントが接続する内部ネットワークから取得した範囲。内部ネットワークが 192.168.0.0/24 であれば、アドレス範囲 192.168.0.10-192.168.0.20 を使用します。IP アドレスが内部ネットワークで意図せず使用されて、クライアントにも付与されてしまうかもしれないという危険があります。
   - どの内部のネットワークとも完全に異なる新しいアドレス範囲を使用します。これはまた、範囲内のアドレスが内部ネットワークで使用されるという機会を防ぎます。

2. 別の 2 個の IP オブジェクトを定義します。
   - wan_ip は、クライアントが接続する（これが wan インタフェースにあると仮定する）外部のパブリック IPv4 アドレスです。
   - lan_ip は、内部ネットワークに接続する（このインタフェースを lan と呼ぶ）インタフェースの内部 IP アドレスです。

3. IPsec トンネルのために「Pre-shared Key」（事前共有鍵）を定義します。

4. 以下のパラメータで IPsec Tunnel オブジェクト（ipsec_tunnel と呼ぶ）を定義します。
- IKE バージョンを IKEv1 に指定します。
- Encapsulation Mode を Transport に設定します。
- 「Local Endpoint」に wan_ip を設定します（NetDefendOS が NAT 変換するデバイスの配下にある場合、代わりに all-nets を指定します）。
- 「Remote Endpoint」に all-nets を設定します。
- Pre-shared key を指定します。
- 使用する IKE と IPsec プロポーザルリストを選択します。
- 送信先ネットワークが「all-nets」であれば、「Advanced Setting」オプションの「Add route statically」は無効にされるべきです。この設定は、初期値で無効です。

5. 以下のパラメータを使用して、PPTP/L2TP サーバオブジェクト（l2tp_tunnel と呼ぶ）を定義します。
- 「Inner IP Address」（内部 IP アドレス）に lan_ip を設定します。
- 「Tunnel Protocol」（トンネルプロトコル）に L2TP を設定します。
- 「Outer Interface Filter」に ipsec_tunnel を設定します。
- 「Server IP」に wan_ip を設定します。
- 「PPP Parameters」タブで Microsoft Point-to-Point Encryption を None のみに設定します。IPsec 暗号化が既に使用されているので、二重暗号化はスループットを低下させます。
- 「IP Pool」に「l2tp_pool」を設定します。
- 「Add Route」タブで内部ネットワークに接続する lan インタフェースでプロキシ ARP を有効にします。
- ルートが自動的にそのテーブルに追加されるように、「Virtual Routing」タブで、「Make interface a member of a specific routing table.」にチェックを入れ、このインタフェースを特定のルーティングテーブルのメンバにします。通常、main テーブルが選択されます。

6. ユーザ認証に対する設定 :
- 「Local User DB」（ローカルユーザ DB）オブジェクトを定義します。（このオブジェクトを TrustedUsers と呼びます。）
- 各ユーザを TrustedUsers に追加します。これは少なくともユーザ名とパスワードの組み合わせから構成されます。また、ユーザにグループ名を指定できます。これは、上の「10.2.3 事前共有鍵を使用した IPsec ローミングクライアント」で同様の手順を説明しています。
- ユーザ認証ルールを定義します。

エージェント	認証ソース	送信元ネットワーク	インタフェース	クライアントソース IP
L2TP/PPTP/SSL VPN	Local	all-nets	l2tp_tunnel	all-nets (0.0.0.0/0)

7. L2TP トンネル経由でトラフィックを許可するために、以下のルールを IP ルールセットに定義します。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
Allow	l2tp_tunnel	l2tp_pool	any	int_net	all_services
Allow/NAT	l2tp_tunnel	l2tp_pool	ext	all-nets	all_services

2 番目のルールは、クライアントが D-Link ファイアウォールの ext インタフェースでインターネットの閲覧を許可するために含まれます。次に、ファイアウォール経由でパブリックインターネットの外側に接続している場合 NAT 変換される必要があるプライベートな内部 IP アドレスをクライアントに割り当てます。

8. クライアントを設定します。Windows™ の場合、ネットワーク接続オプションの「新しい接続を作成する」を選択して「New Connection Wizard」を開始します。このウィザードに入力する主要な情報は以下の通りです。ファイアウォールの名前の解決ができる URL または代わりにその wan_ip の IP アドレス。

その後、**ネットワーク > プロパティ**の順に選択します。表示されたダイアログで L2TP トンネルを選択し、さらにプロパティを選択します。表示されたダイアログで「Networking」タブをクリックし、L2TP に対して「Force」を選択します。また、「L2TP Tunnel」プロパティに戻り、「Security」タブを選択し、「IPsec Settings」ボタンをクリックします。事前共有鍵を入力します。

10.2.6 証明書を使用した L2TP/IPsec ローミングクライアント

証明書が事前共有鍵の代わりに L2TP ローミングクライアントが使用される場合、上で説明した設定における違いは以下の通りです。

1. 証明書には期限があるため、NetDefendOS 日時は正確に設定されなければなりません。

2. ゲートウェイ証明書とルート証明書を NetDefendOS にロードします。

3. IPsec Tunnel オブジェクトを設定する場合、Authentication タブで使用する証明書を指定します。以下の方法で行われます。
   - Authentication Method で「Certificate」を選択します。
   - 「Gateway Certificate」（ゲートウェイ証明書）を選択します。
   - 「Root Certificate」（ルート証明書）を設定します。

4. Windows™ の L2TP クライアントを使用する場合、適切な証明書が、「New Connection Wizard」により接続設定を行う前に、Windows™ にインポートされる必要があります。

ユーザ認証を設定する手順は、証明書への追加セキュリティであるため、オプションとなっています。

後述の「3.9.4 CA サーバアクセス」を参照してください。証明書の有効性についての重要な事柄について説明しています。

10.2.7 PPTP ローミングクライアント

PPTP は、IPsec が使用されず、代わりに PPTP 自身のあまり強くない暗号に依存するため、L2TP よりも設定が簡単です。

主な 2 個目の短所は、トンネルを経由した PPTP 接続を NAT 変換できないことです。そのため、複数のクライアントが、D-Link ファイアウォールに対して単一の接続を試みます。NAT 変換が試されると、接続しようとする最初のクライアントだけが接続に成功します。

PPTP 設定の手順は以下の通りです。

1. 「Address Book」（アドレス帳）で以下の IP オブジェクトを定義します。
   - 内部ネットワークから付与される内部 IP アドレスの範囲である pptp_pool IP オブジェクト。
   - アドレスが生じる内部ネットワークである int_net オブジェクト。
   - lan_ip オブジェクトは、内部ネットワークに接続するインタフェース（このインタフェースを lan と呼ぶ）の内部 IP アドレスです。
   - wan_ip オブジェクトは、クライアントが接続する外部のパブリック IP アドレス（これが wan インタフェースにあると仮定する）です。

2. 以下のパラメータを使用して、PPTP/L2TP オブジェクト（このオブジェクト pptp_tunnel と呼ぶ）を定義します。
   - 「Inner IP Address」（内部 IP アドレス）に ip_net を設定します。
   - 「Tunnel Protocol」（トンネルプロトコル）に PPTP を設定します。
   - 「Outer Interface Filter」に wan を設定します。
   - 「Server IP」に wan_ip を設定します。
   - Microsoft Point-to-Point Encryption に対しては、128 ビットの暗号化以外の全オプションを無効にすることをお勧めします。
   - 「IP Pool」に pptp_pool を設定します。
   - lan インタフェースでプロキシ ARP を有効にします。
   - L2TP のように main ルーティングテーブルへの新しいルートの自動挿入を有効にします。

3. ユーザ認証ルールを定義します。これは L2TP とほぼ同じです。

エージェント	認証ソース	送信元ネットワーク	インタフェース	クライアントソース IP
L2TP/PPTP/SSL VPN	Local	all-nets	pptp_tunne	all-nets (0.0.0.0/0)

4. IP ルールセットに IP ポリシーを設定します。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
Allow	pptp_tunnel	pptp_pool	any	int_net	all_services
Allow/NAT	pptp_tunnel	pptp_pool	ext	all-nets	all_services

   L2TP で説明したように、NAT ルールは、D-Link ファイアウォール経由でクライアントをパブリックインターネットにアクセスさせます。

5. クライアントを設定します。Windows™ に関しては、手順は上記 L2TP で説明した通りですが、事前共有鍵は入力しません。

10.3 IPsec

このセクションでは、NetDefendOS の IPsec トンネルの設定方法と使用方法について説明します。特定のシナリオにおける IPsec の手順のクイックスタートチェックリストについては、次のセクションで確認することができます。

- 「10.2.1 事前共有鍵を使用した IPsec LAN to LAN」
- 「10.2.2 証明書を使用した IPsec LAN to LAN」
- 「10.2.3 事前共有鍵を使用した IPsec ローミングクライアント」
- 「10.2.4 証明書を使用した IPsec ローミングクライアント」

10.3.1 概要

IPsec（Internet Protocol Security）は、ネットワーク層の IP セキュリティを提供するために IETF（Internet Engineering Task Force）によって提起されたプロトコルのセットです。VPN に基づいた IPsec は、大きく以下の 2 つの部分から構成されます。

- IKE（Internet Key Exchange）プロトコル
- IPsec プロトコル（AH/ESP/both）

1 つ目の IKE は、最初のネゴシエーション段階で使用し、2 つの VPN の終端が IP トラフィックにセキュリティを提供するためにどのような方法を使うかを決定します。なお、IKE はそれぞれの接続に対して SA（Security Association）のセットを定義することによって、接続を管理します。SA は一方向性なので、通常各 IPsec 接続に対して少なくとも 2 つが存在します。

2 つ目は実際の IP データの転送で、IKE で事前に決定された暗号化と認証方式を使います。これは、IPsec プロトコルの ESP、AH または両方の組み合わせを使うなどいくつかの方法で実現されます。

このイベントの流れを簡単に説明すると、以下のようになります。

- IKE は IKE がどのように保護されるかをネゴシエーションします。
- IKE は IPsec がどのように保護されるかをネゴシエーションします。
- IPsec は VPN にデータを流します。

以下のセクションでは、詳しくこれらの各手順について記述します。

10.3.1.1 IKE（Internet Key Exchange）

このセクションでは、IKE（Internet Key Exchange）プロトコルと、使用するパラメータについて記述します。

データの暗号化、そして認証はとても単純です。暗号化と認証アルゴリズムとそのための鍵のみが必要になります。IKE（Internet Key Exchange）プロトコルは、セッション鍵を配布するための方式であり、データがどのように保護されるかについて、VPN 終端の合意を行うための方法を提供します。

IKE には 3 つの働きがあります。

- 終端がお互いに認証するための方法を提供する。
- 新しい IPsec 接続を確立する（SA のペアを作成する）。
- 既存の接続を管理する。

IKEv1 ではなく IKEv2 を使用する

IKE プロトコルには IKEv1 とより新しいバージョンの IKEv2 が存在します。NetDefendOS では両方のバージョンをサポートしますが、リモートトンネルピアの互換性のために IKEv1 を使用する必要がない限り、常に IKEv2 を使用することを推奨します。IKEv2 は、トンネルのセットアップ時間を大幅に短縮し、Diffie-Hellman ネゴシエーションの改善など、IKEv1 では利用できない機能を提供します。

セキュリティアソシエーション（SA）

IKE はそれぞれの接続に対して、SA（Security Association）のセットを与えることによって、接続を管理します。SA には、IPsec が使うプロトコル（ESP/AH/ 両方）、転送データの暗号化 / 復号化そして認証に使うセッション鍵と言ったものを含む、個々の接続に関連するすべてのパラメータが記述されています。SA は、単方向であり、一方向だけのトラフィックフローに関連します。そのため、通常、VPN で検出される双方向のトラフィックのために、1 接続あたり 1 個以上の SA が必要とされます。ESP あるいは AH のどちらか一方が使われるような多くの場合、それぞれの接続に対して SA は 2 つ作られ、1 つは入ってくるトラフィックについて、もう一方は出ていくものについて記述されます。ESP と AH の両方が使われる場合、4 つの SA が作られます。

IKE ネゴシエーション

接続セッションのネゴシエーション処理はいくつかのフェーズとモードから構成されます。以下のセクションに詳しく記述しています。

イベントの流れを、以下に簡単に記述します。

- **IKE フェーズ 1**
  - IKE をどうやって保護するかのネゴシエーション。
- **IKE フェーズ 2**
  - IPsec をどうやって保護するかのネゴシエーション。
  - VPN データフローの暗号化と認証で使用されるセッションキーを提供するため、フェーズ 1 の鍵交換から新しい鍵を取得します。

IKE と IPsec ライフタイム

IKE および IPsec 通信ではライフタイム値が設定されています。これにより、Rekey 処理の前に長期間の接続が保持されることを回避します。NetDefendOS ではどちらのライフタイムも 40 秒より短くすることはできません。

2 つのライフタイムは同じ値か、以下の値より大きくなるように設定します。

- IKE ライフタイム：600 秒（10 分）
- IPsec ライフタイム：300 秒（5 分）

NetDefendOS は、再送信の時間を考慮してライフタイム期限の 30 秒前に IPsec セキュリティアソシエーションの Rekey を実行します。つまり、ライフタイムが最小値の 40 秒の場合、IPsec セキュリティアソシエーションは 10 秒ごとに Rekey されます。ライフタイム値が低すぎる場合、NetDefendOS は再構成中に警告メッセージを発行します。

IKE アルゴリズムの提案

IKE の提案は、データを保護する方法の提案です。IPsec 接続を開始する VPN デバイスは、接続を防御するためにサポートするアルゴリズムの組み合わせリストを送信します。そして、どの提案を受け入れるかを通知するために接続のもう片方にあるデバイスにアップします。

応答する VPN デバイスは、このサポートアルゴリズムのリストを受信すると、自身のセキュリティポリシーに適するアルゴリズムの組み合わせを選択し、リストのどれを選択したかを指定することで応答します。受諾できる提案が検出されない場合、リストに受諾できるものがないことを通知することで応答し、診断のためその理由もできる限り提供します。

IPsec 接続を保護する最適な方法を見つけるだけではなく、IKE ネゴシエーション自体を保護する最適な方法を見つけるためにも、互いに許容できるアルゴリズムの組み合わせを見つけるこのネゴシエーションを行います。

アルゴリズムのプロポーザルリストには、データの暗号化と認証のために許容できるアルゴリズムの組み合わせだけではなく、他の IKE に関連するパラメータも含まれています。IKE ネゴシエーションと他の IKE パラメータの詳細については、次に説明します。

IKE フェーズ 1 - IKE セキュリティネゴシエーション

IKE ネゴシエーションは、2 つのフェーズで実行されます。リモートデバイスが一致する事前共有鍵を持つことを確認することによって、はじめのフェーズ「フェーズ 1」は、2 つの VPN ファイアウォールと VPN クライアントが互いに認証するために使用されます。

しかし、プレーンテキストで膨大なネゴシエーションをパブリッシュしたくはないため、残りの IKE ネゴシエーションを保護する方法にはじめに同意します。前のセクションで記述したように、イニシエータが応答者にプロポーザルリストを送信することでこれが行われます。その後、応答者は提案の一つを受諾し、VPN のもう一方の終端を認証してその身分を確認し、また、リモートデバイスに対して自身の証明を行います。
Diffie-Hellman キー交換として知られている技術は、ネゴシエーションにおいて、はじめに双方間で共有秘密に同意するために使用されます。

認証は、事前共有鍵、証明書、または公開鍵暗号を通じ行われます。今日、事前共有鍵は最も一般的な認証方法です。PSK と証明書は NetDefendOS VPN モジュールによってサポートされます。

IKE フェーズ 2 - IPsec セキュリティネゴシエーション

フェーズ 2 では、別のネゴシエーションが実行され、IPsec 接続のパラメータを詳しく説明します。

フェーズ 2 では、VPN データフローを保護するために使用するセッションキーを提供するために、フェーズ 1 の Diffie-Hellman 鍵交換から新しい鍵も引用します。

PFS（Perfect Forwarding Secrecy）が使用されると、各フェーズ 2 のネゴシエーションで新しい Diffie-Hellman 鍵交換が実行されます。これに時間がかかる場合、どのキーも他の以前に使用したどんなキーにも依存していないことを確かめています。どのキーも同じ初期のキー入力マテリアルから引用されることはありません。さらに、あるキーが損なわれたという思いもかけない場合には、どのサーブシーケンスキーも引用されていないことを確認することになっています。

フェーズ 2 のネゴシエーションが終了すると、VPN 接続は確立され、使用可能になります。

IKEv1 ではなく IKEv2 を使用する

NetDefendOS は IKEv1 と IKEv2 両方をサポートしていますが、IPsec トンネルは初期値では IKEv2 を使用するため、IKEv2 使用する設定が推奨されます。IKEv1 は廃止（Obsolete）とみなされます。IKEv2 は IKEv1 と比較して以下の利点があります。

1. IKEv2 では IKEv1 に存在したセキュリティ脆弱性が取り除かれています。
2. IKEv2 では Rekey、NAT-T、Dead Peer Detection をどのように扱うか指定することができます。
3. KEv2 はハンドシェイク期間が短くなっています。
4. IKEv2 ではローミングクライアントの MOBIKE が使用可能です。詳細は「10.3.16　MOBIKE のサポート」を参照してください。
5. IKEv2 は改良中です。

10.3.1.2 IKE 認証

IKE 認証では以下の方式が使用できます。

- 手動の鍵管理
- 事前共有鍵（PSK）
- 証明書

マニュアルキーイング（手動鍵管理）

VPN を設定する最も簡単な方法は「マニュアルキーイング」と呼ばれる方式を使用することです。これは、IKE が全く使用されない方式です。その他のパラメータと同様に暗号化と認証は直接 VPN トンネルの両側に設定されます。この方式は古い認証方式であるため、NetDefendOS ではサポートしていません。

注意　この方式は古い認証方式であるため、NetDefendOS ではサポートしていません。

事前共有鍵（PSK）

事前共有鍵（PSK: Pre-shared Key）の使用は、VPN の終端が秘密鍵を共有する方式です。これは、IKE によって提供されるサービスで、マニュアルキーイングよりも非常に柔軟性のある長所を持っています。

・PSK 長所

事前共有鍵は、設定がシンプルであるという利点があります。トンネル毎に必要となるのは 1 つの鍵のみであり、これはトンネルのエンドポイントで手動で共有されます。

・PSK 短所

PSK を鍵配布に使うためには検討すべき点があります。どのようにリモート VPN クライアントやファイアウォールに事前共有鍵を配布するのかという点です。PSK システムは事前共有鍵が秘密であるという点から、これは大きな問題です。1 つ目の事前共有鍵の配布においてセキュリティが危うくなった場合、新しい事前共有鍵を使用するように構成を変更する必要があります。

証明書

各 VPN ファイアウォールは、自身の証明書と一つ以上の信頼されるルート証明書があります。

認証は、いくつかの項目に基づきます。

- 各終端は、証明書内に検出される公開鍵に対応する非公開鍵を持っており、誰も非公開鍵にはアクセスできません。
- 証明書は、リモートエンドポイントが信頼する誰かに署名されています。

・証明書の長所

柔軟性を付加します。例えば、多くの VPN クライアントは、事前共有鍵とローミングクライアントを使用する場合に設定された同じ事前共有鍵をすべてのクライアントで持たなくても管理されます。一方で、クライアントのセキュリティが侵された場合、クライアントの証明書を無効にすることができます。すべてのクライアントで設定する必要ありません。

・証明書の短所

複雑性です。証明書ベースの認証は、すべての VPN クライアントとファイアウォールがそれ以外の第三者に依存することになるため大きな公開鍵インフラが必要になります。
つまり、設定する必要があるものがさらに多くなり、誤る可能性もまた多いのです。

10.3.1.3 IPsec プロトコル（ESP/AH）

IPsec プロトコルは、VPN を通過する実際のトラフィックを保護するために使用されるプロトコルです。これらのプロトコルに使用される実際のプロトコルと鍵は IKE によって取り決められます。
IPsec には、AH および ESP という 2 つのプロトコルがあります。これらは以下のセクションで説明します。

AH（Authentication Header）

AH は、データストリームを認証する場合に使用されるプロトコルです。

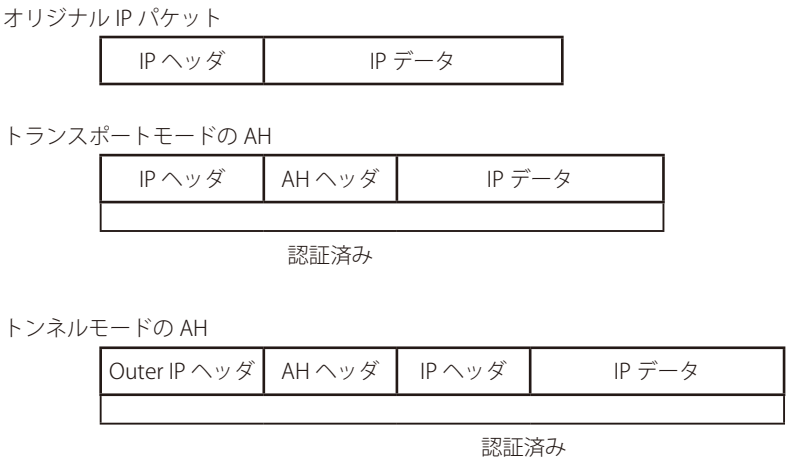


図 10-5　AH プロトコル

IP パケット内のデータから MAC アドレスを取り出すために暗号化ハッシュ機能を使用します。その後 MAC はパケットと一緒に転送され、リモートエンドポイントが元の IP パケットの完全性を検証することを可能にし、また、そのデータがインターネット経由で改ざんされていないことを確実にします。

IP パケットデータとは別に、AH はまた、IP ヘッダの一部を認証します。
AH プロトコルは、オリジナルの IP ヘッダに AH ヘッダを挿入し、トンネルモードでは、オリジナルの内部 IP ヘッダの前ではなく AH ヘッダは、Outer ヘッダに挿入されます。

ESP（Encapsulating Security Payload）

ESP プロトコルは ESP ヘッダを元の IP ヘッダの後に挿入します。トンネルモードでは、外部ヘッダの後かつ元のに内部ヘッダの前に、ESP ヘッダを挿入します。

ESP ヘッダの後のすべてのデータは、暗号化と認証の両方、またはどちらかが行われています。
AH と異なるのは、ESP が IP パケットの暗号化も提供することです。認証フェーズも、ESP ヘッダの後のデータを認証し、そのため Outer IP ヘッダは保護されないという点で異なります。

ESP プロトコルは、IP パケットの暗号化と認証両方に使用されます。暗号化だけ、認証だけを使用することもできます。

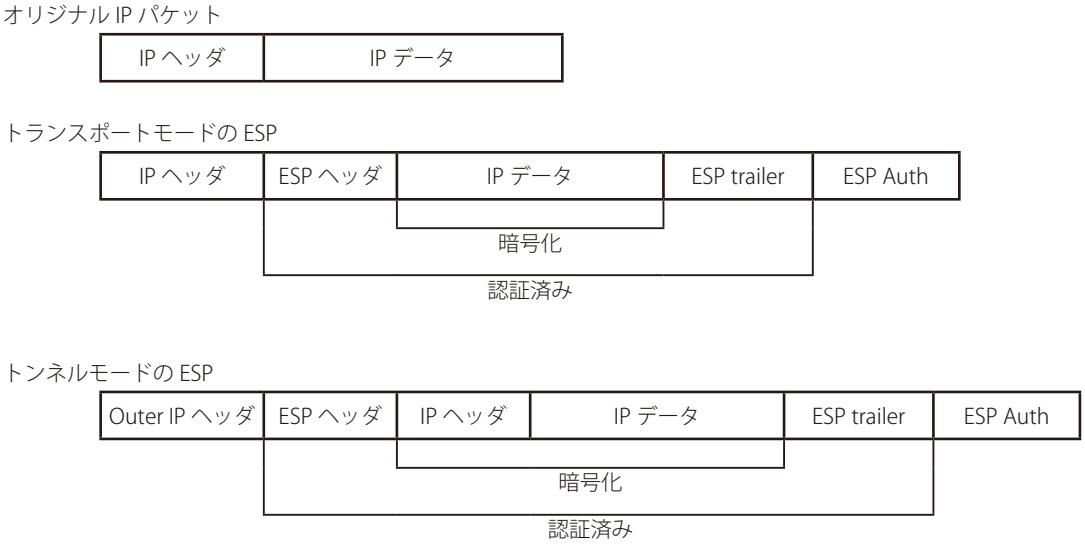


図 10-6　ESP プロトコル

10.3.2 IPsec トンネル

NetDefendOS では IPsec Tunnel コンフィグレーションオブジェクトにより IPsec トンネルを定義することができます。これは、IPsec トンネルのエンドポイントを指定することと同義と言えます。また、IPsec Tunnel オブジェクトは、イーサネットインタフェースと同じフィルタリング、トラフィックシェーピング、コンフィグレーション機能を持つ論理的な NetDefendOS インタフェースとみなされます。最も重要なことは、IP Policy または他の IP ルールセットのエントリにおける Source Interfece と（または）Destination Interface として IPsec Tunnel オブジェクト使用可能であるということです。

リモートでのトンネル確立の開始

別の D-Link ファイアウォールまたは別の IPsec に従うネットワーク製品（または、リモートエンドポイントとして知られている）が、ローカルな D-Link ファイアウォールに IPsec VPN トンネルを確立しようとする場合、NetDefendOS 設定内に現在定義されている IPsec トンネルのリストが評価されます。一致するトンネル定義が見つかると、そのトンネルがオープンされ、関連する IKE と IPsec ネゴシエーションが行われ、リモートエンドポイントに VPN トンネルが確立します。

ローカルなトンネル確立の開始

一方で、保護されたローカルネットワークのユーザは、IPsec トンネルの端に位置しているリソースにアクセスを試みるかもしれません。この場合、NetDefendOS は、リソースの IP アドレスのためのルートが定義済みの IPsec トンネルを通過することがわかり、トンネルの確立がローカルな D-Link ファイアウォールから開始されます。

IP ポリシーは復号化されたトラフィックを制御する

IPsec トンネルが確立されても、そのトンネルからのすべてのトラフィックフローが自動的に信頼されないことに注意してください。その一方で、復号化されたネットワークトラフィックは、IP ルールセットにチェックされます。この IP ルールセットを使用してチェックをする場合、トンネルが NetDefendOS のインタフェースのように扱われるため、トラフィックの送信元インタフェースは関連する IPsec トンネルになります。

さらに、ルートまたはアクセスルールは、NetDefendOS において IPsec トンネルからの特定の送信元 IP アドレスを受諾するために、ローミングクライアントに定義される必要があります。

トラフィックの返送

逆方向に向かう、すなわち IPsec トンネルに入るネットワークトラフィックのために、リバース処理が行われます。最初に、暗号化されていないトラフィックが、ルールセットによって評価されます。IP ポリシーと経路が一致すると、NetDefendOS は、条件に一致する確立された IPsec トンネルを検出しようとします。検出されないと、NetDefendOS は一致する IPsec トンネル定義に指定されたリモートファイアウォールにトンネルを確立しようとします。

囲まれた IPsec トラフィックに IP ポリシーは必要ありません。

IPsec トンネルを使用している場合、通常、管理者は暗号化されていないトラフィックがトンネル（NetDefendOS インタフェースとして扱われるトンネル）に流れることを許可する IP ポリシーを設定します。しかし、IPsec 自身を実行するパケットを明示的に許可する IP ポリシーを設定する必要はありません。

IKE と ESP パケットは、初期値で NetDefendOS の内部の IPsec エンジンによって取り扱われており、IP ルールセットは参照されません。

この動作は、IPsec Advanced Settings セクションの IPsec Before Rules オプションで変更することができます。これを行う理由の例としては、特定の IP アドレスまたはアドレスグループから行われる高い番号の IPsec トンネル接続がある場合があります。これは NetDefendOS の IPsec エンジンの性能を下げてしまうため、IP ポリシーでそのようなトラフィックを明示的に破棄することが、トラフィックがエンジンに到達するのを防止する効率的な方法です。つまり、IP ポリシーは、トンネルに関係するすべてのトラフィックの完全な制御を持つために使用されます。

トンネルの正常性のモニタリング

以下は、問題が検出された場合に、IPsec トンネルの正常性をモニタし、トンネルを再確立するための方式で、IKEv1 と IKEv2 の両方で利用可能です。

- **Dead Peer Detection**

  Dead Peer Detection（DPD）は、IPsec トンネルの正常性をモニタするのに使用されます。これは、オプションでトンネルに有効にできます。また、外部の IPsec ピアもサポートする場合、常に有効（初期値）にすることをお勧めします。IPsec クライアントをローミングする場合、DPD はトンネルの正常性をモニタリングする唯一のオプションです。

  DPD は、トンネルのもう一端にあるピアから到来するトラフィックを探すことで、トンネルの生存状態をモニタリングします。メッセージが特定時間内に検出されない場合、NetDefendOS は、ピアにそれが到達可能かどうかを判断するために DPD-R-U-THERE メッセージを送信します。

  一連の DPD メッセージ送信後にピアの応答がない場合、ピアはデッド（無効）であると見なし、トンネルは終了します。トンネルは通常の方法で再確立されます。例えば、NetDefendOS がトンネルを介してトラフィックを送信する必要がある場合や、外部の IPsec ピアがトンネルの確立を開始する場合などです。

  トンネルで DPD を無効化した場合でも、ピアからの DPD-R-U-THERE メッセージに対しては、NetDefendOS による応答が行われます。これは、IPsec 標準で必要とされるためです。ただし、DPD の無効化により、NetDefendOS 自身の DPD-R-U-THERE 送信は行われません。

  DPD に関する変更可能な IPsec トンネル設定は、最後のトラフィックが検出されてから最初の DPD メッセージを送信するまでの時間の設定のみです。

注意 Auto Establish と DPD の両方を同時に使用できます。

- **トンネルモニタリング**
  NetDefendOS は、IPsec トンネルの正常性をモニタするために、DPD に加え、トンネルモニタリングを提供します。トンネルモニタリングでは、ICMP ping メッセージがトンネルを通じて到達可能な外部ホストが利用できる必要があります。詳しくは「10.3.17 IPSec トンネルモニタリング」を参照してください。

10.3.3 IPsec トンネルプロパティ

以下は、IPsec トンネルオブジェクトに必要な主要なプロパティの概要です。両方の終端が同意できることが非常に重要であるため、トンネルを設定する前に、これらのパラメータが何を行うかを理解することを強くお勧めします。

- **IKE バージョン**
  NetDefendOS は IKEv1 と IKEv2 両方のバージョンをサポートしており、初期値では IKEv2 が使用されます。IKEv1 は現在廃止（Obsolete）であり、古い機器との互換性のみで必要となるため、IKEv2 を使用することが推奨されます。本プロパティを Auto に指定すると、IKEv2 を最初に試行し、その接続が失敗した場合に IKEv1 に対して試行が行われます。

- **ローカル / リモートネットワーク / ホスト**
  これらは、VPN によって保護される IP トラフィック間のサブネットとホストです。LAN-to-LAN 接続では、これらは各 LAN のネットワークアドレスです。ローミングクライアントが使用される場合、リモートネットワークは、大抵 all-nets も設定され、これはローミングクライアントがどこからも接続できることを意味します。

- **ローカルエンドポイント**
  初期値では、IPsec トンネルオブジェクトのこのプロパティは通信で使用されるイーサネットインタフェースの IP アドレスです。より具体的には、このアドレスはインタフェースの core route の IP アドレスです。インタフェースに IPv4/IPv6 両方のコアルートが存在する場合、NetDefendOS は IPsec トンネルのローカルエンドポイントとしてどちらのアドレスを使用することも可能です。

  このプロパティの設定を行うことは、トンネルの送信元アドレスを特定の IP アドレスとすることです。プロパティに IP アドレスが割り当てられた場合、管理者は送信インタフェース上で IP アドレスを ARP パブリッシュするように手動で設定する必要があります。この手順については「3.5.3 ARP パブリッシュ」を参照してください。

  ファイアウォール後方のローカルクライアントが、異なるインタフェース上で確立された IPsec トンネルを介してトラフィックを送信している場合、Local Endpoint プロパティを設定する必要があります。例えば、クライアントが lan インタフェース上に存在し、IPsec トンネルが wan インタフェースといった場合です。そのようなケースでは、Local Endpoint プロパティを wan インタフェースの IP アドレスに設定しなければなりません。

- **リモートエンドポイント**
  リモートエンドポイント（リモートゲートウェイとも呼ばれる）は、IPsec トンネルの片側のピア IP アドレスです。単一の IP アドレスまたは IP アドレス範囲として指定します。ファイアウォールがトンネルイニシエータである場合、単一の IP アドレスを指定します。トンネルが接続ローミングクライアントによって開始されている場合は、リモートエンドポイントは通常、クライアントが所属する IP アドレス範囲 / ネットワークになります。

  リモートエンドポイントは以下のいずれかの方法で指定されます。

  - 単一の IPv4 アドレスまたは IPv4 範囲 / ネットワーク
  - 単一の IPv6 アドレスまたは IPv6 範囲 / ネットワーク
  - FQDN アドレスオブジェクト。FQDN を IP アドレスへ解決する DNS ルックアップが利用可能である場合、この方法が推奨されます。FQDN オブジェクトの作成については「3.1.7 FQDN アドレスオブジェクト」を参照してください。

  ファイアウォールが複数の IP アドレスに対して LAN-to-LAN トンネルセットアップを開始している場合、通常 FQDN オブジェクトが使用されるべきです。FQDN オブジェクトによって複数の IP アドレスの解決可能である場合、NetDefendOS はそれぞれに対して成功するまでトンネルのセットアップを試みます。

  リモートエンドポイントは透過モードでは使用されません。

- **Incoming Interface Filter**
  このプロパティが設定された場合、どのインタフェースに対して NetDefendOS が受信 IPsec 通信をリッスンするか（送信元インタフェース）決定します。このプロパティは、トンネル選択時の通常の手順よりも優先度が高いため、特定のトンネルを特定のインタフェースで受信する通信で使用されるように指定することができます。

- **Local ID と Remote ID**
  ローカル ID とリモート ID は、IKE ネゴシエーションの間にトンネルの各サイドが送信する値であり、事前共有鍵または証明書ベースのトンネルのどちらかで使用されます。

  i. Local ID - IPsec Tunnel オブジェクトのこのプロパティは、ローカルな VPN トンネル終端の識別子を表します。また、これは、IKE ネゴシエーションの間にリモートピアに提示される値です。

  プロパティは、1 つの値だけに設定されますが、ホスト証明書を使用する場合はその中に ID が含まれるので、空白とすることができます。送信された証明書に複数の ID が含まれる場合、このプロパティが、証明書のどの ID を使用するか指定するように設定できます。

  Enforce Local ID プロパティを有効にして NetDefendOS が応答者として機能しているとき、開始プログラムによって提案された ID は、Local ID の値にマッチするようにします。動作の初期値では、提案された ID を無視します。

  ii. Remote ID - ID list オブジェクトを指定するのにこのプロパティを使用できます。ID list オブジェクトには 1 つ以上の ID があります。証明書を使用する場合、リモートピアによって送信された証明書は、ピアが認証されるためにリストの ID の 1 つにマッチする ID を含まなければなりません。証明書を持つ Remote ID プロパティの使用については、「10.3.18 証明書を使用した ID リスト」を参照してください。

  NetDefendOS は、アクセスを保証するためにすべてのリモート ID に健全性のチェックを適用します。通常不正な形式の ID には、DN 名の問題があります。例えば、以下のような不完全なリモート ID 名があります。

```
DN=D-Link, OU=One,Two,Three, DC=SE
```

  管理者が指定すると、NetDefendOS コンフィグレーションをコミットする際にエラーメッセージが示されます。訂正されたリモート ID 形式は以下の通りです。

```
DN=D-Link, OU=One\,Two\,Three, DC=SE
```

- **Originator IP アドレス**

IPsec Tunnel オブジェクトの Originator IP プロパティは、生成元が NetDefendOS 自身である場合にトンネルに流れる送信元 IPv4 アドレスを設定するための手段です。

この IP は、NetDefendOS がログメッセージまたは ICMP ping メッセージを送信するような場合に必要とされます。また、IPsec トンネルのローカルネットワークをリモートネットワークに NAT する場合、生成元の IP が NAT アドレスとして使用する IP アドレスになります。以下で説明する自動選択が適切でない場合、このアドレスを手動で設定する必要があるかもしれません。

このプロパティには 2 個の設定があります。

- **LocalInterface**

  これは初期設定です。Web インタフェースでは、以下のオプションが有効です。
  Automatically pick the address of a local interface that corresponds to the local net
  NetDefendOS は自動的に以下の方法で送信元 IP アドレスを選択します。

  i. NetDefendOS がすべての non-IPsec インタフェースの IP アドレスを参照し、トンネルのローカルネットワークの範囲内で検出した最初の IP アドレスを使用します。

  HA クラスタでは、これは共有 IP とプライベート IP は異なることを意味します。

  ii. 最初のステップで 1 つも適当なアドレスを検出できない場合、トンネルのローカルネットワークから 2 個目の IP アドレスを使用します。これは、ネットワーク内のホストが IP アドレスを既に使用している可能性があります。この場合、以下で説明されるように、手動で IP アドレスを設定する必要があります。

  HA クラスタでは、これは共有 IP とプライベート IP は同じであることを意味します。

- **Manual**
  本オプションでは、管理者は特定の IP を選択することができます。2 つの IP を選択できます。
  i. non-HA IP アドレス。これは、クラスタ状態を除き使用される IPv4 アドレスです。

  ii. HA IP アドレス。このアドレスは共有 IP とプライベート IP として HA クラスタで使用されます。

  トンネル用のローカルネットワークが all-nets であれば、NetDefendOS は IP アドレスを割り当てることができないため、値を手動で割り当てる必要があります。

また、生成元の IP アドレスが core に送信されるように、core ルートが自動的にすべてのルーティングテーブルに追加されることに注意してください。

• 暗号化モード

IPsec は、以下の 2 つのモードで使用されます。

• トンネルモード

トンネルモードはトラフィックがリモートデバイスにトンネルされることを示し、データを解読 / 認証後、トンネルから取り出され、最終送信先に渡します。従って、盗聴者は単に VPN 終端のひとつから別に向かう暗号化されたトラフィックを見るだけとなります。

トンネルモードは、IP ヘッダを含むパケット全体の暗号化によって動作します。データの最終送信先ではない、プロキシとして動作する 2 台のファイアウォール間で主に使用されます。
NAT トラバーサルはトンネルモードでサポートされています。

• トランスポートモード

トランスポートモードでは、IPsec データのペイロードのみが暗号化されます。IP ヘッダは暗号化されません。ファイアウォールが送信先となる、VPN クライアントからファイアウォールへの接続を保護するために主に使用されます。多くの場合、他のトンネルプロトコル（GRE、L2TP など）と一緒に使用され、IPsec による保護の前に、別のプロトコルによって最初にカプセル化されます。
NATT トラバーサルはトランスポートモードではサポートされません。

この設定は、多くの設定で「Tunnel」に設定されます。IKEv2 を使用する場合、Tunnel だけを使用すべきです。

• メイン / アグレッシブモード

IKE ネゴシエーションにはメインモードとアグレッシブモードの 2 つの処理モードがあります。

これら 2 つの違いは、アグレッシブモードは多少早く接続を確立するために、セキュリティファイアウォールの識別情報を転送する時にコストが低い平文でパケットを送信するということです。

ローミングクライアントを使用するシナリオでは、amplification 攻撃に対する脆弱性が高くなるため、Agressive モードを使用しないことをお勧めします。

• IKE 暗号化

これは、IKE ネゴシエーションで使用される暗号化アルゴリズムとそのアルゴリズムに従って使用される暗号鍵のサイズを指定します。

D-Link IPsec でサポートされるアルゴリズムは以下の通りです。
- AES
- Blowfish
- Twofish
- Cast128
- 3DES
- DES

DES は、他の古い VPN インプリメンテーションの一部との相互運用のために含まれています。DES は古いアルゴリズムで、もはや安全だとは考えられていないため、使用は可能な限り避けるべきです。

• IKE 認証

これは、IKE ネゴシエーションで使用される暗号化アルゴリズムを指定します。

D-Link VPN でサポートされるアルゴリズムは以下の通りです。
- MD5
- SHA1
- SHA256
- SHA512
- AES-XCBC（IKEv2 のみ）

注意 SHA1 と MD5 には脆弱性があります

SHA1 には脆弱性があると考えられており、注意して使用する必要があります。また、MD5 は既に安全ではないとみなされ、可能な限り使用を避けるべきです。

• IKE DH グループ

これは、IKE で鍵交換をしている場合に使用する Diffie-Hellman グループを指定します。以下で利用可能な DH グループについて記述します。初期値からグループ番号を上げると、数字の大きいグループ番号ほど多くのコンピュータの資源を使用し、遅いハードウェアプラットフォームに許可できないトンネル設定回数になる可能性があるため、慎重に行われるべきです。

IKEv1 では、トンネルの両端で同じ DH グループを使用する必要があります。IKEv2 は重複したグループを使用したトンネルネゴシエーションが可能です。

- **IKE ライフタイム**

  これは IKE 接続の寿命です。これは、データ量（キロバイト）とともに時間（秒）で指定されます。
  これらのいずれかに達するたびに、新しいフェーズ 1 交換が実行されます。IKE 接続の最後の「incarnation」に一つもデータが転送されないと、誰かが再び VPN 接続を望むまで新しい接続は行われません。この値は、IPsec SA ライフタイムより長く設定する必要があります。

- **PFS**

  PFS が無効の場合、IKE ネゴシエーションのフェーズ 1 における鍵交換の間、はじめのキーイングマテリアルが作成されます。IKE ネゴシエーションのフェーズ 2 では、暗号化と認証セッション鍵はこのはじめのキーイングマテリアルから取り出されます。PFS（Perfect Forwarding Secrecy）を使用することによって、新しいキーイングマテリアルがいつも鍵の再作成に使用されます。 1 つの鍵が成り立たないと、他の一つの鍵もその情報を使用して取得されることはできません

  PFS は、2 つのモードで使われます。1 つ目は鍵における PFS です。フェーズ 2 ネゴシエーションごとに、新たな鍵交換が行われます。もう一つは識別における PFS です。フェーズ 2 ネゴシエーションが終了するたびにフェーズ 1 SA を削除し、フェーズ 2 ネゴシエーションが同じ鍵で暗号化されることがないことを確実にすることにより、識別の保護をより強固にします。

  PFS では、どのような暗号化または認証鍵も成り立つ見込みがないため、通常使用されません。

- **PFS DH グループ**

  PFS と共に使用する Diffie-Hellman グループを指定します。以下の Diffie-Hellman Groups セクションで利用可能な DH グループについて記述します。初期値からグループ番号を上げると、数字の大きいグループ番号ほど多くのコンピュータの資源を使用し、遅いハードウェアプラットフォームに許可できないトンネル設定回数になる可能性があるため、慎重に行われるべきです。

- **IPsec DH グループ**

  IPsec 通信に使用する Diffie-Hellman グループを指定します。以下の Diffie-Hellman Groups セクションで利用可能な DH グループについて記述します。初期値からグループ番号を上げると、数字の大きいグループ番号ほど多くのコンピュータの資源を使用し、遅いハードウェアプラットフォームに許可できないトンネル設定回数になる可能性があるため、慎重に行われるべきです。

- **IPsec 暗号化**

  保護された IPsec トラフィックに使用される暗号化アルゴリズム。
  これは、AH が使用される場合や暗号なしで ESP が使用される場合には必要ではありません。

  NetDefend OS がサポートする暗号化アルゴリズムは以下の通りです。
  - AES
  - Blowfish
  - Twofish
  - Cast128
  - 3DES
  - DES

- **IPsec 認証**

  これは、保護されたトラフィックに使用される認証アルゴリズムです。
  これは、認証なしの ESP を使用することを推奨していませんが、ESP が認証なしで使用される場合には使用されません。

  NetDefend OS がサポートする暗号化アルゴリズムは以下の通りです。
  - MD5
  - SHA1
  - SHA256
  - SHA512
  - AES-XCBC（IKEv2 のみ）

注意 SHA1 と MD5 には脆弱性があります

SHA1 には脆弱性があると考えられており、注意して使用する必要があります。また、MD5 は既に安全ではないとみなされ、可能な限り使用を避けるべきです。

- **IPsec ライフタイム**

  これは VPN 接続の寿命です。
  これは、時間（秒）とデータ量（キロバイト）の両方で指定されます。
  これらの値のいずれかが超過すると、新しい暗号化と認証セッションで鍵の再作成が開始されます。VPN 接続が最後のキー作成の間に使用されないと、接続は終了し、接続が再び必要となると、最初から再オープンされます。この値は、IKE ライフタイムより短く設定する必要があります。

• 自動確立

初期値では、LAN-to-LAN IPsec トンネルは、トラフィックがトンネルをフローする時にだけ確立されます。IPsec トンネルプロパティの Auto Establish を有効にすることで、トラフィックは全くフローせずに、LAN-to-LAN トンネルは確立します。これは以下の状況で役立ちます。

- LAN-to-LAN トンネルのみ（IKEv1 または IKEv2）。ローミングクライアントには使用できません。
- ルートフェイルオーバの際に、代替経路用のトンネルは通常確立されます。
- 再構成の操作を NetDefendOS で実行した後、トラフィックのフローを待たずにトンネルは直ちに再確立されます。

2 つの IPsec トンネルのエンドポイントが A と B であると仮定すると、フローのクライテリアの両方が正しい場合に B で自動確立を有効にすることをお勧めします。

- A は B に IKE ネゴシエーションを開始できません。開始できない理由は以下のいずれである可能性があります。
  - B が NAT を行うデバイスの配下にない。
  - A は、B の IP アドレスを取得するのに DNS を使用している。
  - B は DHCP を通じて IP アドレスを受信している。

- 管理者は、B がパケットの送信をしなくても、トンネルを経由した UDP/TCP 接続を開始することができるものと決定します。例えば、A の背後に位置するクライアントの送信先が、B の背後に位置するサーバであるかもしれません。

• Diffie-Hellman グループ

Diffie-Hellman（DH）は、二者間で、一連のプレーンテキスト交換を通して安全ではない通信チャンネル上で共有秘密鍵を確立できる暗号プロトコルです。二者間の交換は第三者によってモニタされるかもしれませんが、Diffie-Hellman は、同意した共有秘密鍵がを第三者によって識別されること、鍵を使用して暗号化されたデータを解読することを非常に難しくしています。

既述のとおり、Diffie-Hellman は、NetDefendOS における IKE、IPsec、および PFS のための共有秘密鍵を確立するのに使用されます。管理者が設定した Diffie-Hellman グループ番号は、DH 交換に使用されることになっているセキュリティのレベルを NetDefendOS に示します。グループ番号が高いほど、セキュリティは高くなりますが、これは必要とされるハードウェア処理を行うリソースを増やします。

NetDefendOS でサポートされている DH グループは以下の通りです。

- DH グループ 1（768 ビット）
- DH グループ 2（1024 ビット : 初期値）
- DH グループ 5（1536 ビット）
- DH グループ 14（2048 ビット）
- DH グループ 15（3072 ビット）
- DH グループ 16（4096 ビット）
- DH グループ 17（6144 ビット）
- DH グループ 18（8192 ビット）

トンネルに 2 つ以上の DH グループが指定された場合、トンネル両端に一致する最も大きい番号のグループが選択されます。

警告 DH グループ番号が高いほど、より多くのリソースを消費します。

多くのハードウェアプラットフォームが初期値の DH グループ 2 に十分な処理リソースを提供できます。高いグループ番号ほど累進的に多くのリソースを消費します。これは最も高いグループのトンネルセットアップでは、より遅いハードウェアプラットフォームではアクセスできないほど長い（何十秒も）場合があることを意味しています。また、トンネルセットアッププロセスから 100% のプロセッサ利用率とすべてのトラフィックスループットの一時的な停止をもたらす結果となるかもしれません。

10.3.4 IPSec プロポーザルリスト

VPN 接続パラメータに同意するため、ネゴシエーション処理が行われます。ネゴシエーションの結果、IKE および IPsec のアソシエーション（SA）は確立されます。プロポーザルはネゴシエーションのスタート地点にあります。リストの各エントリは VPN トンネルのエンドポイントデバイスがサポートしているアルゴリズムへのパラメータを定義します。初期のネゴシエーション、トンネルのいずれかの端にあるデバイスがサポートするアルゴリズムのセットに同意しようとします。

IKE のプロポーザルと IPsec のプロポーザルの 2 つのタイプがあります。IKE のプロポーザルは IKE フェーズ 1（IKE セキュリティネゴシエーション）中に、IPsec のプロポーザルは IKE フェーズ 2（IPsec セキュリティネゴシエーション）中に使用されます。

プロポーザルリストは複数のプロポーザルをグループ化するために使用されます。ネゴシエーション処理中に、プロポーザルリストはリモート VPN のファイアウォールに一致するプロポーザルが検出されるまで次々に提供されます。複数のプロポーザルリストが、異なる VPN のシナリオのために NetDefendOS に定義できます。2 つの IKE プロポーザルリストと 2 つの IPsec プロポーザルリストは、NetDefendOS にデフォルトで定義されています。

- High
  これは、より高いセキュリティを提供するアルゴリズムの短いリストを構成しています。
  - AES
  - SHA256
  - SHA512
  - AES-XCBC
- Medium
  低いセキュリティですが、古い終端デバイスと高い互換性を提供するアルゴリズムのやや長いリストを構成しています。
  - 3DES
  - AES
  - Twofish
  - SHA1
  - SHA256
  - SHA512
  - AES-XCBC

例題 10.1

プロポーザルリストの作成

この例題は、VPN トンネルで使用するために IPsec プロポーザルリストを作成し、使用する方法を示しています。3DES と AES は暗号化アルゴリズムとして提案されます。ハッシュ関数 SHA256 と SHA512 は両方ともデータパケットが転送中に変更されていないかどうかを確認するために提案されます。特定の IPsec のトンネルオブジェクトを追加する方法は、この例題に説明されていませんので注意してください。後の例題で使用されています。

CLI

はじめに、IPsec アルゴリズムのリストを作成する：

```
DFL-xxxx:/> add IPsecAlgorithms esp-l2tptunnel DES3Enabled=Yes AESEnabled=Yes SHA256Enabled=Yes
            SHA512Enabled=Yes
```

次に、IPsec トンネルへのプロポーザルリストを適用する：

```
DFL-xxxx:/> set Interface IPsecTunnel MyIPsecTunnel IPsecAlgorithms=esp-l2tptunnel
```

Web Interface

はじめに、IPsec アルゴリズムのリストを作成する：

1. **Objects > VPN Objects > IPsec Algorithms > Add > IPsec Algorithms** の順にメニューをクリックします。
2. リストの名前（例：esp-l2tptunnel）を入力します。
3. 次のパラメータをチェックします。
   - 3DES
   - AES
   - SHA256
   - SHA512
4. 「OK」ボタンをクリックします。

次に、IPsec トンネルにプロポーザルリストを適用する：

1. **Network > Interfaces and VPN > IPsec** セクションで、ターゲットにする IPsec トンネルをクリックします。
2. IPsec Algorithms 設定で作成済みの「esp-l2tptunnel」を選択します。
3. 「OK」ボタンをクリックします。

10.3.5 事前共有鍵

事前共有鍵は VPN トンネルの認証に使用されます。鍵は、通信が行われる前に通信相手によって共有される秘密です。通信するためには、両方とも秘密を知っていることを証明します。共有秘密のセキュリティは、どのくらい「よい」パスフレーズであるかによって決まります。例えば一般的な単語のパスフレーズは、辞書攻撃に非常に弱くなります。

あらかじめ共有された鍵は Web インタフェースを通して自動的に生成できますが、CLI を通してコマンド pskgen を使用することで生成することもできます。本コマンドは「CLI Reference Guide」を参照してください。

異なるプラットフォームにおいて PSK 内の ASCII でない文字にご注意ください！

PSK が 16 進数値ではなく、パスフレーズとして指定される場合、異なるプラットフォームにおける異なる暗号化は、ASCII 以外の文字で問題が発生するかもしれません。例えば、Windows™ は、ASCII でない文字を含む事前共有鍵を UTF-16 でコード化しますが、NetDefendOS は UTF-8 を使用します。たとえ、これらがトンネルのどちらの端で同じに見えても、そこには不一致があり、NetDefendOS に接続する Windows™ の L2TP クライアントを設定する場合に問題を引き起こすことがあります。

例題 10.2

事前共有鍵を使用する

この例題は、事前共有鍵を作成し、VPN トンネルに適用する方法を示しています。一般的な単語およびフレーズは辞書攻撃に弱いため、それらは秘密として使用されるべきではありません。ここでは事前共有鍵はランダムに生成された 16 進数の鍵です。この例題では、特定の IPsec トンネルオブジェクトを追加する方法は説明していません。

CLI

はじめに、事前共有鍵を作成する：

```
DFL-xxxx:/> pskgen MyPSK
```

より長くセキュアな 512 ビットの鍵を作成する：

```
DFL-xxxx:/> pskgen MyPSK -size=512
```

または手動で事前共有鍵を追加する

```
DFL-xxxx:/> add PSK MyPSK Type=HEX PSKHex=<enter the key here>
```

次に、IPsec トンネルに事前共有鍵を適用する：

```
DFL-xxxx:/> set Interface IPsecTunnel MyIPsecTunnel PSK=MyPSK
```

Web Interface

はじめに、事前共有鍵を作成する：

1. **Objects > Key Ring > Add > Pre-Shared Key** の順にメニューをクリックします。

2. 以下の情報を入力し、「OK」ボタンをクリックします。
   - Name：事前共有鍵の名前を入力します。例：MyPSK
   - Type: Hexadecimal key
   - Generate Random Key：クリックすると、パスフレーズを生成します。

次に、IPsec トンネルに事前共有鍵を適用する：

1. **Network > Interfaces and VPN > IPsec** の順にメニューをクリックします。

2. ターゲットにする IPsec トンネルをクリックします。

3. 選択した IPsec トンネルの Authentication タブで、Preshared Key のプルダウンメニューから「MyPSK」を選択します。

4. 「OK」ボタンをクリックします。

10.3.6 事前共有鍵を使用した LAN to LAN トンネル

VPN は、地理的に分散しているローカルエリアネットワーク（LAN）がインターネットで安全に通信できるようにします。会社などの組織で考えた場合、地理的に別個のサイトにある LAN がまるで専用のプライベートリンクを経由して通信を行った場合と同等のセキュリティレベルで通信できることを意味します。

ある場所の VPN ゲートウェイから別の場所の VPN ゲートウェイに到達している場合、安全な通信は IPsec トンネルの使用によって実施されます。そのため同時にトンネルを通過するトラフィックに通常のセキュリティ監視を行う間、D-Link ファイアウォールは VPN の実行者となります。このセクションは、事前共有鍵（PSK）で作成される LAN to LAN トンネルの設定を特に行います。

いくつかの手順が PSK を持つ LAN-to-LAN トンネルを設定するために必要です。

- Pre-Shared Key（PSK）オブジェクトを定義します。
- IPsec Tunnel オブジェクトを定義します。
- 少なくとも、IPsec トンネルのローカルネットワーク、リモートネットワーク、リモートエンドポイントを、最初の手順で定義した PSK と共に指定します。
- いずかの方向へのトラフィックフローを許可する IP ポリシーオブジェクトを設定します。
- Add route statically プロパティ（CLI では AutoInterfaceNetworkRoute）が有効化されている場合、リモートネットワークへのルートが自動的に追加されます。このプロパティは初期値で常に有効化されています。
- 同様の方法でトンネルのもう一端にあるピアを設定します。ローカルとリモートネットワークを逆にします。

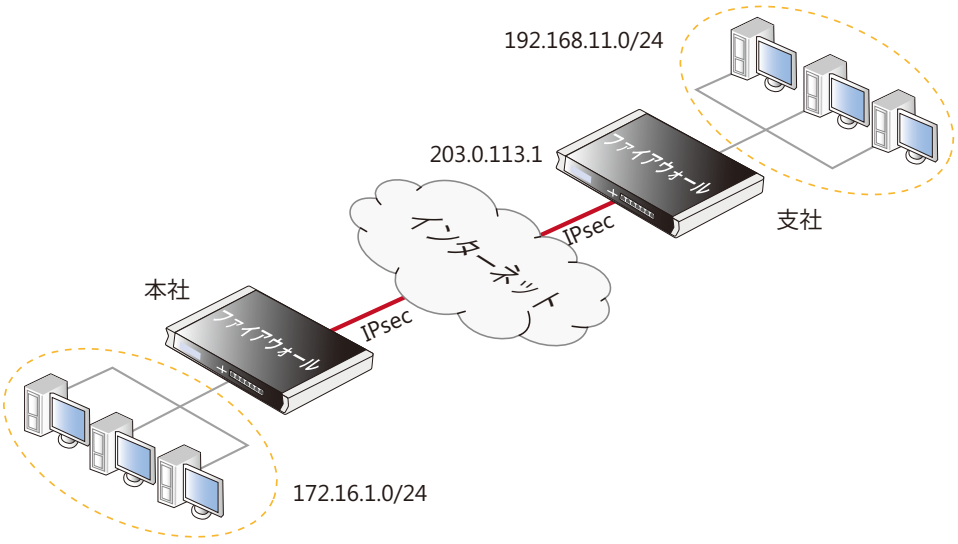
参照 D-Link VPN オブジェクトにより LAN-to-LAN 設定を簡単に行うことができる

ここで説明されている LAN-to-LAN 設定手順は標準の IPsec Tunnel オブジェクトに基づいています。NetDefendOS では、D-Link VPN オブジェクトも提供しており、これらのオブジェクトにより IKEv2 と（または）PSK、または証明書を使用した 2 つの D-Link ファイアウォール間の LAN-to-LAN IPsec 通信の設定を簡単に行うことができます。詳細は「10.3.15.1 LAN to LAN VPN」を参照してください。

例題 10.3

PSK ベースの LAN-to-LAN IPsec トンネルの設定

この例題では、支店のネットワーク 192.168.11.0/24 を持つ lan インタフェースに本社ネットワーク 172.16.1.0/24 を接続するためにパブリックインターネットを経由する IPsec トンネルを設定する方法を説明します。インターネットに接続する支店のファイアウォールイーサネットインタフェースが、パブリック IP アドレス 203.0.113.1 を持っていると仮定します。



デフォルトの IKE と IPsec プロポーザルリストがトンネルの両端で使用されるものとします。

CLI

A. IPsec 認証のために pre-shared key を作成する :

```
DFL-xxxx:/> add PSK my_scecret_key Type=ASCII PSKascii=somesecretasciikey
```

B. IPsec トンネルを設定する :

```
DFL-xxxx:/> add Interface IPsecTunnel ipsec_hq_to_branch LocalNetwork=172.16.1.0/24 RemoteNet-
            work=192.168.11.0/24 RemoteEndpoint=203.0.113.1 PSK=my_secret_key
```

C. トンネルの双方向のトラフィックフローを許可する 2 つの IP ポリシーを設定する :

i. ローカルからリモートネットワークまでのトラフィックフローを許可する IP ポリシーを追加します。

```
DFL-xxxx:/> add IPPolicy Name=hq_to_branch SourceInterface=lan SourceNetwork=172.16.1.0/24
            DestinationInterface=ipsec_hq_to_branch DestinationNetwork=192.168.11.0/24 Service=all_services
            Action=Allow
```

ii. リモートからローカルネットワークまでのトラフィックフローを許可する IP ポリシーを追加します。

```
DFL-xxxx:/> add IPPolicy Name=branch_to_hq SourceInterface=ipsec_hq_to_branch SourceNetwork=192.168.11.0/24
            DestinationInterface=lan DestinationNetwork=172.16.1.0/24 Service=all_services Action=Allow
```

D. トンネルにリモートネットワークへのルートを追加する :

コンテキストをルーティングテーブルに変更します。

```
DFL-xxxx:/> cc RoutingTable main
```

ルートを追加します。

```
DFL-xxxx:/main> add Route Interface=ipsec_hq_to_branch Network=192.168.11.0/24
```

初期値の CLI コンテキストに戻します。

```
DFL-xxxx:/main> cc
DFL-xxxx:/>
```

Web Interface

A. IPsec 認証のために pre-shared key を作成する :

1. **Objects > Key Ring > Add > Pre-Shared Key** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: my_secret_key
- Type: Passphrase
- Shared Secret: パスフレーズを入力します。
- Confirm Secret: パスフレーズを再度入力します。

3. 「OK」ボタンをクリックします。

B. IPsec トンネルを設定する :

1. **Network > Interfaces and VPN > IPsec > Add > IPsec Tunnel** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: ipsec_hq_to_branch
- Local Network: 172.16.1.0/24（これはローミングユーザが接続するローカルネットワークです。）
- Remote Network: 192.168.11.0/24
- Remote Endpoint: 203.0.113.1

3. Authentication タブで Pre-Shared Key に「my_secret_key」を入力します。

4. 「OK」ボタンをクリックします。

C. トンネルの双方向のトラフィックフローを許可する 2 つの IP ポリシーを設定する :

i. ローカルからリモートネットワークまでのトラフィックフローを許可する IP ポリシーを追加します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: hq_to_branch
- Action: Allow
- Service: all_services
- Source Interface: lan
- Source Network: 172.16.1.0/24
- Destination Interface: ipsec_hq_to_branch
- Destination Network: 192.168.11.0/24

3. 「OK」ボタンをクリックします。

ii. リモートからローカルネットワークまでのトラフィックフローを許可する IP ポリシーを追加します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: branch_to_hq
- Action: Allow
- Service: all_services
- Source Interface: ipsec_hq_to_branch
- Source Network: 192.168.11.0/24
- Destination Interface: lan
- Destination Network: 172.16.1.0/24

3. 「OK」ボタンをクリックします。

D. トンネルにリモートネットワークへのルートを追加します。

1. **Network > Routing > Routing Tables > main > Add > Route IPv4** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Interface: ipsec_hq_to_branch
- Network: 192.168.11.0/24

3. 「OK」ボタンをクリックします。

今度は、同様に支店のファイアウォールを設定します。ローカルとリモートゲートウェイネットワークを逆にして、本社のパブリック IP は Remote Endpoint の値になります。両側で同じ PSK 値を使用しなければならないことに注意してください。また、トンネル設定のために IKE ネゴシエーション中に両側で許可される暗号方式を見つけられるように、IKE と IPsec のプロポーザルリストは同じであるか、または少なくとも何らかの重複を持つことが必要です。

10.3.7 IPSec ローミングクライアント

ローミングクライアントの典型的な例として、従業員が、様々な場所からノートパソコンを使用して会社のサーバにアクセスする必要があるケースがあります。安全な VPN のアクセスのための必要性は別として、ローミングクライアントについての別の大きな問題は、モバイルユーザの IP アドレスがあらかじめ知られないことが数多くあるということです。未知の IP アドレスを処理するために、NetDefendOS はルーティングテーブルにトンネルが確立された時にダイナミックに経路を追加することができます。

IPsec ローミングクライアントの暗号化と認証

ローミングクライアント用に IPsec トンネルが設定されると、PSK または証明書のいずれかを使用した認証が実行されます。これは IKEv1、IKEv2 両方で共通です。

クライアントの認証は通常、クライアントがユーザ名とパスワードの認証情報の組み合わせを送信することによって行われます。IKEv1 では XAuth、IKEv2 では EAP を使用します。XAuth と EAP はこのセクションでは説明しませんが、クライアント接続時に認証をトリガーするには、それぞれ個別に Authentication Rule を設定する必要があります。

このセクションの多くの部分は IKEv1 と IKEv2 両方に適用されますが、証明書と EAP 認証を使用した IKEv2 ローミングクライアントの IPsec 設定の詳細については「10.3.13 IKEv2 ローミングクライアントセットアップ」を参照してください。

ローミング VPN オブジェクトにより簡単に IKEv2/EAP の設定が可能

NetDefendOS では、IPsec ローミングクライアントの設定を簡単に行うための Roaming VPN オブジェクトも提供しています。しかしながら、これは EAP 認証の証明書を使用する IKEv2 トンネルのみが対象です。詳細は「10.3.15.2 ローミング VPN」で説明します。

未知の IP アドレスを処理する

クライアントの IP アドレスが事前に知られていない場合、NetDefendOS は、各クライアントが接続する時にダイナミックにルーティングテーブル内に経路を作成する必要があります。下の例題では、この手順を記述しており、ルートを動的に追加するように IPsec トンネルが構成されています。

クライアントがあらゆる場所にローミングを許可される場合、IP アドレスに関係なく、リモートネットワークは、すべての既存の IPv4 アドレスがトンネル経由で接続を許可する all-nets（IP アドレス : 0.0.0.0/0）に設定される必要があります。

ローミングクライアントに VPN トンネルを設定する場合、通常、NetDefendOS により事前に設定されているプロポーザルリストに追加または変更する必要はありません。

ローミングクライアントに動的にルートを追加する

通常、NetDefendOS のルーティングテーブル内のルートには、各クライアントが接続する毎にルートが追加される必要があります。IPsec トンネルプロパティの Add route dynamically（CLI では AddRouteToRemoteNet）を有効化することで、自動的にルートの追加を行うことができます。

同時に、IPsec トンネルプロパティの Add route statically（CLI では AutoInterfaceNetworkRoute）を無効化すべきです。この設定は LAN-to-LAN トンネル設定に使用されるべきであり、有効化されている場合リモートネットワーク（この場合、通常では all-nets）にルートが追加されます。

プロキシ ARP によるクライアント IP アドレスのパブリッシュ

IPsec Tunnel オブジェクトの Proxy ARP Interfaces プロパティにインタフェース名を割り当てることにより、指定 / すべてのインタフェース上の接続ローミングクライアントの IP アドレスをプロキシ ARP でパブリッシュすることができます。

トンネルリストにおけるローミングクライアントの位置

ローミングクライアントが D-Link ファイアウォールに対してトンネルをオープンしようとすると、NetDefendOS は定義済みの IPsec Tunnel オブジェクトのリストを検索し、最初に一致したトンネルを選択します。つまり、リスト内で、ローミングクライアントのトンネルを LAN-to-LAN トンネルの次に配置することが通常望ましい設定となります。これにより、LAN-to-LAN トンネルが意図されたときに、ローミングクライアントのトンネルが誤って選択されないようにします。

ローミングクライアント用の PSK ベース IPsec トンネル

以下の例では、PSK ベースのトンネルを設定する方法を示しています。

例題 10.4

ローミングクライアント用の PSK ベース IPsec トンネルの設定

この例題では、lan インタフェースにある保護されたネットワーク 172.16.1.0/24 にリモートアクセスをするために、それに接続するローミングクライアントに本社ファイアウォールの IPsec トンネルを設定する方法を説明します。

デフォルトの NetDefendOS IKE と IPsec プロポーザルリストがファイアウォールで使用されており、クライアントがトンネル設定の IKE ネゴシエーション段階で許可に至るプロポーザルリストを使用するものとします。この例題で使用される IP ポリシーの Source Translation プロパティは初期値の Auto のままとします。Auto オプションが指定されていると、接続の送信元・送信先 IP アドレスが両方ともプライベート IP アドレスの場合、変換が実行されません。Auto オプションの詳細は「8.5 自動変換」を参照してください。

CLI

A. IPsec 認証のために pre-shared key を作成する :

```
DFL-xxxx:/> add PSK my_scecret_key Type=ASCII PSKascii=somesecretasciikey
```

B. IPsec トンネルを設定する :

```
DFL-xxxx:/> add Interface IPsecTunnel ipsec_roaming LocalNetwork=172.16.1.0/24 RemoteNetwork=all-nets PSK=my_secret_key
```

C. クライアントからのトラフィックを許可する IP ポリシーを作成する :

```
DFL-xxxx:/> add IPPolicy Name=roaming_clients_to_hq SourceInterface=ipsec_roaming SourceNetwork=all-nets
            DestinationInterface=lan DestinationNetwork=172.16.1.0/24 Service=all_services Action=Allow
```

Web Interface

A. IPsec 認証のために pre-shared key を作成する :

1. **Objects > Key Ring > Add > Pre-Shared Key** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: キーの名前（例：my_secret_key）を入力します。
   - Type: Passphrase
   - Shared Secret: 秘密のパスフレーズを入力します。
   - Confirm Secret: パスフレーズを再度入力します。

3. 「OK」ボタンをクリックします。

B. IPsec トンネルオブジェクトを作成する :

1. **Network > Interfaces and VPN > IPsec > Add > IPsec Tunnel** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: ipsec_roaming
   - Local Network: 172.16.1.0/24
   - Remote Network: all-nets

3. Authentication タブで Pre-Shared Key に「my_secret_key」を入力します。

4. 「OK」ボタンをクリックします。

C. クライアントからのトラフィックを許可する IP ポリシーを作成する :

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: client_to_lan
   - Action: Allow
   - Source Interface: ipsec_roaming
   - Source Network: all-nets
   - Destination Interface: lan
   - Destination Network: 172.16.1.0/24
   - Service: all_services

3. 「OK」ボタンをクリックします。

ローカルエンドポイントプロパティ

クライアントがファイアウォールに対して IPsec 通信を開始している状況では、通常、クライアントが最初の IKE リクエストを物理インタフェースに紐づく IP アドレスに送信します。

しかし、インタフェース上で他の IP アドレスが ARP パブリッシュされ、IKE リクエストがそれらのアドレスへ送信される場合、IPsec トンネルプロパティの Local Endpoint プロパティを使用して IKE リクエストを許可する IP アドレスを指定することができます。

NetDefendOS が IPsec トンネル通信を開始した場合、Local Endpoint プロパティは使用されません。

クライアントの Inner/Outer IP は異なるアドレスを設定する

IKEv1 では、トンネルに設定するローミングクライアントの Inner および Outer IP アドレスが異なっている必要があります。同じアドレスになっていると、NetDefendOS によって接続が破棄され、rule=Default_Access_Rule" を含む ruleset_drop_packet ログメッセージが生成されます。

IP アドレスが同じでなければならない場合、トンネルおよびトンネルで送信されるトラフィックに対する個別のルーティングテーブルを使用することにより、正しい設定とすることができます。または、NetDefendOS はクライアントに対して Config Mode を使用して IP プールから一意の IP を割り当てます。

Roaming VPN オブジェクトを使用したシンプルな設定

このセクションでは IPsec Tunnel オブジェクトに基づくローミングクライアントの設定について説明します。設定は Roaming VPN オブジェクトを使用することにより簡単に行うことができます。このオブジェクトでは、ローミングクライアント接続に関連しない IPsec トンネルプロパティが非表示となっており、個別の Authentication Rule を必要としないためクライアント認証を簡略化しています。

Roaming VPN オブジェクトの詳細は「10.3.15 IPsec プロファイルの使用」で説明しています。

IPsec ローミングクライアントの設定

IPsec で使用するクライアントの種類によって、以下のいずれかの設定変更が必要となります。

- D-Link ファイアウォールの URL または IP アドレスを指定してクライアントがリモートトンネルエンドポイントに配置されることを可能にします。
- 認証に使用する事前共有鍵（PSK）を指定します。または、認証に必要な場合、証明書をインストールします（証明書の利用方法は別のセクションで説明します）。
- 使用される IKE と IPsec アルゴリズムを指定し、NetDefendOS が使用するプロポーザルリストに同意できるようにします。
- クライアントがコンフィグモードを使用するかどうかを指定します。

サードパーティ製の利用可能な IPsec ソフトウェア製品が数多く用意されているほか、コンピュータのプラットフォームによっては組み込みのソフトウェアが用意されている場合もあります。ネットワーク管理者は要件に合ったクライアントを使用すべきです。

このドキュメントに出てくるベンダー製 IPsec クライアントは以下の通りです。
- Windows IPsec クライアント（Windows 7 以降）（「10.3.13 IKEv2 ローミングクライアントセットアップ」）
- The Apple iOS IPsec クライアント（「10.3.14 iOS ローミングクライアントの設定」）

10.3.8 証明書を使用した IPSec

このセクションでは、LAN-to-LAN における IPsec と IKEv1 ローミングクライアントのシナリオについて、PSK ではなく証明書を使用する場合の一般的な説明を記載しています。

CA 署名証明書を使用する

CA 署名証明書を使用する認証では、各トンネルエンドポイントで次の 2 種類の証明書を保持します。

- CA ルート証明書。リモートトンネルエンドポイントによって送信される CA 署名ゲートウェイ証明書を検証するために使用されます。

- CA 署名ゲートウェイ証明書（ホスト証明書とも呼ばれる）。エンドポイントが自身を証明するために使用します。公開鍵およびプライベート鍵をそれぞれ含む 2 つのファイルから構成されます。

ゲートウェイ証明書は NetDefendOS によって検証されるため、必要なルート証明書が上記のルート証明書と異なる場合、その別のルート証明書と関連するチェインがファイアウォールにアップロードされる必要があります。

ファイルを NetDefendOS にアップロードする手順については「3.9.2 証明書のアップロードと使用」で説明しています。アップロード後、NetDefendOS コンフィグレーションで IPsec トンネルを定義する際に参照することができます。

CA 署名証明書を使用する場合、管理者の責任により発行機関から適切な CA 署名証明書を取得します。Windows Server など、システムによっては CA サーバへのアクセス機能が用意されています。CA サーバ発行の証明書に関する情報は、「3.9 証明書」を参照してください。

LAN-to-LAN トンネルを使用する場合、組織の外側から証明書にアクセスされることはないため、組織自身のプライベート CA サーバによって署名された証明書を使用することが最適なセキュリティとなります。ローミングクライアントの場合も同様かもしれませんが、一般公衆に対して IPsec 接続を使用する場合、パブリック CA の利用のみが実現可能な選択であるかもしれません。

自己署名証明書を使用する

NetDefendOS の IPsec トンネルは、CA 署名証明書の代わりに自己署名証明書に基づくことができます。これは、トンネルのどちらか一端にあるファイアウォール（または、他のネットワークデバイス）において、種類の異なる自己署名証明書のペアを持つことで設定されます。ただし、これらの証明書の役割（ルート証明書とゲートウェイ証明書）は、それぞれの側で逆の役割となります。

自己署名証明書のペアは cert_A および cert_B という名前で、cert_A はファイアウォール gateway_A にアップロードされるか、または作成され、certB は gateway_B にアップロードされるか、または作成されるものとします。gateway_A では cert_A はゲートウェイ証明書で、cert_B はトンネル用のルート証明書です。gateway_B では状況が逆になります。: cert_B はゲートウェイ証明書で、cert_A はトンネル用のルート証明書です。

cert_A が ateway_A に作成されると、アップロードの必要はなく、秘密鍵は既に gateway_A のキーストアで利用可能であることにご注意ください。cert_B が gateway_A にロードされると、秘密鍵ファイルなしでもルート証明書として保管されます。状況は gateway_B では逆になります。

証明書チェーン

ルート証明書と IPsec トンネルのゲートウェイ証明書の間に証明書チェーンがある場合、チェーン内のすべての中間証明書をアップロードし、トンネル用のルート証明書として設定する必要があります。

設定の例

以下の例題は、前の例題であるローミングクライアント用の IPsec LAN-to-LAN 設定に基づいていますが、認証で PSK ではなく証明書を使用するように編集されています。

例題 10.5

証明書ベースの LAN-to-LAN IPsec トンネルの設定

この例題では、ローカル D-Link ファイアウォールの lan インタフェース上のローカルネットワーク 172.16.1.0/24 から、IPsec をサポートするリモートネットワークデバイスの後方のネットワーク 192.168.11.0/24 に、インターネット経由で接続する IPsec トンネルの設定方法を記載しています。

リモートデバイス側インタフェースの IPsec トンネルのエンドポイントがパブリック IP アドレス 203.0.113.1 であると想定します。
デフォルトの NetDefendOS IKE および IPsec プロポーザルリストを使用します。

CLI

A. SCP を使用して NetDefendOS に証明書ファイルをアップロードする :
詳細は「3.9.2 証明書のアップロードと使用」を参照してください。

B. IPsec トンネルを設定する :

```
DFL-xxxx:/> add Interface IPsecTunnel ipsec_local_to_remote_tunnel LocalNetwork=172.16.1.0/24 RemoteNet-
            work=192.168.11.0/24 RemoteEndpoint=203.0.113.1 AuthMethod=Certificate GatewayCertificate=my_host_
            cert RootCertificates=my_root_cert
```

C. トンネルの双方向のトラフィックフローを許可する 2 つの IP ポリシーを設定する :

i. ローカルからリモートネットワークまでのトラフィックフローを許可する IP ポリシーを追加します。:

```
DFL-xxxx:/> add IPPolicy Name=local_to_remote_traffic SourceInterface=lan SourceNetwork=172.16.1.0/24
            DestinationInterface=ipsec_local_to_remote_tunnel DestinationNetwork=192.168.11.0/24 Service=all_
            services Action=Allow
```

ii. リモートからローカルネットワークまでのトラフィックフローを許可する IP ポリシーを追加します。:

```
DFL-xxxx:/> add IPPolicy Name=remote_to_local_traffic SourceInterface=ipsec_local_to_remote_tunnel SourceNet-
            work=192.168.11.0/24 DestinationInterface=lan DestinationNetwork=172.16.1.0/24 Service=all_services
            Action=Allow
```

D. トンネルにリモートネットワークへのルートを追加する :

この手順はルートが自動的に追加される設定（初期値）であれば不要です。AutoInterfaceNetworkRoute トンネルプロパティが無効化されている場合、以下の手順で手動でルートを追加する必要があります。

コンテキストをルーティングテーブルに変更します。:

```
DFL-xxxx:/> cc RoutingTable main
```

ルートを追加します。:

```
DFL-xxxx:/main> add Route Interface=ipsec_local_to_remote_tunnel Network=192.168.11.0/24
```

初期値の CLI コンテキストに戻します。:

```
DFL-xxxx:/main> cc
DFL-xxxx:/>
```

Web Interface

A. 証明書をアップロードする :

1. **Objects > General > Key Ring > Add > Certificate** の順にメニューをクリックします。

2. 証明書に適切な名前を指定します。(例：my_cert)
3. ソースで「Upload」を選択し、「Browse/ ファイルを選択」をクリックします。
4. 証明書ファイルと関連するプライベート鍵のファイルを指定します。
5. 「OK」ボタンをクリックします。

B. IPsec トンネルを設定する :

1. **Network > Interfaces and VPN > IPsec > Add > IPsec Tunnel** の順にメニューをクリックします。

2. 以下の情報を入力します。:
- Name: ipsec_local_to_remote_tunnel
- Local Network: 172.16.1.0/24
- Remote Network: 192.168.11.0/24
- Remote Endpoint: 203.0.113.1

3. Authentication タブで 以下の設定を行います。:
- Authentication Method: Certificates
- Root Certificate(s): CA サーバルートを選択し、Selected リストに追加します。
- Gateway Certificate: ファイアウォールの証明書を選択します。

4. 「OK」ボタンをクリックします。

C. トンネルの双方向のトラフィックフローを許可する 2 つの IP ポリシーを設定する :

i. ローカルからリモートネットワークまでのトラフィックフローを許可する IP ポリシーを追加します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: local_to_remote_traffic
- Action: Allow
- Service: all_services
- Source Interface: lan
- Source Network: 172.16.1.0/24
- Destination Interface: ipsec_local_to_remote_tunnel
- Destination Network: 192.168.11.0/24

3. 「OK」ボタンをクリックします。

ii. リモートからローカルネットワークまでのトラフィックフローを許可する IP ポリシーを追加します。:

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: remote_to_local_traffic
- Action: Allow
- Service: all_services
- Source Interface: ipsec_local_to_remote_tunnel
- Source Network: 192.168.11.0/24
- Destination Interface: lan
- Destination Network: 172.16.1.0/24

3. 「OK」ボタンをクリックします。

D. トンネルにリモートネットワークへのルートを追加します。:

1. **Network > Routing > Routing Tables > main > Add > Route IPv4** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Interface: ipsec_local_to_remote_tunnel
- Network: 192.168.11.0/24

3. 「OK」ボタンをクリックします。

例題 10.6

ローミングクライアント用の証明書ベース IPsec トンネル

この例題では、オフィスに接続するローミングクライアントがリモートアクセスを行うために本社の D-Link ファイアウォールに IPsec トンネルを設定する方法を記述しています。本社ネットワークは外部ファイアウォールの IP wan_ip を持つ 203.0.113.0/24 ネットワーク範囲を使用します。

Web Interface

A. NetDefendOS および各証明書に必要な証明書をアップロードします。:

1. **Objects > Key Ring > Add > Certificate** の順にメニューをクリックします。
2. Certificate オブジェクトに適当な名前を入れます。
3. Source に Upload を指定します。
4. 「Browse/ ファイルを選択」をクリックします。
5. 証明書ファイルおよび関連するプライベート鍵ファイルを選択します。
6. 「OK」ボタンをクリックします。

B. IPsec トンネルを設定する :

1. **Network > Interfaces and VPN > IPsec > Add > IPsec Tunnel** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: RoamingIPsecTunnel
   - Local Network: 203.0.113.0/24（これはローミングユーザが接続するローカルネットワークです。）
   - Remote Network: all-nets
   - Remote Endpoint: (None)
3. Authentication タブを設定します。
   - 認証方式に Certificate（X.509 証明書）を指定します。
   - Root Certificate(s): 適切な CA サーバルートを選択し、「Selected」リストに追加します。
   - Gateway Certificate: 適切なファイアウォール証明書を選択します。
4. 「OK」ボタンをクリックします。

C. 最後に、トンネルの内側へトラフィックフローを許可する IP ルールを設定します。

証明書のトラブルシューティング

証明書が VPN ソリューションで使用される場合、以下の通り潜在的な問題の原因を参照する必要があります。

- 正しい証明書が正しい目的に使用されていることをチェックします。
- 証明書「.cer」および「.key」ファイルが同じファイル名を持つことをチェックします。例 : my_cert.key と my_cert.cer
- 証明書の期限が切れていないことをチェックします。証明書には指定の期限があり、この期限が切れると、それらを使用することはできず、新しい証明書の発行が必要となります。
- NetDefendOS の日付と時間が正確に設定されていることを確認してください。システム日時が間違っていると、証明書は実際には期限でない時に期限であるとして表示してしまいます。
- 新たに証明書を生成した場合にタイムゾーン問題を考えます。D-Link ファイアウォールのタイムゾーンは、CA サーバのタイムゾーンと同じではなく、証明書はまだローカルゾーンで有効でないかもしれません。
- CA サーバアクセスが問題であるかどうかを確認するために CRL（違反者リスト）のチェックを無効にします。CA サーバ問題については、「3.9.4 CA サーバアクセス」で、より詳しく説明しています。

10.3.9 IPSec トンネル選択

外部ネットワークデバイスが IPsec トンネルのセットアップを開始し、NetDefendOS が Responder として動作する際、NetDefendOS は受信する接続要求に最も一致する IPsec Tunnel オブジェクトを決定する必要があります。

IPsec Tunnel オブジェクトの順序が重要

IPsec Tunnel オブジェクトの一致を検索する際、NetDefendOS は定義済みトンネルリストを上から下に順番に検索します。したがって、リスト内のトンネルの順序が重要となります。以下のルールに従い、トンネルリスト内で配置を決定する必要があります。

- より限定的な条件のトンネルをリストの上に配置する

このルールに従うと、LAN-to-LAN トンネルはローミングクライアントトンネルより通常限定的な条件が設定されているため、先に配置されるべきです。例えば、ローミングクライアントトンネルでは通常 Remote Network プロパティを all-nets に指定し、LAN-to-LAN トンネルでは通常このプロパティを特定のネットワークや範囲に指定します。

構成内に多くの異なる IPsec Tunnel オブジェクトを持つ場合、NetDefendOS がどのトンネルを使用するかを決定する方法について管理者が理解することが有用です。選択決定は 3 つの段階のプロセスで実行されます。

段階 1 - IKE SA 設定

第 1 段階は、ローカルとリモートピア間の安全な制御チャンネルのベースである IKE SA 設定が関連します。使用される構成プロパティは、以下の通りです。

i. ローカルエンドポイント
ii. リモートエンドポイント
iii. 受信インタフェースフィルタ
iv. DH グループ
v. IKE アルゴリズム

段階 2 - 認証

第 2 段階では、ピアは互いに認証します。照合する基準は以下の通りです。

i. 認証方式
ii. Local ID - 指定すると、リモートピアにアクセス可能となります。指定せずに証明書を使用すると、トンネルホスト証明書に指定されたローカル ID がリモートピアにアクセス可能となります。
iii. Remote ID - 指定すると、リモートピアの ID はこのプロパティに割り当てられた ID List にあるいずれかののエントリに一致しなければなりません。詳しくは「10.3.18 証明書を使用した ID リスト」を参照してください。

段階 3 - IPsec SA 設定

最終段階では、IPsec SA がネゴシエートされます。これは段階 2 の追加設定です。

i. ローカルネットワーク
ii. リモートネットワーク
iii. IPsec アルゴリズム
iv. Encapsulation Mode
v. PFS/DH Group
vi. Setup SA Per

10.3.10 IPsec IPv6 サポート

NetDefendOS の IPsec では、以下の点において IPv6 をサポートしています。

- トンネルの確立、つまりトンネルの外側です。このセクションでは IPsec の IPv6 について、当該部分についてのみ説明します。
- トンネル内側の IPv6 トラフィックフロー。「3.2 IPv6 サポート」で詳細を説明しています。

関連イーサネットインタフェースで IPv6 を手動で有効化する

初期値では、IPv6 は全てのイーサネットインタフェースで無効化されています。IPsec IPv6 を使用するには、IPsec 通信で使用するイーサネットインタフェースで IPv6 を有効化する必要があります。イーサネットインタフェースで IPv6 を有効化する方法は「IPv6 通知の有効化」で説明しています。

IPsec トンネルで IPv6 を使用する

IPv4 の代わりに IPv6 アドレスを使用することが可能な IPsec コンポーネントの一覧は以下の通りです。

- IPsec Tunnel オブジェクトの Local Network/Remote Network プロパティを IPv6 ネットワークに指定することができます。
- IPsec Tunnel オブジェクトの Local Endpoint/Remote Endpoint プロパティを IPv6 アドレスに指定することができます。

  Local Endpoint/Remote Endpoint プロパティどちらも IPv6 アドレスに設定することができますが、トンネルでは IPv4 トラフィックを送信するかもしれません。つまり、エンドポイントが IPv6、ローカルおよびリモートネットワークが IPv4 となる可能性があります。
- IKE Config Mode Pool オブジェクトで IPv6 アドレスプールを使用することができます。
- CRL/CA ルックアップが IPv6 アドレスを使用して実行できます。
- Remote Endpoint の FQDN を IPv6 アドレスを使用して解決することができます。

- IPsec Tunnel オブジェクトプロパティは同時に IPv4 と IPv6 を設定することができません。ただし、一部のプロパティは値が設定されず、初期値で <emplty> となるかもしれません。Local Endpoint/Remote Endpoint プロパティがその一例です。<empty> 値は IPv4、IPv6 どちらも許可されることを意味します。
- （IKEv1 における）XAuth または（IKEv2 における）EAP を使用して認証された IP アドレスは、IPv4/IPv6 どちらも許容されます。詳細は「9.2.5 認証ルール」を参照してください。

注意 トンネルモニタリングは IPv4 を設定する必要がある

IPsec トンネルモニタリング機能は、リモートホストの IPv4 のみをサポートしています。本機能については「10.3.17 IPSec トンネルモニタリング」を参照してください。

10.3.11 コンフィグモード

IKE Configuration Mode（Config モード）は、NetDefendOS がリモート IPsec クライアントに設定情報を提供するようにする IKE の拡張です。それは、IP アドレスとそれに対応するネットマスクでダイナミックに IPsec クライアントを構成して、DHCP に関連する他のタイプの情報を交換するために使用されます。NetDefendOS のこの機能は IPv4、IPv6 アドレスを配布するだけです。

コンフィグモードプール

NetDefendOS は IP アドレスを配布する無名の Config Mode Pool オブジェクトを持っています。事前定義済みのプールは用意されていません。このオブジェクトがそれらのアドレスを取得する方法は、以下 2 個の設定のうちいずれかに IP Pool Type プロパティを設定することで決定されます。

- **Pre-defined IP Pool Object**
  配布される IP アドレスは、NetDefendOS 設定にある異なる指定 IP Pool オブジェクトから取得します。これらのオブジェクトの設定については、「5.5 IP プール」を参照してください。

- **Static IP Pool**
  配布される IP アドレスは、Config Mode Pool オブジェクト自身から取得します。この場合、異なる IP Pool オブジェクトを使用するのであれば、IP アドレスの範囲を指定する必要があります。

オプションの IKE Config Mode Pool プロパティ

以下の IKE Config Mode Pool オブジェクトプロパティもクライアントに送信できます。NetDefendOS は、これらの値をクライアントに転送する以外は何も行いません。

項目	説明
DNS	（IP プールに既に提供されている）URL 解決に使用される DNS の IP アドレス。
NBNS/WINS	（IP プールに既に提供されている）NBNS/WINS 解決に使用される DNS の IP アドレス。
DHCP	あらゆる内部の DHCP リクエストをこのアドレスに送信するようにホストに指示します。
Subnets	クライアントがアクセスできるサブネットのリスト。
Prefixes	クライアントがアクセスできる IPv6 サブネット。例：「2001：DB8 :: / 64」

例題 10.7

定義済み IP Pool を使用する Config Mode の設定

この例では、Config Mode Pool オブジェクトは、my_ip_pool と呼ばれる定義済みの IP Pool オブジェクトに関連させることで有効にされます。

CLI

```
DFL-xxxx:/> add ConfigModePool <name> IPPoolType=PreDefined IPPool=my_ip_pool
```

Web Interface

1. **Objects > VPN Objects > IKE Config Mode Pool** の順にメニューをクリックします。
2. **Add > IKE Config Mode Pool** をクリックします。
3. オブジェクトの名前を入力します。
4. 「Pre-defined IP Pool object」を選択します。
5. IP Pool オブジェクトリストから my_ip_pool を選択します。
6. 「OK」ボタンをクリックします。

Config モードオブジェクトを定義した後に、唯一の残りの操作は、IPsec Tunnel と使用するために Config モードを有効にすることです。

IPsec トンネルでコンフィグモードを有効にする

IPsec Tunnel オブジェクトの Config Mode プロパティ値を変更することで、事前定義済みの IP アドレスプールから、接続ローミングクライアントに対して IP アドレス配布することができます。

Config Mode プロパティには以下の値を設定できます。

- **None**
  コンフィグモードは無効です。トンネルのローカルおよびリモートネットワークプロパティ設定により保護されるネットワークが決定します。
- **Client**
  NetDefendOS はローミングクライアントのように動作し、トンネル内のローカルエンドポントのように使用する IP アドレスをリモート IPsec ピアから受信します。オプションで、リモートピアにより DNS サーバアドレスも割り当てられます。このオプションは IKEv1 と IKEv2 両方で使用することが可能であり、このセクションの最後で詳細を説明します。
- **Server**
  NetDefendOS は事前定義済みのアドレスプールから接続ピアに対し IP アドレスを割り当てます。アドレスソースとなる Config Mode Pool も設定する必要があります。

RADIUS/ ローカル DB

このオプションではユーザ認証方式に基づいてユーザに IP アドレスを割り当てることができます。ユーザ認証は Authentication Rule が起動することにより決定します。このオプションのは IKEv1 XAuth 認証または IKEv2 EAP 認証で使用することができます。

Local User Database を使用した認証では、関連する User オブジェクトの Static Client IP Address に割り当てられた値が、配布される IP アドレスとなります。

外部 RADIUS サーバを使用した認証では、ユーザ認証時に割り当て IP アドレスと共に Framed-IP-Address メッセージが返されるようにサーバを設定します。

この方式を使用した IP アドレスの割り当ては、ローミング IPsec クライアント設定を簡単にするための Roaming VPN オブジェクトを使用した場合は利用できないことに注意してください。

例題 10.8

IPsec トンネルと共に Config モードを使用する

前提として、my_cfg_pool という名前の IKE Config Mode Pool オブジェクトと、my_ipsec_tunnel という名前の IPsec Tunnel が既に定義されているものとします。この例題では、トンネルでコンフィグモードを有効にして、コンフィグモードのアドレスプールを設定します。

CLI

```
DFL-xxxx:/> set Interface IPsecTunnel my_ipsec_tunnel ConfigMode=Server IKEConfigModePool=my_cfg_pool
```

Web Interface

1. **Network > Interfaces and VPN > IPsec** の順にメニューをクリックします。
2. my_ipsec_tunnel を選択します。
3. IPsec (Phase-2) タブを開き、Config Mode に Server を指定します。
4. Config Mode Pool から my_cfg_pool を選択します。
5. 「OK」ボタンをクリックします。

IP 検証

NetDefendOS は、IPsec トンネル内の各パケットの送信元 IP アドレスが IKE Config モードで IPsec クライアントに割り当てられている IP アドレスと同じであるかどうか常にチェックします。不適当な組み合わせが検出されると、パケットは、常に破棄され、Warning レベルのシステムレベルでログメッセージが生成されます。このメッセージはクライアントの ID と共に 2 つの IP アドレスを含んでいます。

高度な設定「IPsecDeleteSAOnIPValidationFailure」を有効化することにより、オプションで、検証が失敗する場合に影響を受ける SA を自動的に削除できます 。この設定の初期値は「Disabled」(無効) です。

コンフィグモードクライアントとしての NetDefendOS

NetDefendOS コンフィグモードの Client オプションを使用すると、ファイアウォールはリモート IPsec ピアに接続する IPsec ローミングクライアントのように動作し、トンネル内のローカルエンドポイントの IP アドレスがリモートピアによって割り当てられます。IPsec トンネルは IKEv1、IKEv2 どちらも利用することができます。

NetDefendOS がコンフィグモードクライアントのように動作するためには、IPsec トンネルを以下の通り設定します。

- IKE Version プロパティを IKEv1 または IKEv2 に設定する
- IKEv1 の場合、「Pass username and password to peer via IKE XAuthPass username and password to peer via IKE XAuth, if the remote gateway requires it」設定を有効にします。

  IKEv2 の場合、EAP プロパティを EAP-MSCHAPv2 に指定します。IPsec ピアで必要な場合のみ、EAP-MD5 に指定します。
- ピアとの認証のためのユーザ名とパスワードを入力します。
- IPsec トンネルのローカル、リモートネットワークを all-nets に指定します。
- Config Mode プロパティを Client に指定します。
- Setup per SA プロパティは初期値の Network のままにします。
- オプションで、IPsec Tunnel オブジェクトの IP（トンネル内のローカルエンドポイント）および DNS（FQDN 解決のための DNS サーバ）プロパティにアドレス帳オブジェクトを割り当てます。これらのアドレス帳オブジェクトは IPsec ピアによって配布される値として割り当てられます。

  これにより、実際の IP アドレスを割り当てるリモートピアよりも優先されるアドレス帳オブジェクトを使用して NetDefendOS ルールを設定します。このような設定の典型的な例としては、IP アドレスオブジェクトに割り当てた値を使用して、トラフィックが IP ポリシーで NAT され IPsec トンネルに送信される場合です。

10.3.12 IKEv2 サポート

NetDefendOS は、IKEv1 と IKEv2 プロトコルの両方を使用することで IPsec をサポートします。本セクションでは IKEv2 を使用する場合の、特定の考慮すべき点について説明します。

IKE Version プロパティ

IPsec Tunnel オブジェクトの IKE Version プロパティはトンネルを設定する時に使用する IKE バージョンを決定します。このプロパティは以下の値の 1 つです。

項目	説明
IKEv1	NetDefendOS はトンネル設定に IKEv1 を使用します。これは初期値です。
IKEv2	NetDefendOS はトンネル設定に IKEv2 を使用します。
Auto	NetDefendOS は、最初にトンネル設定に IKEv2 を使用し、失敗すると再度 IKEv1 を使用します。 本オプションでは、事前に EAP または XAuth のどちらが使用されるか認識できないため、それらの認証を設定することはできません。したがって、ユーザ名とパスワードが必要となるローミングクライアントでは Auto を使用できません。 簡略化された IPsec プロファイルオブジェクトである、LAN-to-LAN VPN およびローミング VPN オブジェクトでは IKEv2 のみを使用します。これらは IPsec Tunnel オブジェクトの簡易バージョンであり、詳細は「10.3.15 IPsec プロファイルの使用」で説明しています。

IKEv2 ベースの IPsec トンネルを設定するのは、ほとんど IKEv1 と同じですが、以下の違いに注意する必要があります。

- IKE モードは IKEv1 トンネルだけで使用できます。
- XAuth を使用する認証は、IKEv1 でのみ可能です。IKEv2 を使用する認証には EAP を使用する必要があります。
- AES-XCBC 認証アルゴリズムは IKEv2 だけにサポートされます。AES-XCBC が IKEv1 使用時のプロポーザルリストに使用されると、スキップされます。AES-XCBC が IKEv1 を使用時のプロポーザルリストにおいて唯一のアルゴリズムであると、トンネル設定は失敗します。
- IKEv2 トンネルの Encapsulation Mode プロパティに設定できるのは「Tunnel」だけです。これは、IKEv2 が L2TP と共に使用されるべきでないことを意味します。（「10.4.2 L2TP サーバ」を参照してください。）

EAP 認証設定

IKEv2 におけるローミングクライアントのユーザ名 / パスワード認証は、EAP を使用して行われます。初期値では EAP 認証は無効です。EAP プロパティをいずれかの値に設定することで有効化することができます。

項目	説明
EAP Server	IPsec ピアは RADIUS サーバもしくは NetDefendOS のローカルユーザデータベースに対して認証されます。認証方式は Authentiaction Rule の Authenticatioin Source プロパティで指定され、トンネルの接続試行で起動します。ルールの Authentiaction Agent プロパティは EAP に設定する必要があります。
EAP-MD5	追加の Username および Password プロパティで指定されたユーザ名とパスワードを使用した EAP-MD5 で認証が行われます。
EAP-MSCHAPv2	追加の Username および Password プロパティで指定されたユーザ名とパスワードを使用した EAP-MSCHAPv2 で認証が行われます。

IKEv2 のグローバルで高度な設定

IKEv2 固有の全グローバル設定は、「10.3.22 IPSec の高度な設定」の「IKEv2」という見出しの下に記載しています。

10.3.13 IKEv2 ローミングクライアントセットアップ

本セクションでは NetDefendOS がローミングクライアントと接続するための設定に必要な手順を追って説明します。トンネルでは EAP 認証の IKEv2 を使用し、RADIUS サーバを AAA ソースとして使用します。

このセクションでは IPsec Tunnel オブジェクトを使用した手順を検討するため、個別の Authentiaction Rule オブジェクトの作成について説明します。ローミングクライアントのトンネル設定はローミング VPN オブジェクトによって簡単に行うことができます。このオブジェクトでは、個別の認証ルールを必要とせず、クライアント接続に関連しない多くのプロパティが非表示となっています。ローミング VPN オブジェクトの詳細については「10.3.15 IPsec プロファイルの使用」を参照してください。

設定のために 3 つのパートがあります。

- クライアントと NetDefendOS 内に証明書を正しくインストールする
- NetDefendOS の正しい設定
- 認証に使用する RADIUS サーバの正しい設定

以下の個別のセクションでこれらの 3 つの部分について説明します。

クライアントと NetDefendOS への証明書のインストール

EAP は証明書を使用した認証を必要とし、インストールされる証明書の必要条件は以下の通りです。

- クライアントは適切にインストールされた CA ルート証明書を持つ必要があります。

  Windows™ では、証明書を特定の場所にインストールしなければなりません。NetDefendOS は、Windows 7 以降が動作している Windows クライアントのみサポートしています。

  Windows™ におけるインストールの手順を以下に詳しく説明しており、IKEv2 が正しく機能するように、特定の場所にある必要があります。Apple iOS または Android などの他のクライアントプラットフォームでの証明書設定は、分かりやすいため、詳細には説明していません。

- クライアントが使用するのと同じ CA ルート証明書を、NetDefendOS にもインストールする必要があります。
- さらに、NetDefendOS はルート CA によって署名されているホスト証明書（ゲートウェイ証明書として知られる）を持っている必要があります。このホスト証明書には、以下のプロパティが必要です。

  i. Common Name（CN）または Subject Alternative Name (SAN) のどちらかに、IPsec トンネルのローカルエンドポイントの IP アドレス（クライアントが接続する IP アドレス）または IP アドレスを解決する FQDN の IP アドレスが設定されている必要があります。

  ii. serverAuth プロパティは設定されるべきです。

Windows クライアントのための CA ルート証明書設定

以下は Windows 7 クライアントのための証明書設定の説明です。これは、Windows 7 以降の Windows バージョンでも同様です。（Windows 7 以前のバーションはサポートしていません。）

1. Microsoft Management Console（mmc）を起動し、証明書を追加します。
2. Computer のアカウントオプションを選択します。
3. **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates** の順にフォルダを開きます。

4. 「Import」オプションを選択し、「Certificate Import Wizard」を開始します。

5. インポートする CA ルート証明書ファイルを選択し、Trusted Root Certification Authorities store にインストールします。

   証明書ファイルは決してダブルクリックしてはいけないことに注意してください。ダブルクリックすると、コンテンツは Windows レジストリの Local Computer セクションの代わりに Current User になってしまい、IPsec クライアントに利用できません。

NetDefendOS のコンフィグレーション

NetDefendOS のコンフィグレーションのための設定手順は以下の通りです。

1. NetDefendOS で、接続クライアントに IP アドレスを提供する Config Mode Pool オブジェクトを設定します。

2. ルート証明書が署名するホスト証明書の他に、同じ CA ルート証明書を NetDefendOS に追加します。

3. クライアント接続に使用される IPsec Tunnel オブジェクトを設定します。

4. NetDefendOS に、EAP 認証に使用される RADIUS Server オブジェクトを設定します。MSCHAPv2 の EAP 方式を使用することをお勧めします。

5. 接続クライアントで起動する Authentication Rule オブジェクトを設定します。ルールは、できるだけターゲットとするトラフィックにマッチするようにすべきであり、Agent プロパティを EAP に指定するべきです。

上記の NetDefendOS 設定手順の詳細は、以下の NetDefendOS 設定例で参照することができます。

RADIUS サーバ設定

以下の設定の注意事項は、Microsoft Network Policy Server（NPS）に適用されます。別のタイプの RADIUS サーバを使用する場合は、別途、対応する内容に適応させる必要があります。NPS を使用する場合、以下の手順を実行します。

1. **NPS > Policies > Connection Request Policies** の順にメニューをクリックし、Connection Request Policy を追加します。

2. ネットワークアクセスサーバの Type は Unspecified に設定します。

3. ポリシーの Conditions 部分は任意の制限を指定します。

4. **NPS > Policies > Network Policies** の順にクリックし、制限のない Network Policy を追加します。

5. Constraints で Authentication 方式を選択し、EAP 方式を選択します。すべての EAP オプションをサポートしていますが、EAP-MSCHAP v2 をお勧めします。

6. Constraints の NAS Port Type セクションを選択し、すべてのオプションを無効にします。

7. RADIUS Clients で接続するクライアントを追加します。

ローミング VPN オブジェクトにより IPsec 設定を簡単に行うことができる

下記の例題は、IPsec Tunnel オブジェクトを使用したローミングクライアント用の IPsec トンネル設定の手順を説明しています。IKEv2 トンネルに対しては、ローミング VPN オブジェクトを使用することで設定を簡単に行うことができます。この手順については「10.3.15 IPsec プロファイルの使用」に記載しています。

ローミング VPN オブジェクトではローミングクライアント用の IKEv2 IPsec トンネル絵に関連しない IPsec トンネルプロパティは非表示となっており、EAP 認証用の個別の Authentication Rule も不要です。

下記の例題では、認証ソースとして最初に RADIUS を使用し、次にローカルユーザデータベースを使用する IKEv2 ローミングクライアントによる接続の設定について説明しています。

例題 10.9

RADIUS を使用した IKEv2 EAP クライアントセットアップ

この例題は、NetDefendOS で、EAP 認証を使用したクライアントからの IKEv2 IPsec トンネルのセットアップを許可する方法を説明します。デフォルトの IKE と IPsec プロポーザルリストを使用します。

例題では、以前に説明した通りに、関連した証明書が正しく NetDefendOS とクライアントにインストールされているものとします。また、認証に使用される RADIUS サーバが正しく設定されていると仮定します。

この例題の認証ルールが、トラフィックフィルタリングパラメータとして all-nets と any を使用していることに注意してください。実際には、これらのプロパティの範囲を限定するのがよい方法です。

CLI

A. クライアント IP に config mode IP pool を作成する :

```
DFL-xxxx:/> add ConfigModePool config_mode_pool IPPoolType=Static IPPoolAddress=192.168.189.30-192.168.189.50 IPPool-
            Netmask=255.255.255.0 DNS=192.168.28.4
```

B. IPsec トンネルを設定する :

```
DFL-xxxx:/> add Interface IPsecTunnel my_ikev2_client_tunnel LocalNetwork=lannet RemoteNetwork=all-nets
            AuthMethod=Certificate GatewayCertificate=my_host_cert RootCertificates=my_root_cert
            AddRouteToRemoteNet=Yes AutoInterfaceNetworkRoute=No IKEVersion=2 RemoteEndpoint=all-nets EAP=EAPServer
            RequestEAPID=Yes IKEConfigModePool=config_mode_pool
```

C. 認証用の RADIUS サーバを設定する :

```
DFL-xxxx:/> add RadiusServer my_radius_server IPAddress=203.0.113.20 SharedSecret=MYSHAREDRADIUSSECRETSTRING
```

D. トンネルに認証ルールを設定する :

```
DFL-xxxx:/> add UserAuthRule Agent=EAP AuthSource=RADIUS Interface=any Name=my_ikev2_auth_rule
            OriginatorIP=all-nets RadiusServers=my_radius_server
```

Web Interface

A. クライアント IP に config mode IP pool を作成する :

1. **Objects > IKE Config Mode Pool > Add > IKE Config Mode Pool** の順にメニューをクリックします。
2. Static IP Pool を選択します。
3. 以下の情報を入力します。
   - Name: config_mode_pool
   - IP Pool : 192.168.189.30-192.168.189.50
   - Netmask : 255.255.255.0
   - DNS : 192.168.28.4
4. 「OK」ボタンをクリックします。

B. IPsec トンネルを設定する :

1. **Network > Interfaces and VPN > IPsec > Add > IPsec Tunnel** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_ikev2_client_tunnel
   - IKE Version: IKEv2
   - Local Network: lannet
   - Remote Network: all-nets
   - Remote Endpoint: all-nets
3. IPsec (Phase-2) タブを開き、以下の情報を設定します。
   - Config mode: Server
   - Config Mode Pool: my_cfg_pool
4. Authentication タブを選択します。
   - Authentication Method で Certificate を指定します。
   - Gateway Certificate に my_host_cert を選択します。
   - Root Certificate(s) に my_root_cert を追加します。
   - EAP で EAP Srever を選択します。
   - Request EAP ID オプションを有効にします。

5. Advanced タブを選択します。
   - Add route dynamically オプションを有効にします。
   - Add route statically オプションを無効にします。

6. 「OK」ボタンをクリックします。

C. 認証用の RADIUS サーバを設定する :

1. **Policies > User Authentication > RADIUS > Add > RADIUS Server** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_radius_server
   - IP Address: 203.0.113.20
   - Shared Secret: MYSHAREDRADIUSSECRETSTRING

3. 「OK」ボタンをクリックします。

D. トンネルに認証ルールを設定する :

1. **Policies > User Authentication > Authentication Rules > Add > Authentication Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_ikev2_auth_rule
   - Authentication agent: EAP
   - Authentication source: RADIUS
   - Interface: any
   - Originator IP: all-nets

3. Authentication Options を選択します。

4. RADIUS servers に my_radius_server を追加します。

5. 「OK」ボタンをクリックします。

例題 10.10

ローカルデータベースを使用した IKEv2 EAP クライアントの設定

この例題は、1 つ前の例題「RADIUS を使用した IKEv2 EAP クライアントセットアップ」と同様の設定を行いますが、認証に RADIUS ではなく、Local User Database オブジェクトを使用します。

my_user_db という名前の Local User Database オブジェクトが既に定義済みであり、有効な EAP ユーザのための認証がすべて含まれているものとします。1 つ前の例題の Authentication Rule オブジェクトのみ変更する必要があります。

CLI

A. クライアント IP に config mode IP pool を作成する :

```
DFL-xxxx:/> add ConfigModePool my_cfg_pool IPPoolType=Static IPPoolAddress=192.168.189.30-192.168.189.50 IPPoolNet-
            mask=255.255.255.0 DNS=192.168.28.4
```

B. IPsec トンネルを設定する :

```
DFL-xxxx:/> add Interface IPsecTunnel my_ikev2_client_tunnel LocalNetwork=lannet RemoteNetwork=all-nets
            AuthMethod=Certificate GatewayCertificate=my_host_cert RootCertificates=my_root_cert AddRouteToRemoteNet=Yes
            AutoInterfaceNetworkRoute=No IKEVersion=2 RemoteEndpoint=all-nets EAP=EAPServer RequestEAPID=Yes
            ConfigMode=Server IKEConfigModePool=my_cfg_pool
```

C. トンネルに認証ルールを設定する :

```
DFL-xxxx:/> add UserAuthRule Name=my_ikev2_auth_rule AuthSource=Local Interface=any OriginatorIP=all-nets
            LocalUserDB=my_user_db Agent=EAP
```

Web Interface

A. クライアント IP に config mode IP pool を作成する :

1. **Objects > IKE Config Mode Pool > Add > IKE Config Mode Pool** の順にメニューをクリックします。

2. Static IP Pool を選択します。

3. 以下の情報を入力します。
   - Name: my_cfg_pool
   - IP Pool : 192.168.189.30-192.168.189.50
   - Netmask : 255.255.255.0
   - DNS : 192.168.28.4

4. 「OK」ボタンをクリックします。

B. IPsec トンネルを設定する :

1. **Network > Interfaces and VPN > IPsec > Add > IPsec Tunnel** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_ikev2_client_tunnel
   - IEK Version: IKEv2
   - Local Network: lannet
   - Remote Network: all-nets
   - Remote Endpoint: all-nets

3. Authentication タブで 以下の設定を行います。
   - Authentication Method: Certificates
   - Gateway Certificate に my_host_cert を選択します。
   - Root Certificate(s) に my_root_cert を追加します。
   - EAP (IKEV2) セクションで EAP に EAP Server を指定し、Request EAP ID オプションを有効にします。

4. IPsec (Phase-2) タブを選択し、以下の情報を入力します。
   - Config Mode: Server
   - Config Mode Pool: my_cfg_pool

5. Advanced タブを選択します。
   - Add route dynamically オプションを有効にします。
   - Add route statically オプションを無効にします。

6. 「OK」ボタンをクリックします。

C. トンネルに認証ルールを設定する :

1. **Policies > User Authentication > Authentication Rules > Add > User Authentication Rule** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_ikev2_auth_rule
   - Authentication agent: EAP
   - Authentication source: Local
   - Interface: any

3. Authentication Options タブを選択します。
   - Local User DB で my_user_db を選択します。

4. 「OK」ボタンをクリックします。

10.3.14 iOS ローミングクライアントの設定

NetDefendOS で定義されている標準の IPsec トンネルを使用して、Apple iOS™ デバイスが搭載する標準の IPsec クライアントを使用できます。iOS の IPsec 設定手順は、「10.3.7 IPSec ローミングクライアント」で説明した通り、基本的には他のローミングクライアンの設定と同様です。他の手順と異なる部分について、本セクションで補足します。

NetDefendOS の設定手順は以下の通りです。

1. ファイアウォールにより送信される証明書を認証する CA ルート証明書が、iOS デバイスにインストールされていることを確認します。簡単な確認方法としては、デバイスに証明書を添付してメール送信し、インストール後にそのファイルを開きます。

2. アドレス帳オブジェクトをトンネルに作成します。構成は以下の通りです。
   i. ローカルなエンドポイントとクライアントアドレスが属するネットワーク。例 :192.168.99.0/24
   ii. ローカルなトンネルのエンドポイント。例 :192.168.99.1
   iii. 接続クライアントに配布するアドレス範囲。: 例 :192.168.99.10-192.168.99.250

3. Passphrase (ASCII) の Pre-shared Key (PSK) オブジェクトを作成します。これは、ユーザ名とパスワードに加えて iOS デバイスの IPsec クライアントに入力する共有秘密鍵です。

4. IKE Config Mode Pool オブジェクトを作成し、Static IP Pool オプションを選択して、最初の手順で定義した IP アドレス範囲を関連付けます。

5. ユーザ名とパスワードを持つユーザをローカルユーザデータベースに登録します。また、本機能は RADIUS サーバが実行するかもしれません。

6. IPsec トンネルオブジェクトを定義し、Diffie-hellman group プロパティが 14（2048bit）となるようにします。このグループは Perfect Forward Security プロパティに追加する必要はありません。

7. トンネルの IKE プロポーザルリストについて、暗号化が AES（Rijndael）、Integrity が SHA512 であることを確認します。新しいプロポーザルリストを作成または定義済みのリストを編集することもできます。

8. トンネルの IPsec プロポーザルリストについて、暗号化が AES（Rijndael）、Integrity が SHA512 であることを確認します。新しいプロポーザルリストを作成または定義済みのリストを編集することもできます。

9. IPsec トンネルオブジェクトの他のプロパティは以下の値となります。

   i. Local Network: all-nets
   ii. Remote Network: all-nets
   iii. Remote Endpoint: None
   iv. Encapsulation mode: Tunnel
   v. IKE Config Mode Pool: スタティックな IP プールを選択します。
   vi Authentication: 上で定義した PSK を選択します。
   vii. 内向きトンネル用の XAuth 認証を選択します。
   viii. Add route dynamically（トンネルが確立された時にリモートネットワークにルートをダイナミックに追加する）オプションを有効にします。
   ix. IP Addresses: ローカルなトンネルのエンドポイントアドレスになるように手動で指定します。
   x. Security Association: ネットワーク毎
   xi. Add route statically オプションを無効にします。

10. Local Endpoint プロパティを使用してクライアントが接続する IP アドレスを定義すること男鹿できます。指定しない場合、ローカルエンドポイントはデフォルトでトンネルのローカルイーサネットインタフェースの IP アドレスになります。

11. IPsec トンネルのリストの最後にトンネルを置きます。また、このトンネルが L2TP/IPsec の PSK トンネルと共存できないことに留意してください。

12. 以下のプロパティでユーザ認証ルールを作成します。

   i. Authentication Agent: XAuth
   ii. Authentication Source:Local（または RADIUS）
   iii. Originator IP: all-nets
   iv. Local User DB: ローカルユーザデータベース

13. クライアントトラフィック用の IP ルールを追加します。代表的なルールは、保護されたリソースにアクセスすることを許可する「Allow」ルールとトンネル経由でインターネットに到達する「NAT」ルールです。

10.3.15 IPsec プロファイルの使用

NetDefendOS コンフィグレーションに IPsec トンネルを追加する場合、複数の種類のオブジェクトを使用することができます。基本的な IPsec Tunnel オブジェクトを使用するほかに、特定のケースでトンネル設定を簡単に行うための IPsec プロファイルオブジェクトが用意されています。これらのプロファイルは、ベースとなる IPsec Tunnel オブジェクトの特定のプロパティについて事前定義済みとなっており、残りのプロパティを管理者が設定できるようになっています。

標準の IPsec Tunnel オブジェクトに加えて、以下の簡略化された IPsec プロファイルオブジェクトが利用可能です。

- **LAN-to-LAN VPN**

標準の IPsec Tunnnel をベースとした別の設定です。リモートピア（NetDefendOS システム）への LAN-to-LAN IPsec 通信の設定を簡単に行うことができます。同等の LAN-to-LAN VPN オブジェクトと似たような設定となっています。

リモートピアは、LAN to LAN VPN オブジェクトの初期値（KEv2 with AES-128 および SHA-256、DH group 14 (2048-bits)、Forward Secrecy）をサポートするように設定されているのであれば NetDefendOS システム以外にもなり得ます。

オブジェクトの詳細は「10.3.15.1 LAN to LAN VPN」を参照してください。

- **ローミング VPN**

標準の IPsec Tunnnel をベースとした別の設定です。ローミングクライアント用のトンネル接続の設定を簡単に行うことができます。

オブジェクトの詳細は「10.3.15.2 ローミング VPN」を参照してください。

- **Azure VPN**

標準の IPsec Tunnnel をベースとした別の設定です。LAN-to-LAN トンネルであり、Microsoft Azure 仮想ネットワークへの VPN 接続設定を簡単に行うことができます。

オブジェクトの詳細は「10.3.15.3　Azure VPN」を参照してください。

「LAN-to-LAN VPN」「ローミング VPN」「Azure VPN」オブジェクトの目的は標準 IPsec Tunnel オブジェクトの簡易化です。特定シナリオに関連しないプロパティを非表示とし、適切なデフォルトプロパティ値を使用します。これらのすべてのオブジェクトは IKEv2 に基づいていることに注意して下さい。

以下に続くセクションでこれらのトンネルタイプについて詳細を説明します。

10.3.15.1 LAN to LAN VPN

LAN to LAN VPN オブジェクトは、リモートピア（NetDefendOS システム）への LAN-to-LAN IPsec 通信の設定を簡単に行うための、IKEv2 ベースの IPsec トンネルタイプです。LAN-to-LAN VPN トンネルに適した設定となっています。

このプロファイルでは以下のプロパティを設定することができます。
- ローカル / リモートエンドポイント IP
- リモートネットワーク
- ルートをダイナミックまたはスタティックで追加するオプション。スタティックが初期値です。
- 事前共有鍵または証明書による認証オプション

このトンネルタイプに使用される IPsec トンネルプロパティ設定は以下の通りです。
- IKE Version: IKEv2
- Encryption proposed: AES-128, AES-192, AES-256
- Authentication proposed: SHA-256, SHA-512
- IKE DH Group: 14
- PFS 有効
- PFS DH Group: 14

他の IPsec トンネルプロパティは初期値に設定されています。

NetDefendOS システムではないリモート IPSec ピアであっても、このトンネルタイプの動作を再現できるように設定されているシステムであれば、このトンネルタイプに接続することができます。

LAN-to-LAN VPN オブジェクトによって作成されたトンネルで D-Link 固有のものはありません。このプロファイルは同様に設定されたトンネルのピアとの接続を簡単にするためだけのものです。ピア側で適切な IPsec の設定が行われている場合、D-Link システム以外のピアであることも考えられます。

例題 10.11

LAN to LAN VPN オブジェクトによる IPsec の設定

この例題は「PSK ベースの LAN-to-LAN IPsec トンネルの設定」の設定を元に、LAN to LAN VPN オブジェクトを設定します。

リモートピアは通常別の D-Link ファイアウォールであり、LAN to LAN VPN オブジェクトを使用して同様に設定されます。もう 1 台のファイアウォールでは、異なる Remote Endpoint の値となり、Local Network と Remote Network が逆になります。

CLI

```
DFL-xxxx:/> add Interface LANtoLANVPN ipsec_hq_to_branch LocalNetwork=172.16.1.0/24 RemoteNetwork=192.168.11.0/24 Remo-
            teEndpoint=203.0.113.1 PSK=my_secret_key
```

Web Interface

1. Network > Interfaces and VPN > IPsec > Add > LAN to LAN VPN (Simplified) の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: ipsec_hq_to_branch
   - Remote Endpoint: 203.0.113.1
   - Local Network: 172.16.1.0/24
   - Remote Network: 192.168.11.0/24

3. Authentication で Pre-Shared Key に my_secret_key を設定します。

4. 「OK」ボタンをクリックします。

10.3.15.2 ローミング VPN

ローミング VPN オブジェクトは、標準の IPsec トンネルオブジェクトをベースとした、ローミングクライアント用のトンネル接続設定を簡単に行うためのオブジェクトです。証明書の認証、EAP-MSCHAPv2 による IKEv2 を使用しています。

注意 ローカルクライアントはこのプロファイルではサポートされません。

ローミング VPN プロファイルでは、作成された IPsec トンネルがクライアントトラフィックを同じインタフェースで送受信することを想定しています。これはインターネットを介して接続する外部のローミングクライアントで該当します。しかし、異なるインタフェース上のファイアウォール後方のローカルクライアントには該当しません。したがって、それらのケースではこのプロファイルを使用することはできません。

かわりに標準の IPsec Tunnel オブジェクトを使用します。トンネルの Local Endpoint プロパティに対し、トンネルを終了させるインタフェースの IP アドレスを設定します。Local Endpoint プロパティについては「10.3.3 IPsec トンネルプロパティ」で詳細を説明します。

このプロファイルでは以下の IPsec Tunnel プロパティを設定します。
- 配布される IP プールのアドレスセット。プールオブジェクトを使用せず、IP 範囲を直接指定します。
- オプションの DNS サーバアドレス
- ホスト / ルート証明書（PSK はサポートされていません）
- 認証ソース（RADIUS または Local）。RADIUS オプションでは定義済みの RADIUS Server を指定する必要があります。Local オプションでは Local User Database を使用する必要があります。非表示の Authentication Rule オブジェクトはこの設定により自動的に作成されます。
- RADIUS サーバが使用される場合、サーバはクライアントに IP アドレスを割り当てることはできません。この機能は標準の IPsec Tunnel オブジェクトを使用して行う必要があります。
- トンネルのローカルネットワークは常に内部で all-nets に設定されます。この場合、送信先 IP アドレスが特定のアドレスではないため、IP ポリシーとルートを設定してクライアントから送信されるパケットの処理方法を指定する必要があります。

このトンネルタイプに使用される IPsec トンネルプロパティ設定は以下の通りです。
- IKE Version: IKEv2
- Encryption proposed: AES-128, AES-192, AES-256
- Authentication proposed: SHA-1, SHA-256, SHA-512
- IKE DH Groups: 2, 14
- PFS 有効
- PFS DH Groups: None, 2, 14
- DPD interval: 300 秒

他の IPsec トンネルプロパティは初期値に設定されています。

Authentication Rule は自動的に設定される

Roaming VPN オブジェクトで入力された値に基づき、必要な Authentication Rule が自動的に作成されます。作成された認証ルールは Web インタフェースでは表示されず、編集することもできません。CLI コマンド uarules で閲覧のみ可能です。

IKEv2 トンネルであるため、RADIUS サーバまたはローカルデータベースに対するクライアント認証では常に EAP が使用されます。RADIUS 認証の場合は RADIUS Server オブジェクトを設定する必要があります。この設定については本セクションの最後に例題を示します。

複数のトンネルオブジェクト

複数の Roaming VPN オブジェクトを設定することが可能です。クライアント接続時に選択される Roaming VPN オブジェクトは、クライアント側のルート証明書に依存します。使用されるトンネルは、Roaming VPN オブジェクトリストにおいて、クライアント側のルート証明書と Roaming VPN オブジェクトに紐づくルート証明書が一致する、最初のエントリです。

クライアントには複数のルート証明書が存在する可能性があります。

サポートされるクライアント

このオプションで、公式サポートされるベース VPN クライアントタイプは次のクライアントです。

- Windows 7 から Windows 10 までの built-in クライアント
- MacOS Sierra built-in クライアント
- iOS 10 built-in クライアント
- strongSwan クライアント /Android 7.0 Nougat

これらの環境の古いバージョンも正常に動作する可能性があります。いずれの場合も、クライアントの設定で必要なことは、Roaming VPN オブジェクトで使用されるものと同じルート証明書をインポートすることだけです。これ以外についてはクライアントは初期値の設定で動作し、ユーザ名とパスワードの入力のみが必要となります。

IKEv2 ローミングクライアントや証明書を使用した Windows クライアントの設定については、「10.3.13 IKEv2 ローミングクライアントセットアップ」を参照してください。

例題 10.12

Roaming VPN オブジェクトを使用した IPsec 設定

この例題は、「RADIUS を使用した IKEv2 EAP クライアントセットアップ」を基にしていますが、Roaming VPN オブジェクトを使用して簡単に設定を行う手順となっています。

CLI

A. EAP 認証用の RADIUS サーバを設定する

```
DFL-xxxx:/> add RadiusServer my_radius_server IPAddress=203.0.113.20 SharedSecret=MYSHAREDRADIUSSECRETSTRING
```

B. Roaming VPN オブジェクトを設定する

```
DFL-xxxx:/> add Interface RoamingVPN my_vpn_client_tunnel IPPoolAddress=192.168.189.30-192.168.189.50
            GatewayCertificate=my_host_cert RootCertificates=my_root_cert AuthSource=RADIUS RadiusServer=my_radius_
            server
```

Web Interface

A. EAP 認証用の RADIUS サーバを設定する

1. **Policies > User Authentication > RADIUS > Add > RADIUS Server** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_radius_server
   - IP Address: 203.0.113.20
   - Shared Secret: MYSHAREDRADIUSSECRETSTRING
3. 「OK」ボタンをクリックします。

B. Roaming VPN オブジェクトを設定する

1. **Network > Interfaces and VPN > IPsec > Add > Roaming VPN (Simplified)** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_vpn_client_tunnel
   - IP Pool: 192.168.189.30-192.168.189.50
   - Gateway Certificate：my_host_cert
   - Root Certificate(s)：my_root_cert
   - Authentication Source: RADIUS
   - Radius Server: my_radius_server
3. 「OK」ボタンをクリックします。

10.3.15.3 Azure VPN

Azure VPN オブジェクトは、D-Link ファイアウォールから Microsoft Azure への site-to-site 通信の設定を簡単に行うための、IKEv2 ベースの IPsec トンネルタイプです。ファイアウォール後方にローカルに配置されたコンピュータから Azure 仮想ネットワーク内の仮想マシンまたはロールインスタンスへの通信を可能にします。

このプロファイルでは以下の IPsec Tunnel プロパティを設定します。
- リモートエンドポイント
- ローカルネットワーク
- リモートネットワーク
- ルートをダイナミックまたはスタティックで追加するオプション。スタティックが初期値です。
- PSK

このトンネルタイプに使用される IPsec トンネルプロパティ設定は以下の通りです。
- IKE Version: IKEv2
- Encryption proposed: AES-128, AES-192, AES-256
- Authentication proposed: SHA-256, SHA-512
- IKE DH Groups: 2, 14
- PFS 有効
- PFS DH Groups: 2, 14
- DPD lifetime: 27000 秒

他の IPsec トンネルプロパティは初期値に設定されています。
Azure VPN オブジェクトで作成されるトンネルでは、Azure 固有の NetDefendOS 機能はありません。

例題 10.13

Azure VPN オブジェクトを使用した IPsec 設定

この例題は、「PSK ベースの LAN-to-LAN IPsec トンネルの設定」を基にしていますが、Azure VPN オブジェクトを使用して簡単に設定を行う手順となっています。

CLI

```
DFL-xxxx:/> add Interface AzureVPN ipsec_local_to_azure RemoteEndpoint=203.0.113.1 LocalNetwork=172.16.1.0/24 Remote-
            Network=192.168.11.0/24 PSK=my_secret_key
```

Web Interface

1. **Network > Interfaces and VPN > IPsec > Add > Azure RouteBased VPN (Simplified)** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: ipsec_local_to_azure
   - Remote Endpoint: 203.0.113.1
   - Local Network: 172.16.1.0/24
   - Remote Network: 192.168.11.0/24
3. Authentication で以下の情報を入力します。
   - Pre-Shared Key: my_secret_key
4. 「OK」ボタンをクリックします。

10.3.16 MOBIKE のサポート

IKEv2 の Mobility and Multihoming Protocol 機能では、ローミングクライアントが別のネットワーク（例えば、4G モバイルネットワークから固定の WiFi ネットワーク）に切り替わった場合に IP アドレスを変更することが可能であり、これにより、既存の IPsec トンネルを中断することなくネットワーク間で動作することができます。

NetDefendOS は自動的に MOBIKE with IKEv2 トンネルをサポートし、設定を有効化するなどの作業は必要ありません。ただし、NetDefendOS ではローミングクライアントの IP アドレス変更のみを許可することに注意してください。MOBIKE RFC 4555 では両方のエンドポイントの IP アドレス変更をサポートしていますが、NetDefendOS は自身のローカル IP アドレスの変更は許可しません。

NetDefendOS における MOBIKE 機能の要点は以下の通りです。

- MOBIKE 機能により、クライアントまたは NAT されたデバイスはトンネルネゴシエーション不要で IP と（または）ポートを変更することができます。
- MOBIKE は IKEv2 IPsec トンネルで常に有効化されています。
- MOBIKE はピアで許可されている場合のみ動作します。
- ローミングクライアントのシナリオにおいて、NetDefendOS がトンネルを開始していない場合かつ Responder として動作している場合のみに MOBIKE がサポートされます。
- 各トンネルに Dead peer detection 間隔を設定し、クライアントがサーバよりも前に DPD メッセージを送信するようにすることが可能です。

10.3.17 IPSec トンネルモニタリング

概要

IPsec Tunnel オブジェクトにはいくつかの追加のプロパティがあり、トンネルモニタリング機能も提供します。これは、問題が検出されるとトンネルの正常性をチェックし、トンネルを再確立するのに使用されます。トンネルモニタリングを有効にすると、以下の処理が発生します。

- モニタ設定の際に一つの外部 IPv4 アドレスを指定すると、この IP アドレスへの IPsec トンネルを通じて 1 秒ごとに ICMP ping メッセージが送信されます。これはトンネルが確立している間中起こります。
- これらの ICMP メッセージの送信元 IP はトンネルの Originator IP プロパティの設定値となります。
- 連続した ICMP ping メッセージに対して指定した応答回数を受信しないと、トンネルがもう動作状態ではないと見なし、新しい IPsec トンネル接続のために自動的にネゴシエートを行います。

トンネルモニタ機能は、「4.2.3 ルートフェイルオーバ」で記述したホストモニタリングに類似しており、同じ基本メカニズムを共有します。

トンネル正常性モニタリングの代替手段

トンネルモニタリングは、IPsec トンネルの正常性をモニタする効率的な方法ですが、外部ホストを必要とします。しかし、Auto Establish オプションを使用するより好ましいと言えます。Auto Establish は IKE レベルで動作するという欠点があり、トンネル内のトラフィックフローをモニタしません。トンネルモニタリングと Auto Establish の両方を同時に使用する理由はなく、これは回避すべきです。

（外部の IPsec ピアが DPD をサポートしない場合を除き）トンネルモニタリングが使用されるので、Dead peer detection（DPD）を無効にするべきではありません。両方で有効であれば、DPD はトンネルモニタリングへのコンプリメントとして動作することができます。

IPsec トンネルモニタリングの設定

IPsec Tunnel オブジェクトのモニタ設定には以下の手順が必要です。

- IPsec トンネルでモニタリングを有効にします。
- トンネルを通じてアクセス可能なホストとして一つの IPv4 アドレスを指定します。ルートの追加を行わなくて良いように、IP アドレスは常にトンネルのリモートネットワークの一部にする必要があります。ホスト自身には、ICMPping 要求に応答するように設定を行います。
- オプションでトンネルを再ネゴシエートする前に受信しない連続した応答数を設定します。指定しないと、初期値の 10 になります。

トンネルモニタ状態の参照

「hostmon」コマンドを使用することで、IPsec トンネルモニタの状態を参照できます。以下は、2 つの異なる IPv4 アドレスを使用して 2 つのトンネルに送信したメッセージを参照する例題です。

```
DFL-xxxx:/> hostmon

Monitor sessions:
Session #1:
Failed Latency ms
Reachable Proto Host           Port Interval Sample (act / max) (act / max)
--------- ----- -------------- ---- -------- ------ ----------- -----------
YES       ICMP  192.168.1.1         1000     5      0    / 4    20   / 3000
YES       ICMP  192.168.3.1         1000     5      0    / 4    10   / 3000
```

「hostmon -verbose」コマンドを代わりに使用すると、ICMP メッセージの送信元 IP を参照することができます。

ログへの出力

ログイベントメッセージは以下の場合 NetDefendOS によって生成されます。

- ホストが到達可能であると判断した場合、以下のログメッセージが生成されます。

```
IPSEC prio=Info id=01803600 rev=1 event=monitored_host_reachable
action=none ip=192.168.1.2 tunnel=PSK-NAT
```

- ホストが到達不能であると判断した場合、以下のログメッセージが生成されます。

```
IPSEC prio=Error id=01803600 rev=1 event=monitored_host_unreachable
action=sas_deleted ip=192.168.1.2 tunnel=PSK-NAT
```

例題 10.14

IPsec トンネルモニタリングを有効にする

この例題では、既存の IPsec Tunnel オブジェクト my_ipsec_tunnel1 でトンネルモニタリングを有効にします。モニタリングに使用するホストは IPv4 アドレス 203.0.11.5 を持ち、送信した ICMP メッセージに最大 5 回までの無応答を許容します。

CLI

```
DFL-xxxx:/> set Interface IPsecTunnel my_ipsec_tunnel1 TunnelMonitor=Yes MonitoredIP=203.0.11.5 MaxLoss=5
```

Web Interface

1. **Network > Interfaces and VPN > IPsec** の順にメニューをクリックします。
2. トンネル my_ipsec_tunnel1 を選択します。
3. Advanced タブの Tunnel Monitor で以下のように入力します。
   - Tunnel Monitor オプションを有効にします。
   - Monitored IP: 203.0.11.5
   - Max Loss: 5
4. 「OK」ボタンをクリックします。

10.3.18 証明書を使用した ID リスト

証明書を IPsec トンネルのために認証方法として使用する場合、NetDefendOS は CA 署名付証明書を提示できるすべてのリモートピアを受け付けます。特にローミングクライアントを利用している場合、ここには潜在的な問題があります。

典型的なシナリオ

出張中の従業員が証明書を使用した IPsec を利用して社内ネットワークに接続する場合について考えてみます。組織は自身の CA を管理し、証明書は従業員に配布されます。異なる部署の従業員は、社内のネットワークの異なる部分に接続すると考えられます。例えば、営業部のメンバは受注システムが動作しているサーバに接続する必要があり、技術部門のエンジニアはテクニカルデータベースに接続します。

問題

出張中の従業員が利用する VPN クライアントの IP アドレスは予想できないので、クライアントからの内向き IPsec 接続を前もって区別することはできません。これは、ファイアウォールがクライアントの IP アドレスだけを使用して内部ネットワークの異なる部分に正しくアクセスできないことを意味します。

ID リストのソリューション

識別子リスト（ID リスト）はこの問題の解決法を提供します。NetDefendOS ID List オブジェクトには 1 つ以上の ID オブジェクトがあります。IPsec Tunnel オブジェクトは、ID List オブジェクトに設定された Remote ID プロパティを持つことができます。特定のトンネルが特定のクライアントによって使用されるためには、以下の通りである必要があります。

- リモートクライアントが送信した ID は、トンネル用の ID リストの ID の 1 つに一致しなければなりません。
- また、クライアントが送信した ID は、ID の 1 つとしてクライアントが送信する証明書に存在しなければなりません。

クライアントが接続するとき、NetDefendOS は以下の通り使用する IPsec トンネルオブジェクトを選択します。

- 接続クライアントは IKE ネゴシエーションで NetDefendOS に ID を送信します。
- NetDefendOS はクライアントの照合のために IPsec Tunnel オブジェクトのリストをスキャンします。正常な照合処理については「10.3.9 IPSec トンネル選択」で説明します。
- 一致するトンネルが検出されると、NetDefendOS によってクライアント認証が行われ、クライアントによってトンネルネゴシエーション中に送信される ID 情報を含む証明書をチェックします。

- 最後に、NetDefendOS は一致するトンネルの ID List 内の ID オブジェクトに対して ID の検証を行います。一致する ID が見つからない場合、トンネルの確立は失敗しログメッセージが生成されます。

  不正な形式の ID はすべて無視され、警告ログメッセージが生成されます。

IKEv1．IKEv2 トンネルの両方で ID List を使用することができますが、通常証明書を使用するトンネルのみに関連します。PSK トンネルで ID リストを使用することも可能ですが、トンネルの両端で PSK が一致しなければならないため、リストを使用する必要がありません。

ID の指定

ID オブジェクトプロパティの要否は、オブジェクトの Type プロパティによって決定します。Type プロパティの値は以下のいずれかになります。

- **DistinguishedName**
  クライアントから送信される ID に含まれる識別名（Distinguished Name: DN）と一致します。クライアントの証明書における subjectName フィールドと同じである必要があります。以下の例では、CLI コマンドを使用してこの値を含む ID オブジェクトを作成します。

```
DFL-xxxx:/my_id_list> add ID my_dn_id Type=DistinguishedName CommonName=”John
            Smith” OrganizationName=example OrganizationalUnit=Support
            Country=Sweden EmailAddress=john.smith@example.com
```

  便宜上、識別名のパラメータは個別のプロパティとして指定しています。特定の順序の長い文字列のパラメータ / 値を指定する必要はありません。

- **DNS**
  クライアントから送信される ID に含まれる FQDN と一致します。クライアントの証明書における subjectAltName フィールドと同じになります。以下の例では、CLI コマンドを使用してこの値を含む ID オブジェクトを作成します。

```
DFL-xxxx:/my_id_list> add ID my_email_id Type=E-Mail EMailAddress=john.smith@ex-
            ample.com
```

- **E-Mail**
  クライアントから送信される ID に含まれる E メールアドレスと一致します。クライアントの証明書における subjectAltName フィールドと同じになります。以下の例では、CLI コマンドを使用してこの値を含む ID オブジェクトを作成します。

```
DFL-xxxx:/my_id_list> add ID my_email_id Type=E-Mail E-Mail=john.smith@example.com
```

- **IP**
  クライアントから送信される ID に含まれる IP アドレスと一致します。クライアントの証明書における subjectAltName フィールドと同じになります。以下の例では、CLI コマンドを使用してこの値を含む ID オブジェクトを作成します。

```
DFL-xxxx:/my_id_list> add ID my_ip_id Type=IP IP=203.0.113.5
```

例題 10.15

ID リストを使用する

この例題では IPsec トンネルで使用するために Identification List オブジェクトを作成し、使用する方法を示しています。この識別リストには、プライマリ ID としてタイプ DN(Distinguished name) を持つ 1 つの ID が含まれています。特定の IPsec のトンネルオブジェクトを追加する方法は、この例題に説明されていませんので注意してください。

CLI

はじめに、識別リストを作成する：

```
DFL-xxxx:/> add IDList my_id_list
```

次に、ID を作成する：

```
DFL-xxxx:/> cc IDList my_id_list
DFL-xxxx:/my_id_list> add ID JohnDoe Type=DistinguishedName CommonName=”John Doe” OrganizationName=D-Link
            OrganizationalUnit=Support Country=Sweden EmailAddress=john.doe@D-Link.com
DFL-xxxx:/my_id_list> cc
```

最後に、IPsec トンネルに識別子リストを適用する：

```
DFL-xxxx:/> set Interface IPsecTunnel MyIPsecTunnel AuthMethod=Certificate RemoteID=my_id_list
            RootCertificates=my_root_cert GatewayCertificate=my_gateway_cert
```

Web Interface

はじめに、識別リストを作成する :

1. **Objects > VPN Objects > IKE ID Lists > Add > ID List** をクリックします。
2. リストの名前（例 : example my_id_list）を入力します。
3. 「OK」ボタンをクリックします。

次に、この ID リストに 1 つの ID リストを追加します。:

1. **Objects > VPN Objects > IKE ID Lists** をクリックします。
2. my_id_list を選択します。
3. IDs タブで **Add > ID** をクリックします。
4. ID の名前（例 : JohnDoe）を入力します。
5. Type で Distinguished name を選択します。
6. 以下の情報を入力し、「OK」をクリックします。
   - Common Name: John Doe
   - Organization Name: D-Link
   - Organizational Unit: Support
   - Country: Sweden
   - Email Address: john.doe@D-Link.com

注意 「Name」にはスペースを含むことはできません。

7. 「OK」ボタンをクリックします。

最後に、IPsec トンネルに識別子リストを適用する :

1. **Network > Interfaces and VPN > IPsec** の順にメニューをクリックします。
2. 希望する IPsec トンネルオブジェクトを選択します。
3. Authentication タブで Authentication Method で Certificate を指定します。
4. Root Certificate(s) と Gateway Certificate 設定で適切な証明書を選択します。- 証明書チェーンでは、ルート証明書としてすべての中間証明書をロードする必要があります。
5. AUTHENTICATED IDENTITIES で my_id_list を選択します。
6. 「OK」ボタンをクリックします。

10.3.19 IPsec を使用した DiffServ

Differentiated Services（diffserv）フィールドは、データトラフィックに優先度をつけるためにネットワーク装置によって使用されます。8 ビット diffserv フィールドは 2 つの部分から成ります。: 6 ビットの Differentiated Services Code Point（DSCP）と 2 ビットの Explicit Congestion Notification（ECN）です。NetDefendOS IPsec はこれらの全てを処理し、8 ビットフィールドを分割しません。

IPsec 用のトンネルに関連する DiffServ 値は以下の 3 つのタイプに分割できます。

- トンネル設定のための IKE 交換に関連するパケットの DiffServ 値。
- 外部トンネルの IPsec パケットの DiffServ 値。
- トンネル内部に送信されるパケットの DiffServ 値。

管理者は以下の方法で DiffServ 値を変更できます。

- トンネル設定用に、IKE パケットの DiffServ 値は特定の固定値を持つことができます。
- 外部トンネルパケットの DiffServ を固定値に設定することも、またはトンネル内のパケットの DiffServ フィールドから値をコピーすることもできます。

上の 2 つのオプションを設定する方法を次に説明します。

IKE トラフィックに DiffServ フィールドを指定する

初期値では、トンネル設定の間に NetDefendOS が送信したすべての IKE パケットで、DiffServ 値を 0 に設定します。これは、IPsecTunnel オブジェクトの IKEDSField プロパティを設定することで、トンネルの固定値に変更することができます。例題は以下の通りです。

```
DFL-xxxx:/> set Interface IPsecTunnel my_tunnel IKEDSField=1
```

DiffServ フィールドを外部トンネルに設定する

初期値では、NetDefendOS が送信したすべての IPsec の外部トンネルパケットで、トンネル内にパケットから DiffServ フィールドの値をコピーします。IPsecTunnel オブジェクトに IPsecDSField プロパティを設定することで、DiffServ フィールドを固定値で設定できます。例題は以下の通りです。

```
DFL-xxxx:/> set Interface IPsecTunnel my_tunnel IPsecDSField=1
```

10.3.20 NAT トラバーサル

IKE と IPsec プロトコルは NAT の機能に問題があります。両方のプロトコルは NAT を使用したネットワークを考えて設計されていなかったため、「NAT トラバーサル」と呼ばれる技術が展開しました。NAT トラバーサルは IKE と IPsec プロトコルを NAT ネットワーク上で動作させるために追加された技術です。NetDefendOS は IKE と共に NAT トラバーサルの RFC 3947 標準をサポートしています。

NAT トラバーサルは 2 つの部分から構成されます。

- IKE は IPsec 終端にお互いに NAT トラバーサルをサポートしていること、およびサポートしているドラフトのバージョンを通知します。NetDefendOS は IKE と共に NAT トラバーサルの RFC 3947 標準をサポートしています。
- ESP カプセル化を変更します。NAT トラバーサルが使われていれば、ESP は NAT においてより柔軟に使用できる UDP にカプセル化します。

以下は、IKE と IPsec プロトコルに行われる変更について詳しく記述したものです。

NAT トラバーサルは両端がサポートしていなければ使うことはできません。そのため NAT トラバーサルでは、VPN がもう一方の NAT トラバーサルをサポートした終端に、NAT トラバーサルをサポートしていること、およびサポートしているドラフトのバージョンを通知するための「Vendor ID」を送信します。

NAT 検出の実行

NAT 検出を行うためには、両 IPsec ピアは自分自身の IP アドレスのハッシュに加え、IKE ネゴシエーションに使う送信元 UDP ポートを送信します。この情報を使って、両終端は相手の本来の IP アドレスと送信元ポートを知ることができます。（認識したものと情報の）送信元アドレスとポートが異なっていなければ、このトラフィックは NAT を使用しておらず、NAT トラバーサルは必要ありません。（認識したものと情報の）送信元アドレスとポートが異なっていれば、このトラフィックは NAT を使用しており、NAT トラバーサルが必要です。

ポートを変更する

IPsec の組が NAT トラバーサルが必要だと決定すると、IKE ネゴシエーションは UDP ポート 500 から 4500 に移動します。IKE による NAT の問題を解決するためには、確実に NAT デバイスが UDP パケットを、他のポート 500 への UDP パケットと区別して扱うために、このような処理が必要です。IKE パケットに対しては特殊な扱いをする必要があり、実際に IKE ネゴシエーションが中断する可能性があるため、IKE によって使われる UDP ポートを変更しておかなくてはなりません。

UDP のカプセル化

NAT トラバーサルによって、ESP プロトコルに関わる他の問題も解決することができます。ESP プロトコルは IP プロトコルで TCP や UDP のようにポート情報を持っていません。そのため、同時に同じゲートウェイにおける複数の NAT クライアントを扱うことができないのです。この問題を解決するために、ESP パケットは UDP にカプセル化されます。ESP-UDP トラフィックは、NAT トラバーサルで IKE のために使われるポート 4500 に送られます。ポートが変更されると、その後のすべての IKE 通信はポート 4500 上で行われます。NAT Keep-alive パケットは NAT のマッピングを維持するために定期的に送信され続けます。

NAT トラバーサル設定

多くの NAT トラバーサル機能は、完全に自動で、ファイアウォールの開始時には特別な設定は必要とされません。しかし、ファイアウォールへの応答のために、以下の 2 点に注意してください。

- ファイアウォールに応答する場合、リモートエンドポイントフィールドは、受信した IKE パケットの送信元に関するフィルタとして使用されます。これは、イニシエータの NAT IP アドレスを許可するために設定される必要があります。
- 各事前共有鍵が 1 つのリモートファイアウォールに接続する複数トンネルで使用され、同じアドレスを経由して外側に NAT 変換される場合、IPsec Tunnel オブジェクトの Local ID プロパティがあらゆるトンネルに対して固有であることを確認することが重要です。以下の値のいずれかを使用します。

項目	説明
Auto	Local ID は外向きインタフェースの IP アドレスとして見なされます。2 つのファイアウォールが同じ外部 IP アドレスを持っていない限り、これはお勧めの設定です。
IP	IP アドレスを手動で入力します。
DNS	DNS アドレスを手動で入力します。
Email	Email アドレスを手動で入力します。

10.3.21 代替の LDAP サーバから CRL を取得する

ルート証明書には、通常、証明書または CRL が D-Link ファイアウォールにダウンロードされる必要がある場合、接続するための CA の IP アドレスまたはホスト名が含まれます。Lightweight Directory Access Protocol（LDAP）は、これらのダウンロードのために使用されます。

しかし、いくつかのシナリオでは、この情報は紛失しているか、または管理者が別の LDAP サーバを使用することを望んでいます。LDAP 設定セクションは、代わりの LDAP サーバを手動で指定するために使用されます。

例題 10.16

LDAP サーバを設定する

この例題では、LDAP サーバを手動で設定する方法を示しています。

CLI

```
DFL-xxxx:/> add LDAPServer Host=192.168.101.146 Username=myusername Password=mypassword Port=389
```

Web Interface

1. **Objects > VPN Objects > LDAP > Add > LDAP Server** の順に、メニューをクリックします。
2. 以下の情報を入力します。
   - IP Address: 192.168.101.146
   - Username: myusername
   - Password: mypassword
   - Confirm Password: mypassword
   - Port: 389
3. 「OK」ボタンをクリックします。

10.3.22 IPSec の高度な設定

以下の NetDefendOS の高度な設定は、すべての IPsec トンネルに適用するグローバル設定です。Web インタフェースで **Network > Interfaces and VPN > IPsec > Advanced Settings** の順にメニューをクリックします。

General Settings（IKEv1 and IKEv2）

項目	説明
IPsec DS Field	トンネルごとに値を指定します。指定した値は、IPsec トンネルの一部として NetDefendOS が送信した ESP パケットの外側 IP ヘッダ内の Differentiated Service フィールドにコピーされます。言い換えると、トンネルが送信する内側 ESP パケットの DS フィールドの値に関係なく、この値は交換されます。 値を指定しないと（初期値）、トンネルの内側パケットの DSF 値がトンネルの外向き ESP パケットの外側ヘッダにコピーされます。 ルータなどの他のデバイスを通過する際、DS フィールドの値は、DiffServ アーキテクチャの一部であり、トラフィックに QoS 要求を指定します。詳しくは「11.1 トラフィックシェーピング」を参照してください。
IPsec Max Rules	IPsec トンネルに関連付けできる IP ルールの総数を指定します。ルールの数を減少させることでメモリ要求を抑制できますが、この変更を推奨しません。 初期値 : ハードウェアモデルによって異なります。
IPsec Max Tunnels	許可された IPsec トンネルの総数を指定します。設定は、NetDefendOS が IPsec 用にメモリを割り当てるために使用されます。IPsec のために、より少ないメモリを割り当てる場合、この設定値を減らします。設定値を増やしても、ハードウェアモデルの制限を無効にすることはできません。この設定の設定値の 90% に到達すると、警告ログメッセージが自動的に生成されます。 初期値 : ハードウェアモデルによって異なります。
IKE Send Initial Contact	IKE が「Initial Contact」通知メッセージを送信するべきか否かを決定します。接続がリモートゲートウェイにオープンしており、IPsec SA がない場合、そのゲートウェイを使用して各リモートエンドポイントに本メッセージを送信します。 初期値 : Enabled（有効）
IKE Send CRLs	CRLs（Certificate Revocation Lists）を IKE 交換の部分として送信するべきか否かを決定します。リモートピアが CRL ペイロードを理解していない場合を除き、Enabled に通常設定されるべきです。この設定が適用されるためには再起動が必要です。 初期値 : Enabled（有効）
IPsec Before Rules	NetDefendOS に送信された IKE&IPsec（ESP/AH）トラフィックは、ルールセットを参照せずに IPsec エンジンに直接送られます。 初期値 : Enabled（有効）

項目	説明
IKE CRL Validity Time	CRL には「next update」という項目があり、それによって新しい CRL が CA からダウンロード可能な日時が指定されます。CRL 更新の間隔は CA がどのように設定されているかによります。多くの CA ソフトウェアは、CA 管理者がいつでも新しい CRLs を発行することを許可しているため、「next update」フィールドで、新しい CRL が 12 時間後に利用可能であると指定されていても、ダウンロード用の新しい CRL が既にある可能性があります。 本設定は CRL が有効であると見なされる時間を制限します。IKECRLVailityTime の期限が切れるか、または「next update」時間になると、新しい CRL がダウンロードされます。どちらかが最初に起こります。 初期値 : 86400（秒）
IKE Max CA Path	ユーザ証明書のシグネチャが検証される際、NetDefendOS は、署名されている CA 証明書を見つけるためにユーザ証明書の「issuer name」フィールドを検索します。CA 証明書は別の CA によって順番に署名される可能性があります。信用したというマークされたものが見つけられるまで、また信用される証明書がないとされるまで各証明書は確認されます。 このパスに設定値より多くの証明書があれば、ユーザ証明書は無効であると見なされます。 初期値 : 15
IPsec Cert Cache Max Certs	内部の証明書キャッシュに保持される証明書 /CRL の最大数。証明書キャッシュがフルである場合、LRU（Least Recently Used）アルゴリズムに従って、エントリは削除されます。 初期値 : 1024

General Settings (IKEv2 専用)

項目	説明
XCBC Fallback	有効であると、NetDefendOS は、XCBC（RFC 4344）が EAP 認証中にエラーになると XCBC（RFC 3664）の使用に戻ります。 AES-XCBC-MAC は IKEv2 ネゴシエーションに使用される message authentication code（MAC）を生成する方式です。RFC 3664 は、128 ビットのキー長のみ AES-XCBC-MAC 用にサポートされると定義しています。これは、EAP 認証が少なくとも 512 ビットのセッションキーを使用するので、EAP において問題となります。これを解決するために、512 ビットの EAP キーの開始 128 ビットだけを使用するのが RFC 3664 の事実上の標準となりました。RFC 4434 は、RFC 3664 に代わって、128 ビットより長いキーに適用する別の方式を指定します。 RFC 4434 は RFC 3664 と理論的に下位互換であるべきですが、128 ビットにキーを適用させるこれらの異なる方式とは実際には互換性はありません。この高度な設定では、RFC 4434 を使用する認証がエラーになった場合に、古い RFC 3664 方式の使用に戻る方法を提供します。 設定を無効にすると、より新しい RFC 4434 方式だけが使用され、その方式がエラーになると認証エラーになります。この設定を有効にする場合の欠点は、RFC 4434 と RFC 3664 方式の両方を試行するのに要する計算時間が大きい点です。 初期値 : Enabled（有効）
IPsec SA Keep Time	クライアントの削除が開始された後に SA が待機する時間（秒）。 初期値 : 3
Require Cookie	これはクッキーへの要求を実行するもので、テスト目的だけのために使用されます。 初期値 : Disabled（無効）
Use Client's Attribute	有効であると、Config モードを使用して IP アドレスを割り当てる場合にクライアントが要求したサブネット属性を使用します。 初期値 : Disabled（無効）
IPsec IP Address Validation	有効である場合、解読された送信元 IP アドレスがリモートネットワークにマッチしないと、IPsec トンネルは削除されます。 初期値 : Disabled（無効）
Disable Callstation ID	無効にすると、NetDefendOS は EAP 認証の一部として送信する RADIUS アカウンティングメッセージとともに追加属性 Calling-Station-ID と Called-Station-ID を送信します。 Called-Station-ID は、NetDefendOS によって常に、IKEv2 ネゴシエーションの間に送信された応答者の ID の値に設定されます。利用可能な ID がないと、初期値「1234567891234321」が使用されます。 初期値 : Disabled

項目	説明
Allow Port Change	NAT デバイスがクライアントと D-Link ファイアウォール間で検出されると、IKEv2 ネゴシエーションはポート 500 から 4500 に切り替わり、すべての ESP トラフィックが UDP パケットでカプセル化されます。関連する NAT デバイスがある場合だけ、通常、このポートを変更しますが、NAT がなくても 500 の代わりにポート 4500 を好むクライアントがあるかもしれません。その場合、NetDefendOS は IKEv2 接続を受け付けることができますが、クライアントが IKE データを送信する場合、raw ESP パケットとして送信され、この設定が有効でなければ、UDP でカプセル化されると予想するため、NetDefendOS はパケットを破棄します。 有効であると、NAT がなくてもこの設定は、IKE ポートの変更を許可します。 初期値 : Disabled（無効）
Log Key Material	新しく確立した IPsec SA のそれぞれに対してセッションキーのログへの出力を有効にします。暗号キーと認証キーの両方が 16 進数でログに出力されます。これらのキーにアクセスを行うと、キャプチャーされたパケットをオフラインで解読できることに注意してください。 初期値 : Disabled（無効）
Detect NAT Port Change	インバウンド ESP を使用し、NAT マッピングの変更有無を検出します。 初期値：Enabled（有効）

警告 テストの目的だけでキーのログへの出力を有効にする

暗号化キーが非常に機密性の高い情報であるので、この機能はデバッグ目的だけに有効とするべきです。

Hardware Acceleration 設定

項目	説明
IPsec Hardware Acceleration	IPsec ハードウェアアクセラレーションを設定します。
Disable Public-Key Hardware Acceleration	パブリックキー処理に関して、ハードウェアアクセラレーションを無効にします。
Enable AES-NI acceleration	プロセッサで AES-NI アクセラレーションを有効にします。

プロセッサで AES-NI アクセラレーションを有効にします。

10.3.23 IPSec トラブルシューティング

ここでは、IPsec に見られる一般的な問題を障害調査する方法について記載します。

10.3.23.1 一般的なトラブルシューティング

すべての VPN のタイプにおいて、以下の基本的なトラブルシューティングが行われます。

- すべての IP アドレスが正しく指定されたことをチェックします。
- すべての事前共有鍵とユーザ名 / パスワードが正しく入力されることをチェックします。
- ICMP Ping を使用して、トンネルが働いていること確認します。クライアントがローミングしている場合、D-Link ファイアウォールのローカルネットワークインタフェースの内部 IP アドレスをクライアントから Ping することによって行われます。 (LAN-to-LAN 設定では、ping はどちらかの方向で行われます。)NetDefendOS が Ping に応答可能である場合、以下のルールが IP ルールセットに存在する必要があります。

アクション	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
Allow	vpn_tunnel	all-nets	core	all-nets	ICMP

- 他の IPsec トンネル定義が、正しい定義の妨げとならないようにします。トンネルリストは上から下にスキャンされるため、リモートネットワーク設定に all-nets を指定したトンネルや、リモートエンドポイント設定に none を指定したトンネルを、リストの中で優先順位の高い位置に配置すると、トンネルが適切にセットアップされない可能性があります。この問題により、不正な事前共有鍵メッセージが生成されることがあります。
- クライアントがアクセスするリモートネットワークとローミングクライアントが所属する内部ネットワークの間の IP アドレスが重複しないようにします。

  ローミングクライアントが空港で Wi-Fi などの一時的なネットワークに接続する場合、クライアントは Wi-Fi ネットワークの DHCP サーバから IP アドレスを取得します。また、その IP がトンネル経由でアクセス可能なファイアウォール配下のネットワークに所属する場合、Windows™ は、IP アドレスがクライアントのローカルネットワークで検出されると想定します。そのため、Windows™ は、トンネル経由でリモートネットワークにパケットを送信せず、代わりにそれらをローカルネットワークに送信します。

  ローカル / リモート IP アドレスの重複に関する本問題のソリューションは、IP アドレスをトンネルに送信するクライアントの Windows ルーティングテーブルに新しいルートを作成することです。

- ローミングクライアントのユーザ認証が、ユーザ名 / パスワードをユーザに要求しない場合、以下の詳細な設定を有効にします。
  - IPsec ローミングクライアントに対する IPsecBeforeRules
  - L2TP ローミングクライアントに対する L2TPBeforeRules
  - PPTP ローミングクライアントに対する PPTPBeforeRules

  これらの設定は初期値では有効とするべきであり、NetDefendOS とクライアント間のユーザ認証トラフィックが IP ルールセットを迂回することを確実にします。適切な設定が有効にされないと、明示的なルールが、ローミングクライアントと NetDefendOS 間の認証トラフィックの通過を許可するように IP ルールセットに追加される必要があります。このルールには、core（これは NetDefendOS 自身を意味します。）の宛先インタフェースがあります。

- リモートエンドポイントが URL として指定される場合、プレフィックス dns: が URL のはじめに付加されていることを確認します。例えば、トンネルリモートエンドポイントが vpn.example.com として指定される場合、CLI では、dns:vpn.example.com と指定します。

10.3.23.2 特定の症状

ここでは、2 つの特定の症状について説明します。

1. トンネルは片側から開始できるだけです。
2. トンネルを設定することはできません。また、XAuth を使用していなくても、「ike -snoop」コマンドは config モードの XAuth 問題を報告します。

それぞれについて説明します。

1. トンネルは片側から開始できるだけです。

これは、一般的な問題であり、ローカルまたはリモートネットワークにおけるサイズの不一致、および / または、プロポーザルリストにおけるライフタイム設定の不一致のためです。

これを障害調査するためには、不一致を識別するように両側のローカルネットワーク、リモートネットワーク、IKE プロポーザルリストおよび IPsec プロポーザルリストの設定を検証することが必要です。

例えば、トンネルのいずれか一方の IPsec トンネル設定を考えてみます。

- **サイド A**
  Local Network = 192.168.10.0/24
  Remote Network = 10.10.10.0/24

- **サイド B**
  Local Network = 10.10.10.0/24
  Remote Network = 192.168.10.0/16

このシナリオでは、サイド B に定義されたリモートネットワークは、サイド A のローカルネットワークに定義されたものより大きいことがわかります。これは、サイド A は、サイド B よりネットワークが小さいため、サイド B に向かってトンネルを開始することに成功することを意味しています。サイド B がトンネルを開始しようとしても、規模がサイド A より大きいためサイド A は拒否します。一方の方向が動作する理由は、より小さなネットワークがより安全と見なされ受け入れられるからです。また、これはプロポーザルリストのライフタイムにも適用されます。

2. トンネルを設定することはできません。また、偽の XAuth メッセージを取得しています。

これは基本的に「No proposal chosen」（提案が選択されていない）ことが原因です。これが表示されるケースは、ローカルネットワークまたはリモートネットワークのどちらかのネットワークサイズにエラーがある場合です。NetDefendOS が、それが一種のネットワークの規模問題であると判断したので、config モード要求を送信することによって正しいネットワークを取得する最終的な試みを行います。

両側でトンネルを開始する場合には「ike -snoop」を使用して、両側がフェーズ 2 で送信するネットワークを比較する必要があります。また、その情報を使用して、ネットワーク問題を見つける必要があります。それがネットワークの規模の不一致であるか、または全く一致しないという可能性があります。

10.3.23.3 特定のエラーメッセージ

このセクションでは VPN を使用した場合に表示される特定のエラーメッセージと示す意味を記載します。
説明するメッセージは、以下の通りです。

1. Could not find acceptable proposal / no proposal chosen.
2. Incorrect pre-shared key.
3. Ike_invalid_payload, Ike_invalid_cookie.
4. Payload_Malformed.
5. No public key found.
6. ruleset_drop_packet.

以下に各メッセージの示す意味を詳しく説明します。

1. Could not find acceptable proposal / no proposal chosen

これは最も一般的な IPsec に関連するエラーメッセージです。トンネル設定を開始した側により、トンネルの両側が同意できる一致した提案を見つけることができなかったために、設定の IKE または IPsec のフェーズでネゴシエーションが失敗したことを意味します。

発生したネゴシエーションの場所によって、このメッセージの原因が複数であるので、このエラーメッセージが障害調査に関係します。

- **フェーズ 1 でネゴシエーションが失敗した場合（IKE）**
  IKE プロポーザルリストが一致しません。IKE プロポーザルリストがリモート側のものと一致することをダブルチェックします。良いアイデアは、「ike -snoop -verbose」CLI コマンドを使用して、リモートピアがトンネルの開始を行うことです。次に、リモート側がどんな提案を送信するかを見て、ローカルな IKE プロポーザルリストと結果を比較することができます。少なくとも 1 個の提案は、フェーズ 1 を通過するために一致する必要があります。また、ライフタイムも重要であることを覚えておいてください。これは、後ほど説明する症状 1 で言及されています。

- **フェーズ 2 でネゴシエーションが失敗した場合（IPsec）**
  IPsec プロポーザルリストが一致しません。ローカル IPsec 提案がリモートピアのものと一致することをダブルチェックします。リモート側がトンネルを開始する時、上の「ike -snoop」の使用についての説明と同じ方式を使用できます。また、ローカルのプロポーザルリストに比較もできます。IPsec フェーズで「特別な」こととしては、ネットワークはこのフェーズでネゴシエーションされるということであり、たとえ IPsec プロポーザルリストが一致するように見えても、問題がネットワークの不一致である可能性があります。ある一方のローカルネットワークは、反対側ではリモートネットワークである必要があり、逆もまた同様です。複数のネットワークが複数の IPsec SA、ネットワークあたり 1 つの SA（またはオプションを使用する場合にはホスト）を生成することを忘れないでください。また、ネットワークサイズは両側で正確に同じでなければならないので、定義するネットワークの規模も重要です。後で再び症状のセクションにて言及します。

  また、IPsec トンネルの「IKE」タブにはプロポーザルが選択されない問題に関連するいくつかの設定があります。例えば、PFS（IPsec phase 用）、または DH Group（IKE phase 用）です。

2. Incorrect pre-shared key

いずれかの側の事前共有鍵に関する問題がトンネルネゴシエーションに失敗を引き起こしています。これは、原因が 1 つで、不正な事前共有鍵であるためです。これは、トラブルシューティングにおけるすべてのエラーメッセージの中でおそらく最も簡単なケースです。事前共有鍵が同じタイプ（パスフレーズまたは 16 進数キー）であるか、またトンネルの両側に正しく追加されているかをダブルチェックしてください。

NetDefendOS が事前共有鍵が不正であることを検出した別の原因は、不正なトンネルがトンネルネゴシエーション中に起動したためです。IPsec トンネルは NetDefendOS トンネルリストの先頭から末尾まで処理されますが、最初に、リモートゲートウェイに照合されます。例題は、リモートゲートウェイとして「all-nets」を使用するローミングトンネルがある場合です。NetDefendOS トンネルリストにおいて、意図するトンネルの上にこのトンネルがあると、ローミングトンネルはそのトンネルの前に始動します。

例えば、以下の IPsec トンネル定義を考えてみます。

名称	ローカルネットワーク	リモートネットワーク	ゲートウェイ
VPN-1	lannet	office1net	office1gw
VPN-2	lannet	office2net	office2gw
L2TP	ip_wan	all-nets	all-nets
VPN-3	lannet	office3net	office3gw

上記の表のトンネル L2TP は、リストの中でトンネル VPN-3 より上に配置されているため、リモートゲートウェイの「all-nets」によって、VPN-3 のトンネル定義の前に「一致」することになります（「all-nets」はどのネットワークにも一致します）。これらの 2 つのトンネルは異なる事前共有鍵を使用するため、「Incorrect pre-shared key」（不正確な事前共有鍵）エラーメッセージを生成します。

リストの順番を再整理し、L2TP の上に VPN-3 を移動させると、問題は解決します。ゲートウェイ「office3gw」が正しく一致し、VPN-3 は NetDefendOS によって選択されたトンネルになります。

3. Ike_invalid_payload, Ike_invalid_cookie

この場合、NetDefendOS の IPsec エンジンは、IPsec IKE パケットを受信しますが、既存の IKE に照合することはできません。

トラフィックが存在しないトンネルから到着する場合、VPN トンネルが片側に確立されているだけであると、これがエラーメッセージを引き起こしているかもしれません。例題では、いくつかの理由で、トンネルは開始した側からダウンするだけでターミネータには動作中に見えます。次に、トンネルを通じてパケットを送信しようとしますが、一致しているトンネルを見つけることができないため、イニシエータに到着する時にそれらは破棄されます。

単に問題を解決するためには、まだ動作していると信じている側からトンネルを削除します。また、トンネルが片側だけからダウンした理由に関する調査をお勧めします。DPD が片側でだけ使用された可能もあります。別の考えられる原因は、たとえ「DELETE」パケットを受信しても、削除または移動したトンネルがないという可能性もあります。

4. Payload_Malformed

この問題は、上記の問題に非常によく似ています。考えられる理由は、PSK の Type（パスフレーズまたは 16 進数キー）がいずれかの側で不正であるということです。

IPsec トンネルの両側で同じタイプを使用していることを確認してください。片側で 16 進数、もう片側でパスフレーズを使用している場合に、最も受信する可能性のあるエラーメッセージです。

5. No public key found

認証に証明書を使用するトンネルに対処する時、これが最も一般的なエラーメッセージです。

問題の考えられる原因がかなり大規模であるため、このエラーメッセージの障害調査は非常に難しい場合があります。証明書を扱う時にノーマルログと共に「ike -snoop」ログを組み合わせることが必要かもしれないことを記憶しておくことが非常に重要です。これは、「ike -snoop」が証明書に関して最も多くの情報を提供するわけではなく、ノーマルログは問題は何であるかという重要な手がかりを提供することができるためです。

証明書ベースのトンネルに関する障害調査を開始する前に、最初に PSK トンネルとして設定し、確立が成功したことを検証することをお勧めします。次に、(コンフィグレーションのタイプがそれを防御しない限り) 証明書の使用に移行します。

証明書問題で考えられる原因は以下の通りです。

- いずれかの側の証明書が同じ CA サーバによって署名されていません。
- 証明書の有効期間が終了したか、または、まだ効力を開始していません。クロックが、CA サーバまたは D-Link ファイアウォールのどちらかで不正に設定されているか、または異なるタイムゾーンにある場合に後者が起こる可能性があります。

- D-Link ファイアウォールは、証明書が有効であるかどうか確かめるために、CA サーバの Certificate Revocation List（CRL）に到達することができません。CRL パスが証明書のプロパティで有効であることをダブルチェックしてください。（CRL 機能の使用をオフにすることができます。）また、正しく CA サーバ上の CRL にパスを解決できるように NetDefendOS に設定された DNS クライアントがあることを確認してください。

- 複数の類似またはローミングトンネルが存在し、ID リストを使用してそれらを分割する場合に、接続ユーザの証明書のプロパティに一致する IP リストがないという問題が起こる可能性があります。以下の原因が考えられます。
  - ユーザが認可されていません。
  - 証明書のプロパティがクライアントで不正です。
  - IP リストがこのユーザ / 情報で更新される必要があります。

- L2TP を使用して、クライアント証明書が Windows™ クライアントの間違った証明書ストアにインポートされています。また、クライアントが接続する時に、間違った証明書を使用しています。

6. ruleset_drop_packet

IKEv1 ローミングクライアントがトンネルモードを使用する場合にログメッセージにこれが表れた場合、トンネルにおいてクライアントのローカルな内側 IP アドレスがクライアントのローカルな外側 IP アドレスと同じであることが原因となっています。この場合、ログメッセージには「rule=Default_Access_Rule」もあります。問題は、クライアント IP を割り当てるのに config モードを使用するか、またはトンネルとトンネルが送信するデータに別々のルーティングテーブルを使用することで修正されます。この問題は、「10.3.7 IPSec ローミングクライアント」にも記載されています。

10.3.23.4 ike -stat コマンド

「ipsec」コンソールコマンドは、IPsec トンネルが正しく確立したことを示すために使用されます。代表的な出力例は以下の通りです。

```
DFL-xxxx:/> ipsec

--- IPsec SAs:
Displaying one line per SA-bundle

IPsec Tunnel Local Net       Remote Net     Remote GW
------------ --------------  -------------- -------------
L2TP_IPsec   214.237.225.43  84.13.193.179  84.13.193.179
IPsec_Tun1   192.168.0.0/24  172.16.1.0/24  82.242.91.203
```

トンネル設定の最初の IKE ネゴシエーション段階を確認するために、ike コマンド使用します。

```
DFL-xxxx:/> ike
```

しかし、トンネル設定の詳細な情報を取得するには以下を使用します。

```
DFL-xxxx:/> ipsec -show -verbose -usage
```

警告 「-num=all」オプションの使用に注意してください。

大量のトンネルがあると、これが対応して多量の出力を生成するため、「-num=all」オプションの使用を避けてください。

例えば、大量のトンネルの場合には以下の使用を避けます。

```
DFL-xxxx:/> ipsec -show -num=all
```

大量のトンネルの場合には以下の例題も避けてください。

```
DFL-xxxx:/> ike -tunnels -num=all
```

このような状況では、少ない数を使用したオプションを使用します。例えば、「-num=10」をお勧めします。

10.3.23.5 ike -snoop コマンド

VPN トンネルネゴシエーション

IPsec トンネルを設定する場合、初期のネゴシエーションが、VPN トンネルのどちらかの終端にあるデバイスが使用するプロトコルおよび暗号化方式の合意に失敗するとエラーとなるため問題が生じます。「-verbose」オプションを持つ「ike -snoop」コンソールコマンドは、ネゴシエーションの詳細を表示することでそのような問題の原因を確認するのに使用されるツールです。

ike -snoop の使用

ネットワーク接続または直接ローカルコンソール接続された CLI コンソールを通して「ike-snoop」コマンドを入力することができます。

以下のコマンドでモニタを開始します。

```
DFL-xxxx:/> ike -snoop
```

これは、すべての VPN トンネルの IKE ネゴシエーションのために出力結果をコンソールに送信することを意味します。出力が大量である場合に、1 つの IP アドレス、例えば、IP アドレス 10.1.1.10 への出力に制限するコマンドは以下の通りです。

```
DFL-xxxx:/> ike -snoop 10.1.1.10
```

使用される IPv4 アドレスは、VPN トンネルのリモートエンドポイントの IP アドレスです。（リモートエンドポイントの IP またはクライアント IP のどちらかの）モニタリングをオフにするコマンドは以下の通りです。

```
DFL-xxxx:/> ike -snoop -off
```

初期値では、「ike -snoop」は、常にほとんどの verbose 出力を作成します。「-brief」オプションを使用することでこの出力量を減少させることができます。しかし、これは問題を特定するほどの詳細を提供しないかもしれません。「ike」コマンドの全オプションについては、個別の「CLI Reference Guide」を参照してください。

他にも -match オプションといった有用なコマンドオプションが準備されています。

DFL-xxxx:/> ike -snoop -match

```
DFL-xxxx:/> ike -snoop -match
```

このオプションでは、ネゴシエーション手順をリスト化するだけでなく、実行された一致プロセスの詳細を表示します。トンネルピア間のずれを検出する際に役に立ちますが、標準の -snoop オプションより多くの出力を生成します

「ike -snoop」からの出力結果を初めて見る管理者が解釈するのは困難である場合があります。以下に提示するのは、説明するために代表的な「ike -snoop」の出力結果とその注釈です。想定されるトンネルネゴシエーションは、事前共有鍵に基づいています。証明書に基づくネゴシエーションについてここでは記述しませんが、原則は同じです。

クライアントとサーバ

トンネルネゴシエーションにかかわる 2 つのパーティを本セクションではクライアントとサーバとします。このような状況で、「client」という言葉はネゴシエーションの initiator であるデバイスを指すのに使用され、server は responder であるデバイスを指します。

手順 1. クライアントは、サポートするアルゴリズムリストを送信することで交換を開始します。

verbose オプションの出力結果は、クライアントが最初にサーバに送信するアルゴリズムのプロポーザルを表示します。このリストはサポートするプロトコルと暗号化方式を詳しく述べています。アルゴリズムリストの目的は、クライアントが、サーバによってサポートされるものからマッチするプロトコル / 方式のセットを見つけようとすることです。サーバは、リストを調べて、クライアントが送信したプロトコル / 方式からサポートできる組み合わせを見つけようとします。この照合過程は IKE 交換の主要な目的の 1 つです。

```
Received IKE packet from 192.168.0.10:500 Exchange type :
         Identity Protection (main mode) ISAKMP Version : 1.0
Flags         :
Cookies       : 0x6098238b67d97ea6 -> 0x00000000
Message ID    : 0x00000000
Packet length : 324 bytes
# payloads    : 8
Payloads:
  SA (Security Association)
    Payload data length : 152 bytes
    DOI : 1 (IPsec DOI)
      Proposal 1/1
        Protocol 1/1
          Protocol ID             : ISAKMP
          SPI Size                : 0
          Transform 1/4
            Transform ID          : IKE
            Encryption algorithm  : Rijndael-cbc (aes)
            Key length            : 128
            Hash algorithm        : MD5
            Authentication method : Pre-Shared Key
            Group description     : MODP 1024
            Life type             : Seconds
            Life duration         : 43200
            Life type             : Kilobytes
            Life duration         : 50000
          Transform 2/4
            Transform ID          : IKE
            Encryption algorithm  : Rijndael-cbc (aes)
            Key length            : 128
            Hash algorithm        : SHA
            Authentication method : Pre-Shared Key
            Group description     : MODP 1024
            Life type             : Seconds
            Life duration         : 43200
            Life type             : Kilobytes
            Life duration         : 50000
          Transform 3/4
            Transform ID          : IKE
            Encryption algorithm  : 3DES-cbc
            Hash algorithm        : MD5
            Authentication method : Pre-Shared Key
            Group description     : MODP 1024
            Life type             : Seconds
            Life duration         : 43200
            Life type             : Kilobytes
            Life duration         : 50000
          Transform 4/4
            Transform ID          : IKE
            Encryption algorithm  : 3DES-cbc
            Hash algorithm        : SHA
            Authentication method : Pre-Shared Key
            Group description     : MODP 1024
            Life type             : Seconds
            Life duration         : 43200
            Life type             : Kilobytes
            Life duration         : 50000
```

```
VID (Vendor ID)
  Payload data length : 16 bytes
  Vendor ID   : 8f 9c c9 4e 01 24 8e cd f1 47 59 4c 28 4b 21 3b
  Description : SSH Communications Security QuickSec 2.1.0
VID (Vendor ID)
  Payload data length : 16 bytes
  Vendor ID   : 27 ba b5 dc 01 ea 07 60 ea 4e 31 90 ac 27 c0 d0
  Description : draft-stenberg-ipsec-nat-traversal-01
VID (Vendor ID)
  Payload data length : 16 bytes
  Vendor ID   : 61 05 c4 22 e7 68 47 e4 3f 96 84 80 12 92 ae cd
  Description : draft-stenberg-ipsec-nat-traversal-02
VID (Vendor ID)
  Payload data length : 16 bytes
  Vendor ID   : 44 85 15 2d 18 b6 bb cd 0b e8 a8 46 95 79 dd cc
  Description : draft-ietf-ipsec-nat-t-ike-00
VID (Vendor ID)
  Payload data length : 16 bytes
  Vendor ID   : cd 60 46 43 35 df 21 f8 7c fd b2 fc 68 b6 a4 48
  Description : draft-ietf-ipsec-nat-t-ike-02
VID (Vendor ID)
  Payload data length : 16 bytes
  Vendor ID   : 90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
  Description : draft-ietf-ipsec-nat-t-ike-02
VID (Vendor ID)
  Payload data length : 16 bytes
  Vendor ID   : 7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
  Description : draft-ietf-ipsec-nat-t-ike-03
```

値に関する説明

項目	説明
Exchange type	Main mode または aggressive mode（IKEv1.0 のみ）
Cookies	ネゴシエーションを特定するランダムな数
Encryption algorithm	Cipher
Key length	Cipher key length
Hash algorithm	Hash
Authentication method	Pre-shared key または certificate
Group description	Diffie Hellman（DH）group
Life type	秒または k バイト
Life duration	秒数または k バイト
VID	IPsec ソフトウェアベンダとサポートされる標準。例えば NAT-T

手順 2. サーバはクライアントに応答します。

サーバからの代表的な応答は以下に示されています。これには上記のクライアントリストから選択したもののいずれかと同じプロポーザルが含まれる必要があります。サーバが一致を見つけられないと「No proposal chosen」（選択されたプロポーザルはない）というメッセージが表示され、トンネル設定はエラーになり、「ike -snoop」コマンドの出力は、この時点でストップします。

```
Sending IKE packet to 192.168.0.10:500 Exchange type :
        Identity Protection (main mode) ISAKMP Version : 1.0
Flags         :
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0x00000000
Packet length : 224 bytes
# payloads    : 8
Payloads:
  SA (Security Association)
    Payload data length : 52 bytes
    DOI : 1 (IPsec DOI)
      Proposal 1/1
        Protocol 1/1
          Protocol ID : ISAKMP
          SPI Size    : 0
          Transform 1/1

            Transform ID : IKE
            Encryption algorithm : Rijndael-cbc (aes)
            Key length : 128
            Hash algorithm : MD5
            Authentication method : Pre-Shared Key
            Group description : MODP 1024
            Life type : Seconds
            Life duration : 43200
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID : 8f 9c c9 4e 01 24 8e cd f1 47 59 4c 28 4b 21 3b
    Description : SSH Communications Security QuickSec 2.1.0
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID : 27 ba b5 dc 01 ea 07 60 ea 4e 31 90 ac 27 c0 d0
    Description : draft-stenberg-ipsec-nat-traversal-01
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID : 61 05 c4 22 e7 68 47 e4 3f 96 84 80 12 92 ae cd
    Description : draft-stenberg-ipsec-nat-traversal-02
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID : 44 85 15 2d 18 b6 bb cd 0b e8 a8 46 95 79 dd cc
    Description : draft-ietf-ipsec-nat-t-ike-00
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID : cd 60 46 43 35 df 21 f8 7c fd b2 fc 68 b6 a4 48
    Description : draft-ietf-ipsec-nat-t-ike-02
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID : 90 cb 80 91 3e bb 69 6e 08 63 81 b5 ec 42 7b 1f
    Description : draft-ietf-ipsec-nat-t-ike-02
  VID (Vendor ID)
    Payload data length : 16 bytes
    Vendor ID : 7d 94 19 a6 53 10 ca 6f 2c 17 9d 92 15 52 9d 56
    Description : draft-ietf-ipsec-nat-t-ike-03
```

手順 3. クライアントは鍵交換を開始する

サーバはこの時点でプロポーザルを受け入れており、クライアントは鍵交換を始めます。さらに、NAT 検出ペイロードが、NAT が使用されているかどうか検出するために送信されます。

```
Received IKE packet from 192.168.0.10:500 Exchange type :
         Identity Protection (main mode) ISAKMP Version : 1.0
Flags         :
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0x00000000
Packet length : 220 bytes
# payloads    : 4
Payloads:
  KE (Key Exchange)
    Payload data length : 128 bytes
  NONCE (Nonce)
    Payload data length : 16 bytes
  NAT-D (NAT Detection)
    Payload data length : 16 bytes
  NAT-D (NAT Detection)
    Payload data length : 16 bytes
```

手順 4. サーバは鍵交換データを送信する

サーバは鍵交換データをクライアントに返送します。

```
Sending IKE packet to 192.168.0.10:500 Exchange type :
        Identity Protection (main mode) ISAKMP Version : 1.0
Flags         :
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0x00000000
Packet length : 220 bytes
# payloads    : 4
Payloads:
  KE (Key Exchange)
Payload data length : 128 bytes
  NONCE (Nonce)
Payload data length : 16 bytes
  NAT-D (NAT Detection)
Payload data length : 16 bytes
  NAT-D (NAT Detection)
Payload data length : 16 bytes
```

手順 5. クライアントは識別子を送信する

証明書が使用されている場合、イニシエータは通常 IP アドレスまたは Subject Alternative Name である識別子を送信します。

```
Received IKE packet from 192.168.0.10:500 Exchange type :
         Identity Protection (main mode) ISAKMP Version : 1.0
Flags         : E (encryption)
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0x00000000
Packet length : 72 bytes
# payloads    : 3
  Payloads:
  ID (Identification)
Payload data length : 8 bytes
  ID : ipv4(any:0,[0..3]=192.168.0.10)
HASH (Hash)
  Payload data length : 16 bytes
N (Notification)
  Payload data length : 8 bytes
  Protocol ID : ISAKMP
  Notification : Initial contact
```

上の値に関する説明

項目	説明
Flags	E は暗号化を意味します（使用される唯一のフラグです）。
ID	クライアントの識別子

Notification フィールドは、これが鍵の変更でないことを示すために Initial Contact として示されます。

手順 6. サーバ ID の応答

サーバは自身の ID で応答します。

```
Sending IKE packet to 192.168.0.10:500 Exchange type :
        Identity Protection (main mode) ISAKMP Version : 1.0
Flags         : E (encryption)
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0x00000000
Packet length : 60 bytes
# payloads    : 2
Payloads:
  ID (Identification)
    Payload data length : 8 bytes
    ID : ipv4(any:0,[0..3]=192.168.10.20)
  HASH (Hash)
    Payload data length : 16 bytes
```

手順 7. クライアントはサポートしている IPsec アルゴリズムのリストを送信する

クライアントはサポートしている IPsec アルゴリズムのリストをサーバに送信します。それにはトンネルに許可されている提案ホスト / ネットワークも含まれます。

```
Received IKE packet from 192.168.0.10:500 Exchange type :
         Quick mode ISAKMP Version : 1.0
Flags         : E (encryption)
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0xaa71428f
Packet length : 264 bytes
# payloads    : 5
Payloads:
  HASH (Hash)
    Payload data length : 16 bytes
  SA (Security Association)
    Payload data length : 164 bytes
    DOI : 1 (IPsec DOI)
      Proposal 1/1
        Protocol 1/1
          Protocol ID               : ESP
          SPI Size                  : 4
            SPI Value               : 0x4c83cad2
          Transform 1/4
            Transform ID            : Rijndael (aes)
            Key length              : 128
            Authentication algorithm : HMAC-MD5
            SA life type            : Seconds
            SA life duration        : 21600
            SA life type            : Kilobytes
            SA life duration        : 50000
            Encapsulation mode      : Tunnel
          Transform 2/4
            Transform ID            : Rijndael (aes)
            Key length              : 128
            Authentication algorithm : HMAC-SHA-1
            SA life type            : Seconds
            SA life duration        : 21600
            SA life type            : Kilobytes
            SA life duration        : 50000
            Encapsulation mode      : Tunnel
```

```
          Transform 3/4
            Transform ID             : Blowfish
            Key length               : 128
            Authentication algorithm : HMAC-MD5
            SA life type             : Seconds
            SA life duration         : 21600
            SA life type             : Kilobytes
            SA life duration         : 50000
            Encapsulation mode       : Tunnel
          Transform 4/4
            Transform ID             : Blowfish
            Key length               : 128
            Authentication algorithm : HMAC-SHA-1
            SA life type             : Seconds
            SA life duration         : 21600
            SA life type             : Kilobytes
            SA life duration         : 50000
            Encapsulation mode       : Tunnel
    NONCE (Nonce)
      Payload data length : 16 bytes
    ID (Identification)
      Payload data length : 8 bytes
      ID : ipv4(any:0,[0..3]=10.4.2.6)
    ID (Identification)
      Payload data length : 12 bytes
      ID : ipv4_subnet(any:0,[0..7]=10.4.0.0/16)
```

上の値に関する説明

項目	説明
Transform ID	Cipher
Key length	Cipher key length
Authentication algorithm	HMAC (Hash)
Group description	PFS および PFS グループ
SA life type	秒または k バイト
SA life duration	秒数または k バイト
Encapsulation mode	transport、tunnel または UDP tunnel（NAT-T）
ID	ipv4(any:0,[0..3]=10.4.2.6)

ここで、最初の ID はクライアントの観点ではトンネルのローカルネットワークであり、2 個目の ID はリモートネットワークです。ネットマスクを含んでいると、通常、SA（ネットごと）で、そうでなければ、SA（ホストごと）です。

手順 8. クライアントはサポートしているアルゴリズムのリストを送信する

サーバは、クライアントが送信したリストからマッチしている IPsec プロポーザルを使用して応答します。上の手順 2 のように、サーバが一致を見つけられないと「No proposal chosen」（選択されたプロポーザルはない）というメッセージが表示され、トンネル設定はエラーになり、「ike-snoop」コマンドの出力は、この時点でストップします。

```
Sending IKE packet to 192.168.0.10:500 Exchange type :
        Quick mode ISAKMP Version : 1.0
Flags         : E (encryption)
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0xaa71428f
Packet length : 156 bytes
# payloads    : 5
Payloads:
  HASH (Hash)
  Payload data length : 16 bytes
  SA (Security Association)
    Payload data length : 56 bytes
    DOI : 1 (IPsec DOI)
      Proposal 1/1
        Protocol 1/1
          Protocol ID               : ESP
          SPI Size                  : 4
            SPI Value               : 0xafba2d15
          Transform 1/1
            Transform ID            : Rijndael (aes)
            Key length              : 128
            Authentication algorithm : HMAC-MD5
            SA life type            : Seconds
            SA life duration        : 21600
            SA life type            : Kilobytes
            SA life duration        : 50000
            Encapsulation mode      : Tunnel
  NONCE (Nonce)
Payload data length : 16 bytes
  ID (Identification)
    Payload data length : 8 bytes
    ID : ipv4(any:0,[0..3]=10.4.2.6)
  ID (Identification)
    Payload data length : 12 bytes
    ID : ipv4_subnet(any:0,[0..7]=10.4.0.0/16)
```

手順 9. クライアントトンネル設定を確認する

この最後のメッセージはトンネルが起動して、動作していることを伝えるクライアントからのメッセージです。すべてのクライアント / サーバの交換に成功しています。

```
Received IKE packet from 192.168.0.10:500 Exchange type :
         Quick mode ISAKMP Version : 1.0
Flags         : E (encryption)
Cookies       : 0x6098238b67d97ea6 -> 0x5e347cb76e95a
Message ID    : 0xaa71428f
Packet length : 48 bytes
# payloads    : 1
Payloads:
  HASH (Hash)
    Payload data length : 16 bytes
```

10.4 PPTP/L2TP

クライアントがモデムを使用してダイヤル式公衆交換網にリンクして、アクセスすると、予測不可能な IP アドレスを持つ可能性があり、VPN 経由の保護されたネットワークに特定の問題を起こします。PPTP および L2TP プロトコルの両方が、リモートクライアントから VPN のアクセスを行う 2 つの方法を提供します。本シナリオに関連して最も一般的に使用される機能は、PPTP または L2TP のいずれかとして動作する NetDefendOS の機能で、以下で 2 つのセクションのうちの初めに説明するものです。3 番目のセクションは、さらに NetDefendOS が PPTP または L2TP クライアントとして操作する機能に対応しています。

PPTP/L2TP クイックスタート

L2TP および PPTP について詳しく説明します。代表的なシナリオでの、これらのプロトコルの設定手順に関するクイックスタートチェックリストは以下のセクションで説明します。

- 「10.2.5 事前共有鍵を使用した L2TP ローミングクライアント」
- 「10.2.6 証明書を使用した L2TP/IPsec ローミングクライアント」
- 「10.2.7 PPTP ローミングクライアント」

10.4.1 PPTP サーバ

概要

Point to Point Tunneling Protocol（PPTP）は、マイクロソフトを含む組織である PPTP フォーラムによって設計されています。それは OSI レイヤ 2「データリンク」プロトコル（「付録 D OSI 参照モデル」）で、ダイヤルアップでインターネットアクセスに使用されていた古い Point to Point Protocol（PPP）の拡張です。ダイヤルアップネットワーク経由でリモートサーバに VPN アクセスを提供するために設計された最初のプロトコルの一つであり、まだ広く使用されています。

インプリメンテーション

PPTP は、インターネットを経由し、VPN 環境で異なるプロトコルをトンネルするために使用されます。トンネリングは、Generic Routing Encapsulation（GRE）を使用して IP データに PPP パケットをカプセル化することによって行われます。クライアントは PPP プロトコルを使用した通常の方法で最初に ISP への関係を確立し、次に PPTP サーバとして機能する D-Link ファイアウォールへのインターネットを経由した TCP/IP 接続を確立します。ISP はトンネルが PPTP サーバからクライアントに伸張しているため VPN に気づきません。PPTP 規格は、データが暗号化される方法を定義していません。暗号化は通常マイクロソフトの Microsoft Point-to-Point Encryption（MPPE）規格を使用して実行されます。

配置

PPTP 展開が容易な、クライアントアクセスに便利なソリューションを提供します。PPTP は L2TP のような証明書のインフラを必要としませんが、代わりにクライアントとサーバ間に信頼を確立するためにユーザ名 / パスワードシーケンスに応答します。証明書なしをベースとしたソリューションに提供されるセキュリティレベルは、おそらく PPTP の欠点の 1 つです。PPTP はまた、PPTP サーバによる PPTP クライアントの同時接続数に制限があるため、スケーラビリティの問題もあります。PPTP が IPsec を使用しないので、PPTP 接続は NAT され、NAT トラバーサルは必要とされません。PPTP はマイクロソフトによって Windows 95 以降のオペレーティングシステム内にバンドルされています。

トラブルシューティング PPTP

PPTP を設定する場合の一般的な問題は、ファイアウォールに対する PPTP 通信が発生する前に、ネットワークにおけるルータ、そして / または、スイッチが TCP ポート 1723、そして / または、IP プロトコル 47 をブロックするということです。ログを調べると、以下の形式のログメッセージが現れてこの問題が起こったかどうかを示すことができます。

```
Error PPP lcp_negotiation_stalled ppp_terminated
```

例題 10.17

PPTP サーバを設定する

この例題では、PPTP ネットワークサーバを設定する方法を示しています。

この例題ではアドレス帳に特定のオブジェクトが既に作成されているものとします。
PPTP サーバインタフェースの IP アドレス、（PPTP サーバがリッスンすべき）外部の IP アドレス、およびクライアントに IP アドレスを付与するために PPTP サーバが使用する IP プールを指定する必要があります。

CLI

```
DFL-xxxx:/> add Interface L2TPServer MyPPTPServer ServerIP=wan_ip Interface=any IP=lan_ip IPPool=pptp_pool
            TunnelProtocol=PPTP AllowedRoutes=all-nets
```

Web Interface

1. **Network > Interfaces and VPN > PPTP/L2TP Servers > Add > PPTP/L2TP Server** の順にメニューをクリックします。

2. 以下の通り入力し、「OK」ボタンをクリックします。
   - Name : PPTP サーバの名前を入力します。（例 : MyPPTP Server）
   - Inner IP Address : lan_ip
   - Tunnel Protocol : PPTP
   - Outer Interface Filter : any
   - Server IP : wan_ip

3. PPP Parameters タブで IP Pool 設定に pptp_Pool を選択します。

4. Add Route タブで Allowed Networks に all-nets を選択します。

5. 「OK」ボタンをクリックします。

「Use User Authentication Rules」は初期値で有効です。PPTP トンネルを使用してユーザを認証するためには、認証ルールを設定する必要があります。この例題では記述していません。

10.4.2 L2TP サーバ

Layer2 Tunneling protocol（L2TP）は多くの PPTP 問題を克服する IETF オープンスタンダードです。その設計は Layer2 Forwarding（L2F）プロトコルと PPTP の組み合わせであり、両方の最もよい特徴を利用しています。L2TP 標準は暗号化を実行しないので、通常 L2TP パケットが IPsec によってカプセル化される L2TP/IPsec として知られている IETF 標準と共に実行されます。

注意 MMPE はセキュリティの観点から推奨されません。

Microsoft MPPE は Microsoft Windows™ の暗号化で使用されます。しかしながら、このセキュリティは脆弱であると考えられているため、推奨されません。L2TP でセキュリティを強化するには、IPsec のカプセル化を使用することを推奨します。

クライアントは Local Access Concentrator（LAC）と通信し、LAC は L2TP Network Server（LNS）とインターネットを経由で通信します。D-Link ファイアウォールは LNS として機能します。LAC はインターネットを経由する LNS に IPsec を使用して、事実上、データを PPP セッションのようにトンネリングします。多くの場合、クライアントは自身が LAC として機能します。

L2TP は証明書に基づいており、そのため多くのクライアントの管理がしやすく、PPTP よりも高いセキュリティを提供します。PPTP と異なり、一つのトンネルを経由した複数の仮想ネットワークを設定することが可能です。IPsec に基づいているため、L2TP は NAT トラバーサル（NAT-T）がトンネルの LNS 側で実行されることが必要です。

IPsec トンネルオブジェクトになるように Outer Interface Filter を指定できます。これが行われると、トンネルは問題を起こす可能性があるため、Dynamically add route to remote network オプションを有効にすべきではありません。

注意 すべての DHCP の特別パラメータがクライアントに送信されるというわけではありません。

クライアントに IP を配布するために L2TP/IPsec インタフェースに DHCP が設定される場合、NetDefendOS はすべての DHCP の特別パラメータを返すというわけではありません。これは Window Vista または Windows 7 が動作する Windows ベースの L2TP クライアントが持つ問題の原因となるかもしれません。

例題 10.18

L2TP サーバを設定する

この例題では、L2TP ネットワークサーバ（LNS）を設定する方法を示します。

この例題ではアドレス帳にいくつかのアドレスオブジェクトが既に作成されているものとします。

L2TP サーバインタフェースの IP アドレス、（L2TP サーバがリッスンすべき）外部の IP アドレス、およびクライアントに IP アドレスを付与するために L2TP サーバが使用する IP プールを指定する必要があります。
L2TP サーバが接続を受諾するインタフェースは、仮想 IPsec トンネル上にありますが、この例題には記述されていません。

CLI

```
DFL-xxxx:/> add Interface L2TPServer MyL2TPServer ServerIP=wan_ip Interface=any IP=ip_l2tp IPPool=L2TP_Pool
            TunnelProtocol=L2TP AllowedRoutes=all-nets
```

Web Interface

1. **Network > Interfaces and VPN > PPTP/L2TP Servers > Add > PPTP/L2TP Server** の順にメニューをクリックします。

2. 以下の通り入力し、「OK」ボタンをクリックします。
   - Name : L2TP サーバに適した名前を入力します。（例 : MyL2TPServer）
   - Inner IP Address : ip_l2tp
   - Tunnel Protocol : L2TP
   - Outer Interface Filter : l2tp_IPsec
   - Server IP : wan_ip

3. PPP Parameters タブで IP Pool に L2tp_pool を選択します。

4. Add Route タブで Allowed Networks に all-nets を選択します。

「Use User Authentication Rules」は初期値で有効です。PPTP トンネルを使用してユーザを認証するためには、認証ルールを設定する必要があります。この例題では記述していません。

例題 10.19

IPsec L2TP トンネルを設定する

この例題は、フルに動作する IPsec 暗号化による L2TP トンネルを設定する方法を示し、基本的な VPN 構成の多くの部分を記載しています。

開始する前に、いくつかのアドレスオブジェクト（例 : L2TP のクライアントに割り当てられる予定のネットワーク）を設定する必要があります。プロポーザルリストと PSK も同様に必要とされます。ここでは、前の例題で作成したオブジェクトを使用します。
L2TP トンネルを使用してユーザを認証するためには、ローカルユーザデータベースが使用されます。

IPsec トンネルを設定する際、Local Networok には L2TP トンネルが接続する IP と同じ IP アドレスを指定します。ここでは wan_ip とします。また、トンネル確立時のルートが固定で定義されない（動的に追加される）ように IPsec トンネルを設定します。

さらに、L2TP サーバを設定する際、Inner IP アドレスはクライアントの IP アドレス割り当て元となるネットワークの一部となる必要があります。ここでは lan_ip とします。Outer IP インタフェースフィルタは L2TP サーバが接続を許可するインタフェースです。ここでは IPsec トンネル l2tp_ipsec とします。L2TP クライアントが使用する IP 用に ProxyARP も設定します。

手順 1　新しいローカルユーザデータベースを準備する :

CLI

```
DFL-xxxx:/> add LocalUserDatabase UserDB
DFL-xxxx:/> cc LocalUserDatabase UserDB
DFL-xxxx:/UserDB> add User testuser Password=mypassword
```

Web Interface

1. **System > Device > Users > Local User Databases > Add > Local User Databases** メニューをクリックします。

2. 適切なユーザデータベース名を入力します。（例 : UserDB）

3. Users タブを選択し、Add > User をクリックします。

4. 以下の情報を入力します。
   - Name: testuser
   - Password: mypassword
   - Confirm Password: mypassword

5. 「OK」ボタンをクリックします。

この後、IPsec トンネルを設定しますが、これは後ほど L2TP セクション内で使用されます。L2TP を使用する予定であるので、ローカルネットワークは L2TP トンネルが接続するのと同じ IP、wan_ip です。さらに、IPsec トンネルは、トンネルが確立している時に、ルートがスタティックまたはダイナミックに定義されないように設定される必要があります。

手順 2 IPsec トンネルの設定を続ける :

CLI

```
DFL-xxxx:/> add Interface IPsecTunnel l2tp_ipsec LocalNetwork=wan_ip RemoteNetwork=all-nets PSK=MyPSK
            IKEAlgorithms=Medium IPsecAlgorithms=esp-l2tptunnel EncapsulationMode=Transport
            AutoInterfaceNetworkRoute=No IPsecLifeTimeKilobytes=250000 IPsecLifeTimeSeconds=3600 IKEVersion=1
```

Web Interface

1. **Network > Interfaces and VPN > IPsec > Add > IPsec Tunnel** の順にメニューをクリックします。
2. 適切なユーザデータベース名を入力します。（例 : l2tp_ipsec）
3. 以下の通り入力します。
   - IKE Version: IKEv1
   - Encapsulation Mode: Transport
   - Remote Endpoint: all-nets
4. IPsec Life Time seconds に 3600 を入力します。
5. IPsec Life Time kilobytes に 250000 を入力します。
6. Authentication タブで「Pre-shared Key」を選択します。
7. Pre-shared Key で MyPSK を選択します。
8. Advanced タブで、Add route statically を選択しません。Add route statically オプションも選択しません。
9. 「OK」ボタンをクリックします。

次に L2TP サーバを設定します。内部の IP アドレスは、クライアントがこの lan_ip 内で IP アドレスを割り当てられる必要があります。外側インタフェースフィルタは、L2TP サーバが接続を受け入れるインタフェースであり、これは先に作成される l2tp_IPsec です。さらにプロキシ ARP が、L2TP クライアントが使用する IP に設定される必要があります。

手順 3 L2TP トンネルを設定する :

CLI

```
DFL-xxxx:/> add Interface L2TPServer l2tp_tunnel IP=InterfaceAddresses/lan_ip Interface=l2tp_IPsec
            ServerIP=InterfaceAddresses/wan_ip IPPool=InterfaceAddresses/l2tp_pool TunnelProtocol=L2TP
            AllowedRoutes=all-nets ProxyARPInterfaces=lan
```

Web Interface

1. **INetwork > Interfaces and VPN > PPTP/L2TP Servers > Add > PPTP/L2TP Server** の順にメニューをクリックします。
2. 以下の通り入力します。
   - Name : L2TP トンネルの名前を入力します。（例 : l2tp_tunnel）
   - Inner IP Address : lan_ip
   - Tunnel Protocol : L2TP
   - Outer Interface Filter : l2tp_IPsec
   - Server IP : wan_ip
3. PPP Parameters タブで以下の通り入力します。
   - Use User Authentication Rules : チェックします。
   - IP Pool : l2tp_pool
4. Add Route タブで以下の通り入力します。
   - Allowed Networks : all-nets
   - Proxy ARP : lan インタフェースを選択し、「Selected」リストに移動します。
5. 「OK」ボタンをクリックします。

L2TP トンネルを使用して、ユーザを認証するため、ユーザ認証ルールが設定される必要があります。

手順 4 認証ルールを設定する :

CLI

```
DFL-xxxx:/> add UserAuthRule AuthSource=Local Interface=l2tp_tunnel OriginatorIP=all-nets LocalUserDB=UserDB
            agent=PPP TerminatorIP=InterfaceAddresses/wan_ip name=L2TP_Auth
```

Web Interface

1. **Policies > User Authentication > User Authentication Rules > Add > User Authentication Rule** の順にメニューをクリックします。

2. 適切なルール名を入力します。（例 : L2TP_Auth）

3. 以下の通り入力します。
- Authentication Agent: L2TP/PPTP/SSL VPN
- Authentication Source : Local
- Interface : l2tp_tunnel
- Originator IP : all-nets
- Terminator IP : wan1_ip

4. Authentication Options タブで Local User DB に UserDB を選択します。

5. 「OK」ボタンをクリックします。

手順 5 IP ポリシーを設定する :

CLI

```
DFL-xxxx:/> add IPPolicy Name=allow_l2tp SourceInterface=l2tp_tunnel SourceNetwork=l2tp_pool
            DestinationInterface=lan DestinationNetwork=lannet Service=all_services Action=Allow
```

wan インタフェース経由の接続を NAT する 2 つ目の IP ポリシーを設定します。

```
DFL-xxxx:/> add IPPolicy Name=nat_l2tp SourceInterface=l2tp_tunnel SourceNetwork=l2tp_pool
            DestinationInterface=wan DestinationNetwork=all-nets Service=all_services Action=Allow
            SourceAddressTranslation=NAT NATSourceAddressAction=OutgoingInterfaceIP
```

Web Interface

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 適切なルール名を入力します。（例 : AllowL2TP）

3. 以下の通り入力し、「OK」ボタンをクリックします。
- Action: Allow
- Service: all_services
- Source Interface: l2tp_tunnel
- Source Network: l2tp_pool
- Destination Interface: lan
- Destination Network: lannet

wan インタフェース経由の接続を NAT する 2 つ目の IP ポリシーを設定します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Policy** の順にメニューをクリックします。

2. 適切なルール名を入力します。（例 : NATL2TP）

3. 以下の通り入力します。
- Action: Allow
- Service: all_services
- Source Interface: l2tp_tunnel
- Source Network: l2tp_pool
- Destination Interface: wan
- Destination Network: all-nets

4. Source Translation で以下の設定を行います。
- Address Translation: NAT
- Address Action: Outgoing Interface IP

5. 「OK」をクリックします。

トランスポートモードを使用した IPsec トンネル

上記の例の IPsec トンネルのカプセル化モードは L2TP で Transport に設定されています。これは推奨設定です。Windows™ クライアントはトランスポートモードでだけ機能します。

トランスポートモードでは、以下の項目について注意することが必要です。

- IPsec カプセル化にトンネルモードを使用するときだけ、IKEv2 は動作します。したがって、L2TP では IKEv1 を使用する必要があります。
- IKEv1 でトランスポートモードを使用する場合、IPsec Tunnel オブジェクトの Local Endpoint と Remote Endpoint プロパティだけがトンネル設定用に NetDefendOS によって使用されます。Local Network と Remote Network プロパティは無視されます。
- Add route statically 設定は無効にするべきです。この設定がトランスポートモードでどう機能するかに関して管理者に深い理解がある場合にだけ、有効とするべきです。
- トランスポートモードで Add route statically を有効にし、OutgoingRoutingTable が RoutingTable と同じルーティングテーブルに設定されると、NetDefendOS は警告メッセージを出して、Add route statically を自動的に無効にします。

  これは、許可されていると、IKE/ESP トラフィックがトンネルの確立後に自身のトンネルに送信されるためです。これは、ESP/IKE パケットがトンネルのリモートの終端に送信されないようにトラフィックループを作成することを意味します。

10.4.3 L2TP/PPTP サーバアドバンスド設定

管理者は、以下の L2TP/PPTP サーバの詳細な設定を行うことができます。

項目	説明
L2TP Before Rules	NetDefend Firewall に送信された L2TP トラフィックは、ルールセットを参照せずに L2TP サーバに直接送られます。 初期値 : Enabled（有効）
PPTP Before Rules	NetDefend Firewall に送信された PPTP トラフィックは、ルールセットを参照せずに PPTP サーバに直接送られます。 初期値 : Enabled（有効）

10.4.4 PPTP/L2TP クライアント

PPTP と L2TP プロトコルについては前項で説明されています。PPTP または L2TP サーバとして機能できることに加えて、NetDefendOS は PPTP または L2TP クライアントとして機能することができます。これは、PPTP または VPN が IPsec の代わりに VPN プロトコルとして選ばれる場合に役に立ちます。1 つの D-Link ファイアウォールが、サーバとして動作し、サーバとして動作する別のユニットに接続することができます。

クライアント設定

PPTP と L2TP クライアントのコンフィグレーションオブジェクトは、一般的なプロパティのセットを共有します。

- **General Parameters**

項目	説明
Name	クライアント名。
Tunnel Protocol	PPTP または L2TP クライアントであるかを指定します。
Remote Endpoint	トンネル接続のリモートエンドポイントの IP アドレス。これは、リモート PPTP/L2TP サーバが接続をリッスンするリモートインタフェースの IP アドレスです。リモートのエンドポイントが、FQDN として指定される場合、プレフィックス dns: をはじめに指定する必要があります。例 : dns:server.example.com
Remote Network	トンネルに接続されるリモートネットワーク。トラフィックはクライアントとこのネットワークの間を流れます。
Originator IP Type	トンネル外部のローカルなエンドポイントで IP アドレスを取得する方法を指定します。トンネル内のクライアントからサーバに流れるトラフィックの送信元アドレスではありません。この設定は以下の 2 つの値のいずれかとします。 **i.** Local interface - ローカルエンドポイントの IP はローカルインタフェースの IP アドレスになります。（初期値） **ii.** Manually specified address - IP アドレスは、次に説明される Originator IP プロパティを使用して手動で指定されます。
Originator IP	前のプロパティに Manually specified address オプションを指定すると、これはトンネルの外側の送信元 IP として使用される IP アドレスとなります。ネットワークトポロジによって、このアドレスは、イーサネットインタフェースで ARP パブリッシュされる必要があるかもしれません。

- **Authentication（認証モード）**

項目	説明
Username	本 PPTP/L2TP インタフェースに使用するユーザ名を指定します。
Password	インタフェース用のパスワードを指定します。

- **Security**

項目	説明
IPsec Interface	オプションで使用する IPsecTunnel オブジェクトを指定します。問題を起こす可能性があるため、Dynamically add route to remote network オプションを有効にすべきではありません。
Authentication	使用する認証プロトコルを指定します。
MPPE	Microsoft Point-to-Point Encryption の使用と使用するレベルを指定します。

Dial On Demand が有効になると、PPTP/L2TP トンネルはトラフィックがインタフェースに送信されるまで設定されません。このオプションのためのパラメータは以下の通りです。

項目	説明
Activity Sensing	Dial On Demand がどこで（Outbound、Inbound または Bi-directional）トリガーを行うかを指定します。
Idle Timeout	切断前に待機するアクティブでない時間（秒）。

PPTP クライアント機能の使用

PPTP クライアント機能の 1 つの使用法が以下に記載したシナリオに示されています。

この例では、ファイアウォールの反対側にある PPTP サーバに接続される前に多くのクライアントが NetDefendOS を通じて NAT 変換されます。ひとつ以上のクライアントが、PPTP サーバに接続を試みる PPTP クライアントとして動作している場合、NAT されていることにより、これは動作しません。

このように複数の PPTP クライアントを NAT 変換する 1 つの方法は PPTP ALG を使用することです。（「6.1.8 PPTP ALG」）別の方法は、PPTP サーバに接続する場合にファイアウォールが PPTP クライアントとして動作することで、この設定には以下の要件があります。

- PPTP トンネルは NetDefendOS とサーバ間で定義されます。
- ルートが、NetDefendOS のルーティングテーブルに追加されます。これは、サーバ用のトラフィックが PPTP トンネルを通じてルーティングされる必要があることを指定するものです。

このクライアント手法の使用は、ISP が認証に PPTP を必要とする状況に適しています。

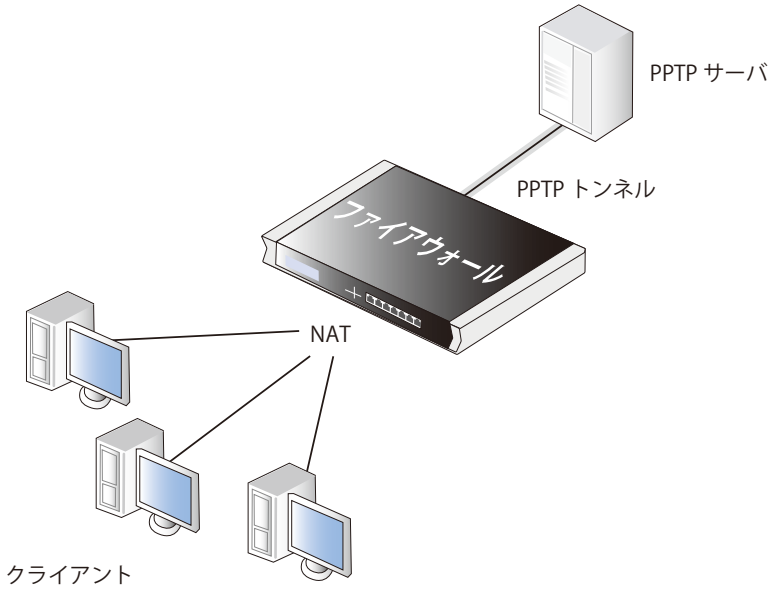


図 10-7　PPTP クライアントの使用

10.4.5 l2tp と pptp コマンド

NetDefendOS は L2TP と PPP の状態をモニタするのに 2 つの CLI コマンドを提供します。

- **l2tp CLI コマンド**

  NetDefendOS は、L2TP クライアントとサーバの両方に関する情報を参照するために CLI コマンド「l2tp」を提供します。すべての L2TP サーバとクライアントの現在の状態を表示するには、以下の通りコマンドを指定します。

```
DFL-xxxx:/> l2tp -state=all
```

  特定の L2TP サーバの全セッションを参照するには、以下の構文とします。

```
DFL-xxxx:/> l2tp -l2tpserver=<L2TP-server-object-name>
```

  以下は、確立済みであるが、接続するクライアントを持たない L2TP トンネルオブジェクト「my_l2tp_tunnel1」の出力例であり、リッスンのみとなっています。

```
DFL-xxxx:/> l2tp -state=all

Active and listening sessions
L2TP Tunnel        Remote GW          State           Tunnel IDs
------------------ ------------------ --------------- ----------------
my_l2tp_tunnel1                       Listening       0      44555
```

  2 つのサーバ、1 つはクライアントを持たないサーバ（listening）、もう 1 つは少なくとも 1 つのクライアントを持つサーバ（established）が存在する場合、出力結果は以下の通りです。

```
DFL-xxxx:/> l2tp -state=all

Active and listening sessions
L2TP Tunnel        Remote GW          State           Tunnel IDs
------------------ ------------------ --------------- ----------------
my_l2tp_tunnel1                       Listening       0      44555
my_l2tp_tunnel2                       Listening       0      30859
my_l2tp_tunnel2    203.0.113.1        Established     32008  39949
```

  また、「-child」オプションを使用してトンネルに子供のセッションが開いていることを調べることもできます。この例題は、以下の通りシングルセッション (#1) がアクティブであることを示しています。

```
DFL-xxxx:/> l2tp -state=active -child

Active sessions
L2TP Tunnel        Remote GW          State           Tunnel IDs
------------------ ------------------ --------------- ----------------
my_l2tp_tunnel1    203.0.113.1        Established     32008  39949
#1                   -                Established     1      1
```

- **pptp CLI コマンド**

  NetDefendOS は、PPTP クライアントとサーバの両方に関する情報を参照するために CLI コマンド「pptp」を提供します。「pptp」コマンド構文と出力は上で説明した「l2tp」コマンドに従っています。例えば、すべての PPTP サーバとクライアントの現在の状態を表示するには、以下の通りコマンドを指定します。

```
DFL-xxxx:/> pptp -state=all

Active and listening sessions
PPTP Tunnel        Remote GW          State
------------------ ------------------ ------------------
my_pptp_tunnel1                       Listening
my_pptp_tunnel1    203.0.113.6        Established
```

これらのコマンドの両方とそれらの全オプションは個別の「NetDefendOS CLI Reference Guide」に記載されています。これらのコマンドのどちらも、現在、Web インタフェースに同等な機能を持っています。

10.5 L2TP バージョン 3

L2TP バージョン 3（L2TPv3）は標準の L2TP（標準の L2TP は L2TPv2 とも呼ばれる）への代替手段であるトンネリングプロトコルです。L2TPv2 は PPP トラフィックをトンネルすることができるだけですが、L2TPv3 は、OSI レイヤ 2 サービスのプロパティをエミュレートする重要な利点があります。これは Layer2 トンネリングまたは Pseudowire とも呼ばれています。またこれは L2TPv3 が IP ネットワークにイーサネットフレームを運ぶことができることを意味し、これにより 1 つ以上のイーサネット LAN がパブリックインターネットを経由して接続することができます。NetDefendOS L2TPv3 はイーサネットと VLAN の両方をトンネルすることができます。

注意 **HA クラスタは L2TPv3 をサポートしません。**
NetDefendOS HA クラスタは L2TPv3 をサポートしません。HA クラスタにこれを設定するべきではありません。

L2TPv2 に L2TPv3 の他の利点の概要は以下の通りです。

- UDP なしで IP 上まで送信されます。L2TPv2 は UDP を必要とします。
- man-in-the-middle または packet-insertion 攻撃に対してより優れたセキュリティを持ちます。
- 1 つのトンネル内にさらに多くのトンネルまたはセッションをサポートします。
- スタティックパラメータを使用して手動で設定でき、コントロールチャンネルを必要としません。

L2TPv3 が持つ他の重要な問題は以下の通りです。

- 標準の L2TP のように、L2TPv3 は送信データの暗号化を提供しません。L2TPv3 トンネルを安全にするなら、IPsec または PPPoE と共に使用するべきです。
- NetDefendOS の L2TPv3 は IPv4 でのみ使用できます。IPv6 は現在、NetDefendOS ではサポートされません。
- NetDefendOS の L2TPv3 サポートにより、D-Link ファイアウォールは L2TPv3 サーバまたはクライアントのどちらかとして機能することができます。2 つの機能を設定する方法を次に説明します。

パススルー設定

NetDefendOS の L2TPv3 クライアントおよびサーバオブジェクトには、2 つのパススループロパティが存在します。

- **DHCP Passthrough**
  DHCP プロトコルトラフィックの送信を許可します。
- **Non-IP Protocol Passthrough**
  非 IPv4 プロトコルトラフィックの送信を許可します。本プロパティが有効化されている場合、例えば IPv6 トラフィックが許可されます。

10.5.1 L2TPv3 サーバ

D-Link ファイアウォールが L2TPv3 サーバとして機能する場合、クライアントとサーバのどちらか一方のネットワークが透過的に相互に接続されているように見えるように L2TPv3 クライアントの接続を許可します。

設定の手順は以下の通りです。最初に非 VLAN シナリオの設定を説明し、次に、VLAN シナリオの設定を説明します。

標準の L2TPv3 サーバの設定

VLAN タグのないパケット用の標準 L2TPv3 の設定には以下の項目が必要です。

A. L2TPv3 Server オブジェクトを定義します。オブジェクトには、以下のプロパティを設定が必要です。

項目	説明
Inner IP Address	Local Network プロパティに使用されるネットワークに IPv4 アドレスを設定します。慣例として、保護されたネットワークに接続する物理インタフェースを使用することをお勧めします。
Local Network	トンネルを通じて保護されたネットワークにアクセスするように設定します。
Protocol	IP（115）または UDP のどちらに対して L2TPv3 によるトンネル化を行うかを指定します。
Outer Interface Filter	L2TPv3 クライアント接続用の listening インタフェースになるように設定します。IPsec がなければ、物理的なイーサネットインタフェースに設定します。暗号化に IPsec を使用するとき、IPsec トンネルオブジェクトに設定します。
Server IP	listening インタフェースの IP アドレスになるように設定します。

B. 保護されたインタフェースの透過モードを有効にします。

保護されたネットワークに接続するイーサネットインタフェースのプロパティの透過モードを有効にするように変更します。

C. 必要な L2TPv3 サーバの高度なオプションを設定します。
いくつかの L2TPv3 クライアントは、サーバオブジェクトに Host Name または Router ID オプションの設定を必要とします。Host Name を None に設定すると、トンネルの Inner IP Address がこの設定に使用されます。

以下の図は L2TPv3 のための典型的なセットアップを示しています。ここで、インタフェース If2 をリッスンする L2TPv3 サーバに接続する L2TPv3 クライアントが、インタフェース If3 の保護されたネットワークにアクセスできるようにします。

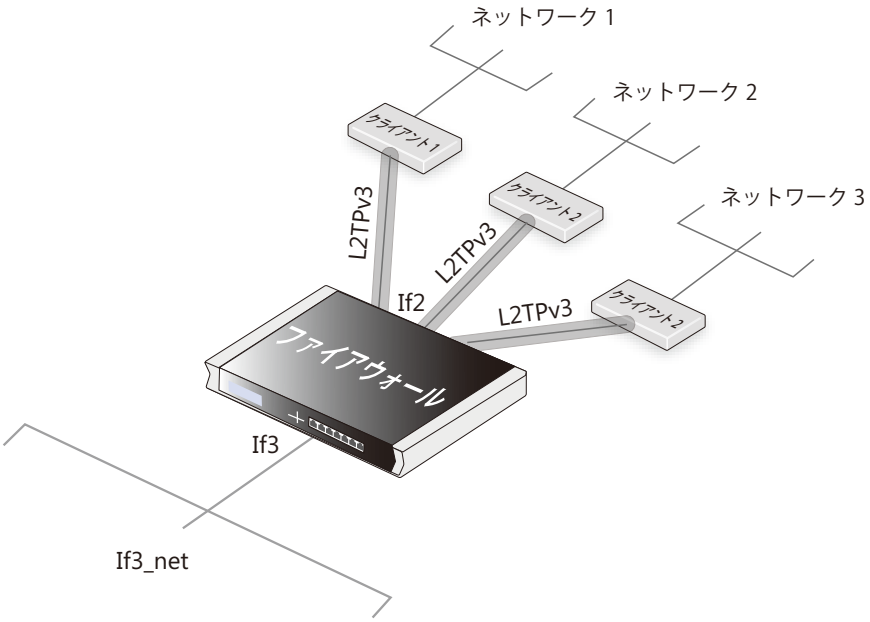


図 10-8　L2TPv3 の例

上のシナリオの設定は以下の例に含まれています。

例題 10.20

L2TPv3 サーバの設定

L2TPv3 Server オブジェクト my_l2tpv3_if は、L2TPv3 クライアントが If2 インタフェースに接続できるように、セットアップされると仮定します。目的は、L2TPv3 を使用して、If3 インタフェースにおける保護されたネットワーク If3_net をクライアントに対してアクセス可能にすることです。

CLI

A. まず、L2TPv3 Server オブジェクトを定義します。

```
DFL-xxxx:/> add Interface L2TPv3Server my_l2tpv3_if IP=If3_ip LocalNetwork=If3_net Interface=If2 ServerIP=If2_ip
```

B. 次に保護されたインタフェースの透過モードを有効にします。

```
DFL-xxxx:/> set Interface Ethernet If3 AutoSwitchRoute=Yes
```

Web Interface

A. まず、L2TPv3 Server オブジェクトを定義します。

1. **Network > Interfaces and VPN > L2TPv3 Servers > Add > L2TPv3 Server** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_l2tpv3_if
   - Inner IP Address: If3_ip
   - Local Network: If3_net
   - Outer Interface Filter: If2
   - Server IP: If2_ip
3. 「OK」ボタンをクリックします。

B. 次に保護されたインタフェース If3 の透過モードを有効にします。

1. **Network > Interfaces and VPN > Ethernet** の順にメニューをクリックします。
2. If3 インタフェースを選択します。
3. オプション Enable transparent mode を選択します。
4. 「OK」ボタンをクリックします。

プロトコルプロパティ

L2TPv3 Server コンフィグレーションオブジェクトには、低いプロトコルレベルで L2TPv3 通信用の転送方式を定義する Protocol プロパティがあります。2 つのオプションがあります。

項目	説明
UDP	下位レベルの転送プロトコルとして UDP を使用するのは、このプロパティの初期設定であり、推奨されます。NAT がネットワークをパススルーする中で使用されている場合は、通信が多くのネットワーク機器を通過できることを保証します。
IP	トランスポートプロトコルとして IP を使用すると、パケット処理が最適化され、より少ない処理リソースの使用でデータを送信する方法を提供します。しかし、ネットワーク機器の中には通過を許可しないものもある可能性があり、NAT がネットワークのパススルーに採用されているところで問題が起こるかもしれません。代わりに UDP を使用することで、そのような問題を解決できます。

暗号化に IPsec を使用する

標準の L2TP（L2TPv2）のように、L2TPv3 は暗号化を提供しません。通信を安全にするためには、L2TPv3 を、IPsec Tunnel オブジェクトに関連付けてして設定すべきです。そうすると listening インタフェースはトンネルになります。

IPsec トンネルのセットアップは標準の L2TP と同じ手順に従います。詳しくは「10.4.2 L2TP サーバ」に記述されます。

例題 10.21

IPsec を使用した L2TPv3 サーバの設定

前の例と同じシナリオですが、今回は L2TPv3 トンネルが、IPsec Tunnel オブジェクト my_ipsec_tunnel を通じてトンネルされるものとします。IPsec トンネルのセットアップは以下の例題には記載しませんが、「10.4.2 L2TP サーバ」の設定に従います。

CLI

A. まず、L2TPv3 Server オブジェクトを定義します。

```
DFL-xxxx:/> add Interface L2TPv3Server my_l2tpv3_if IP=If3_ip LocalNetwork=If3_net Interface=my_ipsec_tunnel
            ServerIP=If2_ip
```

B. 次に保護されたインタフェース If3 の透過モードを有効にします。

```
DFL-xxxx:/> Set Interface Ethernet If3 AutoSwitchRoute=Yes
```

Web Interface

A. まず、L2TPv3 Server オブジェクトを定義します。

1. **Network > Interfaces and VPN > L2TPv3 Servers > Add > L2TPv3 Server** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_l2tpv3_if
   - Inner IP Address: If3_ip
   - Local Network: If3_net
   - Outer Interface Filter: my_ipsec_tunnel
   - Server IP: If2_ip
3. 「OK」ボタンをクリックします。

B. 次に保護されたインタフェース If3 の透過モードを有効にします。

1. **Network > Interfaces and VPN > Ethernet** の順にメニューをクリックします。
2. If3 インタフェースを選択します。
3. General タブでオプション Enable transparent mode を選択します。
4. 「OK」ボタンをクリックします。

VLAN に設定する

NetDefendOS L2TPv3 サーバは、VLAN 接続を通じて外部の保護されたネットワーク接続できるように、VLAN のタグ付きイーサネットフレームを処理することができます。

NetDefendOS を使用してこれを行うには、クライアントが使用する ID と同じ VLAN ID を共に持つ 1 組の VLAN を設定する必要があります。1 つの VLAN がローカルで、保護されたイーサネットインタフェースに設定されます。もう 1 つの VLAN は L2TPv3 サーバインタフェースに設定されます。これらの VLAN の両方が透過モードを有効にしなければなりません。さらに、新しいルーティングテーブルを各ペアに設定し、ペアの VLAN がそのテーブルのメンバになるように設定する必要があります。

以下は VLAN の設定手順の概要です。

A. 以前に説明した通り、L2TPv3 サーバインタフェースのオブジェクトを定義しますが、透過モードを保護されたイーサネットインタフェースで有効にしないでください。

B. 以下のプロパティで NetDefendOS VLAN インタフェースオブジェクトを設定します。

- **i.** VLAN ID はクライアントで送信したパケットの VLAN ID と同じです。
- **ii.** インタフェースは保護されたイーサネットインタフェースです。
- **iii.** ネットワークは保護されたローカルネットワークと同じです。
- **iv.** VLAN の IPv4 アドレスは保護されたローカルネットワークの任意の IP です。
- **v.** この VLAN の透過モードを有効とします。

C. 以下のプロパティで 2 つ目の VLAN インタフェースオブジェクトを設定します。

- **i.** VLAN ID は前の VLAN と同じで、クライアントで送信したパケットの ID と同じです。
- **ii.** インタフェースは以前に定義した L2TPv3 Server オブジェクトです。
- **iii.** ネットワークは保護されたローカルネットワークと同じです。
- **iv.** VLAN の IPv4 アドレスは保護されたローカルネットワークの任意 IP ですが、前の VLAN とは異なります。
- **v.** この VLAN の透過モードを有効とします。

D. ペアに新しい RoutingTable オブジェクトを定義します。

E. 各 VLAN をこの新しいルーティングテーブルのメンバにします。

例題 10.22

VLAN 用の L2TPv3 サーバの設定

my_l2tpv3 という名前の L2TPv3 トンネル設定し、L2TPv3 クライアントが If2 上で通信できるようにします。If3 インタフェースの保護されたネットワーク If3_net をこれらのクライアントがアクセスできるようにします。

さらに、クライアントは VLAN ID 555 を持つトンネル内の VLAN を通じてアクセスします。

2 つの任意の IPv4 アドレス（If3_net が NetDefendOS アドレス帳に定義済みである保護されたネットワークの If3_arbitrary_ip1 と If3_arbitrary_ip2）を想定します。

CLI

A. まず、L2TPv3 Server オブジェクトを定義します。

```
DFL-xxxx:/> add Interface L2TPv3Server my_l2tpv3_if IP=If3_ip LocalNetwork=If3 Interface=If2 ServerIP=If2_ip
```

B. 次に、保護されたインタフェース If3 に VLAN オブジェクトを作成します。

```
DFL-xxxx:/> add Interface VLAN my_vlan_local BaseInterface=If3 VLANID=555 IP=If3_arbitrary_ip1 Network=If3_net
            AutoSwitchRoute=Yes
```

C. 最後に L2TPv3 トンネルインタフェースに VLAN オブジェクト my_l2tpv3_if を作成します。

```
DFL-xxxx:/> add Interface VLAN my_vlan_l2tpv3 BaseInterface=my_l2tpv3_if VLANID=555 IP=If3_arbitrary_ip2
            Network=If3_net AutoSwitchRoute=Yes
```

D. この VLAN ペアに新しい RoutingTable オブジェクトを定義します。

```
DFL-xxxx:/> add RoutingTable my_vlan_rt
```

E. ペアの各 VLAN をこの新しいルーティングテーブルのメンバにします。

```
DFL-xxxx:/> set Interface VLAN my_vlan_local MemberOfRoutingTable=Specific RoutingTable=my_vlan_rt

DFL-xxxx:/> set Interface VLAN my_vlan_l2tpv3 MemberOfRoutingTable=Specific RoutingTable=my_vlan_rt
```

Web Interface

A. まず、L2TPv3 Server オブジェクトを定義します。

1. **Network > Interfaces and VPN > L2TPv3 Servers > Add > L2TPv3 Server** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_l2tpv3_if
   - Inner IP Address: If3_ip
   - Local Network: If3_net
   - Outer Interface Filter: If2
   - Server IP: If2_ip

3. 「OK」ボタンをクリックします。

B. 次に、保護されたインタフェース If3 に VLAN オブジェクトを作成します。

1. **Network > Interfaces and VPN > VLAN > Add > VLAN** の順にメニューをクリックします。

2. If3 インタフェースを選択します。

3. 以下の情報を入力します。
   - Name: my_vlan_local
   - Interface: If3
   - VLAN ID: 555
   - IP Address: If3_arbitrary_ip1
   - Network: If3_net

4. オプション Enable transparent mode を選択します。

5. 「OK」ボタンをクリックします。

C. L2TPv3 トンネルインタフェースに VLAN オブジェクト my_l2tpv3_if を作成します。

1. **Network > Interfaces and VPN > VLAN > Add > VLAN** の順にメニューをクリックします。

2. If3 インタフェースを選択します。

3. 以下の情報を入力します。
   - Name: my_vlan_l2tpv3
   - Interface: my_l2tpv3_if
   - VLAN ID: 555
   - IP Address: If3_arbitrary_ip2
   - Network: If3_net

4. オプション Enable transparent mode を選択します。

5. 「OK」ボタンをクリックします。

D. この VLAN ペアに新しい RoutingTable オブジェクトを定義します。

1. **Network > Routing > Routing Tables > Add > Routing Table** の順にメニューをクリックします。

2. Name に my_vlan_rt を入力します。

3. 「OK」ボタンをクリックします。

E. ペアの各 VLAN をこの新しいルーティングテーブルのメンバにします。

1. **Network > Interfaces and VPN > VLAN** の順にメニューをクリックします。

2. my_vlan_local を選択し、オブジェクトを編集します。
   - Virtual Routing タブを選択します。
   - Make interface a member of a specific routing table を選択します。
   - Routing Table を my_vlan_rt を選択します。
   - 「OK」ボタンをクリックします。

3. my_vlan_l2tpv3l を選択し、オブジェクトを編集します。
   - Virtual Routing タブを選択します。
   - Make interface a member of a specific routing table を選択します。
   - Routing Table を my_vlan_rt を選択します。
   - 「OK」ボタンをクリックします。

10.5.2 L2TPv3 クライアント

D-Link ファイアウォールは L2TPv3 クライアントとしても機能します。これにより、1 つの L2TPv3 トンネルを通じて L2TPv3 サーバに送信されるように、L2TPv3 クライアントとして設定されたリモートファイアウォールがローカルに接続するクライアントからのトラフィックの集信装置として動作できます。

以下の手順が、NetDefendOS を L2TPv3 クライアントに設定するのに必要です。

A. 以下のプロパティで L2TPv3Client オブジェクトを定義します。

項目	説明
Inner IP Address	トンネル内部のローカル IP アドレス。通常、これはローカルなトンネルエンドポイントである物理インタフェースの IP アドレスです。
Local Network	保護されたローカルネットワークはトンネルを通じてアクセス可能です。
Pseudowire Type	通常、これは Ethernet です。VLAN のために VLAN を設定します。
Protocol	通常、これは UDP です。
Remote Endpoint	サーバの IP アドレス。

B. 保護されたネットワークが位置している内側インタフェースの透過モードを有効にします。

例題 10.23

L2TPv3 クライアントのセットアップ

この例題では、L2TPv3 Client オブジェクト my_l2tpv3_client が作成されているものとします。これは IP アドレス l2tpv3_server_ip を持つ L2TPv3 サーバに接続します。

このクライアントは IPsec トンネル l2tpv3_ipsec_tunnel を通じてサーバに接続します。トンネルが既に定義されているものとします。

CLI

A. まず、L2TPv3Client オブジェクトを定義します。

```
DFL-xxxx:/> add Interface L2TPv3Client my_l2tpv3_client IP=inner_client_ip LocalNetwork=If1_net
            PseudowireType=Ethernet Protocol=UDP RemoteEndpoint=l2tpv3_server_ip
```

B. 次に保護されたインタフェース If1 の透過モードを有効にします。

```
DFL-xxxx:/> set Interface Ethernet If1 AutoSwitchRoute=Yes
```

Web Interface

A. まず、L2TPv3 Client オブジェクトを定義します。

1. **Network > Interfaces and VPN > L2TPv3 Client > Add > L2TPv3 Client** の順にメニューをクリックします。

2. 以下の情報を入力します。
- Name: my_l2tpv3_client
- Inner IP Address: inner_client_ip
- Local Network: If1_net
- Pseudowire Type: Ethernet
- Protocol: UDP
- Remote Endpoint: l2tpv3_server_ip

3. 「OK」ボタンをクリックします。

B. 次に保護されたインタフェース If1 の透過モードを有効にします。

1. **Network > Interfaces and VPN > Ethernet** の順にメニューをクリックします。

2. If1 インタフェースを選択します。

3. オプション Enable transparent mode を選択します。

4. 「OK」ボタンをクリックします。

暗号化に IPsec を使用する

先に述べたとおり、L2TPv3 は暗号化を提供しません。パブリックインターネットを通過する暗号化のためには、IPsec を使用するべきです。以下の例題では、L2TPv3 クライアントオブジェクトのプロパティとして使用されるように IPsec トンネルを指定することで実現する方法を示しています。

例題 10.24

IPsec を使用した L2TPv3 クライアントの設定

この例は、前の例と同じですが、暗号化のためにサーバに IPsec トンネルを使用します。IPsec トンネルオブジェクトが l2tpv3_ipsec_tunnel という名前で既に定義されているものとします。

IPsec トンネル設定をここでは示していませんが、「IPsec L2TP トンネルを設定する」に示す L2TP 用の手順と同じです。

CLI

A. L2TPv3Client オブジェクトを定義します。

```
DFL-xxxx:/> add Interface L2TPv3Client my_l2tpv3_client IP=inner_client_ip LocalNetwork=If1_net
            PseudowireType=Ethernet Protocol=UDP RemoteEndpoint=l2tpv3_server_ip IPsecInterface=l2tpv3_ipsec_tunnel
```

B. 次に保護されたインタフェース If1 の透過モードを有効にします。

```
DFL-xxxx:/> set Interface Ethernet If1 AutoSwitchRoute=Yes
```

Web Interface

A. まず、L2TPv3 Client オブジェクトを定義します。

1. **Network > Interfaces and VPN > L2TPv3 Client > Add > L2TPv3 Client** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_l2tpv3_client
   - Inner IP Address: inner_client_ip
   - Local Network: If1_net
   - Pseudowire Type: Ethernet
   - Protocol: UDP
   - Remote Endpoint: l2tpv3_server_ip
   - IPsec Interface: l2tpv3_ipsec_tunnel
3. 「OK」ボタンをクリックします。

B. 次に保護されたインタフェース If1 の透過モードを有効にします。

1. **Network > Interfaces and VPN > Ethernet** の順にメニューをクリックします。
2. If1 インタフェースを選択します。
3. オプション Enable transparent mode を選択します。

「OK」ボタンをクリックします。

VLAN に設定する

NetDefendOS L2TPv3 クライアントは、VLAN 接続を通じて外部の保護されたネットワークに接続できるように、VLAN のタグ付きイーサネットフレームを処理することができます。VLAN の設定はサーバと同じ方法で行います。「10.5.1 L2TPv3 サーバ」に詳しく説明しています。

L2TPv3 クライアントオブジェクトを設定する場合、PseudowireType プロパティの値を VLAN に設定しなければなりません。

10.6 SSL VPN

10.6.1 概要

NetDefendOS は SSL VPN と呼ばれる VPN 接続の追加タイプを提供します。これは、リモートクライアントコンピュータと D-Link ファイアウォール間に安全なトンネルを提供するのに SSL（Secure Sockets Layer）プロトコルを使用します。そして、クライアントにおけるどんなアプリケーションもファイアウォールプロテクトサイドに位置するサーバと安全に通信することができます。

SSL VPN の利点

SSL VPN の主な利点は、HTTPS プロトコルを使用してクライアントとファイアウォール間の安全な通信を可能にすることです。ホテルや空港などローミングするクライアントが操作しなければならないいくつかの環境で、ネットワーク装置は IPsec をはじめとする他のトンネルプロトコルが使用を許可されないことがよくあります。

そのような場合に、SSL VPN は実行可能な簡単かつ安全なクライアント接続ソリューションを提供します。

SSL VPN の短所

SSL VPN の短所は、信頼性の高い伝送のために TCP プロトコルのカプセル化を広範囲に使用するトンネリング技術に依存しているところです。これはいくつかの高負荷状況で著しい遅延を引き起こしてしまう余分な処理オーバヘッドをもたらします。

そのため、SSL VPN は例えば、IPsec より多くの処理リソースを要求します。さらに、IPsec 用のハードウェアアクセレーションは、ハードウェアのプラットフォームによっては処理効率をさらに上げるために利用可能です。

NetDefendOS がサポートする暗号スイートと TLS バージョン

NetDefendOS は SSL VPN 用に多くの暗号アルゴリズムをサポートします。初期値ではその中の一部が有効であり、それぞれを有効または無効にできます。サポートしているすべてのアルゴリズムは「13.9 SSL/TLS 設定」に記載されています。NetDefendOS はバージョン 1.1 を除き、TLS バージョン 1.0 と 1.2 をサポートしていることに注意してください。バージョン 1.2 を無効にして、1.0 だけを使用する方法については「13.9 SSL/TLS 設定」を参照してください。

初期値では、最も高い安全が考慮されている 4 つのアルゴリズムだけが有効です。より弱いアルゴリズムを有効にすることは推奨されません。これは、本来下位互換のために存在するものです。

SSL VPN 設定手順の概要

SSL VPN 設定では以下の手順が必要です。

- **NetDefend のファイアウォール側 :**
  - **i.** SSL VPN 接続を受け付けるために特定のイーサネットインタフェースを構成する SSL VPN インタフェースオブジェクトを作成する必要があります。
  - **ii.** 認証ルールは、到来する SSL VPN クライアントのために定義される必要があり、ルールでは、インタフェースプロパティに上記で作成した SSL VPN オブジェクトの名前を設定する必要があります。

    L2TP/PPTP/SSL VPN にルールの認証エージェントを設定する必要があります。また、ファイアウォールのリスニングインタフェースの外部 IP アドレスにルールのターミネータ IP を設定する必要があります。

    PPP Agent オプションを PAP に設定する必要があります。

  - **iii.** 特定の IP アドレス、ネットワークまたはネットワーク範囲のみトンネル経由でクライアントに対して利用可能にする場合、オプションとして SSL VPN インタフェースにこれを指定できます。そのように設定しない場合、すべてのクライアントトラフィックがトンネルを通過して送信されることが予想できます。
  - **iv.** 適切な NetDefendOS IP ルールを定義して、SSL VPN トンネル内のデータフローを許可します。以下の説明の通り、通常、IP ルールは SSL VPN トンネル自身のセットアップには定義される必要ありません。
  - **v.** SSL VPN トンネル内でデータフローを許可する適切な NetDefendOS IP ルールを定義します。

    以下で記述する通り、通常、SSL VPN トンネル自身の設定用に IP ルールを定義する必要はなくて、トンネルを流れるトラフィック用にだけ必要とされます。

  - **vi.** クライアント IP が ARP パブリッシュされるインタフェースを指定します。これは、ファイアウォールの背後にあるサーバが SSL VPN クライアントに応答を送り返す方法を知るために必要です。

    通常、クライアントに割り当てられた IP が、クライアントがアクセスする必要がある既存のサブネットにある場合のみ、プロキシ ARP を有効にする必要があります。その場合、プロキシ ARP は対応するサブネットを持つインタフェースで有効でなければなりません。トラフィックがファイアウォールによってルーティングされた場合、例えば、Allow または NAT ルールでは、プロキシ ARP は必要ありません。

    NetDefendOS SSL VPN には、すべてのファイアウォールインタフェースにあるすべてのクライアント IP を自動的に ARP パブリッシュするた

めのオプションがありますが、安全性の問題により推奨されません。

vii. SSL VPN トンネルが確立している場合、これらが NetDefendOS によって自動的に追加されるため、ルーティングテーブルでクライアント用のルートを定義する必要はありません。

Net Defends OS の SSL VPN の設定については、「10.6.2 NetDefendOS に SSL VPN を設定する」を参照してください。

- **Windows ベースのクライアント側**
  ファイアウォールにおける正しいインタフェースにトラフィックを送信するために、所有する D-Link VPN SSL クライアントアプリケーションをインストールおよび設定する必要があります。

  ユーザがファイアウォールに Web ブラウザを介してアクセスすると、ログインプロセスの一部として、SSL VPN クライアントソフトウェアのインストールと実行が行われます。ファイアウォールから直接ブラウザ経由で Windows ベースのクライアントソフトウェアは自動的にダウンロードされます。

PPPoE を使用した SSL VPN

パブリックインターネットにおける D-Link ファイアウォールへの接続方法として PPPoE が使用される場合、PPPoE 接続に SSL VPN 機能を持つことが可能です。

これは、SSLVPN トンネルオブジェクトの外部インタフェースのプロパティが物理イーサネットインタフェースの代わりに PPPoE 設定オブジェクトになるように SSL VPN トンネルを設定することで行われます。PPPoE インタフェースオブジェクトの設定については、「3.4.6 PPPoE」を参照してください。

10.6.2 NetDefendOS に SSL VPN を設定する

NetDefendOS で SSL VPN を設定するためには、接続を行う各インタフェースに SSL VPN インタフェースオブジェクトを定義する必要があります。オブジェクトのプロパティは以下の通りです。

General オプション

項目	説明
Name	NetDefendOS 設定の表示に使用されるオブジェクトの記述名。
Inner IP	これは SSL VPN クライアントが接続するトンネル内の IP 番号です。 SSL VPN インタフェースの IP プールから SSL VPN オブジェクトインタフェースに接続する全クライアントに IP を割り当てます。Inner IP と同様にすべてのプールアドレスが同じネットワークに所属する必要があり、これらはファイアウォールと接続するクライアント間の関係を定義します。 プライベート IP ネットワークはこのために使用されるべきです。Inner IP 自体は、接続する SSL VPN クライアントに付与される IP プールアドレスの 1 つである必要はありません。 **注意** Inner IP への ping 送信は可能です トラブルシューティングの目的で Inner IP に ICMP Ping を送信することができます。NetDefendOS が応答するためには、トラフィックが SSL VPN インタフェースから core（つまり NetDefendOS 自身）へのトラフィックフローを許可する IP ルールが存在する必要があります。
Outer Interface	SSL VPN 接続を行うためにリッスンするインタフェース。これは物理的なイーサネットインタフェース、または別の論理インタフェースとすることもできます。例えば、PPPoE インタフェースを使用することができます。
Server IP	クライアントが SSL VPN 接続を行うためにリッスンするインタフェースの IP アドレス。これは通常パブリックインターネット上を Web ブラウザの使用によって最初にアクセスするパブリック IPv4 アドレスになります。この IP について以下の点に注意する必要があります。 • Server IP は指定する必要があり、Outer Interface の IP が初期値とはなりません。 • サーバ IP はインタフェースで ARP バブリッシュされた IP アドレスではありません。 SSL が ARP にパブリッシュされる IP で正常に動作するためには、付随するプロキシ ARP プロパティを持つ core ルートを使用しなければなりません。これは以下の手順で行います。 - Interface プロパティに core、Network プロパティに Server IP アドレスを持つルートを定義します。 - ルートの Proxy ARP プロパティにクライアントが接続しているインタフェースを設定します。 Proxy ARP は、「4.2.6 プロキシ ARP」でより詳しく説明されています。
Server Port	クライアントが SSL VPN 接続のためにリッスンする際に使用するサーバ IP における TCP/IP ポート番号。初期値は SSL の標準のポート番号である 443 です。

Client IP オプション

項目	説明
Dynamic Server Address	クライアントに付与される SSL VPN Server IP の固定の IP アドレスの代わりに、本オプションは完全修飾ドメイン名 (FQDN) を付与することができます。 例えば、FQDN を server.example.com と指定することができます。クライアントが SSL VPN インタフェースに接続すると、次に特定の IP アドレスに DNS を使用して FQDN を解決するクライアントにこの FQDN を付与します。これにより、DNS エントリだけを変更することでサーバアドレスをダイナミックに変更できます。 このオプションが指定されると、上記「General」内の「Server IP」は無視されます。
IP Address Pool	上記の通り、プライベート IPv4 アドレスのプールから新しい SSL VPN 接続用のクライアント IP アドレスが配布されます。このプールは NetDefendOS のアドレス帳に定義された IP アドレスオブジェクトによって指定されます。また、IPsec と共に使用される IP Pool オブジェクトと同じではありません。 プールアドレスは、連続した範囲である必要はありませんが、同じネットワークに所属する必要があります。Inner IP プロパティも、このネットワークに所属する必要がありますが、プール IP の 1 つである必要はありません。 **注意** プールアドレスは、/24 ネットワークサイズを超過してはいけません。 クラス C サブネットのサイズ（ネットマスク 255.255.255.0 を持つ /24 ネットワーク）を超過する IP アドレスを配布すると、SSL VPN は正しく機能しません。
Primary DNS	接続するクライアントに付与するプライマリ DNS アドレス。
Secondary DNS	接続するクライアントに付与するセカンダリ DNS アドレス。
Client Routing	クライアントソフトがアクティブ化すると、初期値では、すべてのクライアントトラフィックが SSL トンネルを通じて送られます。この動作は、特定の IPv4 アドレス、ネットワーク、またはアドレス範囲がトンネルを通じてアクセスできるように指定することで変更できます。 設定した場合、トンネルを通る特定のルートだけがクライアントのルーティングテーブルに加えられ、他のすべてのトラフィックは通常通り送られます。最大 5 つのカスタムルートをトンネルに指定できます。

Add Route オプション

項目	説明
Proxy ARP	別のイーサネットインタフェースに接続するネットワークが SSL VPN クライアントを検出するように、クライアント IP アドレスについてそのインタフェースで明示的に ARP パブリッシュが行われる必要があります。 この「Add Route」オプションにより、ARP パブリッシュのためのインタフェースを選択することができます。多くの場合、クライアントネットワークをパブリッシュする少なくとも 1 つのインタフェースを選択する必要があります。

10.6.3 SSL VPN クライアントのインストール

SSL VPN が機能するように、所有する D-Link SSL VPN クライアントアプリケーションをクライアントコンピュータにインストールする必要があります。これを以下の手順で行います。

1. Web ブラウザをオープンして、ブラウザのナビゲーションフィールドで、SSL VPN 用に設定されたファイアウォールのイーサネットインタフェースの IP アドレスまたは URL の前にプロトコル「https://」を入力する必要があります。

IP アドレスはインタフェースの SSL VPN オブジェクトで設定した Server IP と同じものとします。また、ポートは初期値 443 と異なる場合、IP アドレスの後に指定します。

https と共に、ファイアウォールは CA 署名を持たないブラウザに証明書を送信し、継続のためにはユーザはこれを例外としてを受け付ける必要があります。

2. NetDefendOS はブラウザのログインダイアログを表示します。

3. 入力した認証情報はユーザデータベースでチェックされます。ユーザを認証する場合、次の 2 つの選択肢を提供する Web ページを表示します。

i. Download the D-Link SSL VPN client software
以前にこのオプションを選んだことがない場合、所有する D-Link SSL VPN クライアントアプリケーションをインストールするために、最初に選択する必要があります。

ii. Connect the SSL VPN client
クライアントソフトウェアがインストール済みである場合、本オプションを選択すると、クライアントの実行は開始し、SSL VPN トンネルがファイアウォールに確立されます。これは、次のセクションで詳しく説明しています。

CA 署名入りの証明書の使用

初期値では、上に示されていたダイアログを表示する時、NetDefendOS は自己署名証明書を使用します。CA 署名入りの証明書の使用を希望するのであれば、証明書チェーンを使用するとは限りませんが、RemoteMgmtSettings オブジェクトで設定することができます。言い換えれば、HTTPS Web インタフェースアクセスに使用する証明書は、SSL VPN ログインに使用するのと同じです。これらの証明書を設定については、「2.1.4 Web インタフェース」でより詳しく説明しています。

クライアント SSL VPN ソフトウェアを実行する

D-Link SSL VPN クライアントアプリケーションが実行される場合にはいつも、SSL VPN トンネルが確立されます。逆に、アプリケーションが実行を止めると、トンネルはダウンします。

トンネルが確立される方法には次の 2 つがあります。

- 上記の通り SSL VPN インタフェースを検索するために Web ブラウザを使用してログインします。クライアントソフトウェアをインストールしたら、トンネルを確立するオプションだけを選択します。
- クライアントソフトウェアをインストールしたら、Windows™ の「スタート」メニューでそれを選択することで開始します。次に、SSL VPN クライアントのユーザインタフェースをオープンし、ユーザパスワードを入力して「OK」ボタンを押すと、トンネルは確立され、クライアントコンピュータのアプリケーションが利用できるようになります。

図 10-9　SSL VPN クライアントのログイン

上の 2 つの手法の違いは、SSL VPN クライアントのソフトウェアが SSL VPN インタフェースに対してブラウジングにより開始された場合、トンネル用の正しい設定が SSL VPN クライアントソフトウェアにダウンロードされて、クライアントの設定ファイルとして保存されるという点です。

これらの設定がトンネルセッション間で変更しない限り、SSL VPN クライアントソフトウェアは「スタート」メニューでそれを選択し、同じ SSL VPN インタフェースに接続することで実行を開始することができます。特に、SSL VPN クライアントは、コンフィグレーション内に保存されている証明書のフィンガープリントをインタフェースが送信したフィンガープリントと比較することによって、SSL VPN インタフェースによって使用される証明書をチェックします。

このように証明書をチェックする理由は、悪意がある第三者がファイアウォールとクライアント間の通信を傍受しようとするかもしれない「中間者攻撃」問題を解決するということです。

カスタムサーバの接続

SSL VPN クライアントソフトウェアを開始する場合、以前に接続したことのない D-Link ファイアウォールにおける SSL VPN インタフェースに接続することができます。オプションの「Specify Custom Server」を有効にして、サーバの IP アドレス、ポート、およびログイン証明書を明示的に指定することで、これを実行します。

「Specify Custom Server」オプションを有効にすると、SSL VPN クライアントは Web インタフェースを使用して確立した SSL VPN 接続によって以前にダウンロードしたどのコンフィグレーションファイルのパラメータも無視します。特に、それはファイアウォールが使用する証明書をチェックしません。

カスタムサーバオプションを使用する短所は、証明書のチェックを行わず、「中間者攻撃」問題は残るということです。

クライアント変換の統計情報

SSL VPN クライアントが動作している場合、アイコンがシステムトレーに表示されます。このアイコンをクリックすると、トンネル設定以降に変換されたデータ量を示すクライアントインタフェースが表示されます。

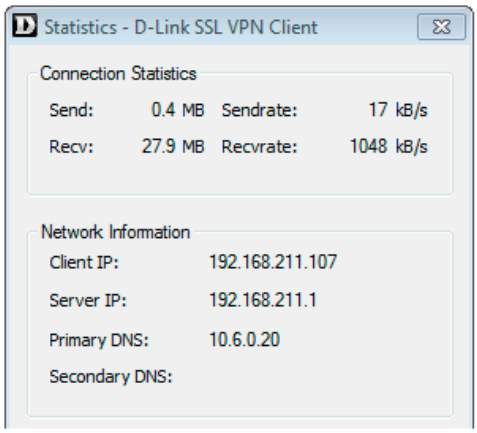


図 10-10 SSL VPN クライアント統計情報

SSL VPN クライアントの操作

SSL VPN クライアントアプリケーションが実行される時にはいつも、以下の処理が生じます。

- ルートが Windows™ のルーティングテーブルに追加されます。このルートは NetDefendOS のデフォルトの「all-nets」ルートと同等です。
- 追加されたデフォルトルートは Windows™ クライアントからのすべてのトラフィックを SSL トンネルを通じて送信します。

  Windows SSL VPN クライアントアプリケーションが終了すると、SSL トンネルはクローズし、Windows™ ルーティングテーブル内のデフォルトルートは削除されます。ルーティングテーブルは元の状態に戻ります。
- SSL 接続は D-Link ファイアウォールの設定済みのイーサネットインタフェースに対して行われ、次に利用可能な IP アドレスは関連する SSL VPN オブジェクトの IP プールからクライアントに付与されます。さらに、クライアント用に 1 つのルートが NetDefendOS ルーティングテーブルに追加されます。

  このルートは付与されたクライアント IP アドレスを関連付けする SSL VPN インタフェースにマップします。
- トラフィックはクライアントとファイアウォール間を NetDefendOS IP ルールに基づいてフローすることができます。

トラフィックフローに IP ポリシーを指定する

Network >Interface and VPN > SSL > Advanced Settings の「SSLVPNBeforeRules」を有効にすると、IP ポリシーは SSL VPN トンネル自身のセットアップに指定する必要はありません。しかし、トンネルを通じたトラフィックのフローを許可するためには、管理者は適切な IP ポリシーを指定する必要があります。

SSL VPN 接続がクライアント側から行われるため、SSL VPN インタフェースオブジェクトは IP ルールのソースインタフェースとするべきであり、ソースネットワークはクライアントに付与可能な IP アドレスの範囲とする必要があります。しかし、ソースネットワークを「all-nets」として設定すると当然動作しますが、通常できるだけ狭い IP アドレス範囲を使用することがより安全となります。

IP ポリシーの指定に関する詳細情報は、「3.6 IP ルールセット」を参照してください。

クライアントの整理

SSL VPN クライアントアプリケーションが何らかの理由で早く終了してしまうと、Windows™ のルーティングテーブルは矛盾のある状態となり、自動的に追加された「all-nets」ルートは削除されない可能性があります。

この問題を改善するために、Windows™ の「スタート」メニューで選択することで D-Link SSL VPN クライアントソフトウェアを開始および停止するべきです。

手動で、クライアントのデフォルトゲートウェイを指定します。

SSL VPN クライアントのサーバへの接続が NAT 変換される場合、DOS コンソールで「route add」コマンドを使用してクライアントのデフォルトゲートウェイへのルートを手動で追加しないことが重要です。

デフォルトゲートウェイがこの方法で追加された場合、リンクが動作を停止する前の短い期間、SSLVPN リンクが確立されて動作し、クライアントが次のメッセージを出します。: SSL stream closed unexpectedly.（SSL ストリームは予期せずクローズしました。）この時にクライアントコンソールが開かれると、SSL ソケットから読んだ時にエラーがあったことを示します。

この問題は、手動でデフォルトゲートウェイルートを加えるのに DOS コンソールを使用しないことで解決されます。代わりに、Windows™ のコントロールパネルを通してこれを行うか、または SSL VPN クライアントソフトによってルートを自動的に追加します。

10.6.4 SSL 設定の例題

例題 10.25

SSL VPN インタフェースをセットアップする

この例では、「my_sslvpn」という名の新しい SSL VPN インタフェースを設定する方法を示しています。

物理インタフェース「If2」がクライアント接続をリッスンするために使用され、アドレス帳に「sslvpn_server_ip」という名の Outer IP アドレスが定義済みであるものとします。SSL VPN を使用して、ファイアウォール「If3」イーサネットインタフェースに接続するネットワークにあるサーバに対して接続が行われます。

また、クライアントに付与可能な IPv4 アドレスが、アドレス帳オブジェクト「sslvpn_pool」に定義されているものとします。これにはアドレス範囲 10.0.0.2-10.0.0.9 を含みます。

別のアドレス帳 IP オブジェクト「sslvpn_inner_ip」は 10.0.0.1 として設定される可能性があり、これはトンネルの NetDefendOS のエンドにある内部 IP です。

手順 1 SSL VPN オブジェクトを作成する

CLI

```
DFL-xxxx:/> add Interface SSLVPNInterface my_sslvpn_if InnerIP=sslvpn_inner_ip IPAddressPool=sslvpn_pool
            OuterInterface=If2 ServerIP=sslvpn_server_ip ProxyARPInterfaces=If3
```

注意 複数のプロキシ ARP インタフェースが必要である場合、「,」（カンマ）で分離したリストで指定されます。例 : If3,If4,If5

Web Interface

1. **Network > Interfaces and VPN > SSL > Add > SSL VPN Interface** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name : 適当な名前を指定します。例：my_sslvpn_if
   - Inner IP: sslvpn_inner_ip
   - Outer Interface: If2
   - Server IP: sslvpn_server_ip
   - IP Address Pool: sslvpn_pool
3. Add Route タブをクリックします。
4. Available リストで If3 インタフェースを選択し、「>>」ボタンを押して、「Selected」リストに移動します。
5. 「OK」ボタンをクリックします。

手順 2 認証ルールを作成する

CLI

```
DFL-xxxx:/> add UserAuthRule Interface=my_sslvpn_if AuthSource=Local LocalUserDB=lannet_auth_users
            OriginatorIP=all-nets Agent=PPP TerminatorIP=sslvpn_server_ip Name=ssl_login
```

Web Interface

1. **Policies > User Authentication > User Authentication Rules > Add > User Authentication Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: ssl_login
   - Authentication Agent: L2TP/PPTP/SSL VPN
   - Authentication Source: Local
   - Interface: my_sslvpn_if
   - Originator IP: all-nets（範囲を特定すると、安全性が高くなります。）
   - Terminator IP: sslvpn_server_ip
3. Authentication Options タブの「Local User DB」で「lannet_auth_users」を選択します。
4. 「OK」ボタンをクリックします。

後は新しい NetDefendOS コンフィグレーションを展開する必要があります。

外部クライアント接続では、Web ブラウザは IP アドレス「my_sslvpn_if」に向けられるべきです。これは、実際の IP アドレスをタイプするか、または IP アドレスに解決できる URL を使用することで、実行されます。

例題 10.26

SSL VPN インタフェースのクライアントルートを設定する

この例題は、SSL VPN トンネル my_sslvpn_if をクライアントのルーティングテーブルに追加されたルートだけが、保護されたネットワーク protected_server_net（NetDefendOS のアドレス帳に定義済みの）へのルートとなるように変更する方法を示します。

CLI

```
DFL-xxxx:/> set Interface SSLVPNInterface my_sslvpn_if Routing=Custom ClientRoutes=protected_server_net
```

Web Interface

1. **Network > Interfaces and VPN > SSL** の順にメニューをクリックします。
2. トンネル my_sslvpn_if を選択します。
3. Client Routing オプションで、アドレスオブジェクトは protected_server_net を Selected から Available に移動します。
4. 「OK」ボタンをクリックします。

第 11 章 トラフィックマネジメント

この章では、NetDefendOS がネットワークトラフィックを管理する方法を記述します。

- 「11.1 トラフィックシェーピング」
- 「11.2 IDP トラフィックシェーピング」
- 「11.3 サーバロードバランシング」

11.1 トラフィックシェーピング

11.1.1 概要

TCP/IP を持つ QoS

TCP/IP の大きな欠点の 1 つは、真の QoS と呼べる機能がないことです。QoS は特定のサービスとユーザのために帯域幅について保証と制限を行う能力です。DiffServ（Differentiated Services）アーキテクチャなどのソリューションは、QoS 情報をネットワーク装置に提供するのにパケットヘッダ内の情報を使用することによって大規模ネットワークで QoS の提供に対処するように設計されています。

NetDefendOS DiffServ サポート

NetDefendOS は、2 つの方法で DiffServ がアーキテクチャをサポートしています。

- はじめに、NetDefendOS は、DSCP（DiffServ Differentiated Services Code Point）を構成する 6 ビットを送信します。
- 次に、本章で後ほど説明されるように、D-LInk ファイアウォールを通過するトラフィックを最優先させることを基本として、DSCP は NetDefendOS トラフィックシェーピングサブシステムによって使用されます。

D-Link ファイアウォールをパケットが横断する場合に、NetDefendOS トラフィックシェーピングが新しい DiffServ 情報を追加しないことを理解することが重要です。本章で後述の NetDefendOS トラフィックシェーピングの優先度は、NetDefendOS 内のトラフィックシェーピングのためにあり、次にパケットに追加される DiffServ 情報には移行されません。

トラフィックシェーピングソリューション

しかし、アプリケーション自身が QoS 情報をネットワークに供給する場合、DiffServ のようなアーキテクチャは実行できません。めったにアプリケーションを動作させない多くのネットワークでは、ネットワークのユーザが自身のトラフィックの優先度を決定します。ユーザを当てにすることができない場合、ネットワーク装置が優先順位と帯域幅割り当てに関して決定をする必要があります。

NetDefendOS は、管理者が D-Link ファイアウォールを通過するネットワークトラフィックに制限と保証を適用できように、QoS コントロールを提供します。この手法は、しばしばトラフィックシェーピングと呼ばれて、より大規模な WAN に発見されるボトルネックを管理するなど LAN の帯域幅を管理するために最適です。VPN トンネルを通過するすべてのトラフィックに適用されます。

トラフィックシェーピングの目的

トラフィックシェーピングは多くの設定パラメータに関して IP パケットを検証および問い合わせを行うことで処理します。目的は以下の通りです。

- 優先度を低く設定されたパケットを待ち行列に入れて帯域制限を行い、帯域幅の需要が低くなってからそれらを送信します。
- パケットバッファがフルになるとパケットを破棄します。破棄されるパケットは輻輳の原因になっているものが選ばれます。
- 管理者の選択によりトラフィックにプライオリティをつけます。通信回線がフルの間に高いプライオリティのものが増えると、プライオリティの低いものは高いトラフィックに道を空けるために一時的に制限されます。
- 帯域幅保証の提供。これは、通常高いプライオリティとして帯域を保証されている特定量のトラフィックを処理することで実行されます。そして、保証を越えたトラフィックは他のトラフィックと同じプライオリティを持ち、残りのプライオリティのないトラフィックと争います。

トラフィックシェーピングは、通常、優先度がないトラフィックを送る前に、大容量データをキューに入れ、プライオリティ付きのトラフィックの仕分けを行うことはしません。そうするよりも、プライオリティのあるトラフィックの量を測り、プライオリティのないトラフィックへの制限をダイナミックに行います。そうすることにより、プライオリティのあるトラフィックのスループットを下げないようにします。

注意 トラフィックシェーピングは、SIP ALG と共に動作しません。

SIP ALG を使用するサービスオブジェクトを持つ IP ポリシーのトリガーとなるあらゆるトラフィック接続もトラフィックシェーピングを免れることはできません。

11.1.2 NetDefendOS におけるトラフィックシェーピング

NetDefendOSは、D-Linkファイアウォールを通過するパケットに大規模なトラフィックシェーピング機能を提供します。異なる通信速度とトラフィックの保証は、IP ルールセットのポリシーが作成されるのと同様に、トラフィックの送信元、送信先およびプロトコルパラメータに基づきポリシーとして作成されます。

NetDefendOS におけるトラフィックシェーピングの 2 つのキーコンポーネント

- パイプ
- パイプルール

パイプ

パイプはトラフィックシェーピングのための基本的なオブジェクトであり、データのパケットが流れる概念的なチャンネルです。それには、通過するトラフィックが処理される方法を定義する様々な特性があります。管理者は必要とされる分の多くのパイプを定義します。初期値は None です。

パイプはかなり単純なもので、通過するトラフィックの種類やその行き先について関知しません。通過するデータを単純に測定し、管理者は、以下の説明するように全体としてパイプに設定した制限を適用するか、Precedences または（および）Groups に制限を適用します。

NetDefendOS は同時に数百のパイプを処理することができます。しかし実際の多くのシナリオでは、少数のパイプを設定するだけ十分です。各プロトコルに対して個別にパイプを設定するシナリオでは、何十ものパイプ設定が必要となるかもしれません。また、個々のパイプが各クライアントに割り当てられるという ISP シナリオでは、大量のパイプが必要であるかもしれません。

パイプルール

1 つ以上のパイプルールでパイプルールセットが構成されます。これは、どのトラフィックがどのパイプを通過するかを決定します。

注意 送信元インタフェースとして any を使用しないでください。

パイプルールにおけるフィルタ条件はできる限り限定的して、特定のインタフェースおよびネットワークに対して起動されることが望ましい動作です。特に、送信元インタフェースとして any を指定することは避けてください。この設定を行うと、シナリオによってはトラフィックシェーピングが同じトラフィックに 2 回適用されてしまいます。

IP ルールセットによって新しい接続が許可されると、一致するパイプルールについて、パイプルールセットがチェックされます。他のルールセットと同様に、上から下（最初から最後）の順でエントリをスキャンします。最初の一致ルール（もしあれば）によって、接続がトラフィックシェーピングの対象となるかどうかが決定されます。パイプルールを起動しない接続はトラフィックシェーピングの対象とならず、最大帯域幅を使用する可能性があります。

パイプルールのルールセットは、初期値で定義されているルールはなく空です。トラフィックシェーピングの機能を開始するためには、少なくとも 1 つのルールを作成する必要があります。

パイプルールチェーン

パイプルールが定義される場合、そのルールと共に使用されるパイプが指定され、それらはパイプルール内にある 2 つのリストうち一方に置かれます。これらのリストは以下の通りです。

- **Forward Chain**
  これらは、ファイアウォールから外向きの（出発する）トラフィックに使用されるパイプです。1 つ、なし、または一連のパイプが指定されます。
- **Return Chain**
  これらは、内向きの（到着する）トラフィックに使用されるパイプです。1 つ、なし、または一連のパイプが指定されます。

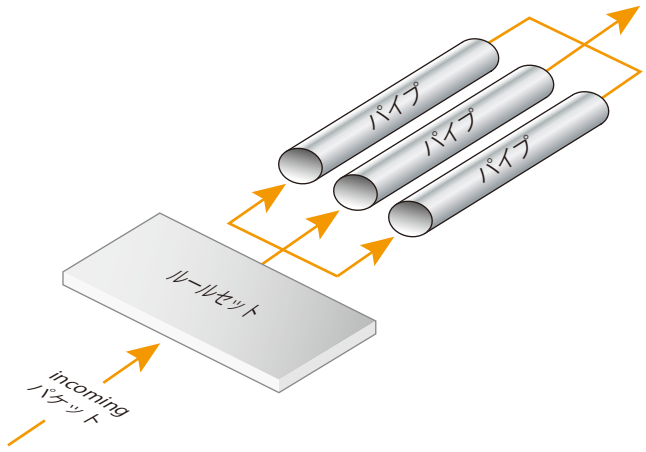


図 11-1　パイプ経由のパケットフロー

使用されているパイプは、パイプリストで指定されます。1 つのパイプが指定されると、それは特性がトラフィックに適用されるパイプです。一連のパイプが指定されると、これらはトラフィックが通過するパイプのチェーンを形成します。チェーンは概ね 8 本のパイプでできています。

シェーピングからトラフィックを明示的に除外する

パイプがパイプルールリストに指定されないと、ルールを始動するトラフィックは、どんなパイプも通過せず、ルールセットにあるどんなパイプルールにも従わないことを意味します。

これは特定のトラフィックを明白にトラフィックシェーピングから除外する手段を提供します。そのようなルールは絶対に必要というわけではありませんが、パイプルールセットの始めに置かれていれば、それらは後のルールによる偶然のトラフィックシェーピングを防御することができます。

パイプ FwdFast IP ルールで動作しない

NetDefendOS IP ルールセットに FwdFast ルールを始動するトラフィックフローを使用してトラフィックシェーピングが動作しないことを理解することが重要です。

これは、接続のトラッキングを行うサブシステムである NetDefendOS ステートエンジンを使用することによってトラフィックシェーピングが実行されないためです。FwdFast IP ルールはステートエンジンで接続を設定しません。代わりに、パケットは接続の一部でないと見なされて、ステートエンジンを迂回しながら個別にそれらの宛先に転送されます。

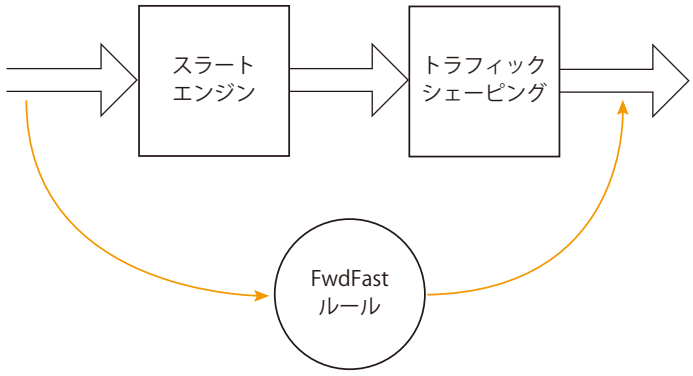


図 11-2　トラフィックシェーピングを迂回する FwdFast ルール

アプリケーションコントロールと共にパイプを使用する

Application Control 機能を使用するとき、特殊なアプリケーション用に帯域幅を定義するために、直接 Application Rule オブジェクトにパイプオブジェクトを関連付けることができます。例えば、BitTorrent peer-to-peer アプリケーションに割り当てられた帯域幅をこのように制限できます。

詳しくは「3.7 アプリケーションコントロール」を参照してください。

11.1.3 シンプルな帯域制限

パイプの基本的な使用は、帯域幅の制限です。さらに、これは多くの計画を必要としないシナリオです。以下の例ではインバウンドトラフィックだけに帯域幅の制限を適用します。これはインターネット接続に最も問題を起こしやすい方向です。

例題 11.1

簡単な帯域制限を適用する

どんなトラフィックであるかに関わらず、2Mbps で転送されるすべてのトラフィックを制限する簡単なパイプの作成から始めます。

CLI

```
DFL-xxxx:/> add Pipe std-in LimitKbpsTotal=2000
```

Web Interface

1. **Policies > Traffic Management > Pipes > Add > Pipe** の順にメニューをクリックします。
2. パイプに適切な名前（例 : std-in）を指定します。
3. Pipe Limits タブで「Total (Kilobits per second)」に 2000 を指定します。
4. 「OK」ボタンをクリックします。

しかし、パイプを簡単に作成しても、多くを実行することはできません。実際にはトラフィックはパイプ経由で送信される必要があります。これは IP ルールにパイプを割り当てることによって行われます。

ここでは上記の内向きトラフィックを制限するためにパイプを使用します。この制限は、実際のデータパケットに適用され、接続には適用されません。また、接続を開始したコンピュータではなく、データがシャッフルされている方向に注目します。

すべてが内側から送信されることを許可する単純なルールを作成します。さらに、リターンチェーンに作成したパイプを追加します。これは、この接続（outside-in）のリターン方向に移動するパケットが、「std-in」パイプを通過するべきであることを意味しています。

CLI

```
DFL-xxxx:/> add PipeRule ReturnChain=std-in SourceInterface=lan SourceNetwork=InterfaceAddresses/lannet
            DestinationInterface=wan DestinationNetwork=all-nets Service=all_services name=Outbound
```

Web Interface

1. **TrafficManagement > Traffic Shaping > Add > Pipe Rule** の順にメニューをクリックします。
2. パイプに適切な名前（例 : outbound）を指定します。
3. 以下の情報を入力します。
   - Service: all_services
   - Source Interface: lan
   - Source Network: lannet
   - Destination Interface: wan
   - Destination Network: all-nets
4. Traffic Shaping タブの「Return Chain」で「std-in」を選択し、「Selected」リストに移動します。
5. 「OK」ボタンをクリックします。

この設定は、外部からのすべてのトラフィックを 2Mbit/ 秒に制限します。どの優先順位も適用されず、どのダイナミックバランシングも行われません。

10.1.4 双方向の帯域制限

単一のパイプを使用する

単一のパイプは、通過の合計を計算する場合、トラフィックがどの方向から来るのかを気にかけません。内向きと外向きトラフィックの両方に同じパイプを使用することは NetDefendOS に許可されますが、それは双方向のパイプの制限を適切に区切ることはありません。以下のシナリオがこれを明確にします。

前の例題では内向き方向だけに帯域幅を制限しています。ここでは、多くの設定でそれが最初にフルになる方向であるためにこの方向を選択しました。今度は両方向に外向きの帯域幅を制限したい場合にどうするべきか検討します。

2Mbps の外向きトラフィックを 2Mbps の内向きトラフィックからとは区別したいために forward chain に std-in を挿入するだけでは動作しません。2Mbps の内向きトラフィックに加えて、パイプを経由して 2Mbps の外向きトラフィックを通過させると、計 4Mbps になります。パイプの制限が 2Mbps であるため、実行できるのは各方向に 1Mbps 程度となります。

4Mbps 合計パイプの制限を上げても、一つのパイプが内向き 2Mbps、外向き 2Mbps に意図されていることを知らないため、問題は解決しません。合計 4Mbps になっても、外向き 3Mbps と内向き 1Mbps という結果になるかもしれません。

代わりに 2 つに分けたパイプを使用する

双方向における帯域管理の推奨方法は、2 つのパイプ（一方は内向き、他方は外向きトラフィック）を使用することです。説明中のシナリオでは、各パイプには希望の結果となるように 2Mbps の制限があります。以下の例ではこれに関する設定を行います。

例題 11.2

2 方向の帯域制限を適用する

この例題では、以前の例題を既に実施しているものとします。

外向きトラフィックに対して 2 つ目のパイプを作成する。:

CLI

```
DFL-xxxx:/> add Pipe std-out LimitKbpsTotal=2000
```

Web Interface

1. **Policies > TrafficManagement > Pipes > Add > Pipe** の順にメニューをクリックします。
2. パイプに適切な名前（例 : std-out）を指定します。
3. 「Total (Kilobits per second)」に 2000 を指定します。
4. 「OK」ボタンをクリックします。

外向き帯域制御に対してパイプを作成した場合、前の例で作成したルールのパイプチェーンに追加する :

CLI

```
DFL-xxxx:/> set PipeRule Outbound ForwardChain=std-out
```

Web Interface

1. **TrafficManagement > Traffic Shaping > Pipe Rules** の順にメニューをクリックします。
2. 前に作成したパイプルール上で右クリックし、「Edit」ボタンをクリックします。
3. Traffic Shaping タブの「Forward Chain」で「std-out」を選択し、「Selected」リストに追加後、「OK」ボタンをクリックします。

これにより、すべての外向き接続が各方向に対して 2Mbps に制限されます。

11.1.5 チェーンを持つ Differentiated Limit の作成

前の例題では、すべての外向き接続にスタティックなトラフィック制限が適用されました。今度は他のトラフィック以上にネットサーフィンを制限したい場合、何をすべきか検討します。総帯域幅制限は 250Kbps であり、Web のネットサーフィンの内向きトラフィックに 125Kbps が割り当てられていると仮定します。

不正確なソリューション

ここでは、内向き、外向きの 2 つの「surfing」パイプを設定します。しかし、通常外向きトラフィックを制限する必要はありません。これは、Web サーフィンは通常長い内向きの答えに従う短い外向きのサーバリクエストで成り立っているためです。

「surf-in」パイプは、そのため、最初に 125Kbps 制限で内向きトラフィックに作成されます。次に、新しいパイプルールは「surf-in」パイプを使用するサーフィンに設定され、「std-in」パイプを通じて「すべてのもの」を指示するルールの前に置かれます。このようにサーフィントラフィックは「surf-in」パイプを通過し、すべてが先に作成済みのルールとパイプに処理されます。

残念ながら、合計 250Kbps の一部分として内向きのサーフィントラフィックに最大 125Kbps を割り当てるという希望した結果にはなりません。内向きトラフィックは 2 つのパイプの 1 つを通過します。一方は 250Kbps が可能で、他方は 125Kbps が可能で、内向きトラフィックの合計は 375Kbps となりますが、これは実際の制限 250Kbps を超えています。

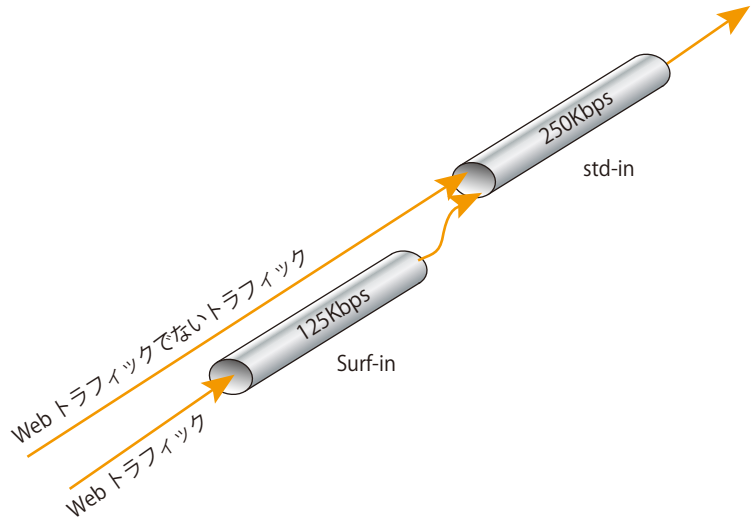


図 11-3　チェーンを使用した Differentiated Limits

そのため、125Kbps の制限帯域でサーフィンする場合、125Kbps が「std-in」パイプの半分を占有します。何のサーフィンもなければ、「std-in」パイプ経由を許可された 250Kbps すべてが、残りのトラフィックに使用可能になります。

これを解決するために、サーフィンするトラフィックパイプルールにおける「std-in」入力パイプに従って「surf-in」パイプのチェーンを作成します。次に、内向き surf トラフィックは、「surf-in」をはじめに通過し、最大 125Kbps に制限されます。その後、残りの内向きトラフィックと共に「std-in」パイプを通過し、合計 250Kbps の制限を適用します。

これは Web 閲覧のための帯域幅保証を提供しませんが、代わりに 125Kbps に制限し、すべてに対して 125Kbps の帯域保証を提供します。Web 閲覧のために、先入れ先出しの普通のルールが 125Kbps 帯域の取り合いの場合に適用されます。これは、125Kbps を意味していますが、ご使用の接続がフラッドされている場合、より低速であることを意味します。

このようにパイプの設定は、特定のトラフィックタイプに対する最大値を制限するだけです。これは、競合する異なるタイプのトラフィックにプライオリティを付与しません。

11.1.6 優先度

優先度の初期値は 0

NetDefendOS トラフィックシェーピングパイプを通過するすべてのパケットが優先度を持っています。今までのところの例では、優先度が明確に設定されていないため、すべてのパケットは、同じデフォルト優先度の 0 を持っています。

8 個の可能な優先度レベル

8 個の優先度（0 から 7 までの番号）があります。優先度 0 は、最も重要度が低い優先度（最低優先度）で、7 が最も高い重要（最高優先度）です。優先度は、個別のトラフィックキューとして参照されます。優先度 2 のトラフィックは、優先度 0 のトラフィックの前に転送され、優先度 4 のトラフィックは、優先度 2 の前に転送されます。

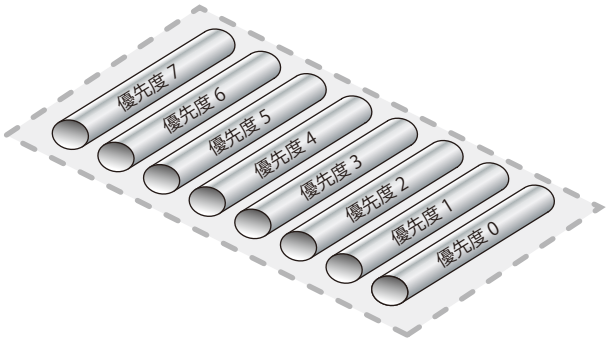


図 11-4　8 個のパイプ優先度

優先度は相対的である

優先度は、別の優先度よりもより高い、または低いという事実から来ており、番号からではありません。例えば、2 つの優先度がトラフィックシェーピングのシナリオで使用される場合、0 と 3 の代わりに 4 と 6 の優先度を選択しても結果に違いはありません。

トラフィックへの優先度の割り当て

優先度がパケットに割り当てられる方法は、それを制御するパイプルールによって決定され、3 つの方法の 1 つが実行されます。

- 最初のパイプの優先度を使用する。
  各パイプは、デフォルト優先度を持ち、パケットはそれらが通過する最初のパイプのデフォルト優先度を取得します。
- 割り当てられた優先度を使用する。
  パイプルールは明確に優先度を割り当てます。
- DSCP ビットを使用する。
  パケット内の DSCP ビットからパケットを取得します。DSCP は、Type of Service（ToS）ビットが IP パケットヘッダに含まれている DiffServ アーキテクチャのサブセットです。

パイプに優先度を指定する

パイプが設定される場合、デフォルト優先度、最小優先度および最大優先度が指定されます。デフォルト優先度は以下の通りです。

- 最小優先度 : 0
- デフォルト優先度 : 0
- 最大優先度 : 7

デフォルト優先度は、前の項で記述したようにパイプルールによって明確に割り当てされていないとパケットが取得した優先度になります。

最小優先度および最大優先度はパイプが処理する優先度範囲を定義します。パケットが最小優先度よりも低い優先度が既に割り当てられて到達する場合、その優先度は最小に変更されます。同様に、パケットが最大優先度よりも高い優先度が既に割り当てられて到達する場合、その優先度は最大に変更されます。

各パイプに対して、個別の帯域制限が、オプションで各優先度レベルに指定されるかもしれません。
これらの制限値は kbit/ 秒および（または）パケット / 秒で指定されます。両方が指定されると、はじめに到達した制限が使用される制限となります。

優先度が使用される場合、全体としてパイプの制限の合計が指定される必要があり、それのよってパイプは容量がどのくらいであるか、いつ優先度が使用されるかを理解します。

注意　帯域幅を指定する

ネットワークトラフィック帯域幅を指定する場合、接頭語の Kilo は 1024 ではなくて 1000 を意味することを覚えていてください。例えば、3Kbps は 3000 ビット / 秒を意味します。

同様に、接頭語 Mega はトラフィック帯域幅で 100 万を意味します。

優先度制限は保証でもある

優先度制限は制限と保証の両方を意味します。優先度に指定された帯域幅は、また帯域幅がより低い優先度を犠牲にして有効になることを保証します。特定の帯域幅が超えると、超過分のトラフィックは最も低い優先度に落とされます。最も低い優先度には、次に説明される特別な意味があります。

最低（ベストエフォート）優先度

最小パイプ優先度として定義される優先度には、特別な意味があります。それは、ベストエフォートの優先度として動作します。この優先度で処理されるすべてのパケットは、「先入れ、先出し」を基本にいつも処理されます。

ベストエフォートより高い優先度を持ち、その優先度の制限を超えたパケットは、自動的に最低優先度（ベストエフォート）に転送され、最低優先度を持つパケットと同様に処理されます。

以下の図は、最低優先度は 2、最高優先度は 6 です。優先度 2 はベストエフォート優先度としてみなされます。

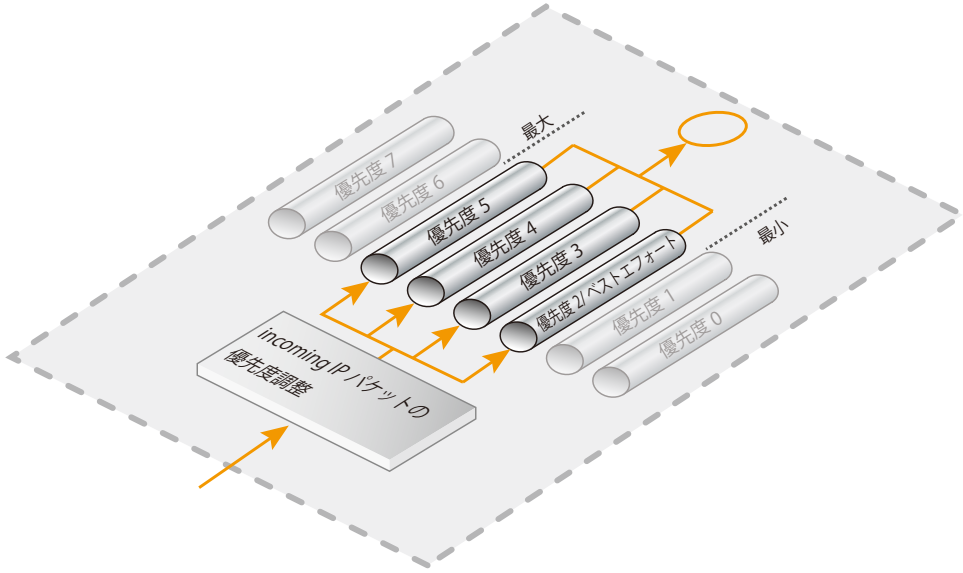


図 11-5　パイプ優先度の最小値と最大値

最低優先度の制限

この優先度が単純により高い優先度では使用されない予備帯域幅を使用するため、通常は最低（ベストエフォート）優先度に制限を指定する必要はありません。しかし、最低優先度によって使用される帯域幅を制限する必要があれば、制限値を指定します。これは、特定のトラフィックタイプが最低優先度を持っているが、制限された帯域幅を利用する必要がある場合です。

優先度はパイプが一杯の時だけ適用される

パイプに割り当てられた総帯域幅に到達するまで、優先度は効果はありません。優先度間に競争がない場合、パイプ制限に到達する（パイプが一杯になる）までこれが当てはまります。

パイプが一杯の時に、NetDefendOS は、低い優先度のパケットの前に送信される優先度制限を超えない範囲でより高い優先度のパケットを持つトラフィックを最優先にします。最低優先度のパケットは、送信されるまでバッファにおかれ、バッファスペースが枯渇すると、それらは破棄されます。

パイプに合計の制限値が指定されないと、パイプは無制限の帯域幅を持ち、その結果フル状態にはならないと、優先度は意味がないと言えます。

優先度の適用

続いて、SSH と Telnet トラフィックが他のトラフィックより高い優先度を持つようなリクエストを追加します。これを行うためには、SSH と Telnet のために特別にパイプルールを追加して、ルールにより優先度が高くなるように優先度（例えば 2）を設定します。他のトラフィックに使用されるこの新しいルールに同じパイプを指定します。

これにより、SSH と Telnet ルールはこれらのサービスに関連するパケットにより高い優先度を設定し、これらのパケットは他のトラフィックと同じパイプ経由で送信されます。そして、パイプは、パイプ設定内に指定された総帯域幅の制限を超えた場合に、これらの高い優先度のパケットがはじめに送信されることを確実にします。高い優先度のトラフィックがパイプに指定されている最大優先度よりも低いものを使用する場合、低い優先度のパケットはバッファにおかれてから送信されます。バッファリング処理は、フロー速度を低下させるため、「スロットリングバック」と呼ばれます。

保証の必要性

しかし、最優先するトラフィックがリアルタイムオーディオなどの連続のストリームであると、連続してすべての利用可能な帯域幅を使用するため、ネットサーフィン、DNS または FTP などの他のサービスに対しては受け入れがたいほど長い待ち時間となるなどの問題が発生します。
低い優先度のトラフィックが帯域の一定部分を取得することを保証するための方法が必要とされ、これは Bandwidth Guarantees で保証されます。

保証として優先度を使用する

帯域幅保証の制限を指定することは、その優先度には利用可能な最低帯域幅があることを保証するものです。パイプを通じて流れるトラフィックは、低い優先度を持つトラフィックを犠牲にしてそれが持つ優先度に指定された保証を受けます。

前の例題から優先度を付与された SSH と Telnet トラフィックを 96Kbps 保証に変更するためには、std-in パイプに対する優先度 2 の制限を 96Kbps に設定します。

これは、内向き SSH と Telnet トラフィックは 96Kbps に制限されることを意味するわけではありません。ベストエフォート優先度を超える優先度の制限は、特定の優先度にトラフィックを渡す量の制限だけを行います。

96Kbps 以上の優先度 2 トラフィックが到着すると、どんな余分なトラフィックもベストエフォート優先度まで移行します。ベストエフォート優先度の全パケットが「先入れ先出し」を基本として送信されます。

注意 最も低い優先度への制限には意味がありません。
最も低い（ベストエフォート）の優先度または低い優先度に最大の制限を設定しても意味がなく、NetDefendOS に無視されます。

Differentiated 帯域保証

Telnet のトラフィックに特別に 32Kbps の保証を、SSH トラフィックに 64Kbps の保証を付与したい場合、検討すべき問題があります。優先度 2 には 32Kbps の制限を、優先度 4 には 64Kbps の制限を設定し、各優先度を通じて異なるタイプのトラフィックを通過させることができます。しかし、このアプローチには明確に 2 つの問題があります。

- どのトラフィックが、より重要であるのか。この課題はここではそれほど問題となりませんが、トラフィックシェーピングのシナリオが複雑になるにつれて、より重要になります。
- 優先度の数は制限されます。これは、いずれのシナリオにおいても（「どのトラフィックがより重要か」という課題を除いた場合でさえ）十分ではないかもしれません。

ここでの解決策は、前に作成した「surf」パイプと同様に telnet トラフィックと SSH トラフィックの 2 つのパイプを作成することです。

はじめに、「std-in」パイプから 96Kbps の制限を削除し、2 つの新しいパイプ、「ssh-in」と「telnet-in」を作成します。両方のパイプのデフォルト優先度を 2 に設定し、優先度 2 の制限値を、それぞれ 32Kbps、64Kbps に設定します。

その後、ポート 22 から 23 をカバーするように前に定義したルールを、それぞれ 22 と 23 をカバーするように 2 つに分割します。

両方のルールの転送チェーンを「std-out」とします。改めて、この例題を簡略化するために、（クライアント指向の設定において最初に設定される想定の）内向きトラフィックだけに着目します。

「std-in」に追随する「ssh-in」にポート 22 のルールのリターンチェーンを設定します。
「std-in」に追随する「telnet-in」のポート 23 にリターンルールを設定します。
両方のルールについて、優先度を「Use defaults from first pipe」に設定します。「ssh-in」と「telnet-in」パイプ両方のデフォルト優先度は 2 です。ルールセットの優先度 2 よりもむしろこのアプローチを使用して、単にパイプ「ssh-in」と「telnet-in」のデフォルト優先度を変更することにより簡単にすべての SSH および Telnet トラフィックの優先度を変更することができます。

「ssh-in」と「telnet-in」パイプの合計の制限を設定しなかったことに注目してください。合計制限値は、各チェーンの最後にある「std-in」によって実施されるため、設定する必要はありません。

「ssh-in」と「telnet-in」パイプは「プライオリティフィルタ」として動作します。これにより、優先度 2 でそれぞれ予約されている 64Kbps と 32Kbps を超えるトラフィックが、「std-in」に到達しないようにします。それらの保証を超過している SSH と telnet トラフィックは優先度 0 で「std-in」と「ssh-in」パイプのベストエフォートとして「std-in」に到着します。

注意 リターンチェーンの順序が重要です。
ここでは、リターンチェーン内のパイプの順番が重要です。「std-in」が「ssh-in」と「telnet-in」の前に配置されている場合、トラフィックは「std-in」に優先度 0 で到達するため、利用可能な帯域 256Kbps を他のすべてのトラフィックと競い合います。

11.1.7 パイプグループ

NetDefendOS はグループ内の個別のリソースユーザにパイプ帯域幅を分割することでパイプ内により詳しい制御レベルを提供します。
以下の 1 つに従って、各ユーザを識別することができます。

- 送信元 IP
- 送信先 IP
- 送信元ネットワーク
- 送信先ネットワーク
- 送信元ポート TCP（IP を含む）
- 送信先ポート（IP を含む）
- 送信先インタフェース
- 送信元インタフェース

この機能は、パイプで Grouping オプションを可能にすることで、有効になります。そして、グループの個々のユーザはパイプ内のそれらに指定された制限および / または保証を持つことができます。例えば、送信元 IP でグループ化する場合、各ユーザはそれぞれのユニークな送信元 IP アドレスに対応します。

ポートのグループ化は IP アドレスを含む

ポートによるグループ化が選択される場合、これは暗に IP アドレスを含んでいます。例えば、ホストコンピュータ A のポート 1024 はホストコンピュータ B のポート 1024 と同じではありません。それは、グループでユニークなユーザを識別するポートと IP アドレスの組み合わせです。

ネットワークごとのグループ化にはサイズが必要である

送信元または送信先ネットワークによってグループ化が行われる場合、ネットワークサイズを指定する必要があります。つまり、ネットワークのネットマスクを NetDefendOS に指定する必要があります。

グループの制限値を指定する

グループ化の方法を選択後、Group Limits を指定します。これらの制限値は以下の 1 つ、または両方から構成されます。

- **グループ制限値の合計**
  この値はグループ化の中で各ユーザに制限を指定します。例えば、グループ化が送信元 IP アドレスによって行われて、指定された合計が 100Kbps であると、100Kbps より大きい帯域幅を持つ IP アドレスはないということになります。
- **グループ優先度保証**
  さらに、合計グループ制限に代わるものとして、個別の優先度が指定された値を持っています。事実、これらの値はグループ内の各ユーザのための保証（制限ではない）です。例えば、優先度 3 には 50Kbps の値があり、優先度を持つ各ユーザ（つまり、グループ化を選択した場合には各送信元 IP）はより低い優先度の犠牲の下に 50Kbps を保証されると言えます。各ユーザの優先度は、特定ユーザに始動する異なるパイプルールにより割り当てる必要があります。

  例えば、グループ化が送信元 IP による場合、異なるパイプルールは違う IP で始動し、適切な優先度を持つ同じパイプにトラフィックを送信します。

  優先度値の潜在的合計が明確にいくつかの環境でパイプの容量より大きくすることができてから、これらの保証を使用する時の総パイプ制限を指定するのが重要です。

グループ合計と優先度を組み合わせる

グループ優先度とグループ合計の使用を結合することができます。これは以下のことを意味します。

- グループ内のユーザを最初にパイプルールによって優先度に分けます。
- ユーザは、その後、それらの優先度に指定された保証を受けることができます。
- 結合したトラフィックは総グループ制限を受けます。

以下の図は、送信元 IP に従ってグループ化が選択されたフローを示しています。

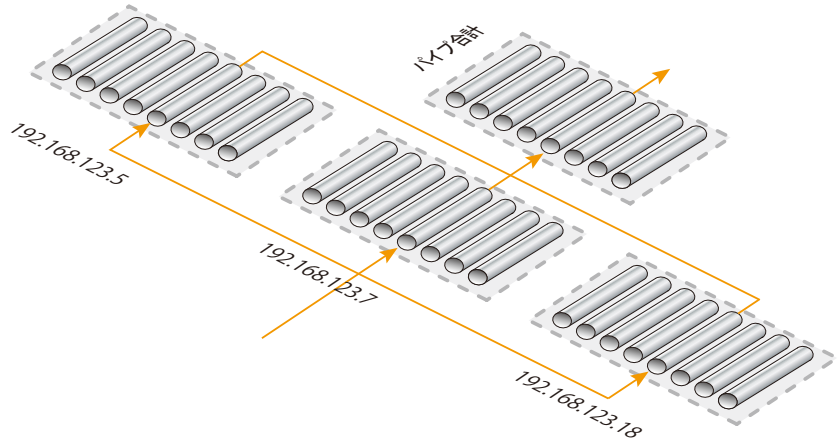


図 11-6　IP アドレス単位でグループ化されたトラフィック

別のグループの簡単な例題

パイプの総帯域幅制限が 400bps である別の状況を考えてみます。多くの宛先 IP アドレスにこの帯域幅を割り当てて、それらの IP アドレスがすべて帯域幅 100bps を超えないようにする場合、以下の手順が必要です。

- パイプ制限は通常通りの 400bps を設定します。
- 送信先 IP の値を持つようにパイプに対してグループ化オプションを設定します。
- パイプのグループ制限の合計を 100bps に設定します。

この時帯域幅は「先入れ、先出し」に基づいて割り当てられますが、宛先 IP アドレスが 100bps を超えることはありません。また、接続数が増えても、総帯域幅が 400 bps のパイプ制限を超えることはありません。

パイプとグループ制限優先度値の組み合わせ

グループ化が送信元 IP などのオプションの 1 つで有効にされて、優先度のいくつかの値がグループ制限値より下に指定されているものとします。これらをパイプ制限に対応する優先度に指定される値に組み合わせる方法を考えてみます。

この場合、グループ制限優先度値は保証され、同じ優先度のパイプ制限値が限界です。例えば、トラフィックは送信元 IP ごとにグループ化され、グループ制限優先度 5 の値は 5Kbps、パイプ制限優先度 5 の値は 20Kbps である場合、4 番目のユニークな IP（4 x 5 = 20 Kbps）の後、優先度制限値は到達し、保証はもはや受けられなくなります。

ダイナミックバランシング

総グループ制限を指定する代わりに、ダイナミックバランシングオプションを有効にすることができます。このオプションにより、すべてのアドレスがその数に関わらず、利用できる帯域幅に均等に分配され、パイプ制限までこれが行われます。総グループ制限の 100 bps をダイナミックバランシングに指定している場合、ユーザはそれ以上の帯域幅を使用しません。

優先度とダイナミックバランシング

既に説明した通り、グループに総制限を指定するだけでなく、制限にグルーピング内の各優先度を指定することができます。30bps のグループ制限に優先順位 2 を指定すると、パイプルールに優先度 2 を割り当てられたユーザは、パイプを使用するユーザ数に関わらず、30bps まで保証されます。通常のパイプ優先だけでは、優先順位 2 を持つユーザが 30bps を超えるトラフィックを送信すると、ベストエフォート優先順位が格下げになります。

前の例では、各内部ユーザがインバウンド SSH トラフィックを受け取るために保証される帯域幅を制限できます。これにより、優先順位の高い利用可能な帯域幅を 1 つのユーザがすべて使いきってしまうことを防げます。
最初に、ssh-in パイプのユーザをグループ化するため、制限は内部ネットワークの各ユーザに適用されます。パケットが到着した後、ssh-in パイプのグルーピングを「Destination IP（宛先 IP 単位）」で行うよう選択します。

ここで、優先順位 2 の制限をユーザあたり 16Kbps に設定することによって、ユーザ単位の制限を指定します。これは、各ユーザが SSH トラフィックにおいて 16Kbps 以上保証されないことを意味します。好みに応じて、ユーザごとにグループ総帯域幅を 40Kbps などの値に制限することもできます。

SSH を 5 ユーザ以上が同時に使用する場合、問題となります。16Kbps を 5 倍すると、64Kbps を超えてしまいます。パイプの総制限を用いることがやはり効果的であり、各ユーザは、優先順位の最も低い帯域幅を競合的に使用するのと同様に、利用可能な優先順位 2 の帯域幅も競合的に使用するのがよい方法です。何人かのユーザはまだ 16Kbps で利用可能です。
ダイナミックバランシングを有効にしてこの状況を改善することができ、これにより 5 ユーザすべてが、制限された帯域幅を同じだけ使用できます。5 番目のユーザが SSH トラフィックを生成し始める時、バランシングは、ユーザあたりの制限をおよそ 13Kbps（64Kbps を 5 ユーザで割った値）に下げます。

ダイナミックバランシングは、各パイプの優先順位内で個別に実行されます。これは、ユーザが、ある少ない高優先トラフィックと、ベストエフォートトラフィックのより大きなチャンクを割り当てられる場合、すべてのユーザが、高優先順位のトラフィックだけでなく、ベストエフォートトラフィックも平等に共有することを意味します。

11.1.8 VPN とトンネルにおけるトラフィックシェーピング

IPsec やその他のトンネルプロトコルでトラフィックシェーピング機能を使用する場合、以下の点に注意する必要があります。

・トンネルでオーバーヘッドが発生する

VPN トンネル内でトラフィックを計測するためにトラフィックシェーピングを設定する場合、オーバーヘッドがない未処理のデータとなることに注意してください。つまり、トラフィックを送信するトンネルで使用される帯域よりも通常少なくなります。IPsec などの VPN プロトコルでは、データ制限と暗号化により、データに大幅なオーバーヘッドが発生します。トンネル化された IPsec データに対するトラフィックシェーピングパイプで、実際に利用可能な帯域より 20% 程度少ない値に設定することを推奨します。

・パイプルールはトンネルまたはトンネル内のデータによって起動される

トンネルまたはトンネル化されたデータに対して起動する Pipe Rule オブジェクトを設定し、トラフィックシェーピングを実行することができます。トンネルで起動するパイプルールを使用することが推奨されます。この場合、トラフィックシェーピングによりトンネル内側ではなく外側のデータが測定されるため、上記の帯域問題を回避することができます。

Pipe Rule がトンネル自体に対して起動される場合、Pipe Rule の Source Interfece プロパティを core に指定する必要があります。any に指定するとルールが 2 回（トンネルとトンネルデータに対して）起動してしまう可能性があるため、そのように設定することは避けてください。

11.1.9 トラフィックシェーピング推奨事項

パイプ制限の重要性

トラフィックシェーピングは、NetDefendOS パイプが一杯の時だけ効果を発揮します。これはつまり、総制限が許可する限りのトラフィックを通します。500Kbps のパイプが低優先順位のトラフィック 400Kbps と高優先のトラフィック 90Kbps を通信させる場合は、帯域幅に 10Kbps の余裕があるため、通信が制限される原因にはなりません。このため、トラフィックシェーピングにおいてパイプの通信量が分かるよう、パイプの総制限を指定することが重要であり、優先順位方式は完全にこの機能に依存します。

グループ制限に依拠する

総パイプ制限が指定されない特殊なケースは、グループ制限が代わりに使用される場合です。その時帯域幅制限が用いられるので、その場合、例えば、ネットワークの各ユーザが固定の帯域幅リソースを共有する必要があります。ISP ではこの方法が使用されることもあり、「Destination IP」グルーピングを指定することにより、個々のユーザ帯域幅を制限します。唯一の制約は各ユーザにかけられているため、パイプが一杯になったことを知ることは重要ではありません。優先順位が使用されている場合は、パイプ最大値が使用されます。

制限は、利用できる帯域幅を超えてはいけない

パイプ制限が利用できる帯域幅より大きい場合、パイプは、物理的な接続が限界に達してもそれを認識しません。接続が 500Kbps で、総パイプ制限が 600kpbs に設定されている場合、パイプは一杯ではないと認識し、優先順位を低く下げません。

制限は、利用できる帯域幅よりもわずかに低くする

パイプ制限は、ネットワーク帯域幅よりもわずかに低くしてください。推奨は、パイプ制限を物理的な制限の 95% にすることです。全帯域幅の中で 5% は大きいので、帯域幅が増えるにつれてこの差異は不要になります。

パイプ制限を低くする根拠は、NetDefendOS がトラフィックを処理する方法にあります。パケットがファイアウォールを離れるアウトバウンド接続では、パケットの送信を決定する際のソフトウェアの遅延と、パケットが実際にはバッファから発信されることから、NetDefendOS が接続をわずかにオーバロードしてしまう可能性があります。

インバウンド接続では、到着するパケットの制御が少なく、トラフィックシェーピングサブシステムによって処理される事柄があることから、NetDefendOS が状況の変化に慣れるために要する時間を考慮し、実際の接続制限をわずかに下回るパイプ制限を設定することが重要です。

帯域幅への攻撃

トラフィックシェーピングは、DoS 攻撃やその他フラッド攻撃など、襲ってくるリソース消費攻撃を阻止することはできません。NetDefendOS は、ファイアウォール背後のホストから送られてくる以外のパケットを回避しますが、もし攻撃によりオーバフローが生じた場合、接続がオーバロードに陥ることは回避できません。

リークを監視する

ネットワークのボトルネックを阻止および形成するよう設定した場合、このボトルネックを通過するすべてのトラフィックは必ず、定義済みの NetDefendOS パイプを通過します。

パイプの知らないインターネット接続を経由するトラフィックがあった場合、NetDefendOS はこのインターネット接続が一杯になってもそれを認識できません。リークから生じる問題は上記の場合とまったく同じです。パイプに測定されないトラフィックの「リーク」は、管理者の管理対象外にあって同じ接続を共有する第三者が帯域幅を消費することと同様の影響があります。

トラブルシューティング

実際の設定で何が起こっているのかを詳しく知るために、次のコンソールコマンドが使用できます。

```
DFL-xxxx:/> pipe -u <pipename>
```

これにより、各パイプにおける現在のアクティブユーザの一覧が表示されます。

11.1.10 トラフィックシェーピングの概要

NetDefendOS トラフィックシェーピングは、ネットワークパケットの制御および優先付けを行う高度なメカニズムを提供します。使用について以下のポイントに要約します。

- パイプルールにより管理するトラフィックを選択します。
- パイプルールは、パイプを通してトラフィックを送信します。
- パイプは、認められるトラフィックの最大量の制限を持つことができます。
- パイプは、パイプの総制限が指定されている場合のみ、一杯になったことを認識できます。
- 1 つのパイプでは、一方方向のトラフィックだけを扱うことが必要です（ただし、双方向のパイプも可能です）。
- パイプのトラフィックが別のパイプに送り込めるよう、パイプはつなぐことができます。
- 特定のトラフィックタイプにパイプの優先順位を与えることができます
- 保証でもある最大制限を優先順位に与えることができます。これを超えるトラフィックは、ベストエフォート優先順位とも呼ばれる最低優先のパイプに送信されます。
- ベストエフォート優先順位では、すべてのパケットが「先着順」に扱われます。
- パイプ内で、グループを基にトラフィックを分割することもできます。例えば、送信元 IP アドレス単位で分割することができます。グループ内（例えば、各送信元 IP アドレス）の各ユーザは、制限 / 保証の与えられるグループにおいて、最大の制限および優先順位を与えられることができます。
- グループメンバが最大制限を持つ場合、パイプ制限を指定する必要はありません。
- ダイナミックバランシングを使用して、グループのすべてのユーザが公平かつ平等に帯域幅を使用できるよう指定できます。

11.1.11 パイプの例

本セクションでは、さらに多くのシナリオを紹介し、特定の問題を解決するために、どのようにトラフィックシェーピングを使用するかを説明します。

基本的なシナリオ

最初のシナリオでは、以下の図で示すように構成を検証します。ここでは送受信のトラフィックが 1 メガビット / 秒に制限されています。

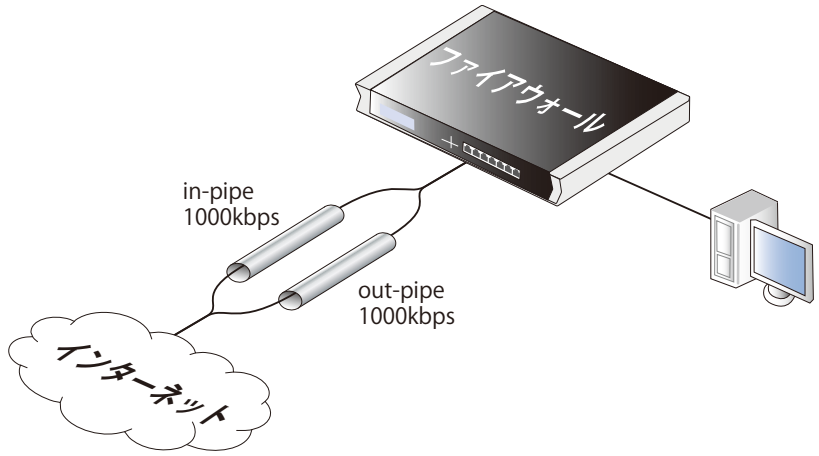


図 11-7　基本的なトラフィックシェーピングのシナリオ

この場合に 2 つの異なるパイプを使用するのは、これらが物理リンクの性能に一致しやすいためです。これは、ADSL などの非同期なリンクでは事実です。

最初に、in-pipe および out-pipe と呼ばれる 2 つのパイプを以下のパラメータを使用して作成します。

パイプ名	Min Prec	Def Prec	Max Prec	Grouping	Net size	Pipe limit
in-pipe	0	0	7	PerDestIP	24	1000kbps
out-pipe	0	0	7	PerSrcIP	24	1000 Kbps

ダイナミックバランシングを両方のパイプに有効とします。PerDestIP と PerSrcIP の代わりに、いくつかのネットワークが内部にあると、PerDestNet と PerSrcNet を使用することができます。

次に、トラフィックがパイプを通過する以下のパイプルールを作成します。

ルール名	Forward Pipes	Return Pipes	送信元ネットワーク	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス
all_1mbps	out-pipe	in-pipe	lan	lannet	wan	all-nets	all_services

ルールはすべてのトラフィックをデフォルト優先度レベルにして、パイプは総トラフィックを 1Mbps に制限します。パイプでダイナミックバランシングを有効にすることは、この容量に関する公正な割り当てがすべてのユーザに行われることを意味します。

複数の優先度を使用する

本社からインターネットをアクセスする異種のトラフィックに優先度を割り当てることによって上記例題を拡張してみます。

インターネットに対して対称の 2/2Mbps リンクを持つものとします。以下のユーザに降順の優先度とトラフィック要求を割り当てます。

- 優先度 6 - VoIP（500kpbs）
- 優先度 4 - Citrix（250kpbs）
- 優先度 2 - 他のトラフィック（1000kpbs）
- 優先度 0 - Web+ 他のレベルからの残り

この体系を実行するために、in-pipe と out-pipe を使用します。はじめに各パイプに Pipe Limits を入力します。これらは上記のリストに対応しています。

- 優先度 6 - 500
- 優先度 4 - 250
- 優先度 2 - 1000

次に、パイプルールを作成します。

ルール名	Forward Pipes	Return Pipes	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス	優先度
web_surf	out-pipe	in-pipe	lan	lannet	wan	all-nets	http-all	0
voip	out-pipe	in-pipe	lan	lannet	wan	all-nets	H323	6
citrix	out-pipe	in-pipe	lan	lannet	wan	all-nets	citrix	4
other	out-pipe	in-pipe	lan	lannet	wan	all-nets	all_services	2

これらのルールは、上から下まで処理され、サービスに基づく優先度に異種のトラフィックを入れ込みます。最初に特定トラフィックタイプを識別するためにカスタマイズされたサービスオブジェクトを作成する必要があります。トラフィックも迂回しないことが重要であるため、エンドにおけるすべてのサービスは以前のルールから通過するものをとらえます。そうでない場合、使用するパイプは動作しません。

パイプチェーン

優先度 0 にあふれ出ないように、必要条件は、優先度 2 の容量（他のトラフィック）を 1000Kbps に制限するものとします。これはパイプチェーンを使用して行われます。ここで、Pipe Limit に 100 を持つ in-other および out-other という新しいパイプを作成します。次に、もう片方のパイプルールは、これらを使用するように変更されます。

ルール名	Forward Pipes	Return Pipes	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス	優先度
other	out-other out-pipe	in-other in-pipe	lan	lannet	wan	all-nets	all_services	2

in-other および out-other は、はじめは双方向のパイプチェーンであることに注意してください。これは、in-pipe と out-pipe に入り、VoIP、Citrix、および Web サーフィンのトラフィックと競争する前に、すぐにトラフィックを制限するためです。

VPN シナリオ

今までに記述したケースでは、すべてのトラフィックシェーピングは、ただ一つの D-Link ファイアウォール内部で生じています。VPN は、通常本社と支社間の通信に使用されます。その場合、パイプは双方向のトラフィックを制御できます。VPN では、それはパイプルール用の送信元と送信先インタフェースであるトンネルです。

以前に記述した重要な注意事項は、VPN プロトコルで使用されるオーバヘッドのために Pipe Total 値を考慮することです。原則として、基本的な物理接続の容量が 2Mbps である VPN トンネルには、1700bps の Pipe Total が妥当です。

また、同じ物理リンクを使用して、すべての VPN でないトラフィックをパイプに挿入することを忘れないことが重要です。

パイプチェーンは、VPN オーバヘッドの問題のソリューションとして使用されます。また、このオーバヘッドを許容する制限が、VPN トンネルトラフィックに置かれ、VPN ではないトラフィックは物理リンク速度に一致するパイプに挿入されます。

これを行うために、まず外向きトラフィックと内向きトラフィックのために個別のパイプを作成します。高い優先度を持つ VPN トンネルに VoIP トラフィックは送信されます。ベストエフォート優先度で他のすべてのトラフィックを送信します。（これに関する説明は上記を参照してください。）再び、2/2Mbps の対称リンクを仮定します。

必要なパイプは、以下の通りです。

- vpn-in
  - 優先度 6 : VoIP 500kpbs
  - 優先度 0 : ベストエフォート

  合計 : 1700

- vpn-out
  - 優先度 6 : VoIP 500kpbs
  - 優先度 0 : ベストエフォート

  合計 : 1700

- in-pipe
  - 優先度 6 : VoIP 500kpbs

  合計 : 2000

- out-pipe
  - 優先度 6 : VoIP 500kpbs

  合計 : 2000

次に、以下のパイプルールが、正しいパイプと優先度レベルにトラフィックを入れ込むのに必要です。

ルール名	Forward Pipes	Return Pipes	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス	優先度
vpn_voip_out	vpn-out out-pipe	vpn-in in-pipe	lan	lannet	vpn	vpn_remote_net	H323	6
vpn_out	vpn-out out-pipe	vpn-in in-pipe	lan	lannet	vpn	vpn_remote_net	all_services	0
vpn_voip_in	vpn-in in-pipe	vpn-out out-pipe	vpn	vpn_remote_net	lan	lannet	H323	6
vpn_in	vpn-in in-pipe	vpn-out out-pipe	vpn	vpn_remote_net	lan	lannet	all_services	0
out	out-pipe	in-pipe	lan	lannet	wan	all-nets	all_services	0
in	in-pipe	out-pipe	wan	all-nets	lan	lannet	all_services	0

この設定で、すべての VPN トラフィックは 1700bps に制限され、トラフィックの合計は 2000Kbps に制限されます。また、それがベストエフォートに押し込まれる前にリモートサイトへの VoIP は、500Kbps の容量を保証されます。

パイプを使用した SAT

例えば Web サーバまたは FTP サーバなどで SAT が使用されていると、そのトラフィックはパイプに入れられる必要があります。そうでないと、トラフィックはトラフィックシェーピングから逃れ、計画された QoS を台無しにします。さらに、サーバトラフィックが外部から開始されるので、パイプの順番を逆にする必要があります。: フォワードパイプは in-pipe、リターンパイプは out-pipe です。

簡単なソリューションは、パイプルールの終わりに「catch-all-inbound」ルールを置くことです。しかし、外部インタフェース（wan）は、内部から外部 IP アドレスに送出されるトラフィックをパイプに置くのを避けるために、ソースインタフェースであるべきです。従って、この最後のルールは以下の通りになります。

ルール名	Forward Pipes	Return Pipes	送信元インタフェース	送信元ネットワーク	送信先インタフェース	送信先ネットワーク	サービス	優先度
all-in	in-pipe	out-pipe	wan	all-nets	core	all-nets	all_services	0

注意 SAT および ARP が実行される IP アドレス

SAT が ARP 処理済みの IP アドレスから行われる場合、wan インタフェースは宛先である必要があります。

11.2 IDP トラフィックシェーピング

11.2.1 概要

IDP トラフィックシェーピング機能は、NetDefendOS Intrusion Detection と Prevention（IDP）サブシステムから来る情報に基づいて実行されるトラフィックシェーピングです。IDP についての詳しい情報は、「7.6 侵入検知と防御」を参照してください。

この機能は、IDP ルールの Action プロパティに Pipe を設定することによって利用できます。アクションを選択すると追加のプロパティが表示されます。それらついては本セクションで別途説明します。

アプリケーションが関連する帯域幅の使用

IDP トラフィックシェーピングで解決できる典型的な問題は、帯域幅を多く使用するアプリケーションで引き起こされたトラフィック管理問題における処理です。典型なケースは、Bit Torrent と Direct Connect を含むピアツーピア（P2P）データ転送アプリケーションに関係するトラフィックです。

そのようなアプリケーションですばやく帯域幅を吸収するため、P2P 転送で作成された高負荷ロードは、他のネットワークユーザのためのサービス品質でしばしばマイナスの影響があります。そのため、ISP または企業ネットワークの管理者が、そのようなアプリケーションで消費される帯域幅を制御する必要があります。IDP トラフィックシェーピングでは、この機能を提供します。

IDP とトラフィックシェーピングの組み合わせ

P2P などのトラフィックタイプを制御する場合の課題の 1 つは、他のトラフィックとそれを区別することです。NetDefendOS IDP にシグネチャデータベースは、この識別を実行する有効性の高い手段を提供します。また、これへの拡張として、NetDefendOS は、ターゲットトラフィックを認識した場合に NetDefendOS トラフィックシェーピングサブシステムを通じてスロットリングを適用する機能を提供します。IDP トラフィックシェーピングは 2 つの機能の組み合わせです。

ここでは、IDP サブシステムに識別されたトラフィックフローが自動的にトリガーとなり、それらのフローを制御するトラフィックシェーピングパイプの設定をします。

11.2.2 IDP トラフィックシェーピングの設定

IDP トラフィックシェーピング設定の手順は以下の通りです。

1. ターゲットするトラフィックで始動する IDP ルールを定義します。

   選択された IDP シグネチャは、どのトラフィックをターゲットとするか決定し、また、そのシグネチャには、通常、特定のアプリケーションタイプに関連することを示す「POLICY」という名前があります。

2. パイプオプションであるルールのアクションを選択します。

   これは、IDP トラフィックシェーピングがルールを始動する接続、または続いて起こる関連した接続で実行されることを示しています。

3. ルールに帯域幅を選択します。

   これは、ターゲットとするトラフィックに許可される合計の帯域幅です。評価されるトラフィックは、フローの方向に関係なく、トリガー接続におけるフローと関連するあらゆる接続からフローの組み合わせです。

   始動される IDP がどんな制限も受けないうちに接続をオープンします。

4. オプションで Time Window（秒）を入力します。

これは、ルール起動後、オープンしている関連する接続に対してトラフィックシェーピングが適用される時間です。

通常、P2P 転送は、制御情報の転送を許可する最初の通信で開始され、その後に他のホストへの多数のデータ転送通信が続きます。

IDP は最初の通信を検出し、他の通信がオープンした後で Time Window の期間が設定されてトラフィックシェーピングの対象となります。Time Window の期限が切れた後にオープンした接続は、トラフィックシェーピングの対象にはなりません。

Time Window を 0 に設定すると、最初のトリガー接続をフローするトラフィックのみがトラフィックシェーピングの対象となります。IDP ルールを起動しないその他の関連する接続は、トラフィックシェーピングの対象となりません。

5. オプションで Network を指定します。

Time Window の値が 0 以上の場合、Network を指定することができます。管理者はこの IP アドレス範囲により、トラフィックシェーピングの対象となる、IDP ルールを起動するその後の関連する接続をさらに細かく区別することができます。トラフィックシェーピングの適用範囲となるためには、関連する接続の少なくとも 1 つが指定 IP 範囲である必要があります。

11.2.3 プロセスフロー

IDP トラフィックシェーピングがどのように適用されているかをより理解するために、以下の処理手順を参照してください。

1. D-Link ファイアウォールから他のものへの新しい接続が 1 台のホストによってオープンされて、トラフィックはフローを開始します。NetDefendOS は、接続の送信元および送信先 IP アドレスに気づきます。

2. 接続時のトラフィックフローが IDP ルールのトリガーとなります。IDP ルールには、アクションとしてパイプを持つため、接続上のトラフィックは、IDP ルールに指定されたパイプトラフィックシェーピングの帯域幅を受けます。

3. IDP ルールを始動しない新しい接続が確立されますが、新しい接続にはルールを始動した接続と同じ送信元または送信先 IP があります。また、送信元または送信先が Network として指定された IP 範囲のメンバであれば、接続のトラフィックには、オリジナルのトリガー接続に対してトラフィックシェーピングを実行するパイプが含まれています。

Network が指定されていないと、この新しい接続は、送信元または送信先が一致した場合にトリガーする接続のパイプトラフィックにも含まれます。

11.2.4 Network を指定する重要性

どちらの側も IDP を起動することが可能

上記のフロー処理に関する説明を読むと、Network の指定がなぜ重要であるかをより理解することができます。IDP サブシステムは、接続のどの側面が、ルールを始動するかはわかりません。これは、開始クライアント側であったり、応答サーバ側であったりします。両側のトラフィックフローが制限されると、トラフィックを絞るべきではない接続に予期せぬ結果をもたらすかもしれません。

予期せぬ結果

この予期しないトラフィックシェーピングについて説明するために、クライアント A が P2P トラフィックとともにホスト X に接続し、パイプアクションを持つ IDP ルールを起動すると仮定すると、この接続はトラフィックシェーピングの対象となります。また、別のクライアント B が今回は Web をサーフィンするトラフィックとともにホスト X に接続すると、IDP ルールは始動されませんが、ホスト X が関連しているからといってクライアント A の接続と一緒にトラフィックシェーピングの対象となるべきではありません。

除外するホスト

これらの予期しない結果を回避するためには、ホスト X ではなく Network 範囲にクライアント A とクライアント B の IP アドレスを指定します。これにより、IDP を起動しない新しい接続をトラフィックシェーピングに含める場合に、ホスト X が決定に関与しないようにします。

Network の範囲にクライアント B を含めることは直観に反するかもしれませんが、クライアント B のトラフィックが P2P 転送に関連する場合に、トラフィックシェーピングの対象となる可能性があることを想定しているため、このような設定としています。

Network が指定されないと、クライアント A またはホスト X に関連する全ての接続がトラフィックシェーピングの対象となりますが、これは通常は望ましくないでしょう。

11.2.5 P2P シナリオ

以下の図は、P2P に関係する典型的なシナリオを示しています。以下に手順を説明します。

- IP アドレス 192.168.1.15 を持つクライアントは、トラッキングサーバ 81.150.0.10 に接続 (1) を経由して P2P ファイル転送を開始します。
- この接続は、P2P アプリケーションをターゲットにする IDP シグネチャを使用して設定される NetDefendOS の IDP ルールを始動します。
- ルール内のパイプアクションは、指定の容量にトラフィックシェーピングするパイプを設定し、接続をそれに追加します。
- ファイルホスト 92.92.92.92 に続く接続 (2) が IDP ルールの Time Window 以内に発生すると、トラフィックはパイプに追加されて、シェーピングを受けます。
- 192.168.1.15 が所属するクライアントネットワークは、理想を言うと IDP ルール用の Network アドレス範囲に含まれるべきです。

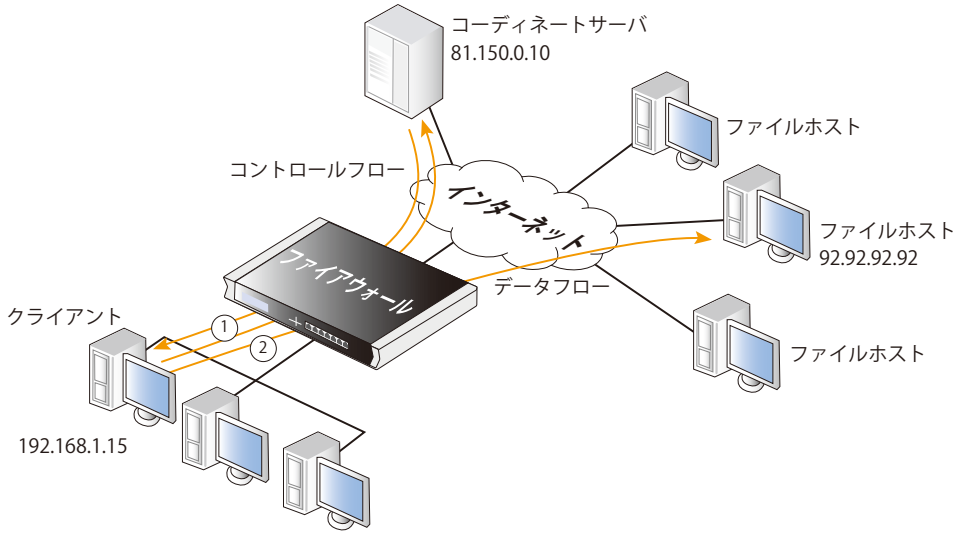


図 11-8　IDP トラフィックシェーピング P2P のシナリオ

11.2.6 トラフィックシェーピングオブジェクトの参照

参照するホスト

IDP トラフィックシェーピングには、それに関連する「idppipes」という特別な CLI コマンドがあり、現在トラフィックシェーピングを受けるホストを調べて、操作を行います。

IDP トラフィックシェーピングによってトラフィックを絞られるすべてのホストを表示するために、以下のコマンドを使用します。

```
DFL-xxxx:/> idppipes -show
Host        kbps Tmout
----------- ---- -----
192.168.1.1 100  58
```

コマンド使用してトラフィックシェーピングからホスト（この場合は IP アドレスは 192.168.1.1）を削除することができます。

```
DFL-xxxx:/> idppipes -unpipe -host=192.168.1.1
```

idppipes コマンドに関する詳細は、「Log Reference Guide」で参照できます。

パイプの参照

IDP トラフィックシェーピングは、自動的に作成される一般的な NetDefendOS パイプオブジェクトを利用します。これらのパイプには、通常最も高い優先度が割り当てられ、Group 機能を使用してトラフィックを絞ります。

しかし、Web インタフェースで現在定義済みのトラフィックシェーピングオブジェクトを検証する場合、作成済みのパイプは管理者から見えませんが、CLI の pipes コマンド使用することで、それらを検証し、操作することができます。

例えば、以下の CLI コマンドを使用して、現在定義済みのすべてのパイプを表示します。

```
DFL-xxxx:/> pipes -show
```

IDP トラフィックシェーピングパイプは、次に説明する特定の命名規約によって認識されます。

パイプの命名

NetDefendOS は、アップストリーム（送信）フロートラフィックを使用したパイプにはパターン IDPPipe_<bandwidth>、ダウンストリーム（受信）フロートラフィックを使用したパイプには IDPPipe_<bandwidth>R を使用して、IDP トラフィックシェーピングで自動的に作成したパイプに名前をつけます。名前の重複が起こると、数字の接尾語を追加します。

例えば、1000Kbps の制限で作成されたはじめのパイプは、アップストリームトラフィックには IDPPipe_1000、ダウンストリームトラフィックには IDPPipe_1000R という名前が付けられます。同じ制限を持つパイプには、IDPPipe_1000_(2) および IDPPipe_1000R_(2) が使用されます。さらに重複すると、接尾語 (3) が使用されます。

パイプは共有されます。

設定された IDP アクションと作成されたパイプ間には、1 対 1 の関係はありません。2 つのパイプが設定済みの帯域幅の値ごとに作成されており、一つはアップストリーム（送信）トラフィック用で、もう一つはダウンストリーム（受信）トラフィック用です。「Source IP」機能を使用することでグループ化されているアップストリームパイプ内のトラフィックと「Destination IP」機能を使用してグループ化されているダウンストリームパイプ内のトラフィックと共に複数のホストが各方向に同じパイプを使用します。

11.2.7 帯域幅制限の代わりの保証

必要な場合、IDP トラフィックシェーピングは、特定のアプリケーションの帯域幅制限と逆のことを行うために使用されます。

管理者が帯域幅レベルの保証（例えばあるアプリケーションに 10M ビット）を希望する場合、必要な帯域幅を指定するパイプアクションを持つアプリケーションに始動するために IDP ルールを設定します。その後、自動的に作成されるトラフィックシェーピングパイプは、初期値で最も高い優先度を付与されるため、その帯域幅は保証されます。

11.2.8 ログへの出力

IDP トラフィックシェーピングは以下のイベントに関するログメッセージを生成します。

- パイプオプションを持つ IDP ルールが始動すると、ホストまたはクライアントが Network 範囲に表示されます。
- サブシステムが将来のロックされる接続を持つホストを追加する場合。
- 新しい接続にパイプを行うタイマの期限が切れる場合、ホストから（へ）の新しい接続にはもはやパイプが行われないことを示すログメッセージが生成されます。

また、あまり一般的でない条件を示す他のログメッセージもあります。「Log Reference Guide」ですべてのログメッセージを参照できます。

11.3 サーバロードバランシング

11.3.1 概要

サーバロードバランシング（Server Load Balancing: SLB）機能により、管理者は SLB_SAT のアクションを持つ IP ルールの使用または SLB Policy オブジェクトを使用して、クライアントアプリケーション要求を多くのサーバに広げることができます。本セクションでは両方の方式について説明します。

NetDefendOS は、ネットワークアプリケーションのいくつかの面を改善することができる強力なツールです。

- 性能
- スケーラビリティ
- 信頼性
- 容易な管理

複数サーバを通過するロードを共有する原理である SLB の利点は、アプリケーションの性能の向上はできませんが、シングルサーバよりも多くのリクエストを処理できるサーバのクラスタ（サーバファームともいう）の実行を促進するという拡張性を向上することです。

以下の図は、D-Link ファイアウォールが管理している外部ユーザによって内部サーバのアプリケーションへのインターネットアクセスを示しています。

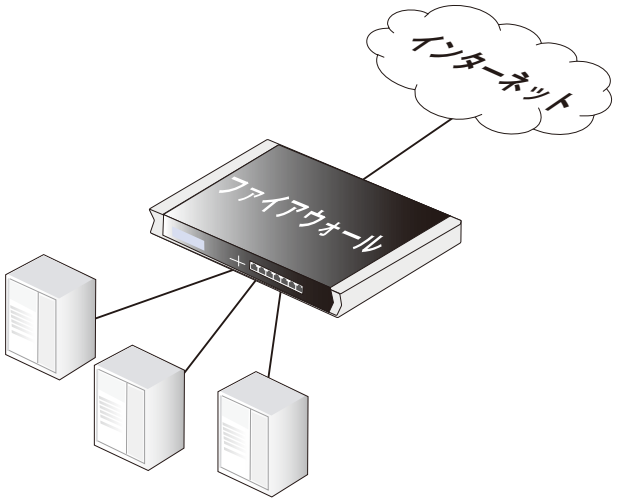


図 11-9　サーバロードバランシング構成

SLB の追加の利点

性能改善とスケーラビリティに加えて、SLB は以下の別の利点も提供します。

- 性能の改善に加え、SLB は、負荷を共有しているサーバを積極的にモニタすることでネットワークアプリケーションの信頼性を向上させます。SLB は、サーバの故障や混雑を検出して、回復するまでそのサーバにはどんなリクエストも向かわせません。
- さらに SLB は、ネットワーク管理者がサービスを中断しないで、サーバまたはアプリケーションを動作させることを意味しています。各サーバは、再起動、アップグレード、削除、または交換が可能で、さらに新しいサーバとアプリケーションは、残りのサーバファームやアプリケーションの動作に影響を与えずに追加や移動ができます。
- また、ネットワークモニタリングと配分される負荷共有の組み合わせは、DoS（Denial Of Service）攻撃に特別な保護レベルを提供します。

SLB 配置の注意事項

SLB を配置する場合、以下の問題について考慮する必要があります。

- どのサーバを通過する負荷を分散するのか。
- どの SLB アルゴリズムを使用するのか。
- 「stickiness」を使用するのか。
- どのモニタリング方式を使用するのか。

以下のセクションでは、それぞれについてより詳しく説明します。

サーバを識別する

SLB 配置において重要な最初の手順は、負荷が分散されるサーバを識別することです。サーバファームはひとつの「仮想サーバ」として動作するように設定されたサーバの集団です。SLB によって一つの仮想サーバとして処理されるサーバを指定する必要があります。

11.3.2 SLB 分配アルゴリズム

サーバセット経由で負荷を共有する方法を決定するためにはいくつかの方法があります。NetDefendOS は、負荷分散のために以下に示す 2 つのアルゴリズムをサポートしています。

項目	説明
Round-robin（ラウンドロビン）	このアルゴリズムは、ローテーションに基づいたサーバのリストによって接続を分配します。最初の接続には、サーバファームからランダムに選び接続を割り当てます。次の接続では、アルゴリズムはサーバリストを参照し、次の順番のサーバに対して負荷を転送します。サーバの能力、現在存在する接続やレスポンスタイムなどにかかわらず、すべての有効なサーバは順番に新しい接続を受けます。 このアルゴリズムは、すべてのサーバが同じ数のリクエストを受信することを保証するため、すべてのサーバが同じ能力を持つサーバファームには最適で、リクエストへの負荷処理もおおよそ同じになります。
Connection-rate（接続レート）	このアルゴリズムは、各サーバが特定の時間枠に受信するリクエスト数を考慮します。この時間枠は Window Time（ウィンドウ時間）として知られています。SLB は、最後のウィンドウ時間（秒）に最も低い接続数を持つサーバに対して次のリクエストを送信します。 ウィンドウ時間は、管理者が変更できる設定です。初期値は 10（秒）です。
Resource-usage（リソース使用率）	NetDefendOS に負荷情報を返すサーバに基づく方式であり、接続割り当ては常に最も少ない負荷のサーバとなります。 サーバは NetDefendOS REST API を使用して負荷情報を返します。サーバ上で動作するカスタムソフトウェアはこの API で記述されている必要があります。API の詳細は 707 ページの「付録 I REAT API の使用方法」を参照してください。 REST API を使用するには適切な Remote Management オブジェクトが NetDefendOS に設定されている必要があります。このオブジェクトにより、API を使用する外部ソフトウェアからのアクセスが許可されます。設定方法は「付録 I REAT API の使用方法」の最初の章に記載されています。

11.3.3 Stickiness の選択

SSL 接続などのいくつかのシナリオでは、同じサーバが一連の接続に同じクライアントから使用されることが重要です。適切な「Stickiness」オプションを選択することでこれを実行します。そして、ラウンドロビンまたは接続レートアルゴリズムのどちらかを使用します。「Stickiness」オプションは以下の通りです。

項目	説明
None	このモードは、初期値であり、「Stickiness」は適用されないことを意味します。同じ IP アドレスまたはネットワークからすべての新しい接続がされていても、他の接続から独立していると見なされます。従って、同じクライアントからの連続した接続は異なるサーバに渡されるかもしれません。 同じクライアントから来る一連の接続に同じサーバを使用しなければならない場合は、これは許容できないかもしれません。そうであれば、「Stickiness」が必要です。
IP address stickiness	このモードでは、特定クライアントからの一連の接続は、同じサーバで扱われます。これは、同じホストへの反復した接続が必要である HTTPS のような TLS または SSL サービスに特に重要です。
Network stickiness	本モードは、「Stickiness」が単一の IP アドレスの代わりにネットワークに関連付けされることを除いて、「IP Stickiness」と同様です。ネットワークは、パラメータとしてサイズを定義することによって指定されます。 例えば、ネットワークサイズが 24（初期値）として指定されると、IP アドレス「10.01.01.02」がネットワーク「10.01.01.00/24」に所属すると見なされて、「Stickiness」が適用されるネットワークになります。

Stickiness のパラメータ

IP Stickiness または Network Stickiness のいずれかが有効になると、以下の Stickiness パラメータを調整することができます。

項目	説明
Idle timeout	接続が作成されると、接続用の送信元 IP アドレスはテーブルに記憶されます。各テーブルのエントリは、スロットして参照されます。作成後、エントリはここに指定した時間（秒）有効であると見なされます。接続が作成されると、テーブルエントリがタイムアウトを超えていない場合には、テーブルは同じ送信元 IP をテーブルで検索します。一致が見つかると、「Stickiness」は、新しい接続が同じ送信元 IP から前の接続と同じサーバに向かうことを保証します。 この設定の初期値は 30（秒）です。
Max slots	このパラメータは、「Stickiness」テーブルに存在するスロット数を指定します。テーブルがいっぱいになると、最も古いエントリは、それがまだ有効であっても（Idle Timeout は超えていない）、新規エントリに道をあけるために破棄されます。テーブルがいっぱいになると、Stickiness は、破棄された送信元 IP アドレスのためにも失われる可能性があるかもしれません。そのため、管理者は、確実に Max Slots が Stickiness を必要とする接続の予想数を収容できる値に設定されるようにします。 この設定の初期値はテーブルに 2048 スロットです。
Net size	リソースが「Stickiness」を実行する場合に、各 IP アドレスに一致が必要な処理とメモリリソースを指定します。Network Stickiness オプションを選択することで、これらのリソース要求を抑制することができます。 Network Stickiness オプションが選択される場合、この項目は新しい接続の送信元 IP に関連付けられるべきであるネットワークのサイズを指定します。Stickiness テーブル検索は個別の IP アドレスを比較しませんが、送信元 IP アドレスが既にテーブル内の前の接続と同じネットワークに所属していると、代わりに比較されます。同じネットワークに所属していると、同じサーバへの Stickiness が結果として生じます。 この設定の初期値はネットワークサイズ 24 です。

11.3.4 接続レートアルゴリズムとスティッキーな接続

ここでは、異なる SLB アルゴリズムを使用して「Stickiness」がどのように機能するかをさらに説明します。

以下の図は例題のシナリオです。
この例では、D-Link ファイアウォールは異なるアドレスを持つ 3 つのクライアントからの接続を 2 つのサーバに振り分けています。Stickiness は有効となっています。

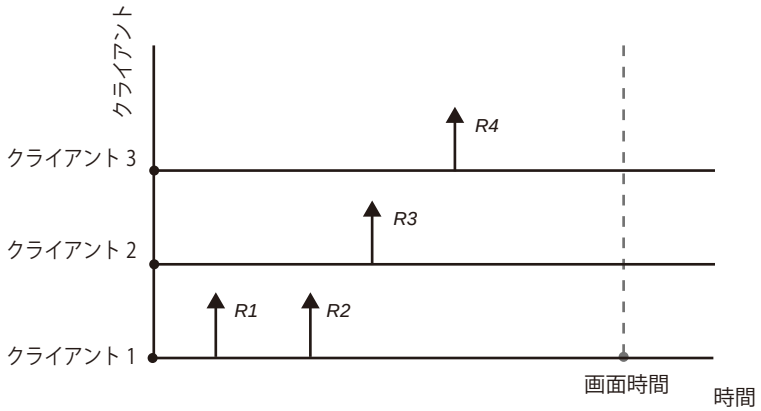


図 11-10 3 つのクライアントからの接続

ラウンドロビンアルゴリズムが使われた場合、クライアント 1 からの最初のリクエスト R1、R2 はスティッキー接続により両方とも 1 つのサーバ 1 に割り当てられます。クライアント 2 からの次のリクエスト R3 はサーバ 2 に割り当てられます。クライアント 3 からの R4 がやってくると、サーバ 1 の順番になり R4 が割り当てられます。

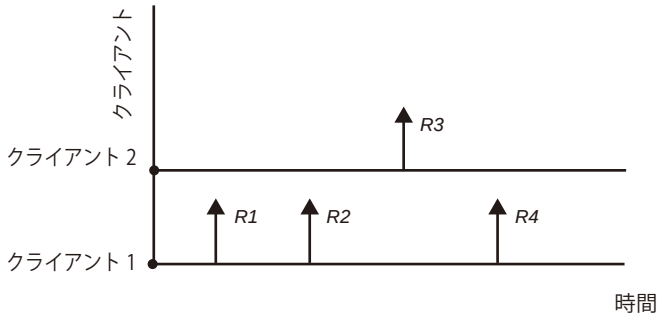


図 11-11 スティッキーとラウンドロビン

接続レートでは、R1 と R2 はスティッキー接続により同じサーバに割り当てられます。しかし、次のリクエスト R3 と R4 は Window Time で設定された分配計測期間内の新しい接続の数により、異なるサーバに割り当てられます。

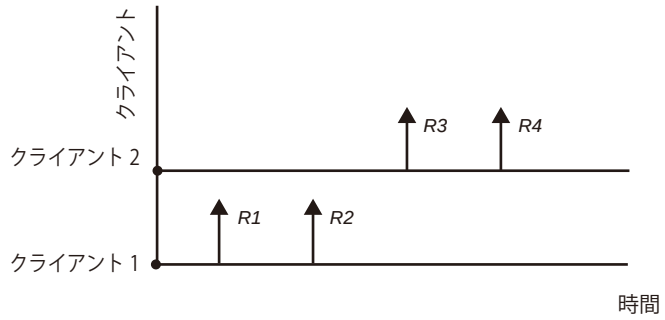


図 11-12 スティッキーと接続レート

どちらのアルゴリズムを選んだかに関わらず、サーバが停止するとトラフィックは他のサーバに送られます。そしてサーバが再びオンラインになると、自動的にサーバファームに組み込まれ、再びリクエストを受けるようになります。

サーバステータスの表示とサーバの一時停止

SLB がアクティブ状態の場合、Web インタフェースの Status > Server Load Balancing からステータスを確認することができます。サーバと割り当てられた接続が表示されます。

ステータス画面の Maintenance 項目には「Pause（一時停止）」ボタンがあり、新しい接続の割り当て対象から一時的にサーバを削除することができます。サーバが休止された場合であっても、サーバへの既存接続は NetDefendOS によってクローズされませんが、新しい接続は割り当てられません。

一方で、stickiness が有効の場合、休止状態となっているサーバに対しても（stickness 要件に対応するために）新しい接続の割り当てが行われます。

11.3.5 サーバヘルスモニタリング

SLB は、サーバヘルスモニタリングを使用して SLB 設定内のサーバの状態を継続的にチェックします。SLB は、現在の状態などの各サーバの接続レートをチェックするために異なる OSI をモニタすることができます。使用しているアルゴリズムにかかわらず、サーバが故障していれば、回復するまでそれ以上のリクエストは送信しません。

SLB は、管理者が特定のルーティングテーブルの場所を設定しない限り、デフォルトのルーティングテーブルを使用します。

D-Link の SLB は以下のモードを提供します。

ICMP Ping

OSI レイヤ 3 で動作します。SLB は、サーバファーム内の各独立したサーバの IP アドレスを ping します。これは、どんなサーバの故障も検出します。

TCP 接続

OSI レイヤ 4 で動作します。SLB は、各サーバの指定ポートに接続を試みます。例えば、サーバがポート 80 に Web サーバを動作させるものとして指定されると、SLB はそのポートに TCP SYN リクエストを送信します。SLB が、サーバからの TCP SYN/ACK を受信しないと、SLB はサーバのポート 80 はダウンしているものとしてマークします。SLB は、サーバからのレスポンスなし、通常のレスポンス、およびクローズされているポートレスポンスを認識します。

11.3.6 サーバ接続失敗後の動作

モニタリングによってサーバ利用不可の状態が検出されると、利用可能なサーバに対して新しい接続が自動的に送信されます。このセクションでは、サーバ接続に失敗し、接続クライアントがその失敗を認識していない状態における NetDefendOS の動作を説明します。

Active Connection Reset 設定

SLB でモニタリング設定を使用する場合、IP Rule と SLBPolicy オブジェクトで追加のプロパティ「Active Connection Reset」が利用可能になります。このプロパティにより、NetDefendOS がサーバ接続失敗後に既存接続に対してどのような処理を行うかを指定します。

NetDefendOS の動作の要約

プロトコルおよび Active Connection Reset 設定に基づいて、NetDefendOS は以下の動作となります。

- **Active Connection Reset 設定：無効（初期値）**
  失敗したサーバに対してクライアントがパケットを送信すると、プロトコルに応じて以下の処理が発生します。

  i. TCP
  NetDefendOS は接続をクローズし、TCP RST を送り返します。

  ii. UDP
  NetDefendOS は接続をクローズし、ICMP Port Unreachable (3) を送り返します。

  iii. ICMP または他のプロトコル
  NetDefendOS は接続をクローズし、ICMP Protocol Unreachable (2) を送り返します。

- **Active Connection Reset 設定：有効**
  サーバの失敗を検出直後、プロトコルに応じて以下の処理が発生します。

  i. TCP
  失敗検出直後、NetDefendOS は接続をクローズし、TCP RST を送り返します。

  ii. UDP
  失敗検出直後、NetDefendOS は接続をクローズし、メッセージは送信されません。

  iii. ICMP または他のプロトコル
  失敗検出直後、NetDefendOS は接続をクローズし、メッセージは送信されません。

NetDefendOS が接続をクローズした後にサーバクライアントがトラフィックを送信すると、新しい接続として処理されて利用可能なサーバにルーティングされます。

注意 Active Connection Reset はリソースを消費します。

Active Connection Reset 設定が有効化されている場合、すべての接続ステートを追跡するため、NetDefendOS で追加の処理リソースが必要となります。接続が多いとファイアウォール経由のトラフィックに影響を及ぼす可能性があります。

11.3.7 SLB の設定

このセクションに含まれる例題では、最初に SLB Policy オブジェクト、次に IP Rule を使用した別の方式による SLB 設定の方法について説明します。SLB Policy を使用することをお勧めします。

SLB の設定を行うには以下の手順を実施します。

1. SLB を有効にする各サーバにオブジェクトを定義します。
2. これらのオブジェクトすべてに含まれるグループを定義します。
3. この IP アドレスグループを参照する SLB Policy オブジェクトを IP ルールセット内に定義します。ポリシーの送信先インタフェースとして、NetDefendOS 自身が接続を処理することを意味する core を指定します。

例題 11.3

SLB ポリシーを使用した SLB の設定

この例題では、サーバ負荷分散は NetDefend Firewall の背後に位置する 2 つの HTTP Web サーバ間で実行されます。これらの 2 つの Web サーバは、プライベート IPv4 アドレス 192.168.1.10 と 192.168.1.11 を持っています。外部のクライアントによるアクセスは、IPv4 アドレス wan_ip を持つ wan インタフェースを経由します。

モニタリング、分散方法、およびスティッキングのためのデフォルト SLB 値が使用されます。

CLI

A. 各 Web サーバにアドレスオブジェクトを作成します。:

```
DFL-xxxx:/> add Address IP4Address server1 Address=192.168.1.10

DFL-xxxx:/> add Address IP4Address server2 Address=192.168.1.11
```

B. SLB Policy オブジェクトを指定します。:

```
DFL-xxxx:/> add SLBPolicy SourceInterface=wan SourceNetwork=all-nets DestinationInterface=core
            DestinationNetwork=wan_ip Service=http-all Name=my_web_slb_policy SLBAddresses=server1,server2
```

上はインターネット上の外部クライアントによるアクセスのみ許可します。また、内部のクライアントの lannet へのアクセスを許可するために、wan および lan インタフェースの両方を組み合わせた Interface Group オブジェクトを使用して IP ポリシーを書き直す必要があります。

A-2: まず、InterfaceGroup を作成します。:

```
DFL-xxxx:/> add Interface InterfaceGroup my_if_group Members=wan,lan
```

B-2: 次に、SLBPolicy オブジェクトを作成します。:

```
DFL-xxxx:/> add SLBPolicy SourceInterface=my_if_group SourceNetwork=all-nets DestinationInterface=core
            DestinationNetwork=wan_ip Service=http-all Name=my_web_slb_policy SLBAddresses=my_server_group
```

Web Interface

A. 各 Web サーバにオブジェクトを作成します。:

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。
2. 適切な名前（例 : server1）を入力します。
3. IP アドレスに 192.168.1.10 を入力します。
4. 「OK」ボタンをクリックします。
5. 上記を繰り返して、192.168.1.11 IP アドレスのために server2 と呼ばれるオブジェクトを作成します。

B. SLB_SAT IP ルールを指定します。:

1. **Policies > Firewalling > Main IP Rules > Add > SLB Policy** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: my_web_slb_policy
   - Source Interface: wan
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip
   - Service: http-all
3. server1 と server2 を Selected に追加します。
4. 「OK」ボタンをクリックします。

上はインターネット上の外部クライアントによるアクセスのみ許可します。また、内部のクライアントの lannet へのアクセスを許可するために、wan および lan インタフェースの両方を組み合わせた Interface Group オブジェクトを使用して IP ポリシーを書き直す必要があります。

A-2: まず、InterfaceGroup を作成します。:

1. **Network > Interfaces and VPN > Interface Groups > Add > Interface Group** の順にメニューをクリックします。

2. 以下を入力します。
   - Name: my_if_group
   - Selected: wan 及び lan

3. 「OK」ボタンをクリックします。

B-2. 次に、SLBPolicy オブジェクトを作成します。:

1. **Policies > Firewalling > Main IP Rules > Add > SLB Policy** の順にメニューをクリックします。

2. 以下の情報を入力します。
   - Name: my_web_slb_policy
   - Source Interface: my_if_group
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip
   - Service: http-all
   - Selected: server1 および server2

3. 「OK」ボタンをクリックします。

例題 11.4

IP ルールを使用した SLB の設定

この例題では、サーバ負荷分散は NetDefend Firewall の背後に位置する 2 つの HTTP Web サーバ間で実行されます。これらの 2 つの Web サーバは、プライベート IPv4 アドレス 192.168.1.10 と 192.168.1.11 を持っています。外部のクライアントによるアクセスは、IPv4 アドレス wan_ip を持つ wan インタフェースを経由します。

モニタリング、分散方法、およびスティッキングのためのデフォルト SLB 値が使用されます。ファイアウォール配下のクライアントは Web サーバにアクセスできるように、NAT ルールは、SLB_SAT ルールに関連して使用されます。Allow ルールは、外部クライアントによるアクセスを許可するために使用されます。

この例題は繰り返されますが、「SLB ポリシーを使用した SLB の設定」内の単一の IP Policy オブジェクトを使用することにご注意ください。

CLI

A. 各 Web サーバにアドレスオブジェクトを作成します。:

```
DFL-xxxx:/> add Address IP4Address server1 Address=192.168.1.10
DFL-xxxx:/> add Address IP4Address server2 Address=192.168.1.11
```

B. 2 つの Web サーバのアドレスを含む IP4Group を作成します。:

```
DFL-xxxx:/> add Address IP4Group server_group Members=server1,server2
```

C. SLB_SAT IP ルールを指定します。

```
DFL-xxxx:/> add IPRule Action=SLB_SAT SourceInterface=any SourceNetwork=all-nets DestinationInterface=core
            DestinationNetwork=wan_ip Service=http-all SLBAddresses=server_group Name=web_slb
```

D. サーバへの内部のクライアントアクセス用に NAT ルールを指定します。:

```
DFL-xxxx:/> add IPRule Action=NAT SourceInterface=lan SourceNetwork=lan-net DestinationInterface=core
            DestinationNetwork=wan_ip Service=http-all NATAction=UseInterfaceAddress Name=web_slb_nat
```

E. Allow IP ルールを外部クライアントに指定します :

```
DFL-xxxx:/> add IPRule Action=Allow SourceInterface=wan SourceNetwork=all-nets DestinationInterface=core
            DestinationNetwork=wan_ip Service=http-all NATAction=UseInterfaceAddress Name=web_slb_allow
```

Web Interface

A : Web サーバにオブジェクトを作成します。

1. **Objects > Address Book > Add > IP4 Address** の順にメニューをクリックします。
2. 以下の通り入力し、「OK」ボタンをクリックします。
   - Name : server1
   - Address : 192.168.1.10
3. 上記を繰り返して、192.168.1.11 IP アドレスのために server2 と呼ばれるオブジェクトを作成します。

B : 2 個の Web サーバアドレスを含む IPv4 グループを作成します。

1. **Objects > Address Book > Add > IP4 Group** の順にメニューをクリックします。
2. 以下の通り入力し、「OK」ボタンをクリックします。
   - Name : server_group
   - Members : server1 と server2 を「Selected」リストに移動し、グループに追加します。

C : SLB_SAT IP ルールを指定します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: web_slb
   - Action: SLB SAT
   - Service: HTTP
   - Source Interface: wan
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip
3. SLB Settings タブで「Server addresses」の server_group を「Selected」リストに追加します。
4. 「OK」ボタンをクリックします。

手順 D : 照合する NAT IP ルールを内部のクライアントに指定します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: web_slb_nat
   - Action: NAT
   - Service: http-all
   - Source Interface: lan
   - Source Network: lan_net
   - Destination Interface: core
   - Destination Network: wan_ip
3. 「OK」ボタンをクリックします。

手順 E : ALLOW IP ルールを外部クライアントに指定します。

1. **Policies > Firewalling > Main IP Rules > Add > IP Rule** の順にメニューをクリックします。
2. 以下の情報を入力します。
   - Name: web_slb_allow
   - Action: Allow
   - Service: http-all
   - Source Interface: wan
   - Source Network: all-nets
   - Destination Interface: core
   - Destination Network: wan_ip
3. 「OK」ボタンをクリックします。

注意 FwdFast ルールは、SLB と共に使用されるべきではありません。

SLB は、機能するために NetDefendOS ステートエンジンが接続の情報を常に取得することが必要です。これらのルールによって送信されるパケットがステートエンジン制御下にあるため、FwdFast IP ルールを SLB と共に IP ルールを使用するべきではありません。

第 12 章 High Availability（高可用性）

この章では、NetDefendOS における High Availability（高可用性）フォルトトレランスについて記述します。

- 「12.1 概要」
- 「12.2 High Availability（高可用性）メカニズム」
- 「12.3 High Availability（高可用性）設定」
- 「12.4 HA（高可用性）の問題」
- 「12.5 HA クラスタの更新」
- 「12.6 リンクモニタと HA」
- 「12.7 High Availability（高可用性）アドバンスド設定」

12.1 概要

High Availability（高可用性）クラスタ

NetDefendOS の High Availability（HA）は D-Link ファイアウォール設置にフォルトトレランス機能を提供し、既存のファイアウォールにバックアップ（スレーブ）の D-Link ファイアウォールを追加することで動作します。「マスタ」と「スレーブ」ファイアウォールは同期リンクを使用して相互に接続して論理的な高可用性クラスタを形成します。他のユニットがスタンバイ状態やアクティブでない場合、クラスタ内のユニットの 1 つがアクティブになります。

初期設定では「スレーブ」はアクティブでない状態で、「マスタ」をモニタしています。「マスタ」が応答しない状況を「スレーブ」が検出すると、フェイルオーバが実行され「スレーブ」がアクティブとなります。その後「マスタ」が完全に機能を回復した場合でも、「スレーブ」はアクティブのまま動作します。今度は「マスタ」が「スレーブ」をモニタし、フェイルオーバは「スレーブ」が機能を失った場合にだけ行われます。これは、フォルトトレランスのアクティブ / パッシブ実行と呼ばれることがあります。

注意 High Availability（高可用性）はすべての NetDefend モデルで使用できるわけではありません。
HA 機能は DFL-260E および 860E では使用できません。

HA には同じハードウェアが必要である

HA クラスタのマスタとスレーブは、通常、同じ D-Link ハードウェアコンフィグレーションを持ちます。D-Link は異なるハードウェアを使用するクラスタをサポートしていません。2 つの異なるハードウェアモデルで構成される HA クラスタを、D-Link はサポートしていません。

「マスタ」とアクティブなユニット

クラスタ内の「マスタ」ユニットがいつもアクティブユニットとは限らないということは、覚えておくべきです。アクティブユニットとは、ある時点で、すべてのトラフィックを処理するファイアウォールのことです。「マスタ」の動作に障害が起こりフェイルオーバが行われれば、「スレーブ」がアクティブユニットになります。

クラスタユニットの相互接続

クラスタ内では、「マスタ」ユニットと「スレーブ」ユニットは、NetDefendOS で同期インタフェースと呼ばれる同期接続で直接相互に接続しています。「マスタ」と「スレーブ」上の通常のインタフェースからそれぞれ 1 つずつがこの目的専用にあてられ、相互にクロスオーバケーブルで接続されます。

ハートビートとして知られている特別なパケットは、sync インタフェースとして設定されるイーサネットインタフェースを通じて 1 つのクラスタユニットから別のクラスタユニットに NetDefendOS によって連続して送信されます。また、インタフェースがそれらを送信しないように明示的に設定されないと、これらは他のすべてのイーサネットインタフェースに送信されます。これらの特別なパケットにより両ユニットの動作状態をモニタすることができます。ハートビートパケットが両方向に送信されることでパッシブなユニットはアクティブユニットの状態について理解し、またアクティブユニットもパッシブの状態を理解します。

ハートビートのメカニズムについては、「12.2 High Availability（高可用性）メカニズム」でさらに詳しく説明します。

クラスタマネジメント

Web インタフェースまたは CLI を通じてクラスタを管理する場合、1 つのクラスタユニットのコンフィグレーションを変更することができます。また、これは、自動同期を両方のクラスタで有効（初期値）にすると、自動的に他のユニットにコピーされます。自動同期をオフにして、クラスタユニットを個別に変更することは推奨されません。

自動同期はコンフィグレーションの変更を保存すると、一方のユニットからもう一方へのフェイルオーバ処理が伴います。例えば、変更が非アクティブなユニットに行われて保存されると、非アクティブなユニットは、もう片方のクラスタユニットをアップデートできるようにアクティブなユニットになります。非アクティブなユニットを変更するのが通常の方法ですが、変更をアクティブまたは非アクティブなユニットのいずれにするのかは重要ではありません。

アクティブなユニットを変更すると、2 つのフェイルオーバが起こります。アクティブなユニットは、まずアップデートできるように非アクティブな状態になり、次に、他のユニットのアップデートのためにアクティブになります。この方式はアクティブなユニットをアクティブなまま残します。これはいくつかの環境で必要とされます。例えば、機能が L2TP などの HA をサポートしていない場合に、接続が失われません。

例題 12.1

自動クラスタ同期を有効にする

この例題では、既に HA クラスタの一部である D-Link ファイアウォールにおける自動クラスタ同期を有効にします。HA が有効の場合、この設定は初期値で有効ですが、この例題は完全にするために提供するものです。この設定では常に両方のクラスタユニットで同じ値になるように設定されるべきです。

CLI

```
DFL-xxxx:/> set HighAvailability Enabled=Yes SyncIface=<interface>
```

Web Interface

1. **System > Device > High Availability** の順にメニューをクリックします。
2. Enable High Availability オプションを有効にします。
3. Sync interface を指定します。
4. 「OK」ボタンをクリックします。

ロードシェアリング

D-Link HA（高可用性）クラスタでは、一方のユニットがアクティブの時は他方がアクティブでなくなり、また、1 つのクラスタには 2 つのファイアウォール、すなわち「マスタ」と「スレーブ」だけが存在しているので、ロードシェアリングは行われません。アクティブでないユニットが行う唯一の処理機能は、アクティブユニットが動作していないことを検出した時に、アクティブユニットの状態を複製して処理しているトラフィックを引き継ぐことです。

冗長性の拡大

High Availability（高可用性）クラスタを実行すると、ネットワークにおける障害の 1 つを解決することができます。ルータ、スイッチ、およびインターネット接続は、依然として潜在的な障害の発生元となるので、これらの冗長性は考慮しなくてはなりません。

HA とリンクモニタを使用してネットワーク障害を防御する

NetDefendOS のリンクモニタ機能を使用すると、ホストとの接続性をチェックすることができます。そのため、ホストへ到達できない場合、そのホストへの異なる接続を持つピアへ HA フェイルオーバが開始されます。これは、通常の HA 機能を拡張したもので、1 台のファイアウォールと複数のホスト間のネットワーク障害を回避することができます。この記述については、「2.4.2 リンクモニタ」で詳しく説明しています。

12.2 High Availability（高可用性）メカニズム

このセクションでは、NetDefendOS が High Availability（高可用性）機能を実行するのに使用するメカニズムについて詳しく説明します。

基本原理

D-Link High Availability（高可用性）は、冗長性のある、ステート同期のハードウェアコンフィグレーションを提供します。接続テーブルと他の重要な情報のようなアクティブなユニットは、同期インタフェースによって連続してアクティブでないユニットにコピーされます。クラスタがフェイルオーバすると、アクティブでないユニットはどの接続がアクティブであるかを感知するので、トラフィックはとぎれることなくフローします。

インアクティブシステムは、十分な「クラスタハートビート」を感知しない場合、アクティブシステムはもう機能していないと検出します。「ハートビート」は、他のすべてのインタフェース同様、同期インタフェースに送信されています。

ハートビート回数

NetDefendOS ではアクティブシステムから 1 秒あたり 5 回の「ハートビート」を送信していますが、3 回「ハートビート」が送信されないと（すなわち 0.6 秒後）と、フェイルオーバが開始されます。すべてのインタフェースに「ハートビート」を送信することで、インアクティブユニットはアクティブユニットの健全性の全体図を得ることができます。同期が意図的に切断されていたとしても、インアクティブユニットが他のインタフェースから共有スイッチ経由で十分な「ハートビート」を受信していれば、フェイルオーバは起きないこともありますが、同期インタフェースは通常のインタフェースの 2 倍の「ハートビート」を送信しています。

わずかな遅れが通常の作動中に起こることもあるので、「ハートビート」はより短い間隔では送信されません。システムの他の部分がアクティブであっても、ファイルを開くなどの動作が、インアクティブシステムをアクティブにするに足るだけの遅延を引き起こすこともあります。

重要 インタフェースへのハートビートの送信を無効にする

管理者は、必要に応じてどのインタフェースへの「ハートビート」の送信も手動で無効にすることができます。これはイーサネットインタフェースコンフィグレーションオブジェクトのプロパティです。ハートビートを送信するインタフェースが少ないほど、システムの正常性を正確に判断するのに十分なハートビートを受信できないというリスクが高くなるため、これは推奨されません。

この推奨の例外は、イーサネットインタフェースが全く使用されない場合です。未使用のインタフェースに送信するハートビートを無効にすることをお勧めします。この理由は、未使用のインタフェースに送信されるハートビートは常に失われるため、システムの正常性ついて正しく識別できない可能性があるからです。したがって、「不正確な」フェイルオーバという結果になり、おそらく両方のユニットがアクティブになります。

ハートビートの特性

クラスタハートビートは以下の特長を持っています。

- 送信元 IP は送信ファイアウォールのインタフェースです。
- 送信先 IP は送信するインタフェースのブロードキャストアドレスです。
- IP TTL はいつも 255 です。NetDefendOS が他の TTL のどれかを持つクラスタハートビートを受信しないと、パケットはルータを越えたものと見なされ、そのために少しも信頼されません。
- クラスタハートビートはポート 999 からポート 999 に送信される UDP パケットです。
- 送信先 MAC アドレスは共有ハードウェアアドレスのマルチキャストアドレスで、UniqueSharedMac が有効（初期値）である場合、以下の形式となります。

```
11-00-00-00-mm-mm-nn
```

「mm」はインタフェースバス、スロット、ポートから成るビットマスクであり、「nn」はクラスタ ID を示します。UniqueSharedMac が有効化されていない場合、以下の形式となります。

```
11-00-00-c1-4a-nn
```

セキュリティのため、通常のユニキャストパケットでリンクレイヤのマルチキャストが使用されます。ユニキャストパケットを使用すると、ローカルの攻撃者がスイッチを騙してハートビートを別のどこかへルーティングしてしまい、非アクティブシステムがそれらを受信できないということになる可能性があります。

フェイルオーバ時間

通常フェイルオーバの時間は約 1 秒なので、クライアントはフェイルオーバをパケット損失のわずかなバーストとして感じるだけです。TCP の場合は、フェイルオーバ時間が通常の再送処理のタイムアウト範囲内で問題がないので、TCP はロストしたパケットを非常に短い時間で再送処理して送信を続けます。UDP は本質的に不信頼プロトコルなので、再送処理は許容しません。

共有された IP のアドレスと ARP

「マスタ」と「スレーブ」は共有する IP アドレスについて知っています。IP アドレスへの ARP クエリや、ARP 設定セクションまたはプロキシ ARP を経由して公開されている他 IP アドレスは、アクティブシステムによって応答が行われます。共有する IP アドレスのハードウェアアドレスと他の公開されているアドレスは実際のインタフェースのハードウェアアドレスに関係していません。代わりに、MAC アドレスは NetDefendOS によって以下の形式でクラスタ ID から構成されます。UniqueSharedMac が有効（初期値）である場合、以下の形式となります。

```
11-00-00-00-mm-mm-nn
```

「mm」はマスターノードのバス / スロット / ポートの組み合わせであり、「nn」はクラスタ ID を示します。クラスと ID はネットワーク内の各 NetDefendOS クラスタで一意である必要があります。UniqueSharedMac が有効化されていない場合、以下の形式となります。

```
11-00-00-c1-4a-nn
```

共有 IP アドレスは常に同じハードウェアアドレスを持つため、フェイルオーバ発生時、クラスタと同じ LAN に接続されたユニットの ARP キャッシュ更新に遅延は発生しません。

クラスタメンバがそのピアがもはや操作不能であることを検出すると、共有するハードウェアアドレスを送信者のアドレスとして使用している全インタフェースに、多くの ARP クエリをブロードキャストします。これによりスイッチやブリッジは共有ハードウェアアドレスに到達するパケットを送信する場所をミリ秒で再学習します。フェイルオーバにおける唯一の遅延はアクティブユニットがダウンしていることを検出する時です。

また、ARP クエリは、定期的にブロードキャストしてスイッチが共有ハードウェアアドレスに向かうパケットの送信先を忘れないようにします。

プロミスキャスモード

HA クラスタのイーサネットインタフェースは、HA が機能するようにプロミスキャスモードで動作する必要があります。このモードは、イーサネットインタフェースの MAC アドレスにマッチしない宛先 MAC アドレスを持つトラフィックが NetDefendOS に送信されて、インタフェースによって破棄されないことを意味します。NetDefendOS はプロミスキャスモードを自動的に有効にさせます。管理者はこれについて心配する必要はありません。

管理者が CLI コマンド「ifstat<ifname>」を入力すると、Receive Mode 状態の行では、Normal の代わりにモードが変化したのを示すために、隣に Promiscuous 値が表示されます。詳しくは「3.4.2 イーサネットインタフェース」を参照してください。

アンチウィルスと IDP を使用した High Availability（高可用性）

NetDefendOS クラスタでアンチウィルスまたは IDP サブシステムを有効にすると、アンチウィルスのシグネチャデータベースまたは IDP パターンデータベースへの更新が日常的に起こります。これらの更新は外部の D-Link データベースのダウンロードにより行われ、それらの新しいデータベースコンテンツをアクティブにするためには、NetDefendOS 再構成が必要です。

データベース更新により、以下のような一連のイベントが High Availability（高可用性）クラスタに発生します。

1. アクティブな（マスタ）ユニットは D-Link サーバから新しいデータベースファイルをダウンロードします。クラスタの共有 IP アドレス経由でダウンロードは行われます。
2. アクティブな（マスタ）ノードは新しいデータベースファイルを無効なピアに送信します。
3. 無効な（スレーブ）ユニットは再構成して新しいデータベースファイルをアクティブにします。
4. 今度は、アクティブな（マスタ）ユニットが、スレーブユニットにフェイルオーバを引き起こす新しいデータベースファイルをアクティブにするために再構成されます。これで、スレーブはアクティブなユニットになります。
5. マスタの再構成の完了後に、フェイルオーバが再び起こるので、マスタは再度アクティブなユニットになります。

sync エラーの処理

High Availability（高可用性）クラスタにまれに発生する状況は、マスタとスレーブ間の sync 接続が失敗して、その結果、無効なユニットが、もうハートビートとステートの更新を受信できなくなることです。

そのような失敗が発生すると、両方のユニットは機能し続けても、相互の同期を失うという結果になります。つまり、無効なユニットには、アクティブなユニットのステートの正しいコピーがもうないということです。無効なユニットは、同期が失われたことがわかるため、この状況ではフェイルオーバは発生しません。

sync インタフェースの失敗により、アクティブなユニットは hasync_connection_failed_timeout ログメッセージの生成を行います。しかし、無効なユニットが動作していないような場合にも、このログメッセージが生成されることに注意してください。

sync インタフェースのエラーは、各ユニットに対する特定の CLI コマンドからの出力を比較することによって確認できます。「stats」コマンドを使用して、接続数を比較することができます。IPsec トンネルが過度に使用される場合、ipsecglobalstat -verbose コマンドを代わりに使用することが可能であり、IPsec SA、IKE SA、アクティブユーザ、および IP プール統計情報の数における顕著な違いが同期エラーを示します。sync インタフェースが正しく機能しているなら、各クラスタからの統計情報にはいくつかの軽微な違いだけがあり、これらは、エラーの場合に見られる違いと比較されます。

切断された sync インタフェースが接続ケーブルを交換することで修復されると、2 つユニットの再同期が自動的に行われます。sync インタフェースが現在正しく機能しているのであれば、各クラスタユニットからの統計情報にまだわずかな差があるかもしれませんが、これらは故障の際に見られる差と比べて、小さくなります。

平常と異なる状態では、アクティブユニットと非アクティブユニット間の同期は自動的に行われません。この場合、強制的に再度同期を行うためには、同期しない非アクティブなユニットを手動で再起動する必要があるかもしれません。以下の CLI コマンドを使用することで行うことができます。

```
DFL-xxxx:/> shutdown
```

非アクティブなユニットの再起動により、以下が行われます。

- 再起動の間、非アクティブなユニットは、アクティブなユニットに状態が初期化されていることを示すためにメッセージを送信し、送信先のアクティブなユニットのすべての状態を要求します。
- アクティブなユニットはすべての状態をコピーして、非アクティブなユニットに送信します。
- 非アクティブなユニットは、システム障害があると、フェールオーバに成功した後に同期します。

非アクティブなユニットの再起動は、アクティブなユニットのすべての状態が非アクティブなユニットに送信された時にだけ行われます。

12.3 High Availability（高可用性）設定

このセクションは High Availability（高可用性）クラスタの設定を段階的に説明します。セットアップを以下のサブセクションで説明します。

- HA クラスタの物理的な設定と IP アドレスの決定については、「12.3.1 ハードウェアセットアップ」に最初に記載します。
- 次に、NetDefendOS のコンフィグレーションについて記述します。これは以下の通り分けられます。
  - **i.** Web インタフェースウィザードの使用については、「12.3.2 HA セットアップのウィザード」で説明します。
  - **ii.** ウィザードを使用しない NetDefendOS セットアップの実行については、「12.3.3 手動の HA セットアップ」で説明します。
- 最後に HA 操作の確認については「12.3.4 クラスタ機能の正しい検証」で記述します。

12.3.1 ハードウェアセットアップ

HA クラスタのハードウェアをセットアップする手順は以下の通りです。

1. 同じモデルの 2 つの同じ D-Link ファイアウォールと利用可能な同じイーサネットインタフェースのセットを使用して開始します。新たに両方を購入するか、またはクラスタを作成するために、既存のハードウェアユニットに、新しいユニットを追加することもできます。

2. マスタとスレーブユニットの両方が NetDefendOS の同じバージョンで実行しなければなりません。

3. 物理的接続の実施 :

- 別々のスイッチまたは別々のブロードキャストドメインを通じて、マスタとスレーブがマッチしているインタフェースを接続してください。他のペアとは切り離されている各インタフェースのペアにトラフィックを保持することが重要です。

- 相互モニタのためにユニットが使用している「マスタ」と「スレーブ」上に固有なインタフェースを選択します。これが同期インタフェースになります。同様のシステムであると想定されるので、「マスタ」と「スレーブ」双方で使われている同じインタフェースを選択することを推奨します。

重要 sync インタフェースは固有である必要があります。

あるハードウェアでは、インタフェースは、インタフェースのセットを結合させるスイッチファブリックのパートであるかもしれません。

そのようなインタフェースを HA sync インタフェースとして使用すると、同じスイッチに接続する他のインタフェースを同じ目的で使用することはできません。

また、sync インタフェースを含むように設定された NetDefendOS の IP ルールはないことを覚えておいてください。

- sync インタフェースを共に接続します。これは、適切なケーブルを使用するか、または、個別のスイッチ（または、ブロードキャストドメイン）を通じて行われます。

4. クラスタ内の各インタフェース用の共有 IP アドレスを定めます。あるインタフェースは共有アドレスだけを持ち、また、他のインタフェースは、IP4 HA Address オブジェクトに指定されている各インタフェースに対して個別にユニークなアドレスを持っています。共有アドレスと固定アドレスは以下のように使われます。

- IP4 HA Address オブジェクト内のインタフェースに指定された個別アドレスにより、そのインタフェースを通じたリモート管理が可能となります。また、これらのアドレスは、IP ルールがこれを許可するために定義されると ICMP を使用して「Ping」されます。初期値では、ICMP クエリはルールセットによって破棄されます。

  どちらかのユニットが動作していない場合も、各 IP アドレスは到達不能になります。これらの IP アドレスは、通常プライベートですが、パブリックインターネットを経由した管理アクセスが必要な場合にはパブリックである必要があります。

  IP4 HA Address オブジェクトを通じて個別アドレスをインタフェースに割り当てないと、サブネット 127.0.0.0/8 からの IP アドレスであるデフォルトアドレス localhost（ループバックアドレス）を割り当てる必要があります。localhost オブジェクトは 2 つのアドレスとして動作し、マスタには 127.0.0.1、スレーブには 127.0.0.2 を使用します。

  IP HA Address オブジェクトに指定された各 IP アドレスに対する ARP クエリは、通常の IP ユニットが行うように通常のハードウェアアドレスを使用してアドレスを所有するファイアウォールによって応答が行われます。

- その設定が明らかに別のアドレスを指定しない限り、1 つの共有 IP アドレスがルーティングに使用され、それがダイナミックアドレス変換にも使用されます。

注意 マスタとスレーブ管理 IP を別にする必要があります。

共有 IP アドレスは、リモート管理またはモニタリングの目的では使用されるべきではありません。例題のために、High Availability（高可用性）クラスタ内のファイアウォールのリモート管理用 SSH や SNMP を使用する場合、ファイアウォールの個別の IP アドレスが使用される必要があります。

この理由で、クラスタユニットのマネジメント IP アドレスは別にする必要があります。マスタと異なるようにスレーブのマネジメント IP が変更することをお勧めします。管理 IP アドレスを変更する方法については、「2.1.2 管理アクセスの設定」に記載しています。

一般的な High Availability（高可用性）クラスタネットワーク接続

以下の図はネットワークにおける一般的な High Availability（高可用性）クラスタ接続を示しています。「マスタ」ファイアウォール上の全インタフェースは通常関連する「スレーブ」インタフェースを持ち、これらを同じネットワークに接続します。これは他のネットワークに個別のスイッチ（またはブロードキャストドメイン）を経由して「マスタ」と「スレーブ」双方にある同じインタフェースを接続して行います。

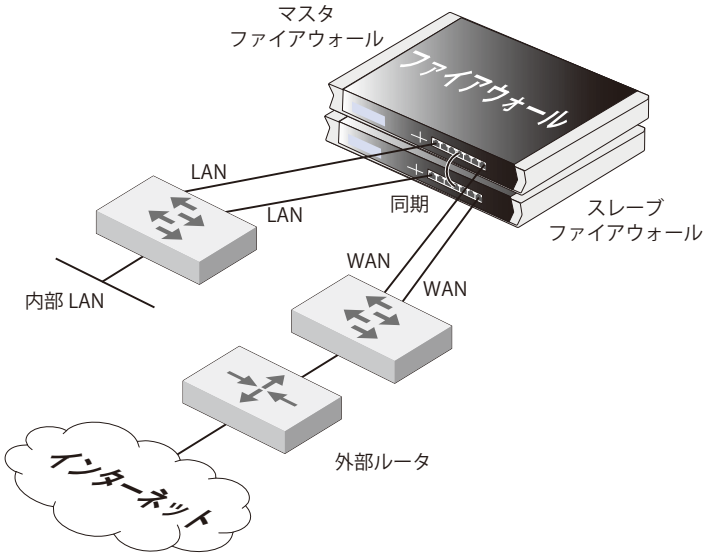


図 12-13 High Availability（高可用性）設定

上記シナリオでは、「マスタ」内の lan インタフェースと「スレーブ」内の lan インタフェースを内部のネットワークに接続する同じスイッチ接続します。同様に、「マスタ」内の wan インタフェースと「スレーブ」内の wan インタフェースも外部のインターネットに接続するスイッチに接続します。

注意 図はクロスケーブルを使用した sync 接続を示しています。

上の図は、各ユニットの sync インタフェース間をクロスオーバケーブルで使用した接続を示しています。この接続は、代わりにスイッチまたはブロードキャストドメインを経由することもできます。

ウィザードと手動のソフトウェアセットアップ

ソフトウェアセットアップ手順は現在、以下の 2 つのセクションに分かれています。

- 手早く簡単なセットアップ用に「12.3.2 HA セットアップのウィザード」
- ウィザードのない段階的な手動のセットアップ用に「12.3.3 手動の HA セットアップ」

12.3.2 HA セットアップのウィザード

NetDefendOS は、HA セットアップ手順を自動化するためにウィザードを提供します。ウィザードは、2 度実行される必要があります。
1 回目は HA クラスタのマスタユニットに接続される時で、2 回目はクラスタのスレーブユニットに接続される時です。各ユニットでこれを行う手順は以下の通りです。

1. Web インタフェースを通じた D-Link ファイアウォールに接続します。
2. **Objects > Address Book** の順にクリックし、クラスタの各インタフェースのペアに IP4 HA Address オブジェクトを作成します。各オブジェクトにはインタフェースのペアとしてマスタとスレーブの IP アドレスがあります。IP4 HA Address オブジェクトに含めることは、リモート管理に使用されるどんなインタフェースにも必須ですが、他のインタフェースにはオプションです。プライベートアドレスは、マスタとスレーブユニットの管理インタフェース用の IP4 HA Address オブジェクトのアドレスとは違うものにする必要があります。
3. 次の手順の前に、新しいコンフィグレーションの保存とアクティブ化を行います。
4. Web インタフェースで **System > Device > High Availability** にクリックしていき、「Start Wizard」ボタンを押します。マスタとスレーブユニットのためのウィザードが次の A および B で説明されます。
5. 新しいコンフィグレーションを保存し、アクティブ化します。

A. マスタセットアップのためのウィザードを動作する

1. 同期に使用する NodeType、ClusterID、および Interface を指定します。
2. クラスタで使用される 2 つのハードウェアモデルが異なる場合、これを示す必要があります。（本オプションの説明は、下の「12.3.5 ユニークな共有 MAC」を参照してください。）
3. 共有 IP アドレスと必要に応じて、作成済みの個々の IP4 HA Address オブジェクトを選択します。管理インタフェース IP が必ずマスタとスレーブで異なることを確認してください。
4. ウィザードは、マスタのセットアップが完全であることを確認します。

B. スレーブセットアップのためのウィザードを動作する

1. 同期に使用する NodeType、ClusterID、および Interface を指定します。
2. クラスタで使用される 2 つのハードウェアモデルが異なる場合、これを示す必要があります。（本オプションの説明は、下の「12.3.5 ユニークな共有 MAC」を参照してください。）
3. ウィザードは、それがマスタユニットに同期することを認識します。
4. 希望のインタフェースとのマッピングを選択します。
5. ウィザードは、スレーブのセットアップが完全であることを確認します。

新しいマスタユニットをインストールする

HA ウィザードがスレーブユニットからマスタユニットではなく、マスタユニットからスレーブを同期させる上記プロセスに注意するべきです。これは、スレーブが機器の故障などのために新しいユニットに交換されるような場合、コンフィグレーションをマスタからコピーするため、初期のセットアップを実行するのにウィザードを使用できることを意味します。

しかし、使用するコンフィグレーションを持つのがスレーブユニットで、同期するのがマスタユニットであるケースも考えてみます。これに当てはまるのは、マスタユニットが故障し、新品のユニットに交換しなければならない場合です。

これを解決するために、2 つの方式があります。
方式 A.　新しいマスタにスレーブのコンフィグレーションをコピーします。

新しいマスタユニットを設定する最も簡単で最も迅速な方法は以下の通りです。

1. 通常のコンフィグレーションバックアップ機能を使用して、既存のスレーブユニットに存在するコンフィグレーションのバックアップを作成します。
2. スレーブから新しいマスタユニットに対してバックアップを復元します。
3. 管理インタフェースを通して、マスタになるように新しいマスタユニットの HA 指定を変更し、両方に同じ名称をつけないようにデバイス名を変更してください。

方式 B.　スレーブをマスタに変更する

2 番目の、少し複雑なアプローチは、スレーブユニットをマスタに変更し、その後、通常と同じウィザードを使用して、コンフィグレーションをコピーすることです。

スレーブからマスタへの変更は、管理インタフェースを通じて、ユニットの HA 指定をマスタになるように変更することで行われます。しかし、残された問題は、接続するスイッチの ARP キャッシュが有効にならないということです。これらのキャッシュのアップデートを強制的に行うためには、スイッチを再起動するか、または CLI コマンドの「arp -notify」を（以前はスレーブであった）新しいマスタが発行を行います。

Validation Timeout 期限内（初期値で 30 秒）に古いコンフィグレーションに逆戻りするため、スレーブをマスタに変更するこのプロセスは、迅速に行われる必要があります。その時間内に、ARP キャッシュ問題も提起しなければなりません。この問題を解決するためには、ARP 問題を処理する前に手動で新しいコンフィグレーションをコミットするか、または高度な設定 Validation Timeout を増やすことで利用可能な時間をのばします。

12.3.3 手動の HA セットアップ

ウィザードなしで High Availability（高可用性）クラスタを手動で設定する手順は以下の通りです。

1. Web インタフェースを使用して「マスタ」ユニットに接続します。
2. **System > Device > High Availability** の順にクリックします。
3. Enable High Availability チェックボックス をチェックします。
4. Cluster ID を設定します。クラスタ ID を設定します。クラスタごとにユニークなものにします。
5. Sync Interface を選択します。
6. Node Type に Master を選択します。
7. **Objects > Address Book > Add > IPv4 HA Address** の順にメニューをクリックします。各インタフェースに IPv4 HA アドレスオブジェクトを作成します。

   オブジェクトの作成は、リモート管理に使用されるインタフェースのペアに必須ですが、他のインタフェースではオプションです。（その場合、デフォルトループバックアドレス localhost を使用します。そして、これは 127.0.0.0/8 サブネットワークからの IP アドレスです。）マスタとスレーブユニットの管理インタフェース用の IPv4 アドレスは別にする必要があります。

8. オプションで関連インタフェースのペアに IP6 HA Address オブジェクトを作成します。IPv6 アドレスを使用して管理アクセスまたログ機能は使用できません。しかし、HA クラスタがアクティブ、または HA がアクティブでない場合に外向き ICMP ping メッセージの送信元として使用されていると、プライベート IP アドレスは内向きの ICMP メッセージによって ping されます。
9. **Network > Interfaces and VPN > Ethernet** の順にメニューをクリックして、リスト内の各インタフェースにいき、IP Address フィールド内にそのインタフェースの共有 IP アドレスを入力します。

   各インタフェースの「Advanced」タブで「Private IP Address」に前の手順で定義した IP4 HA オブジェクトの名前を設定します（NetDefendOS は、自動的に「Master」と「Slave」の IP アドレスからそのオブジェクトに指定されている適切なアドレスを選択します）。

注意　IP アドレスはパブリックアドレスとすることができます。

ここで使用される場合、「プライベート IPv4 アドレス」は厳密に正しくありません。パブリックインターネットを経由する管理アクセスが必要であると、IP4 HA Address オブジェクトに使用されたいずれかのアドレスがパブリックであるかもしれません。

10. 設定を保存し、新しい設定を有効にします。
11. もう一方の D-LInk ファイアウォールにも上記の手順を繰り返しますが、ノードタイプは「Slave」を選択します。

クラスタの構成の変更

両方のファイアウォールのコンフィグレーションは同じである必要があります。管理のために Web のインタフェースまたは CLI を使用する場合、自動同期が有効であれば、2 つのユニットのコンフィグレーションは自動的に同期されます。コンフィグレーションに何か変更をするためには、「マスタ」、または「スレーブ」のいずれかに管理者としてログオンし、変更後に保存とアクティブ化を行います。変更は自動的に両方のユニットに実施されます。自動同期については、「12.1 概要」でより深く説明されます。

12.3.4 クラスタ機能の正しい検証

重要 マスタとスレーブの両方にシャットダウンを実行してください。

クラスタを設定した後に、両方のクラスタユニットにシャットダウン操作を実行することが強くお勧めします。それらは、ほとんど同時に再起動します。これは、Web インタフェースまたは CLI コマンドを使用して、ユニットごとに個別に行われます。

```
DFL-xxxx:/> shutdown
```

これにより、確実に両方のユニットが相互に正しく同期を行います。この手順はスキップできますが、同期が成功しないか、または他の問題が起こる場合には必要とされます。

クラスタが正しく機能していることを検証するには、まずそれぞれのユニットの ha コマンドを使用します。「マスタ」については、次のように表示されます。

```
DFL-xxxx:/> ha

This device is an HA MASTER
This device is currently ACTIVE (will forward traffic)
HA cluster peer is ALIVE
```

次に stat コマンドを使って、「マスタ」、「スレーブ」両方が同数の接続を持っているかを検証します。以下のような行を含む表示がされます。

```
Connections 2726 out of 128000
```

低い方の値が現在の接続の値で、高い方の値はライセンスの接続制限値です。

以下のポイントもまたクラスタ設定に関連しています。

- これがネットワーク内の最初のクラスタでない場合、アドバンスド設定の ClusterID は、ユニークな値を持つよう変更する必要があります。（初期値は 0 です）。こうするとクラスタの MAC アドレスは確実にユニークなものになります。

- また、各インタフェースがそれぞれの MAC アドレスを持つように、アドバンス設定の「Use Unique Shared Mac」を有効にすることも推奨します。これを有効にしない場合、インタフェースは 1 つの MAC アドレスを共有してスイッチを混乱させることがあります。

  Advanced setting の Dynamic High Buffers（Web インタフェースの **System > Advanced Settings > Misc. Settings** で参照される）が、クラスタ内の両ユニットで有効になるように設定されていることを確認してください。この設定は、接続数の増加を処理するために NetDefendOS が割り当てるメモリを決定します。NetDefendOS の再起動が、この設定変更を有効にするために必要とされます。これは CLI コマンドを使用して実行されます。

  ```
  DFL-xxxx:/> shutdown
  ```

  クラスタが非常に大量の（例えば数万）の同時接続があるところでは、Dynamic High Buffers オプションを有効にする代わりに、これに高い値を設定することが必要であるかもしれません。High Buffers に非常に高い値を設定するのは、大量の接続がある状況には合っていますが、スループットの向上には不利であると言えます。

  これらの設定の詳細詳報は、「13.10 その他の設定」を参照してください。

12.3.5 ユニークな共有 MAC

High Availability（高可用性）設定のために、NetDefendOS は高度なオプション Use Unique Shared MAC Address を提供します。初期値では、これは有効であり、大抵の構成で無効にする必要はありません。

ユニークに共有される MAC ドレスを有効にする

この設定を有効にする効果は、一つのユニークな MAC アドレスが一致するハードウェアインタフェースの各ペアに使用されると、例えば、マスタユニット上の lan1 インタフェースがスレーブユニットの lan1 インタフェースと同じ MAC アドレスを持っているように見えることです。

問題の診断

この設定を無効にすると、High Availability（高可用性）クラスタは機能しますが、スイッチが共有された ARP テーブルを使用するスイッチタイプの制限数に問題が起こります。
そのような問題は、診断するのが困難です。そういうことでいつも設定を有効にすることが最適です。

12.4 HA（高可用性）の問題

High Availability（高可用性）クラスタの設定、管理に際し、以下の問題点を考慮してください。

ALG は同期される状態ではありません
ALGs のどのアスペクトも、NetDefendOS 高可用性クラスタで同期する状態ではありません。これは、クラスタがもう一方のピアにフェイルオーバする際に、ALG に処理されるすべてのトラフィックがフリーズすることを意味します。しかし、クラスタが 30 秒程度で本来のピアにフェイルバックすると、フリーズセッションと関連する転送は再び動作を開始します。

透過モード
HA ではループを回避できないため、HA でこれを設定するべきではありません。スイッチは送信するため、透過モードにはステートの同期がありません。

VPN トンネル同期
NetDefendOS は HA クラスタの IPsec トンネル用に完全な同期を提供します。フェイルオーバが発生しても、内向きクライアントはトンネルを再確立する必要はありません。

しかし、NetDefendOS は以下の HA サポートを提供しません。
- PPTP
- L2TP
- L2TPv3
- SSL VPN

これらのトンネルタイプにフェイルオーバが起こる場合、元のトンネルが機能していないと見なされると、内向きクライアントはトンネルを再確立しなければなりません。これのタイムアウトはクライアントによって変わり、通常数秒から数分の範囲にあります。

DHCP
DHCPv6 と同様に IPv4 DHCP のためのサーバは、完全な HA 同期をサポートします。しかし、IPv4 DHCP と DHCPv6 の両方のクライアントはサポートされません。いずれかのクライアントタイプがインタフェースで有効であると、コンフィグレーションのコミットを行う時に Shared HA IP アドレスが設定されないというエラーが発生します。

リアルタイムモニタ
リアルタイムモニタは自動的にアクティブなファイアウォールを追跡することはありません。リアルタイムモニタのグラフでは接続カウントの移行だけを表示します。その時、クラスタはおそらく他のユニットへのフェイルオーバを行っています。

すべてのクラスタインタフェースで IP アドレスが必要である
双方の HA クラスタユニットにおけるインタフェースのすべてに、有効なプライベート IP4 アドレスオブジェクトを割り当てる必要があります。定義済みの IP オブジェクトのローカルホストは、このために割り当てられます。インタフェースが無効にされたとしても、アドレスを割り当てる必要性があります。

SNMP
SNMP 統計情報は、「マスタ」と「スレーブ」間で共有されません。SNMP マネージャには、フェイルオーバ能力はありません。従って、クラスタ内の両方のファイアウォールは、別々にポーリングする必要があります。

ログへの出力
ログデータはマスタとスレーブの両方から送られてきます。これは、ログレシーバを両方からのログを受信するために設定する必要があることを意味します。また、すべてのログクエリが 1 つの結果画面にすべてのログデータを与えるソースとして、マスタとスレーブの両方を含むべきです。
通常、非アクティブなユニットはライブトラフィックに関するログエントリを送信しないので、出力は 1 つの D-Link ファイアウォールからのものと同様に見えるはずです。

固定 IP の使用
「マスタ」と「スレーブ」の固定 IP アドレスは、ファイアウォールを管理する以外に安全に使用することはできません。その IP が所属するファイアウォールが動作すると固定 IP が見えなくなるため、NAT 接続に送信元 IP として固定 IP を使用する、または固定 IP 上でサービスを公開すると必ず問題が起こります。

共有 IP は「0.0.0.0」に設定しない
共有 IP アドレスとして IPv4 アドレス「0.0.0.0」を割り当てるのを回避する必要があります。これは、この目的のために有効なものではなく、NetDefendOS が Lockdown モードに入ることを引き起こします。

故障インタフェース

NetDefendOS が継続して動作できなくなる箇所で故障しない限り、故障したインタフェースは検出されません。つまり、アクティブなユニットがインタフェースのどれかを経由してアクティブでないファイアウォールに動作中を示すハートビートを送信可能である場合、フェイルオーバは発生しないことを意味します。

しかし、NetDefendOS リンクモニタリング機能を利用することによって、インタフェース障害の際に迅速な HA フェイルオーバをトリガーするように NetDefendOS を設定することができます。詳しくは「12.6 リンクモニタと HA」を参照してください。

クラスタ ID の変更

動作中の環境でクラスタ ID を変更することは、2 つの理由からお薦めできません。まず、クラスタ ID の変更は、共有 IP のハードウェアアドレスを変更することになり、ローカルネットワークに割り当てられているすべてのデバイスはタイムアウトになるまで ARP 内に古いハードウェアアドレスを保持しているため、それらに問題を引き起こします。そのようなユニットは ARP キャッシュがクリアされるようにする必要があります。

次に、この変更は、ファイアウォールが異なる設定を使用している限りクラスタ内のそのファイアウォール間の接続を中断します。これは、両方のファイアウォールを、同時にアクティブにしてしまいます。

ハートビートパケットの無効チェックサム

クラスタハートビートパケットは故意に無効のチェックサムで作成されます。これはハートビートパケットが送信されないようにするために行います。あるルータでは、この無効チェックサムをログメッセージにフラグする場合もあります。

OSPF を動作させる

OSPF がルーティングメトリックを決定するのに使用されると、代表ルータとしてクラスタを使用できません。OSPF が動作する場合、クラスタと同じ OSPF エリアで利用可能な別の代表ルータが必要です。また、理想的にはメインの代表ルータがエラーになった場合に OSPF メトリックを提供する 2 番目のバックアップ用の代表ルータも必要です。

PPPoE トンネルと DHCP クライアント

HA クラスタの共有された IP アドレスに関係する理由のため、PPPoE トンネルと DHCP クライアントを HA クラスタでは設定するべきではありません。

未使用のインタフェースでハートビートを無効にする

使用されていないイーサネットインタフェースではハートビートを無効にするをことをお勧めします。これが完了していないと、HA メカニズムが未使用のインタフェースを障害インタフェースであると見なすため、フェイルオーバを引き起こすか両方のユニットがアクティブになるリスクがあります。クラスタにある未使用のインタフェースの割合が高いほど、未使用のインタフェースへのハートビートの送信による影響が著しくなります。

両方のユニットがアクティブになる

HA クラスタの不正なコンフィグレーションの場合では、最悪のシナリオでは、マスタとスレーブが他のユニットがエラーになったと考えて、両方が同時にアクティブになり、正しいトラフィックフローに障害が起こる結果となります。

通常、これは、両方のユニットによって生成されたログメッセージを調べることによって、識別されます。アクティブ - アクティブという状況は 未使用のインタフェースがハートビートをオフにしない（以前に記述したとおり）、または通信できない sync インタフェースなどの接続問題によって引き起こされる可能性があります。

12.5 HA クラスタの更新

HA クラス内のマスタとスレーブに動作する NetDefendOS のソフトウェアバージョンは同じにする必要があります。新しい NetDefendOS バージョンが利用可能になって、両方のユニットにインストールする場合、この更新は 1 回に 1 ユニットに対して行います。

クラスタの更新処理において重要なことは、無効なユニットのアップグレードはクラスタの動作に影響せず、少しの間だけユニットを無効にすることです。

設定手順は以下の通りです。

1. どのユニットが無効であり、最初に更新させるかを確認します。

2. 無効なユニットがもう一度有効なユニットと同期すると、無効なユニットが有効なユニットになるようにフェイルオーバを引き起こします。

3. 無効のユニットを更新します。両方のユニットを再度同期させて、新しい NetDefendOS バージョンを持たせます。

これらの 3 つの手順についてより詳細に説明します。

1. クラスタ内でどれが無効のユニットであるかを確認します。

現在無効のユニットを最初に更新します。そのため、これを特定することが必要です。これを行うためには、クラスタユニットの 1 つに CLI コンソールを使用して接続し、「ha」コマンドを発行します。以下は、ユニットが有効な場合の一般的なアウトプットの例です。

```
DFL-xxxx:/> ha

This device is a HA SLAVE
This device is currently ACTIVE (will forward traffic)
This device has been active:
HA cluster peer is ALIVE
```

このユニット（スレーブ）は現在有効なユニットであるため、もう片方（マスタ）は無効のユニットです。

2. 無効のユニットを更新します。

無効のユニットを特定した後、新しい NetDefendOS バージョンでこのユニットを更新します。これは、まるでユニットがクラスタにないかのように正確に行われます。例えば、更新を行うために Web インタフェースを使用することができます。

注意 無効のユニットが ALIVE であることを確認します。

次の手順に移る前に、無効なユニットが完全に操作可能でソフトウェアの更新完了後に有効なユニットに同期できることを確認します。これを行うためには、無効なユニット上で CLI コマンド「ha」を発行します。コマンドからの出力は、ステータスが ALIVE であることを示すはずです。

```
DFL-xxxx:/> ha

This device is a HA SLAVE
This device is currently INACTIVE (won't forward traffic)
This device has been inactive: 2 sec
HA cluster peer is ALIVE
```

3. フェイルオーバを引き起こします。

今度は、CLI コンソールを使用して（古い NetDefendOS バージョンが動作中の）有効なユニットに接続し、「ha -deactivate」コマンドを発行します。これによって、有効なユニットは無効になり、無効なユニットは有効になります。

```
DFL-xxxx:/> ha -deactivate

HA Was:
ACTIVE HA going INACTIVE...
```

フェイルオーバに成功したことをチェックするためには、再度「ha」コマンドを発行し、出力に「INACTIVE」および「ALIVE」が表示される必要があります。

4. 無効のユニットを新しく更新します。

   フェイルオーバが完了したら、新しい NetDefendOS バージョンで無効なユニットを新しく更新します。手順 2 のように、まるでユニットがクラスタの一部でないかのように普通に行われます。

5. 再同期を待ちます。

   2 番目のソフトウェアの更新が完了すると、2 個のユニットは自動的に再同期してクラスタは操作を続けます。有効および無効なユニットの役割は逆にされます。有効なユニットを無効にして、無効のユニットを有効にする場合、CLI コマンド「ha -activate」が使用されます。

12.6 リンクモニタと HA

リダンダントネットワーク経路

HA 設定を使用する場合、インターネットなどの不可欠なリソースにリダンダント経路を使用することが重要と言えます。HA 設定内のマスタデバイスからネットワークへの経路への接続が失敗する可能性があると言えます。この場合、この失敗がリソースへの違う経路を持つスレーブユニットにフェイルオーバを始動させることが望ましいかもしれません。

モニタする経路

NetDefendOS リンクモニタを使用して指定ネットワーク経路の利用率をモニタリングすることができます。リンクモニタにより、管理者は ICMP「ping」要求とこれに伴うリンクステータスを使用した到達性のモニタを行う特定のホストを指定することができます。これらのホストが到達不能になると、リンクエラーと見なしてスレーブへのフェイルオーバを開始することができます。スレーブが違うネットワークリンクを使用しており、異なるホストの到達性をモニタリングしていると、トラフィックはフローを継続することができます。

共有 IP アドレスの使用

Link Monitor オブジェクトの本プロパティが有効であると、リンクモニタの ping が各ユニットの個々の IP を使用して送信する代わりに、共有 IP アドレスから送信されます。これは、パブリック IPv4 アドレスが送信側のインタフェースで利用できない場合に役に立ちます。

詳しいリンクモニタの読み取り

リンクモニタについては「2.4.2 リンクモニタ」を参照してください。

12.7 High Availability（高可用性）アドバンスド設定

High Availability（高可用性）に以下の NetDefendOS Advanced settings を行うことができます。

項目	説明
Sync Buffer Size	クラスタピアから承認を待っている間、バッファする sync データ量（Kbyte）。 初期値 : 4096
Sync Packet Max Burst	バーストで送信するステート sync パケットの最大数。 初期値 : 100
Initial Silence	起動時または再設定後に待機する時間（秒）。HA クラスタ内のアクティブなユニットが非アクティブなユニットに到達不可と判断した場合、非アクティブユニットが再度到達可能になることを想定して、通常の同期トラフィックを 1 分間送信し続けます。ネットワークを不必要にフラッディングさせないために、1 分経過後は、所定の待機時間後にのみ送信するようになります。この待機時間の長さは本オプションの値に基づきます。 初期値 : 5
Use Unique Shared Mac	各インタフェースに対してユニークに共有される MAC アドレスを使用します。この設定の詳しい説明については、「12.3.5 ユニークな共有 MAC」を参照してください。 初期値 : Enabled（有効）
Deactivate Before Reconf	本設定が有効な場合、非アクティブノードによってアクティブノードが正常に動作していないことが検出され主導権の引継ぎが行われることに依存せず、再構成が発生する前に非アクティブノードへのアクティブノードのフェイルオーバが発生します。本設定を有効にすると、構成展開の間に、ノードがアクティブでない時間を短くします。 初期値 : Enabled（有効）
Reconf Failover Time	HA 再構成時のフェイルオーバ前の無通信時間（秒）。 初期値は 0 で、すぐに再構成することを意味します。
HA Failover Time	非アクティブなフェイルオーバを起動する前に、クラスタのアクティブなユニットが無応答である時間（ミリ秒）。 初期値 :750

第 13 章 詳細設定

本章は NetDefendOS に設定可能な詳細設定について説明します。設定は以下のカテゴリに分けられます。

注意 変更をアクティブにする

詳細設定を変更した後に、新しい値が効力を発するように新しい NetDefendOS の設定が展開される必要があります。

- 「13.1 IP レベル設定」
- 「13.2 TCP レベル設定」
- 「13.3 ICMP レベル設定」
- 「13.4 ステート設定」
- 「13.5 接続タイムアウト設定」
- 「13.6 プロトコル毎のサイズ制限」
- 「13.7 フラグメント化の設定」
- 「13.8 ローカルフラグメントリアセンブリ設定」
- 「13.9 SSL/TLS 設定」
- 「13.10 その他の設定」

13.1 IP レベル設定

General

Log Checksum Errors

誤ったチェックサムを含む IP パケットの発生をログに出力します。通常、これは、ネットワーク転送の間に破損したパケットの結果です。すべてのネットワーク機器（ルータとワークステーションの両方）がチェックサムエラーを含む IP パケットを廃棄します。しかし、攻撃が不正なチェックサムを利用することはほとんどありません。

初期値 : Enabled

Log non IP4/IPv6

IPv4 または IPv6 でない IP パケットの発生をログに出力します。

初期値 : Enabled

Log Received TTL 0

「Time To Live」（TTL）値が 0 に設定して受信した IP パケットの発生をログに出力します。どんな環境下でもネットワーク装置は TTL0 のパケットを決して送るべきではありません。

初期値 : Enabled

Log TTL 0 Forward Attempts

セキュリティゲートウェイの外側に対して予定されている TTL=0 の IPv4 アドレスの送信試行をログに出力します。

初期値 : DropLog

Log 0.0.0.0 Src

不正な送信元アドレス「0.0.0.0」をログに出力します。

初期値 : Drop

Block 0 Net

送信側アドレス「0.*」をブロックします。

初期値 : DropLog

Block 127 Net

送信側アドレス「127.*」をブロックします。

初期値 : DropLog

Block Multicast Src

マルチキャストの両方の送信側アドレス（224.0.0.0 - 255.255.255.255）をブロックします。

初期値 : DropLog

TTL Min

受信元で受け付ける最小の TTL 値。

初期値 : 3

Multicast TTL Min

受信元で受け付ける最小のマルチキャスト TTL 値。
初期値 : 3

TTL on Low

TTL が規定された TTLMin 値を下回るパケットに行うアクションを決定します。
初期値 : DropLog

Multicast TTL on Low

非常に低いマルチキャスト値に行うアクションを決定します。
初期値 : DropLog

Default TTL

パケットが生成されている場合に NetDefendOS が使用すべき TTL を指定します。通常、これらの値は、64 ～ 255 です。
初期値 : 255

Layer Size Consistency

各「レイヤ」（イーサネット、IP、TCP、UDP、ICMP）に含まれるサイズ情報が他のレイヤのものと一致していることを検証します。
初期値 : ValidateLogBad

SecuRemoteUDP Compatibility

IP データが UDP total length フィールドが指定するよりも 8 バイト長いことを許可します。Checkpoint SecuRemote は NAT-T ドラフトに違反します。
初期値 : Disabled（無効）

IP Option Sizes

「IP オプション」のサイズについて検証します。これらのオプションは、各 IP ヘッダの終わりに追加される可能性のある情報の小さなブロックです。本機能は、既知のオプションタイプのサイズをチェックし、どんなオプションも IP ヘッダ自体に規定されているサイズ制限を超えていないことを保証します。
初期値 : ValidateLogBad

IP Option Source/Return

送信元ルーティングオプションが許可されるか否かを指定します。これらのオプションにより、パケットの送信者は各ルータおよびファイアウォールを経由して送信される方法を制御することができます。これらはとても大きなセキュリティリスクとなります。NetDefendOS は、この設定にかかわらず、これらのオプションによって指定された送信元ルート経路に従いません。
初期値 : DropLog

IP Options Timestamps

タイムスタンプオプションは、何時にパケットがルートに従って送信されたかを示すようにパケットルート上の各ルータとファイアウォールに指示します。これらのオプションは正常なトラフィックで発生しません。また、タイムスタンプは、パケットが送信側から最終到達先まで取ったルートを「記録する」ために使用されます。NetDefendOS は、この設定にかかわらずこれらのオプションに情報を入力しません。
初期値 : DropLog

IP router alert option

ルートアラートが含まれる IP パケットを処理する方法。
初期値 : ValidateLogBad

IP Options Other

上で指定した以外のオプション。
初期値 : DropLog

Directed Broadcasts

NetDefendOS が、直接接続しているネットワークのブロードキャストアドレスに向かうパケットを送信する否かを指定します。また、ルールセクションに行を追加するよって本機能を実行することは可能ですが、ここで簡単にするために、ここで含めることもできます。この検証の形式は、より特化されるために、ルールセクションのエントリよりも高速です。
初期値 : DropLog

Transparent Mode NAT Broadcasts

透過モードにおいて NAT ルールに適合するブロードキャストパケットの処理方法を指定します。
初期値 : DropLog

IP Reserved Flag

IP ヘッダの「reserved」フィールドにデータがある場合に、NetDefendOS が何を行うかを指定します。通常の環境下では、これらのフィールドは 0 になっています。OS の指紋押捺で使用されます。

初期値 : DropLog

Strip DontFragment

この設定によって指定されたサイズと同じか小さいパケットのために「Don't Fragment」フラグを除去します。

初期値 : 65535 バイト

Multicast Mismatch option

イーサネットと IP マルチキャストアドレスが一致しない場合に行うアクション。

初期値 : DropLog

IPv6

Log HopLimit 0 Forward Attempts

HopLimit=0 の外向き IPv6 パケットの転送試行について、ログを出力します。

初期値 : DropLog

IPv6 Anycast Source

エニーキャストの送信元アドレスによるパケットを破棄し、ログに出力します。

初期値 : DropLog

HopLimit Min

受信元で受け付ける IP の Hop Limit の最小値。

初期値 : 3

Multicast HopLimit Min

受信元で受け付けるマルチキャスト IP の Hop Limit の最小値。

初期値 : 1

HopLimit on Low

ユニキャストの Hop Limit 値が非常に低い場合に行うアクションを決定します。

初期値 : DropLog

Multicast HopLimit on Low

マルチキャストの Hop Limit 値が非常に低い場合に行うアクションを決定します。

初期値 : DropLog

Default HopLimit

セキュリティゲートウェイから送信されるパケットの Hop Limit の初期値を決定します。設定値の範囲は 32-255 です。

初期値 : 255

IP6Flow

IPv6 のフローラベルヘッダフィールドを検証します。

初期値 : Ignore

IP6TC

IPv6 のトラフィッククラスヘッダフィールドを検証します。

初期値 : Ignore

IP6MaxExtHdr

IPv6 拡張ヘッダの最大サイズ。

初期値 : 256

IP6OnMaxExtHdr

IP6MaxExtHdr の値を上回った時の IPv6 拡張ヘッダ長を検証します。

初期値 : DropLog

Reject Unordered Extension Headers

拡張ヘッダが制限を超過した場合に ICMPv6 エラーを送信します。
初期値 : Disabled

IP6MaxOptHdr

IPv6 拡張ヘッダ毎に許可されるオプションの合計数。
初期値 : 8

IP6OnMaxOptHdr

IP6MaxOptHdr の値を上回った時の IPv6 拡張ヘッダ毎のオプション数を検証します。
初期値 : DropLog

IP6ValidateSyntax

IPv6 構文違反を検証します。
初期値 : ValidateLogBad

IP6OPT_PADN

IPv6 PadN オプションデータフィールドがゼロ以外の場合に検証します。
初期値 : StripLog

IP6OPT_JUMBO

IPv6 Jumbogram パケットを検証します。
初期値 : ValidateLog

IP6OPT_RA

ルータ警告オプションパケットを検証します。
初期値 : Ignore

IP6OPT_HA

ホームアドレスオプションパケットを検証します。
初期値 : Ignore

IP6OPT_OTH

不明なオプションタイプを検証します。
初期値 : RFC2460Log

IP6_RH0

Type0 ルーティングヘッダオプションを検証します。
初期値 : RFC5095NoSupport

IP6_RH2

Type2 ルーティングヘッダオプションを検証します。
初期値 : RFC2460NoSupportLog

IP6_RHOther

Type0 または Type2 以外のルーティングヘッダオプションを検証します。
初期値 : RFC2460NoSupportLog

IP6OnLocalUnrecognizedHdr

認識されない IPv6 ヘッダが含まれる SGW 向きのパケットのアクションを決定します。
初期値 : DropLog

13.2 TCP レベル設定

TCP Option Sizes

TCP オプションのサイズを検証します。本機能は、上で説明した IPOptionSizes と同じ方法で動作します。
初期値 : ValidateLogBad

TCP MSS Min

TCP MSS の最小の許可サイズを決定します。このサイズを下回る最小セグメントサイズを含むパケットは次の設定に従って処理されます。
初期値 : 100 バイト

TCP MSS on Low

TCPMSS オプションが規定された TCPMSSMin を下回るパケットに行うアクションを決定します。低過ぎる値は不十分に書かれた TCP スタックで問題を起こします。
初期値 : DropLog

TCP MSS Max

最大の許可 TCP MSS サイズを決定します。このサイズを超える最大セグメントサイズを含むパケットは次の設定に従って処理されます。
初期値 : 1460 バイト

TCP MSS VPN Max

TCPMSSMax を持つ場合のように、許可される最も高い Maximum Segment Size です。しかし、この設定は VPN 接続で MSS を制御するだけです。このように、NetDefendOS は、すべての VPN 接続で TCP によって使用される有効なセグメントサイズを減少させることができます。ホストが MTU discovery を実行する方法を知らなくても、これは VPN 接続における TCP のフラグメント化を減少させます。

本設定は最大の IPsec MTU サイズおよび物理インタフェースに処理される最大のパケットサイズより小さくする必要があります。

初期値 : 1400 バイト

TCP MSS On High

TCP MSS オプションが規定された TCPMSSMax 値を超えたパケットに行うアクションを決定します。高過ぎる値は、不十分に書かれた TCP スタックで問題を起こすか、またはフラグメント化された大量のにパケットをもたらすかもしれません。これらは性能に悪影響を与えます。
初期値 : Adjust

TCP MSS Log Level

ログに決定する時、高過ぎる TCPMSSOnHigh によってログに出力されないと、高すぎる TCP MSS に関して、いつログに出力するのかを決定します。
初期値 : 7000 バイト

TCP Auto Clamping

TCPMSSMax に加え、関連するインタフェースの MTU に従って自動的に TCP MSS を抑制します。
初期値 : Enabled

TCP Zero Unused ACK

それが使用されていない場合、NetDefendOS が TCP パケット内の ACK シーケンス番号を設定するべきか否かを決定します。いくつかのオペレーティングシステムがこのようにシーケンスナンバー情報を明らかにしており、それは、侵入者に確立した接続をハイジャックしやすくしています。
初期値 : Enabled

TCP Zero Unused URG

すべてのパケットから URG ポインタを削除します。
初期値 : Enabled

TCP Option WSOPT

NetDefendOS が画面縮尺オプションを扱う方法を決定します。これらは、TCP によって使用される画面サイズを増やすために使用されます。つまり、送信側が ACK を予測する前に送信できる情報量です。OS の指紋押捺で使用されます。WSOPT は現代ネットワークでは一般的なことです。
初期値 : ValidateLogBad

TCP Option SACK

NetDefendOS が選択している承認オプションを扱うか方法を決定します。これらのオプションはすべてのシリーズの代わりに ACK の個々のパケットに使用されます。これは、大規模なパケット損失を経験する接続の性能を向上することができます。OS の指紋押捺で使用されます。SACK は現代ネットワークでは一般的なことです。

初期値 : ValidateLogBad

TCP Option TSOPT

NetDefendOS がどのようにタイムスタンプオプションを扱うかを決定します。PAWS（Protect Against Wrapped Sequence numbers）方式によって規定されているように、TSOPT は、受信者が注意しなくても、上限を超えるシーケンス番号（32 ビット形式）を防御するために使用されます。通常、これは問題ではありません。TSOPT を使用して、TCP スタックは、パケットが送信先へ、または送信先から移動するのにかかる時間を測定することによって、その接続を最適化します。この情報は、通常の場合よりも速く再送を行うために使用されます。OS の指紋押捺で使用されます。TSOPT は現代ネットワークでは一般的なことです。

初期値 : ValidateLogBad

TCP Option ALTCHKREQ

NetDefendOS がどのように代替のチェックサムリクエストオプションを扱うかを決定します。これらのオプションは、始めは TCP のよりよいチェックサムの使用のためのネゴシエーション時に使用されることを意図されていました。しかし、今日の標準システムでは解釈されません。NetDefendOS が標準アルゴリズム以外のチェックサムアルゴリズムを理解できないように、これらのオプションは決して受け入れられません。通常、ALTCHKREQ オプションは現代のネットワークで決して見られません。

この TCP オプションは RFC 6247 ではもはや使用されておらず、いくつかのネットワーク装置にだけに利用することに注意してください。

初期値 : StripLog

TCP Option ALTCHKDATA

NetDefendOS がどのように代替のチェックサムデータオプションを扱うかを決定します。これらのオプションは、上記 ALTCHKREQ によって許可された代替のチェックサムを送信するために使用されます。通常、現代のネットワークで決して見られません。

この TCP オプションは RFC 6247 ではもはや使用されておらず、いくつかのネットワーク装置にだけに利用することに注意してください。

初期値 : StripLog

TCP Option CC

NetDefendOS がどのように接続カウントオプションを扱うかを決定します。

この TCP オプションは RFC 6247 ではもはや使用されておらず、いくつかのネットワーク装置にだけに利用することに注意してください。

初期値 : StripLogBad

TCP Option Other

NetDefendOS が、上記設定で網羅されなかった TCP オプションをどのように処理するかを指定します。通常、これらのオプションは現代のネットワークにはありません。

初期値 : StripLog

TCP SYN/URG

NetDefendOS では、SYN（Synchronize）フラグと URGURG（Urgent data）フラグの両方がオンの場合に TCP パケットをどのように処理するかを指定します SYN フラグの存在は、新しい接続がオープンされた処理中であることを示し、URG フラグはパケットが緊急の注意を必要とするデータを含むことを意味します。不十分に実装しているTCP スタックでコンピュータをダウンするのに排他的に使用されるので、単一のパケットでこれらの 2 つのフラグをつけるべきではありません。

初期値 : DropLog

TCP SYN/PSH

SYN と PSH（Push）フラグがともにつけられている状態で、NetDefendOS がどう TCP パケットを処理するかを指定します。PSH フラグは、受信スタックが直ちにパケット内の情報をコンピュータの宛先アプリケーションに送信するべきであることを意味しています。不十分に実装している TCP スタックにクラッシュするリスクを引き起こすため、これらの 2 つのフラグは同時につけるべきではありません。しかし、Apple 社の MAC システムによっては標準通りに TCP を実装しておらず、PSH フラグがつけられている状態でいつも SYN パケットを送出してしまいます。このため、標準に厳密に準拠するとそのようなパケットを破棄するべきであるという事実にもかかわらず、NetDefendOS は通常、PSH フラグを削除して、パケットの通過を許可します。

初期値 : StripSilent

TCP SYN/RST

TCP RST フラグは SYN と組となっています。通常、無効です。（strip=strip RST）

初期値 : DropLog

TCP SYN/FIN

TCP FIN フラグは SYN と組となっています。通常、無効です。（strip=strip FIN）

初期値 : DropLog

TCP SYN Fragmented

フラグメンテーションデータは SYN と組となっています。通常無効ですが DoS 攻撃に対して使用することができます。

初期値 : DropLog

TCP SYN with data

ペイロードデータは SYN と組となっています。通常無効ですが DoS 攻撃に対して使用することができます。

初期値 : DropLog

TCP FIN/URG

NetDefendOS が、FIN（Finish、close connection）フラグと URG フラグが両方がつけられている場合に TCP パケットをどのように処理するかを指定します。「重要」なデータを送信するのと同時には通常接続の終了を行わないため、通常、これは決して起こるべきではありません。このフラグ組み合わせは、不十分に実装している TCP スタックをクラッシュするために使用され、OS の指紋押捺にも使用されます。

初期値 : DropLog

TCP URG

NetDefendOS が、他のどんなフラグにも関係なく URG フラグを持つ TCP パケットをどう処理するかを指定します。多くの TCP スタックとアプリケーションは、間違った方法で Urgent フラグを処理して、最悪の場合作業を止めてしまいます。しかし、FTP や MS SQL サーバなどのいくつかのプログラムが URG フラグをほとんどいつも使用していることに注意してください。

初期値 : StripLog

TCPE ECN

NetDefendOS が、Xmas または Ymas フラグのいずれかがにつけられている TCP パケットをどう処理するかを指定します。これらのフラグは、OS の指紋押捺で使用されます。

また、Explicit Congestion Notification と呼ばれる開発中の標準は、これらの TCP フラグを利用しますが、この標準をサポートしているオペレーティングシステムが少ない間は、フラグを削除するべきです。

初期値 : StripLog

TCP Reserved Field

NetDefendOS が、TCP ヘッダの通常、0 であるはずの「予備フィールド」に示された情報をどのように処理するかを指定します。本フィールドは Xmas および Ymas フラグと同じではありません。OS の指紋押捺で使用されます。

初期値 : StripLog

TCP NULL

NetDefendOS が、SYN、ACK、FIN または RST フラグのいずれもついいない TCP パケットをどのように処理するのかを指定します。TCP の規格によると、そのようなパケットは不正であり、いくつかのファイアウォールがそれらを検出できないので、OS の指紋押捺とステルスポートスキャナの両方に使用されます。

初期値 : DropLog

TCP Sequence Numbers

この設定は、TCP セグメントに占有されたシーケンス番号の範囲をセグメントが送信される前に受信するピアによってアナウンスされた受信画面と比較するかどうかを決定します。TCP シーケンス番号の検証は、（FwdFast ルールを使用して転送されるパケット上ではなく）ステートエンジンによって追跡される接続においてのみ可能です。可能な値は以下の通りです。

- Ignore - 有効にしません。シーケンス番号が完全に消去されることを意味します。
- ValidateSilent - 確認して送信します。
- ValidateLogBad - 確認し、エラーの場合、送信してログに出力します。
- ValidateReopen - 正常なトラフィックのような再オープンの試みを確認します。確認して送信します。
- ValidateReopenLog - 正常なトラフィックのような再オープンの試みを確認します。確認して、エラーの場合はログに出力します。
- ReopenValidate - 再オープンの試みをまったく確認しません。確認して送信します。
- ReopenValidLog - 再オープンの試みをまったく確認しません。確認して、エラーの場合ログに出力します。

初期値 : ValidateLogBad

注意 TCPSequenceNumbers 設定に関する注意

初期値の ValidateLogBad（または、代わりの ValidateSilent）は、TCP を再開する試みの事実上の動作で、以前に使用したシーケンス番号を使用した再オープンの試みを拒否することを意味します。

ValidateReopen と ValidReopenLog は、古い NetDefendOS バージョンで見られる初期動作を行う特別な設定です。現在の TCP 画面（または前回使用した TCP 画面）内に置かれたシーケンス番号を使用した再開の試みだけが許可されます。

これは ValidateLogBad/ValidateSilent より制限されたもので、何らかの有効な TCP の再開の試みをブロックします。これについて最も顕著な影響は、一般的な Web サーフィントラフィック（比較的少ないクライアントよりリクエストされる短いけれども完全なトランザクションで 2,3 秒の間隔でランダムに発生します。）が格段に遅くなることです。一方、非常にノーマルな TCP トラフィックはいつも通り動作を続けます。

しかし、TCP の再開の試みをまったく許可しないことで同じ効果が得られるため、ValidateReopen または ValidateReopenLog のいずれかを使用することはお勧めしません。これらの設定はほとんど下位互換性のために存在しています。

ReopenValidate と ReopenValidLog は、ValidateLogBad または ValidateSilent よりも制限の少ない変数です。特定のクライアントおよび（または）オペレーティングシステムは、TCP 接続の再開時に無作為で抽出されたシーケンス番号の使用を試みます。そして、これらの設定ではうまく動作しません。その影響はランダムに発生しますが、おそらく再度、Web サーフィントラフィックは影響を受けます。初期設定の代わりにこれらの値を使用すると、TCP 再開のためのシーケンス番号の有効化を完全にできないようにします。一度、接続が確立されると、通常の TCP シーケンス番号の有効化が再開されます。

Allow TCP Reopen

クライアントがクローズ状態の TCP 接続を再オープンすることを許可します。
初期値 : Disabled（無効）

13.3 ICMP レベル設定

General

ICMP Sends Per Sec Limit

NetDefendOS が 1 秒間に生成する可能性のある ICMP メッセージの最大数を指定します。これには ping の応答、送信先未到達メッセージ、および TCP RST パケットを含んでいます。つまり、本設定はルールセクション内の「Reject」ルールによって 1 秒間に生成される「Reject」を制限します。

初期値 : 500/ 秒

Silently Drop State ICMPErrors

NetDefendOS が、ステートフルに追跡されているオープンな接続に関係する ICMP エラーを警告なしで破棄するかどうか指定します。これらのエラーがこの設定によって破棄されないと、それらは検証のために他のパケットと同様にルールセットに送られます。

初期値 : Enabled

IPv6

ICMP6MaxOptND

ICMP6 ND ヘッダごとの最大オプション合計数を指定します。

初期値 : 32

ICMP6NDOnMaxOptND

拡張ヘッダ毎のオプション数を検証します。

初期値 : DropLog

13.4 ステート設定

Connection Replace

利用可能なスペースがないと、もっとも古いコネクションをリプレースして NetDefendOS に新しいコネクションを追加します。

初期値 : ReplaceLog

Log Open Fails

ルールセクションがパケットの通過を許可する決定を行ういくつかの場合に、ステートフルインスペクションメカニズムが、次にパケットが新しい接続のオープンを許可しない決定を行う可能性があります。これには、例えばルールセクションによって許可されたのに、接続を確立できないという、SYN フラグがオフの TCP パケットがあります。そのようなパケットは新しい接続をオープンすることはできません。さらに、新しい接続は ICMP ECHO（Ping）以外の ICMP メッセージによってオープンされることはありません。この設定は、NetDefendOS がそのようなパケットの発生をログに出力するかどうかを決定します。

初期値 : Enabled（有効）

Log Reverse Opens

NetDefendOS が既にオープンしている接続を経由して新しい接続をオープンしようとするパケットをログに出力するか否かを決定します。これは SYN フラグがある TCP パケットと ICMP ECHO パケットに適用されるだけです。UDP などの他のプロトコルの場合には、リモートピアによる新しい接続のオープンを行うか否かを決定する方法がありません。

初期値 : Enabled（有効）

Log State Violations

NetDefendOS が TCP SYN パケットに応じて TCP FIN を取得するなど予測される接続の状態遷移図に違反するパケットをログに出力するか否かを決定します。

初期値 : Enabled（有効）

Log Connections

NetDefendOS を接続のログに出力する方法を指定します。

- NoLog - どんな接続のログにも出力を行いません。その結果、ログへの出力が IP ルールセットの Allow または NAT ルールのどちらに対して有効にされるかどうかは、それらがログに出力されないため重要ではありません。しかし、FwdFast、Drop、および Reject ルールは、ルールセクションの設定に規定されている通りにログに出力されます。
- Log - 短い形式で接続をログに出力します。これは、接続に関する短い記述であり、実行を許可されたルールや適用するすべての SAT のルールを取得します。さらに、接続のクローズ時にも、ログに出力されます。
- LogOC - Log に対するように接続をオープンおよびクローズする 2 つのパケットを含んでいます。接続がタイムアウトの結果、クローズされると、終了パケットはログに出力されません
- LogOCAll - 接続のオープンまたはクローズに伴うすべてのパケットのログを取得します。TCP の場合は、これは SYN、FIN または RST フラグを持つすべてのパケットを保護します。
- LogAll - 接続におけるすべてのパケットのログを取得します。

初期値 : Log

Log IP Reputation

IP レピュテーションログを有効化します。

初期値 : Enabled（有効）

Log Connection Usage

これは NetDefendOS State エンジンで設定した接続を通過するあらゆるパケットへのログメッセージを生成します。NetDefendOS 管理トラフィックなど送信先が D-Link ファイアウォール自身であるトラフィックは、この設定が行われることはありません。ログメッセージはポート、サービス、送信元 / 送信先 IP アドレス、およびインタフェースを含んでいます。扱いにくい大容量のログを生成し、スループットを非常に低下させるため、本設定は診断と試験目的のためだけに有効とします。

初期値 : Disabled（無効）

Dynamic Max Connections

ダイナミックに最大接続数の値を割り当てます。

初期値 : Enabled（有効）

Max Connections

上の Max Connections が無効にされると、この設定は適用されます。NetDefendOS がどんな時もオープンを維持する接続数を指定します。各接続は約 150 バイトの RAM を消費します。この設定がダイナミックである場合、NetDefendOS は製品に許可されている接続数の使用を行います。

初期値 : 8192

13.5 接続タイムアウト設定

本セクションの設定では、自動的に接続がクローズされる前に、データが通過しないなど接続がアイドル状態を維持する時間を指定します。各接続には、それぞれの方向に 1 つの 2 つのタイムアウト値があることにご注意ください。2 つの値のうち、いずれかが 0 に到達すると、接続はクローズされます。

TCP SYN Idle Lifetime

接続がクローズされる前に、完全には確立していない TCP 接続がアイドル状態を維持する時間を指定します。

初期値 : 60（秒）

TCP Idle Lifetime

クローズ前に完全に確立した TCP 接続がアイドル状態を維持する時間を指定します。SYN フラグがオフであるパケットが一度双方向に移動すると、接続は完全に確立するようになります。

初期値 : 262144（秒）

TCP FIN Idle Lifetime

最終的にクローズされる前に、クローズしようとしている TCP 接続がアイドル状態を維持する時間を指定します。FIN フラグを持つパケットがあらゆる方向に移動した場合、接続はこの状態に到達します。

初期値 : 80（秒）

UDP Idle Lifetime

クローズ前に UDP 接続がアイドル状態を維持する時間を指定します。UDP 接続をクローズしようとしている場合、UDP は合図を送る方法がないため、このタイムアウト値を通常低くします。

初期値 : 130（秒）

UDP Bidirectional Keep-alive

両側に UDP 接続を継続することを許可します。初期値は、すべてのタイムデータが、接続をオープンした側からデータを送信する場合には、NetDefendOS が（アイドル状態ではなく）アクティブ状態として接続にマークをつけます。UDP ライフタイム内に接続オープン側からデータを受信しない場合、もう一方でデータの送信が行われていたとしても、通信はクローズされます。

初期値 : Disabled（無効）

Ping Idle Lifetime

クローズされる前に、Ping（ICMP ECHO）接続がアイドル状態を維持する時間を指定します。

初期値 : 8（秒）

IGMP Idle Lifetime

IGMP の接続ライフタイム

初期値 : 12（秒）

Other Protocols Idle Lifetime

クローズされる前に、未知のプロトコルを使用している接続が、アイドル状態を維持する時間を指定します。

初期値 : 130（秒）

13.6 プロトコル毎のサイズ制限

本セクションには、IP レベル（例 :TCP、UDP および ICMP など）直下のプロトコルに課されたサイズ制限に関する情報があります。

ここで指定された値はパケットに含まれる IP データに関係します。イーサネットの場合では、シングルパケットはフラグメント化なしで最大 1480 バイトの IP データを含むことができます。それに加え、20 バイトの IP ヘッダと 14 バイトのイーサネットヘッダがあり、1514 バイトのイーサネットネットワークにおける最大のメディア転送ユニットに対応しています。

Max TCP Length

ヘッダを含む TCP パケットの最大サイズ（バイト）を指定します。TCP は最大パケットサイズに合うように送信するセグメントに適応するため、通常、この値はフラグメント化されていないパケットに収容できる IP データ量に関係します。しかし、いくつかのそれほど一般的でない VPN システムではこの値を 20-50 バイト増加する必要があるかもしれません。
初期値 : 1480

Max UDP Length

ヘッダを含む UDP パケットの最大サイズ（バイト）を指定します。リアルタイムアプリケーションの多くが、大容量で断片化された UDP パケットを使用するため、本値を非常に高くする必要があります。そのようなプロトコルが使用されていない場合は、UDP パケットに必要なサイズ制限は 1480 バイトまで下げることができます。
初期値 : 60000 バイト

Max ICMP Length

ICMP パケットの最大サイズ（バイト）を指定します。Ping パケットは、要求されるとより大きくすることはできますが、ICMP エラーメッセージは 600 バイトを決して超えるべきではありません。大きい Ping パケットを使用したいと思わない場合、この値を 1000 バイトまで下げます。
初期値 : 10000 バイト

Max ICMPv6 Length

ICMPv6 パケットの最大サイズ（バイト）を指定します。
初期値 : 10000 バイト

Max GRE Length

GRE パケットの最大サイズ（バイト）を指定します。GRE（Generic Routing Encapsulation）には PPTP（Point to Point Tunneling Protocol）データの転送を含めてさまざまな用途があります。この値は、オリジナルのプロトコルおよび約 50 バイトにかかわらず VPN 接続の通過を許可されるパケットの最大サイズを設定します。
初期値 : 2000 バイト

Max ESP Length

EPS パケットの最大サイズ（バイト）を指定します。EPS（Encapsulation Security Payload）は、暗号化が適用される IPsec によって使用されます。この値は、オリジナルのプロトコルおよび約 50 バイトにかかわらず VPN 接続の通過を許可されるパケットの最大サイズを設定します。
初期値 : 2000 バイト

Max AH Length

AH パケットの最大サイズ（バイト）を指定します。AH（Authentication Header）は、認証だけが適用される IPsec によって使用されます。この値は、オリジナルのプロトコルおよび約 50 バイトにかかわらず VPN 接続の通過を許可されるパケットの最大サイズを設定します。
初期値 : 2000 バイト

Max SKIP Length

SKIP パケットの最大サイズ（バイト）を指定します。
初期値 : 2000 バイト

Max OSPF Length

OSPF パケットの最大サイズを指定します。OSPF は、より大きい LAN に主に使用されるルーティングプロトコルです。
初期値 : 1480

Max IPIP/FWZ Length

IP-in-IP パケットの最大サイズ（バイト）を指定します。IP-in-IP は、IPsec が使用されていない場合、Checkpoint Firewall-1 VPN 接続によって使用されます。この値は、オリジナルのプロトコルおよび約 50 バイトにかかわらず VPN 接続の通過を許可されるパケットの最大サイズを設定します。
初期値 : 2000 バイト

Max IPsec IPComp Length

IPComp パケットの最大サイズ（バイト）を指定します。
初期値 : 2000 バイト

Max L2TP Length

レイヤ 2 トンネルプロトコルパケットの最大サイズ（バイト）を指定します。
初期値 : 2000 バイト

Max Other Length

上で指定されていないプロトコルに所属するパケットの最大サイズ（バイト）を指定します。
初期値 : 1480 バイト

Log Oversized Packets

NetDefendOS は、サイズを超えたパケットの発生をログに出力するかどうか指定します。
初期値 : Enabled

13.7 フラグメント化の設定

IP は最大 65536 バイトのデータまで送信できます。しかし、イーサネットなどの多くのメディアはそのような大量のパケットを送信することはできません。それを解決するために、IP スタックはデータを断片化して、分離したパケットと、受信者が正しくオリジナルのパケットを組み立て直すのに役立つ IP ヘッダおよび情報を送信します。

しかし、多くの IP スタックは、不正に断片化されたパケットを侵入者に利用されてシステムダウンを引き起こされるという事実のために処理することはできません。NetDefendOS は、多くの方法でフラグメント化攻撃に対する保護を提供します。

General

Pseudo Reass Max Concurrent

同時に再組み立てするフラグメントする最大数。すべての断片化しているパケットを破棄するためには、PseudoReass_MaxConcurrent に 0 を設定します。
初期値 : 1024

IPv4

Illegal Fragments

NetDefendOS が不正に組み立てられたフラグメントを処理する方法を決定します。「不正に組み立てられた」の項では、重複フラグメント、異なるデータを持つ複製のフラグメント、不正なフラグメントサイズなどについて言及します。可能な設定は以下の通りです。

- Drop - ログに出力せずに不正なフラグメントを破棄します。さらに、組み立て直されるパケットは疑わしく、ログへの出力は詳しい追跡を行う場合に使用されることにご注意ください。
- DropLog - 不法なフラグメントを破棄して、ログに出力します。さらに、組み立て直されるパケットは疑わしく、ログへの出力は詳しい追跡を行う場合に使用されることにご注意ください。
- DropPacket - 不正なフラグメントと前に保存されたすべてのフラグメントを破棄します。さらに、このパケットのフラグメントが ReassIllegalLinger（秒）の間、通過するのを容認しません。
- DropLogPacket - DropPacket としてイベントのログを取得します。
- DropLogAll - DropLogPacket のように ReassIllegalLinger（秒）の間に到着する本パケットに所属するフラグメントのログを取得します。

各フラグメントを破棄するか、または全パケットを禁止するかの選択は、2 つの要素によって決定されます。

- 全体のパケットを破棄することがより安全です。
- 不法なフラグメントを受信した結果、全パケットを破棄することを選択すると、攻撃者は、リアセンブリ中に不正なフラグメントを送信することで通信を遮断して、この方法でほとんどすべての通信を妨害します。

初期値 : DropLog - 個々のフラグメントを破棄し、リアセンブリの試みは「疑わしい」ことにご注意ください。

Duplicated Fragment Data

同じフラグメントが一度以上到着する場合、受信者に到着する途中で複製されたか、または攻撃者がパケットのリアセンブリを中断させようとしているか、いずれかであることを意味しています。より可能性のある方を決定するために、NetDefendOS はフラグメントのデータコンポーネントを比較します。比較は、フラグメント内の 2-512 までのランダムな位置（抽出される各位置の 4 バイト）で行われます。非常に多くのサンプル数で、この比較が行われれば、不整合な複製をより見つけやすくなります。しかし、比較を多くするほど、CPU の負荷が高くなる結果になります。

初期値：Check8（8 つのランダムな位置（合計 32 バイト）を比較します。）

Failed Fragment Reassembly

リアセンブリは以下の原因の 1 つのために失敗する可能性があります。

- いくつかのフラグメントは ReassTimeout または ReassTimeLimit 設定によって規定された時間内に到達しませんでした。これは、1 つ以上のフラグメントがインターネットを経由している途中で紛失してしまったことを意味します。これは非常に一般的に発生します。
- NetDefendOS は、新しい断片化されているパケットが到着し、システムは一時的にリソースを使い果たすため、やむを得ずリアセンブリ手順を中断しました。このような状況で、古いリアセンブリの試みは、破棄または「失敗した」とマークされます。
- 攻撃者は、不正に断片化されているパケットを送信しようとしました。

通常の状況下では、それらが頻繁に発生する場合、失敗をログに出力したいとは思わないかもしれません。しかし、「疑わしい」フラグメントに関係する失敗をログに出力することは、有益であるかもしれません。例えば、IllegalFrags 設定が DropPacket よりむしろ Drop に設定されると、そのような失敗が発生するかもしれません。

以下の設定は FragReassemblyFail に利用可能です。

- NoLog - ノーリアセンブリ試みが失敗しても、ログへの出力は行われません。
- LogSuspect -「疑わしい」フラグメントが関連した場合にだけ、失敗したリアセンブリの試みをログに出力します。
- LogSuspectSubseq - LogSuspect に似ていますが、続いて起こるパケットのフラグメントをパケットが到着した場合にログに出力します。
- LogAll - 失敗したすべてのリアセンブリの試みについてログに出力します。
- LogAllSubseq - LogAll のように似ていますが、続いて起こるパケットのフラグメントをパケットが到着した場合にログに出力します。

初期値 : LogSuspectSubseq

Dropped Fragments

パケットがルールセクションの設定の結果としてシステムへのエントリを拒否される場合、そのパケットの各フラグメントをログに出力することも有効であるかもしれません。DroppedFrags 設定は NetDefendOS が行う方法を指定します。このルールに可能な設定は以下の通りです。

- NoLog - ルールセットに定義されたようにログへの出力は行われません。
- LogSuspect -「疑わしい」フラグメントで影響を受けるリアセンブリを試みたもので破棄された各フラグメントのログを取得します。
- LogAll - いつも破棄された各フラグメントのログを取得します。

初期値 : LogSuspect

Duplicate Fragments

同じフラグメントが一度以上到着する場合、受信者に到着する途中で複製されたか、または攻撃者がパケットのリアセンブリを中断させようとしているか、いずれかであることを意味しています。DuplicateFrags は、そのようなフラグメントをログに出力するべきであるかどうか決定します。また、それらに含まれたデータが一致しない場合、DuplicateFragData は、そのようなフラグメントについてログへの出力を行うことができることに注意してください。

可能な設定は以下の通りです。

- NoLog - 通常の状況下でログへの出力はされません。
- LogSuspect - リアセンブリ手順が「疑わしい」フラグメントによって影響を受けた場合、複製されたフラグメントをログに出力します。
- LogAll - いつも複製されたフラグメントをログに出力します。

初期値 : LogSuspect

Fragmented ICMP

ICMP ECHO（ping）を除き、フラグメント化が決して必要とされるべきではない非常に小さなデータを含む場合、通常、ICMP メッセージはフラグメント化されるべきではありません。Fragmented ICMP は、NetDefendOS が ICMP ECHO か ECHOREPLY のいずれでもないフラグメント化されている ICMP メッセージを受信する場合に行うアクションを決定します。

初期値 : DropLog

Minimum Fragment Length

パケットの最終的なフラグメント以外の全フラグメントの最小サイズ（バイト）を決定します。小さ過ぎるフラグメントが大量に到着すると、IP スタックに問題を起こす可能性ありますが、通常、この制限を非常に高く設定することはできません。送信側が非常に小さいフラグメントを作成するケースはあまりありません。しかし、送信側は 1480 バイトのフラグメントを送り、受取側への経路上のルータか VPN トンネルが次に有効な MTU を 1440 バイトまで減少させます。これにより多くの 1440 バイトのフラグメントと同数の 40 バイトのフラグメントを作成する結果となります。これが引き起こす潜在的な問題のため、NetDefendOS の初期設定は、可能な限り小さいフラグメント 8 バイトの通過を許可するように設計されています。すべてのメディアサイズが知られている内部の使用のためには、本値を 200 バイト以上まで上げることができます。
初期値 : 8 バイト

Reassembly Timeout

リアセンブリの試みは、前のフラグメントの受信に関する Reassembly Timeout（秒）内にフラグメントが到着しないと、中止されます。
初期値 : 65（秒）

Max Reassembly Time Limit

最初に受信フラグメントが到着してから Max Reassembly Time Limit（秒）後にリアセンブリは試みは通常中止されます。
初期値 : 90（秒）

Reassembly Done Limit

パケットが一度組み立て直されると、NetDefendOS は、フラグメント、例えばパケットの古い複製フラグメントが到着することを防ぐために短期間でこれを覚えることができます。
初期値 : 20（秒）

Reassembly Illegal Limit

全パケットが一度不正としてマークされると、NetDefendOS は、フラグメント、例えばパケットの余分なフラグメントが到着することを防ぐためにメモリにこれを保持します。
初期値 : 60（秒）

IPv6

Illegal Fragments

不正に構成されたフラグメントを処理する方法を決定します。重複フラグメント、不正なサイズのフラグメントなどが含まれます。
初期値 : DropLog

Duplicated Fragment Data

重複フラグメントを比較して検証します。
初期値：Check8（8 つのランダムな位置（合計 32 バイト）を比較します。）

Failed Fragment Reassembly

タイムアウトまたはパケット損失により再組立ての試行に失敗したパケットのログ出力動作を指定します。
初期値 : LogSuspectSubseq

Dropped Fragments

ルールベースで破棄されたパケットのフラグメントについて、ログ出力動作を指定します。
初期値 : LogSuspect

Duplicate Fragments

受信した重複フラグメントのログ出力動作を指定します。
初期値 : LogSuspect

Reject Bad Fragment Length

不正なデータ長のフラグメントの受信時に Parameter Problem エラーを送信します。
初期値 : Disabled

Ignore Stub Fragments

M フラグがクリアされ、フラグメントオフセットが 0 であるフラグメントを無視します。
初期値 : Disabled

Minimum Fragment Length

パケットの最終的なフラグメント以外の全フラグメントの最小サイズ（バイト）を決定します。
初期値 : 8

Reassembly Timeout

最後のフラグメント受信後、Reassembly Timeout（秒）内に次のフラグメントが到着しないと、リアセンブリの試行は中止されます。
初期値 : 65

Maximum Reassembly Time Limit

最初に受信フラグメントが到着してから Max Reassembly Time Limit（秒）後に、リアセンブリの試行は中止されます。
初期値 : 90

Reassembly Done Limit

パケットが組み立て直された後、Reassembly Done Limit（秒）の期間、再組み立てを覚えておくことで、そのパケットの古い重複フラグメントなどが到着することを防ぐことができます。
初期値 : 20

Reassembly Illegal Limit

パケット全体が不正とマークされた後、Reassembly Illegal Limit（秒）の期間、メモリにこの情報を保持しておくことで、そのパケットのフラグメントが到着することを防ぐことができます。
初期値 : 60

Send Error On Timeout

フラグメントリアセンブリのタイムアウトが発生した場合に ICMPv6 エラーを送信します。
初期値 : Disabled

13.8 ローカルフラグメントリアセンブリ設定

Max Concurrent

同時に再組み立てするフラグメントする最大数。
初期値 : 256

Max Size

ローカルに再組み立てされるパケットの最大サイズを指定します。
初期値 : 10000

Large Buffers

（2K 以上）の大きいローカルのリアセンブリバッファ（上記サイズ）。
初期値 : 32

13.9 SSL/TLS 設定

これらのグローバル設定は SSL VPN と TLS ALG の両方の操作に影響します。(「10.6 SSL VPN」と「6.1.11 TLS ALG」を参照してください。)

Minimum Allowed Version

これは NetDefendOS がサポートする SSL のバージョンを選択します。オプションは以下の通りです。

- TLSv1.0 - TLS バージョン 1.0 または 1.2 が許容される
- TLSv1.2- TLS バージョン 1.2 のみ許容される。

NetDefendOS は、RFC 5246 によって定義されるように、TLS バージョン 1.2 のサポートを提供します。TLS バージョン 1.1 はサポートされません。
初期値 : TLSv1.2

SSL Processing Priority

SSL 処理が新しい SSL 接続の開始に使用できる CPU リソースの最大値。この設定は SSL 処理を利用するすべての NetDefendOS サブシステムに影響します。

割り当てられた CPU 時間の割合が十分でない場合、いくつかの SSL 接続設定が重い SSL 負荷の元でエラーになり、以下のログメッセージは表れる可能性があります。

```
SSL Handshake: Disallow ClientKeyExchange. Closing down SSL connection
```

この問題を解決するには、初期値の Normal（約 17%）から High（約 25%）または Very（約 50%）に利用できる最大 CPU リソースを増やします。しかし、高い CPU 割り当ては逆に他の NetDefendOS サブシステムのレスポンスに影響を与えるかもしれません。

SSL 接続設定に割り当てられる CPU 時間を減らす理由がなければ、通常、優先度を下げる必要はありません。
初期値 : Normal（約 17%）

推奨される SSL/TLS 暗号スイート

以下の暗号スイートはセキュリティのため使用する推奨のセットです。

TLS ECDHE RSA WITH AES 128 CBC SHA256

暗号 TLS ECDHE RSA WITH AES 128 CBC SHA256 を有効にします。
初期値 : Enabled

TLS ECDHE RSA WITH AES 256 CBC SHA1

暗号 TLS ECDHE RSA WITH AES 256 CBC SHA1 を有効にします。
初期値 : Enabled

TLS ECDHE RSA WITH AES 128 CBC SHA1

暗号 TLS ECDHE RSA WITH AES 128 CBC SHA1 を有効にします。
初期値 : Enabled

TLS RSA WITH AES 256 CBC SHA256

暗号 TLS_RSA_WITH_AES_256_CBC_SHA256 を有効にします。
初期値 : Enabled

TLS RSA WITH AES 256 CBC SHA1

暗号 TLS_RSA_WITH_AES_256_CBC_SHA1 を有効にします。
初期値 : Enabled

TLS RSA WITH AES 128 CBC SHA256

暗号 TLS_RSA_WITH_AES_128_CBC_SHA256 を有効にします。
初期値 : Enabled

TLS RSA WITH AES 128 CBC SHA1

暗号 TLS_RSA_WITH_AES_128_CBC_SHA1 を有効にします。
初期値 : Enabled

TLS RSA 3DES 168 SHA1

暗号 RSA_WITH_3DES_168_SHA1 を有効にします。
初期値 : Enabled

推奨されない SSL/TLS 暗号スイート

以下の暗号スイートは、低いセキュリティのため推奨されず、初期値で無効にしていますが、必要であれば推奨されませんが、有効にすることができます。

TLS RSA RC4 128 SHA1

暗号 RSA_WITH_RC4_128_SHA1 を有効にします。
初期値 : Disabled

TLS RSA RC4 128 MD5

暗号 TLS_RSA_WITH_RC4_128_MD5 を有効にします。
初期値 : Disabled

TLS RSA EXPORT 1024 RC4 56 SHA1

暗号 TLS_RSA_EXPORT1024_WITH_RC4_56_SHA1 を有効にします。
初期値 : Disabled

TLS RSA EXPORT 1024 RC4 40 MD5

暗号 TLS_RSA_EXPORT1024_WITH_RC4_40_MD5 を有効にします。
初期値 : Disabled

TLS RSA EXPORT 1024 RC2 40 MD5

暗号 TLS_RSA_EXPORT1024_WITH_RC2_40_MD5 を有効にします。
初期値 : Disabled

TLS RSA EXPORT NULL SHA1

暗号 TLS_RSA_EXPORT_WITH_NULL_SHA1 を有効にします。（暗号化はなく、メッセージ検証のみ）
初期値 : Disabled

TLS RSA EXPORT NULL MD5

暗号 TLS_RSA_EXPORT_WITH_NULL_MD5 を有効にします。（暗号化はなく、メッセージ検証のみ）
初期値 : Disabled

重要 AES、3DES アルゴリズムが推奨されます。

初期値では、AES と 3DES 以外のすべての対称暗号化アルゴリズムが無効にされます。これを変更することは推奨されません。このドキュメントが書かれた時点では、初期値でアルゴリズムが無効になると危険であると見なされます。

管理者が、弱いアルゴリズムのどれかを有効にすると、NetDefendOS は、コンフィグレーションがコミットされる時に警告を出して、Web インタフェースの System Summary ページに警告を表示し続けます。

13.10 その他の設定

UDP Source Port 0

送信元ポート 0 を持つ UDP パケットを扱う方法。
初期値 : DropLog

Port 0

送信先ポート 0 の TCP/UDP パケットと送信元ポート 0 の TCP パケットを扱う方法。
初期値 : DropLog

Dynamic High Buffers

NetDefendOS が自動的に High Buffers の値を指定するかどうかを判断します。初期値は総使用可能メモリの 3% で、最低値は 1024 です。これに加えてバッファのために割り当てられる付加的な 512 キロバイトが常にあることに注意してください。

この設定は、新しい値を適用するために NetDefendOS の再起動を必要とします。再構成では十分ではありません。
初期値 :Enabled

High Buffers

Dynamic High Buffers が有効でないと、このバッファ数が 1M バイト以上の RAM に割り当てられます。問題を障害調査する時に、この値を上げると、解決される場合があります。

この設定は、新しい値を適用するために、「shutdown」コマンドを使用した NetDefendOS の再起動を必要とします。再構成では十分ではありません。
初期値 :1024

重要 高いバッファを設定するのは推奨されません。

Dynamic High Buffersの設定を有効にすることは、多くのコンフィグレーションに推奨されます。まれに、NetDefendOSのサポート担当者は、いくつかの特定の問題のために、それを無効にして、固定値を指定することを推奨するかもしれません。

NetDefendOS をアップグレードする場合、新しいバージョンのメモリ要件が変わるため、Dynamic High Buffers を有効とし、NetDefendOS が自動的に必要なメモリを割り当てることを許可すべきです。サポート担当者は、依然としてアップグレード後に固定値を使用することを推奨するかもしれません。

Local Undelivered

オープンポートに一致しないセキュリティゲートウェイへのパケットの処理方法を指定します。（SNMP、SCP、NETCON など）。
初期値 :DropLog

Anti-Virus Cache Lifetime

アンチウィルスキャッシュ内のエントリの生存時間（分）を指定します。この設定は「6.4.5 アンチウィルスキャッシュ」で、より詳しく説明されます。
初期値 :20

WCF Performance Log

ダイナミックな Web コンテンツフィルタリングの性能ログを有効、または無効にします。詳しくは、「6.2.6 WCF 性能ログ」で説明されます。
初期値 : Disabled

Max HTTP Pipelining Requests

HTTP におけるパイプラインリクエストの最大値を指定します。
初期値：64

Allow IP Rules

NetDefendOS の IP ルールの利用を有効、または無効にします。無効にすると、IP ルールセットに IP Policy オブジェクトしか設定することができません。この設定を無効にしても、既存の IP Rule オブジェクトは影響を受けません。
初期値 : Enabled

Enable Poll Offload

Poll Offloading は、特定のハードウェアプラットフォームで利用可能であり、別のプロセッシングコアにインタフェースのポーリング機能を配布することでスループットを向上する機能です。初期値では有効であり、デバッグ目的だけで無効にするべきです。
初期値 : Enabled

Enforce Strong Passwords

新しく作成または編集するパスワードについて、事前定義した複雑なルールに適合する必要があります。本オプションを有効化する前に設定したパスワードは検証されません。
初期値 : Enabled

付録 A セキュリティ更新サービス

概要

以下の NetDefendOS 機能はすべて、有効なサブスクリプションが機能する必要があります。:

- Anti-Virus
- Intrusion Detection and Prevention（IDP）
- Web コンテンツフィルタリング
- アプリケーションコントロール
- IP レピュテーション

さらに、定期的にこれらの機能のいくつかに関連するデータベースは更新されます。これらの機能が動作して最新のデータベース更新にアクセスするためには、有効な D-Link セキュリティ更新サブスクリプションが存在する必要があります。これを以下の手順で行います。:

- D-Link の販売代理店からサブスクリプション定期的に購入します。
- 購入時に、サービス対象ユーザ用の固有のアクティベーションコードを受け取ります。
- ご使用の D-Link ファイアウォールシステムの Web インタフェースで **Status > Maintenance > License** メニューをクリックし、このアクティベーションコードを入力します。NetDefendOS がこのコードが受諾すると、その旨が表示され更新サービスはアクティブになります。これを行うときに、NetDefendOS がインターネットにアクセスできることを確認してください。

注意 登録と更新サービスの詳細については「付録 G 登録＆アクティベーション手順」を参照してください。

情報更新サービスのリニューアル

Web インタフェースでは **Status > Maintenance > License** メニューをクリックし、アクティブ化されている更新サービスとサブスクリプションの終了日をチェックすることができます。

重要 期限の終了に関するアラートが現れたら、サブスクリプションを更新してください。

現在のサブスクリプションが終了する前に、サブスクリプションの更新をします。期限が終了するまで放置しないでください。NetDefendOS は、サブスクリプションの終了を警告するために Web インタフェースにアラートを発行します。アラートは終了する 23 日～ 30 日前に現れます。期限チェックが 7 日間毎に NetDefendOS によって行われます。

データベース更新をモニタリングする

Web インタフェースでは、**Status > Maintenance > Update Center** の順にメニューをクリックし、自動データベース更新を設定できます。
管理者は最後の更新を行った日とその時のステータスもチェックできます。

Web インタフェースの同じエリアで、Update を選択することにより手動で更新を行い、データベースに最新のシグネチャをダウンロードすることもできます。

注意 データベースをアップデートすると、処理に中断が起こります。

1 度アップデートをダウンロードすると、アンチウイルスなどのいくつかのデータベース更新が少しの処理遅延を必要とします。これにより、ファイアウォールのトラフィックフローはしばらく停止します。そのため、早朝などの低いトラフィックの時間帯に更新タイミングを設定することが最善であると言えます。データベースの削除は、処理に同様の休止を起こします。

データベースコンソールコマンド

コンソールコマンドを経由してデータベースを直接制御できます。

データベース更新を行う

IDP データベース更新はコマンドを使用していつでも実行することができます。

```
DFL-xxxx:/> updatecenter -update=idp
```

アンチウィルスも同じくコマンドを使用して更新できます。

```
DFL-xxxx:/> updatecenter -update Antivirus
```

更新ステータスを問い合わせる

IDP 更新のステータスを取得するためにコマンドを使用します。

```
DFL-xxxx:/> updatecenter -status=idp
```

AV 更新のステータスを取得します。

```
DFL-xxxx:/> updatecenter -status=antivirus
```

サーバステータスを問い合わせる

D-Link ネットワークサーバのステータスを取得するためにコマンドを使用します。

```
DFL-xxxx:/> updatecenter -servers
```

本コマンドは、以下の通り、すべての利用可能なサーバの情報を示します。

項目	説明
Server IP	サーバの IPv4 アドレス。
Response time	各サーバとのテスト通信からの現在の応答時間（ミリ秒）。
Packet loss	そのサーバのテストで検出されたパケット損失。
Precedence	1 つのサーバが Primary でその他が Backup として指定されます。Primary は常に NetDefendOS へのダウンロードに使用されます。利用できなくなると、バックアップサーバがプライマリになります。

ローカルデータベースを削除する

IDP またはアンチウィルスのいずれかの操作中に発生する技術的な問題は、データベースを削除し、リロードすることで解決されることがあります。IDP に対しては、以下のコマンドを使用します。

```
DFL-xxxx:/> updatecenter -removedb=idp
```

アンチウィルスデータベースを削除するためには、以下のコマンドを使用します。

```
DFL-xxxx:/> updatecenter -removedb=antivirus
```

一度削除すると、NetDefendOS を再起動し、データベースの更新を行う必要があります。 IDP またはアンチウィルスのいずれかが長期間使用されない場合、データベースを削除することをお勧めします。

注意 「updatecenter」と共に等号またはスペースを使用できます。

「updatecenter」コマンドオプションでは、オプションとその値の間の符号は、スペースまたは等号が使用されます。例題は以下の通りです。:

```
udpatecenter -update=antivirus
```

以下の通りに記載できます。

```
updatecenter -update antivirus
```

サブスクリプション期限満了の動作

サブシステムによって、サブスクリプション期限満了の動作は異なります。以下の項目があります。

- **Anti-Virus**
  サブスクリプション期限後もアンチウイルススキャンの処理は通常通り動作しますが、サブスクリプションが更新されるまで、シグネチャデータベースをアップデートしません。

- **IDP**
  サブスクリプション期限満了は、アンチウイルスと同様の動作が起こります。IDP のスキャンはそれまで通り動作しますが、サブスクリプションが更新されるまで、シグネチャデータベースをアップデートしません。

- **Web コンテンツフィルタリング**
  サブスクリプション期限満了により機能は無効となり、すべての Web サイトが許可されることになります。サブスクリプションの期限が終了すると、以下のログメッセージが NetDefendOS によって生成されます。

  ```
  content_filtering_disabled no_valid_license
  ```

- **アプリケーションコントロール**
  サブスクリプション期限満了により、すべてのアプリケーションでは「unknow」（未知）とタグ付けをされます。管理者が設定したアプリケーションコントロールの処理内容によって、トラフィックは、許可、または破棄されます。

  さらに、警告期限終了メッセージが CLI コンソールに表示され、期限終了のためとトラフィックに unknown タグが付いていることを示すログメッセージが生成されます。

- **IP レピュテーション**
  サブスクリプションの期限が過ぎると、IP レピュテーション検索は行われず、通常のトラフィックフローが継続します。IP レピュテーションログは有効化されていても出力されません。DoS Protection や Botnet Protection などの Threat Prevention オブジェクトが有効化されている場合、それらのオブジェクトに対しても IP レピュテーション検索は行われず、ブラックリストへの追加や接続の破棄も行われません。

これらのすべての機能のために、Web インタフェースで **Status > Maintenance > License** の順にメニューをクリックしていくと、終了日にそった関連サブスクリプションの現在の状態を参照できます。

付録 B IDP シグネチャグループ

IDP スキャンでは、以下のシグネチャグループを選択することができます。これらのグループは D-Link アドバンスト IDP サービスでのみ利用可能です。下記のシグネチャのグループ名は以下の形式になります。

```
group_subgroup
```

各エントリの IDS、IPS、Policy の Type 値は複数となる場合があるため、一覧には記載されていません。

現在のすべての IDP シグネチャは以下に記載されています。

http://security.dlink.com.tw

アドバイザリは NetDefend Live メニューの NetDefend IPS オプションから確認できます。

シグネチャの使用方法に関する詳細は「7.6 侵入検知と防御」を参照してください。

グループ名	侵入のタイプ
APP_AMANDA	Amanda, a popular backup software
APP_ETHEREAL	Ethereal
APP_ITUNES Apple	iTunes player
APP_REALPLAYER	Media player from RealNetworks
APP_REALSERVER	RealNetworks RealServer player
APP_WINAMP	WinAMP
APP_WMP MS Windows	Media Player
AUTHENTICATION_GENERAL	Authenticantion
AUTHENTICATION_KERBEROS	Kerberos
AUTHENTICATION_XTACACS	XTACACS
BACKUP_ARKEIA Network b	ackup solution
BACKUP_BRIGHTSTOR	Backup solutions from CA
BACKUP_GENERAL	General backup solutions
BACKUP_NETVAULT	NetVault Backup solution
BACKUP_VERITAS	Backup solutions
BOT_GENERAL	Activities related to bots, including those controlled by IRC channels
BROWSER_FIREFOX	Mozilla Firefox
BROWSER_GENERAL	General attacks targeting web browsers/clients
BROWSER_IE	Microsoft IE
BROWSER_MOZILLA	Mozilla Browser
COMPONENT_ENCODER	Encoders, as part of an attack
COMPONENT_INFECTION	Infection, as part of an attack
COMPONENT_SHELLCODE	Shell code, as part of the attacks
DB_GENERAL	Database systems
DB_MSSQL MS	SQL Server
DB_MYSQL	MySQL DBMS
DB_ORACLE	Oracle DBMS
DB_SYBASE	Sybase server
DCOM_GENERAL	MS DCOM
DHCP_CLIENT	DHCP Client related activities
DHCP_GENERAL	DHCP protocol
DHCP_SERVER	DHCP Server related activities
DNS_EXPLOIT	DNS attacks
DNS_GENERAL	Domain Name Systems
DNS_OVERFLOW	DNS overflow attack
DNS_QUERY	Query related attacks
ECHO_GENERAL	Echo protocol and implementations
ECHO_OVERFLOW	Echo buffer overflow
FINGER_BACKDOOR	Finger backdoor
FINGER_GENERAL	Finger protocol and implementation

グループ名	侵入のタイプ
FINGER_OVERFLOW	Overflow for Finger protocol/implementation
FS_AFS	Andrew File System
FTP_DIRNAME	Directory name attack
FTP_FORMATSTRING	Format string attack
FTP_GENERAL	FTP protocol and implementation
FTP_LOGIN	Login attacks
FTP_OVERFLOW	FTP buffer overflow
GAME_BOMBERCLONE	Bomberclone game
GAME_GENERAL	Generic game servers/clients
GAME_UNREAL	UnReal Game server
HTTP_APACHE	Apache httpd
HTTP_BADBLUE	Badblue web server
HTTP_CGI	HTTP CGI
HTTP_CISCO	Cisco Embedded Web Server
HTTP_GENERAL	General HTTP activities
HTTP_MICROSOFTIIS	HTTP Attacks specific to MS IIS web server
HTTP_OVERFLOWS	Buffer overflow for HTTP servers
HTTP_TOMCAT	Tomcat JSP
ICMP_GENERAL	ICMP protocol and implementation
IGMP_GENERAL	IGMP
IMAP_GENERAL	IMAP protocol/implementation
IM_AOL	AOL IM
IM_GENERAL	Instant Messenger implementations
IM_MSN	MSN Messenger
IM_YAHOO	Yahoo Messenger
IP_GENERAL	IP protocol and implementation
IP_OVERFLOW	Overflow of IP protocol/implementation
IRC_GENERAL	Internet Relay Chat
LDAP_GENERAL	General LDAP clients/servers
LDAP_OPEN	LDAP Open LDAP
LICENSE_CA-LICENSE	License management for CA software
LICENSE_GENERAL	General License Manager
MALWARE_GENERAL	Malware attack
METASPLOIT_FRAME	Metasploit frame attack
METASPLOIT_GENERAL	Metasploit general attack
MISC_GENERAL	General attack
MSDTC_GENERAL	MS DTC
MSHELP_GENERAL	Microsoft Windows Help
NETWARE_GENERAL	NetWare Core Protocol
NFS_FORMAT	Format
NFS_GENERAL	NFS protocol/implementation
NNTP_GENERAL	NNTP implementation/protocol
OS_SPECIFIC-AIX	AIX specific
OS_SPECIFIC-GENERAL	OS general
OS_SPECIFIC-HPUX	HP-UX related
OS_SPECIFIC-LINUX	Linux specific
OS_SPECIFIC-SCO	SCO specific
OS_SPECIFIC-SOLARIS	Solaris specific
OS_SPECIFIC-WINDOWS	Windows specific
P2P_EMULE eMule	P2P tool
P2P_GENERAL General	P2P tools
P2P_GNUTELLA Gnutella	P2P tool
PACKINGTOOLS_GENERAL	General packing tools attack
PBX_GENERAL	PBX

グループ名	侵入のタイプ
POP3_DOS	Denial of Service for POP
POP3_GENERAL	Post Office Protocol v3
POP3_LOGIN-ATTACKS	Password guessing and related login attack
POP3_OVERFLOW	POP3 server overflow
POP3_REQUEST-ERRORS	Request Error
PORTMAPPER_GENERAL	PortMapper
PRINT_GENERAL	LP printing server: LPR LPD
PRINT_OVERFLOW	Overflow of LPR/LPD protocol/implementation
REMOTEACCESS_GOTOMYPC	Goto MY PC
REMOTEACCESS_ PCANYWHERE	PcAnywhere
REMOTEACCESS_RADMIN	Remote Administrator (radmin)
REMOTEACCESS_VNC-CLIENT	Attacks targeting at VNC Clients
REMOTEACCESS_VNC-SERVER	Attack targeting at VNC servers
REMOTEACCESS_WIN-TERMINAL	Windows terminal/Remote Desktop
RLOGIN_GENERAL	RLogin protocol and implementation
RLOGIN_LOGIN-ATTACK	Login attacks
ROUTER_CISCO	Cisco router attack
ROUTER_GENERAL	General router attack
ROUTING_BGP	BGP router protocol
RPC_GENERAL	RFC protocol and implementation
RPC_JAVA-RMI	Java RMI
RSYNC_GENERAL	Rsync
SCANNER_GENERAL	Generic scanners
SCANNER_NESSUS	Nessus Scanner
SECURITY_GENERAL	Anti-virus solutions
SECURITY_ISS	Internet Security Systems software
SECURITY_MCAFEE	McAfee
SECURITY_NAV	Symantec AV solution
SMB_ERROR	SMB Error
SMB_EXPLOIT	SMB Exploit
SMB_GENERAL	SMB attacks
SMB_NETBIOS	NetBIOS attacks
SMB_WORMS	SMB worms
SMTP_COMMAND-ATTACK	SMTP command attack
SMTP_DOS	Denial of Service for SMTP
SMTP_GENERAL	SMTP protocol and implementation
SMTP_OVERFLOW	SMTP Overflow
SMTP_SPAM	SPAM
SNMP_ENCODING	SNMP encoding
SNMP_GENERAL	SNMP protocol/implementation
SOCKS_GENERAL	SOCKS protocol and implementation
SSH_GENERAL	SSH protocol and implementation
SSH_LOGIN-ATTACK	Password guess and related login attacks
SSH_OPENSSH	OpenSSH Server
SSL_GENERAL	SSL protocol and implementation
TCP_GENERAL	TCP protocol and implementation
TCP_PPTP	Point-to-Point Tunneling Protocol
TELNET_GENERAL	Telnet protocol and implementation
TELNET_OVERFLOW	Telnet buffer overflow attack
TFTP_DIR_NAME	Directory Name attack
TFTP_GENERAL	TFTP protocol and implementation
TFTP_OPERATION	Operation Attack

グループ名	侵入のタイプ
TFTP_OVERFLOW	TFTP buffer overflow attack
TFTP_REPLY	TFTP Reply attack
TFTP_REQUEST	TFTP request attack
TROJAN_GENERAL	Trojan
UDP_GENERAL	General UDP
UDP_POPUP	Pop-up window for MS Windows
UPNP_GENERAL	UPNP
VERSION_CVS	CVS
VERSION_SVN	Subversion
VIRUS_GENERAL	Virus
VOIP_GENERAL	VoIP protocol and implementation
VOIP_SIP	SIP protocol and implementation
WEB_CF-FILE-INCLUSION	Coldfusion file inclusion
WEB_FILE-INCLUSION	File inclusion
WEB_GENERAL	Web application attacks
WEB_JSP-FILE-INCLUSION	JSP file inclusion
WEB_PACKAGES	Popular web application packages
WEB_PHP-XML-RPC	PHP XML RPC
WEB_SQL-INJECTION	SQL Injection
WEB_XSS	Cross-Site-Scripting
WINS_GENERAL	MS WINS Service
WORM_GENERAL	Worms
X_GENERAL	Generic X applications

付録 C アンチウィルス MIME ファイルタイプ

NetDefendOS アプリケーションレイヤゲートウェイ（ALG）には、ダウンロードしたファイルのコンテンツが、ファイル名内のファイルタイプが示すタイプに一致することを確認する機能があります。MIME 検証が行われるファイルタイプがこの付録にあり、これが適用される ALG は以下の通りです。

- HTTP ALG
- FTP ALG
- POP3 ALG
- SMTP ALG

この付録リストは、ダウンロードしたファイルのコンテンツがファイルタイプと一致しているかを NetDefendOS でチェックして確認する MIME ファイルタイプのリストです。MIME 検証とファイルタイプについての詳細は、「6.1.2 HTTP ALG」を参照してください。

ファイルタイプ拡張子	アプリケーション
3ds	3d Studio files
3gp	3GPP multimedia file
aac	MPEG-2 Advanced Audio Coding File
ab	Applix Builder
ace	ACE archive
ad3	Dec systems compressed Voice File
ag	Applix Graphic file
aiff, aif	Audio Interchange file
am	Applix SHELF Macro
arc	Archive file
alz	ALZip compressed file
avi	Audio Video Interleave file
arj	Compressed archive
ark	QuArk compressed file archive
arq	Compressed archive
as	Applix Spreadsheet file
asf	Advanced Streaming Format file

ファイルタイプ拡張子	アプリケーション
ash	Shell script
avr	Audio Visual Research Sound
aw	Applix Word file
awk	AWK Script
bash	Bash shell script
bh	Blackhole archive format file
bmp	Windows Bitmap Graphics
book	FrameMaker Book
box	VBOX voice message file
bsa	BSARC Compressed archive
bz, bz2	Bzip UNIX compressed file
cab	Microsoft Cabinet file
cdr	Corel Vector Graphic Drawing file
cgm	Computer Graphics Metafile
chz	ChArc compressed file archive
class	Java byte code
cmf	Creative Music file
core/core	dump Unix core dump
cpl	Windows Control Panel Extension file
Csh	C shell script
dbm	Database file
dcx	Graphics Multipage PCX Bitmap file
deb	Debian Linux Package file
djvu	DjVu file
dll	Windows dynamic link library file
dpa	DPA archive data
dvi	TeX Device Independent Document
eet	EET archive
egg	Allegro datafile
elc	eMacs Lisp Byte-compiled Source Code
emd	ABT EMD Module/Song Format file
esp	ESP archive data
exe	Windows Executable
fgf	Free Graphics Format file
flac	Free Lossless Audio Codec file
flc	FLIC Animated Picture
fli	FLIC Animation
flv	Macromedia Flash Video
gawk	GAWK script
gdbm	Database file
gif	Graphic Interchange Format file
gzip, gz, tgz	Gzip compressed archive
hap	HAP archive data
hpk	HPack compressed file archive
hqx	Macintosh BinHex 4 compressed archive
icc	Kodak Color Management System, ICC Profile
icm	Microsoft ICM Color Profile file
ico	Windows Icon file
imf	Imago Orpheus module sound data
Inf	Sidplay info file
ipa	iPhone application archive file
it	Impulse Tracker Music Module
java	Java source code
jar	Java JAR archive

ファイルタイプ拡張子	アプリケーション
jng	JNG Video Format
jpg, jpeg, jpe, jff, jfif, jif	JPEG file
jrc	Jrchive compressed archive
jsw	Just System Word Processor Ichitaro
kdelnk	KDE link file
ksh	Shell script
latex	LaTeX Source Document
lha	LHA compressed archive file
lim	Limit compressed archive
lisp	LIM archive data
lzh	LZH compressed archive file
maker	FrameMaker Print file
md	MDCD compressed archive file
mdb	Microsoft Access Database
mid,midi	Musical Instrument Digital Interface MIDI-sequence Sound
mif	FrameMaker MIF file
mmf	Yamaha SMAF Synthetic Music Mobile Application Format
mml	FrameMaker MML file
mng	Multi-image Network Graphic Animation
mod	Ultratracker module sound data
mp3	MPEG Audio Stream, Layer III
mp4	MPEG-4 Video file
mpg,mpeg	MPEG 1 System Stream , Video file
mpv	MPEG-1 Video file
Microsoft files	Microsoft office files, and other microsoft files
msa	Atari MSA archive data
msg	Saved news text
nawk	NAWK script
niff, nif	Navy Interchange file Format Bitmap
noa	Nancy Video CODEC
nsf	NES Sound file
obj, o	Windows object file, linux object file
ocx	Object Linking and Embedding (OLE) Control Extension
ogg	Ogg Vorbis Codec compressed WAV file
out	Linux executable
pac	CrossePAC archive data
pbf	Portable Bitmap Format Image
pbm	Portable Bitmap Graphic
pdf	Acrobat Portable Document Format
pe	Portable Executable file
pfb	PostScript Type 1 Font
pgm	Portable Graymap Graphic
pgp	Pretty Good Privacy files
pkg	SysV R4 PKG Datastreams
pl	PERL Program file
pll	PAKLeo archive data
pma	PMarc archive data
png	Portable (Public) Network Graphic
ppm	PBM Portable Pixelmap Graphic
ps	PostScript file
psa	PSA archive data
psd	Photoshop Format file
qt, mov, moov	QuickTime Movie file
qxd	QuarkXpress Document

ファイルタイプ拡張子	アプリケーション
ra, ram	RealMedia Streaming Media
rar	WinRAR compressed archive
rbs	ReBirth Song file
riff, rif	Microsoft Audio file
rm	RealMedia Streaming Media
rpm	RedHat Package Manager
rtf, wri	Rich Text Format file
sar	Streamline compressed archive
sbi	SoundBlaster instrument data
sc	SC spreadsheet
sgi	Silicon Graphics IRIS Graphic file
sh	Shell script
sid	Commodore64 (C64) Music file (SID file)
sit	StuffIt archives
sky	SKY compressed archive
snd, au	Sun/NeXT audio file
so	UNIX Shared Library file
sof	ReSOF archive
sqw	SQWEZ archive data
sqz	Squeeze It archive data
stm	Scream Tracker v2 Module
svg	Scalable Vector Graphics file
svr4	SysV R4 PKG Datastreams
swf	Macromedia Flash Format file
tar	Tape archive file
tcsh	Shell script
tex	TeX Source
tfm	TeX font metric data
tiff, tif	Tagged Image Format file
tnef	Transport Neutral Encapsulation Format
torrent	BitTorrent Metainfo file
ttf	TrueType Font
txw	Yamaha TX Wave audio files
ufa	UFA archive data
vcf	Vcard file
viv	VivoActive Player Streaming Video file
wav	Waveform Audio
wk	Lotus 1-2-3 document
wmv	Windows Media file
wrl, vrml	Plain Text VRML file
xcf	GIMP Image file
xm	Fast Tracker 2 Extended Module , audio file
xml	XML file
xmcd	xmcd database file for kscd
xpm	BMC Software Patrol UNIX Icon file
yc	YAC compressed archive
zif	ZIF image
zip	Zip compressed archive file
zoo	ZOO compressed archive file
zpk	ZPack archive data
zsh	Shell script
z	Unix compressed file

付録 D OSI 参照モデル

OSI（Open System Interconnection）モデルは、異なるプロトコルをさまざまなネットワークアプリケーション 7 個の小さく、より管理しやすいレイヤに分類することによって、コンピュータ間の通信に基本の枠組みを定義します。OSI モデルは、 1 つのコンピュータのアプリケーションから来るデータがネットワークという手段を経由して、別のコンピュータのアプリケーションに転送される方法を記述しています。

データトラフィックの制御は 1 つのコンピュータ内のアプリケーションレイヤから開始し、一番下のレイヤに向かって処理を行っていき、別のコンピュータに向かってネットワークを通過し、その後階層の上に送信することで 1 つのレイヤから次のレイヤに渡されます。各レイヤは特定のプロトコルセットを処理するため、アプリケーションを実行するタスクは異なるレイヤに伝搬されることができ、独立して実行されることができます。OSI モデルは、ARP、サービス、および ALG など多くの NetDefendOS 機能の操作を理解するために有効です。

レイヤ番号	レイヤの目的
レイヤ 7	アプリケーション
レイヤ 6	プレゼンテーション
レイヤ 5	セッション
レイヤ 4	トランスポート
レイヤ 3	ネットワーク
レイヤ 2	データリンク
レイヤ 1	物理

図 D-1　OSI 7 層モデル

各レイヤは、以下の機能を実行します。:

レイヤ 7 - アプリケーションレイヤ
直接アプリケーションをサポートするユーザインタフェースを定義します。
プロトコル : HTTP、FTP、DNS、SMTP、Telnet、SNMP など。ALG はこのレベルで動作します。

レイヤ 6 - プレゼンテーションレイヤ
さまざまなアプリケーションを残りのレイヤが理解できる一定のネットワークフォーマットに変換します。

レイヤ 5 - セッションレイヤ
ネットワークを経由するセッションの確立、維持および終了を行います。
プロトコル : NetBIOS、RPC など。

レイヤ 4 - トランスポート層
データフローを制御し、エラー処理を提供します。
プロトコル : TCP、UDP など。

レイヤ 3 - ネットワーク層
アドレッシングとルーティングを行います。
プロトコル : IP、OSPF、ICMP、IGMP など。

レイヤ 2 - データリンク層
データを組み立てます。
プロトコル : Ethernet、PPP など。ARP はこのレベルで動作します。

レイヤ 1 - 物理層
ハードウェアサポート接続を定義します。

付録 E DFL-260E/860E のポートベース VLAN

NetDefend DFL-260E と DFL-860E のファイアウォールにおける VLAN サポートは 2 つのタイプに分かれます。

- LAN インタフェース以外のイーサネットインタフェースでは、VLAN は、通常の方法で NetDefendOS にそれらを設定することで作成されます。パケット内の VLAN タグを追加および認識するタスクを行うのが NetDefendOS です。それはハードウェア機能ではありません。

  「3.4.4 VLAN」 で DFL-260E と DFL-860E における VLAN の標準タイプの設定方法が説明されています。

- LAN インタフェースでのみ、VLAN は異なる方法で NetDefendOS に設定されます。

  すべての LAN インタフェースが一般的なハードウェアスイッチファブリックにより共に接続されます。また、このファブリックは、インタフェースに設定されたどんな VLAN に対するタグ付きパケットの管理も行います。これによりポートベース VLAN を設定することができます。

  この付録は、LAN インタフェースのポートベース VLAN 設定について説明します。

LAN インタフェースにおける VLAN 配置には、以下の特性があります。:

- DFL-260E と DFL-860E の LAN インタフェースのそれぞれには、別々の VLAN でまたは VLAN グループの一部がある可能性があります。
- DFL-260E と DFL-860E の LAN インタフェースを、各 VLAN に任意の数の物理ポートを使用して VLAN グループにすることができます。例えば、最初の 2 つのインタフェースを 1 つの VLAN のパーツにするように、次に 2 つのインタフェースを 2 つ目の VLAN のパーツにするように、残りは通常の操作のままにするように、インタフェースを分割することができます。
- VLAN でない LAN インタフェースは、1 つのインタフェースとして LAN という論理インタフェース名で動作を続けます。

VLAN の設定

ポートベース VLAN を設定する方法を例題で説明します。以下のとおり、LAN インタフェースを分割する要件を仮定します。:

- 最初の LAN インタフェースは、通常、スイッチファブリックを通じて動作を続けます。したがって、これは論理的な NetDefendOS インタフェース lan になります。
- LAN インタフェース 2、3、および 4 は論理名 lan_port2-4 で個別の VLAN になります。残りの LAN インタフェース 4 は論理名 lan_5_plus で 1 つの VLAN になります。これは、DFL-260E の 5 番目のインタフェースと DFL-860E の上の 5 番目～ 8 番目のインタフェースを含みます。

これらの VLAN を設定するには、Web インタフェースで以下の手順を実行してください。:

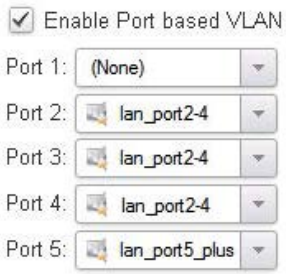
1. VLAN オブジェクトを定義する
Web インタフェースでは、**Network > Interfaces and VPN > VLAN > Add> VLAN** に行き、2 つの新しい VLAN オブジェクトを追加します。各 VLAN では、VLAN ID、IP アドレス、および Network プロパティのために任意の値を割り当てます。VLAN ID だけが、LAN インタフェースに固有である必要があります。IP アドレスはパブリック IPv4 アドレスであってはいけません。

Web インタフェースに表示される VLAN リストの出力結果を以下に示します。

# ▲	Name	Interface	VLAN ID	IPv4 Address	IPv6 Address...	Network
1	lan_port2-4	lan	200	192.168.20.1		192.168.20.0/24
2	lan_port5_plus	lan	300	192.168.30.1		192.168.30.0/24

2. LAN インタフェースに VLAN を関連付けます。
Network > Interfaces and VPN > Miscellaneous > Switch Management の順にメニューをクリックします。ポートベース VLAN を有効にして、それぞれの番号を付けた LAN インタフェースに希望のコンフィグレーションを得るように適切な VLAN に関連付けを行います。

例えば、以下の画面はこれが Web インタフェースで表示する結果を示しています。



DFL-860E のためには、上記のリストに続いて以下の追加を行います。

この最後のダイアログは、ポートベース VLAN をサポートする D-Link ファイアウォールの Web インタフェースだけで利用可能です。

ポートベース VLAN の問題

ポートベース VLAN を設定する時に、管理者が意識するべきいくつかの問題があります。

- **ポートベース VLAN を VLAN トランクスに混ぜることができません。**
  ポートベース VLAN 機能を使用している場合、LAN インタフェースのすべてがアクセスポートとして動作しており、802.1q VLAN トランク用には使用できません。

- **MAC アドレスが重複します。**
  すべての LAN インタフェースの MAC アドレスは同じです。これは、スイッチが、2 つの異なる IP アドレスにもかかわらず、同じ MAC アドレスを持つファイアウォールに 2 つの接続を持つかもしれないことを意味します。いくつかのスイッチではこれが問題となるかもしれません。その状況では、別々のスイッチを使用することで回避するべきです。

付録 F 初期設定

DFL-260E

前面パネルの記述	ファイアウォール内の名前	インタフェース定義	インタフェースの IP アドレス	DHCP ステータス
WAN	WAN	Static IP	0.0.0.0	無効
DMZ	DMZ	Static IP	172.17.100.254/24	無効
1 ～ 5	LAN	Static IP	192.168.10.1/24	無効

DFL-860E

前面パネルの記述	ファイアウォール内の名前	インタフェース定義	インタフェースの IP アドレス	DHCP ステータス
WAN1	WAN1	Static IP	0.0.0.0	無効
WAN2	WAN2	Static IP	192.168.120.254/24	無効
DMZ	DMZ	Static IP	172.17.100.254/24	無効
1 ～ 8	LAN	Static IP	192.168.10.1/24	無効

DFL-870

前面パネルの記述	ファイアウォール内の名前	インタフェース定義	インタフェースの IP アドレス	DHCP ステータス
1	WAN1	DHCP	0.0.0.0	有効
2	WAN2	Static IP	192.168.120.254/24	無効
3	DMZ	Static IP	172.17.100.254/24	無効
4	LAN1	Static IP	192.168.10.1/24	無効
5	LAN2	Static IP	192.168.11.1/24	無効
6	LAN3	Static IP	192.168.12.1/24	無効

DFL-1660

前面パネルの記述	ファイアウォール内の名前	インタフェース定義	インタフェースの IP アドレス	DHCP ステータス
1	WAN1	DHCP	0.0.0.0	有効
2	WAN2	Static IP	192.168.120.254/24	無効
3	DMZ	Static IP	172.17.100.254/24	無効
4	LAN1	Static IP	192.168.10.1/24	無効
5	LAN2	Static IP	192.168.20.1/24	無効
6	LAN3	Static IP	192.168.30.1/24	無効

DFL-2560

前面パネルの記述	ファイアウォール内の名前	インタフェース定義	インタフェースのＩＰアドレス	DHCP ステータス
1	WAN1	DHCP	0.0.0.0	有効
2	WAN2	Static IP	192.168.120.254/24	無効
3	DMZ1	Static IP	172.17.100.254/24	無効
4	DMZ2	Static IP	172.17.110.254/24	無効
5	DMZ3	Static IP	172.17.120.254/24	無効
6	DMZ4	Static IP	172.17.130.254/24	無効
7	LAN1	Static IP	192.168.10.1/24	無効
8	LAN2	Static IP	192.168.20.1/24	無効
9	LAN3	Static IP	192.168.30.1/24	無効
10	LAN4	Static IP	192.168.40.1/24	無効

DFL-2560G

前面パネルの記述	ファイアウォール内の名前	インタフェース定義	インタフェースのＩＰアドレス	DHCP ステータス
1	WAN1	DHCP	0.0.0.0	有効
2	WAN2	Static IP	192.168.120.254/24	無効
3	DMZ1	Static IP	172.17.100.254/24	無効
4	DMZ2	Static IP	172.17.110.254/24	無効
5	DMZ3	Static IP	172.17.120.254/24	無効
6	DMZ4	Static IP	172.17.130.254/24	無効
7	LAN1	Static IP	192.168.10.1/24	無効
8	LAN2	Static IP	192.168.20.1/24	無効
9	LAN3	Static IP	192.168.30.1/24	無効
10	LAN4	Static IP	192.168.40.1/24	無効

管理設定

設定項目		設定内容
管理者アカウント	ユーザ名	admin
	パスワード	admin

付録 G 登録＆アクティベーション手順

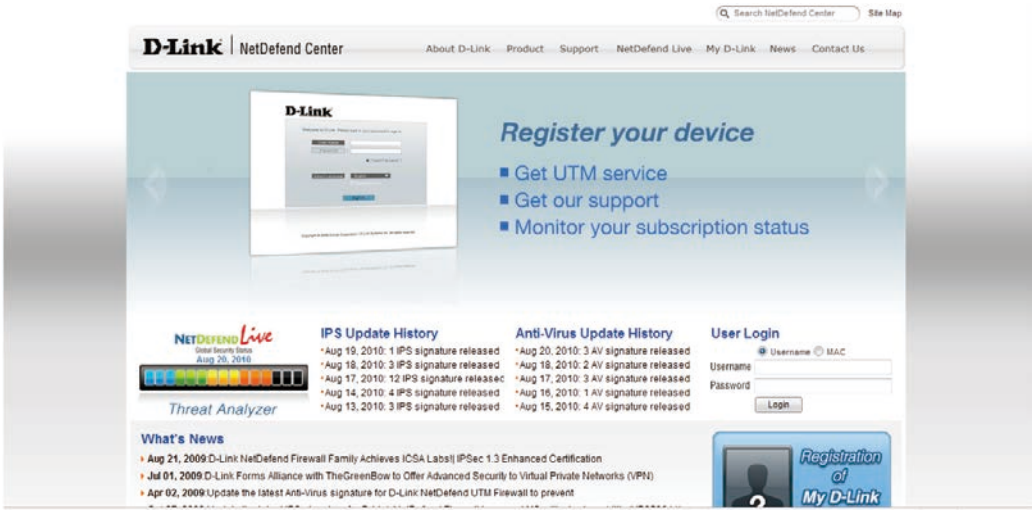
Introduction

D-Link NetDefend UTM firewalls DFL-260E/860E/1660/2560/2560G integrate Intrusion Prevention System, gateway Anti-Virus and Web Content Filtering, for improving Layer 7 content inspection performance, D-Link adopt UTM acceleration technology to increase IPS and AV throughput, and web surfing control database contains millions of URLs for Web Content Filtering. IPS, Anti-Virus and URL database real-time update service to protect your enterprise network from application exploits, network worms, malicious code attacks and management employees Internet access behavior. Three database of UTM firewall should be kept up to date against a variety of threats from the Internet. Today D-Link delivers NetDefend UTM Subscription, including NetDefend IPS, Anti-Virus and WCF update services individually; to ensure your UTM firewall' s service database **i**s accurate and up-to-date.

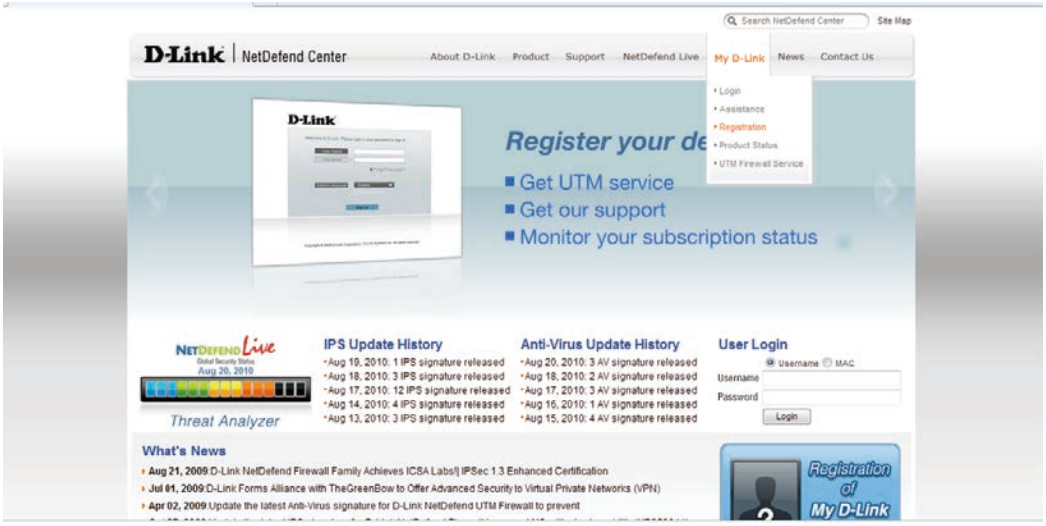
Apply for a D-Link Membership

You need to visit D-Link NetDefend Security Portal, which provides a registration platform and abundant professional security resources to customers,

1. Please launch your browser and input the following URL: http://security.dlink.com.tw.

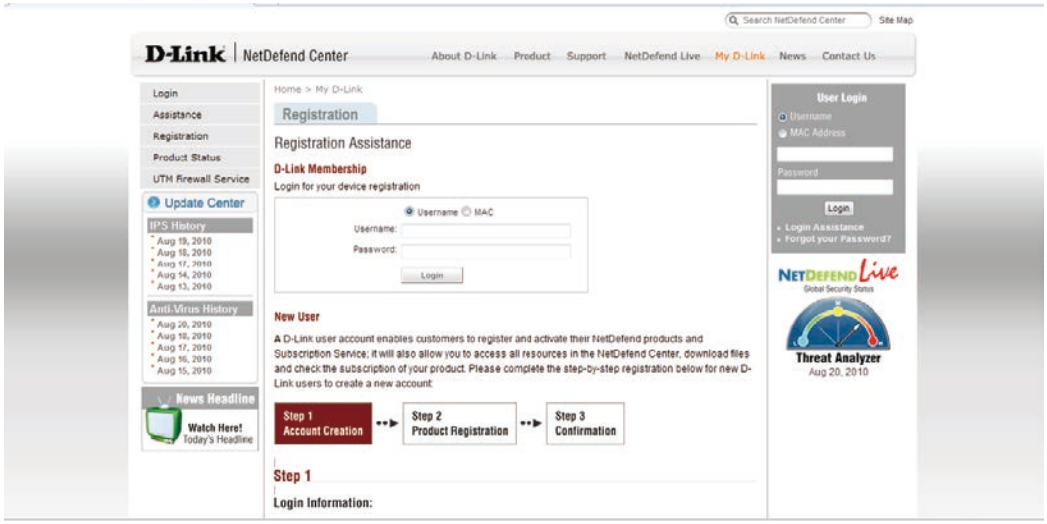


2. Go to "My D-Link" in the menu bar, and click "Registration" from the pull down menu.



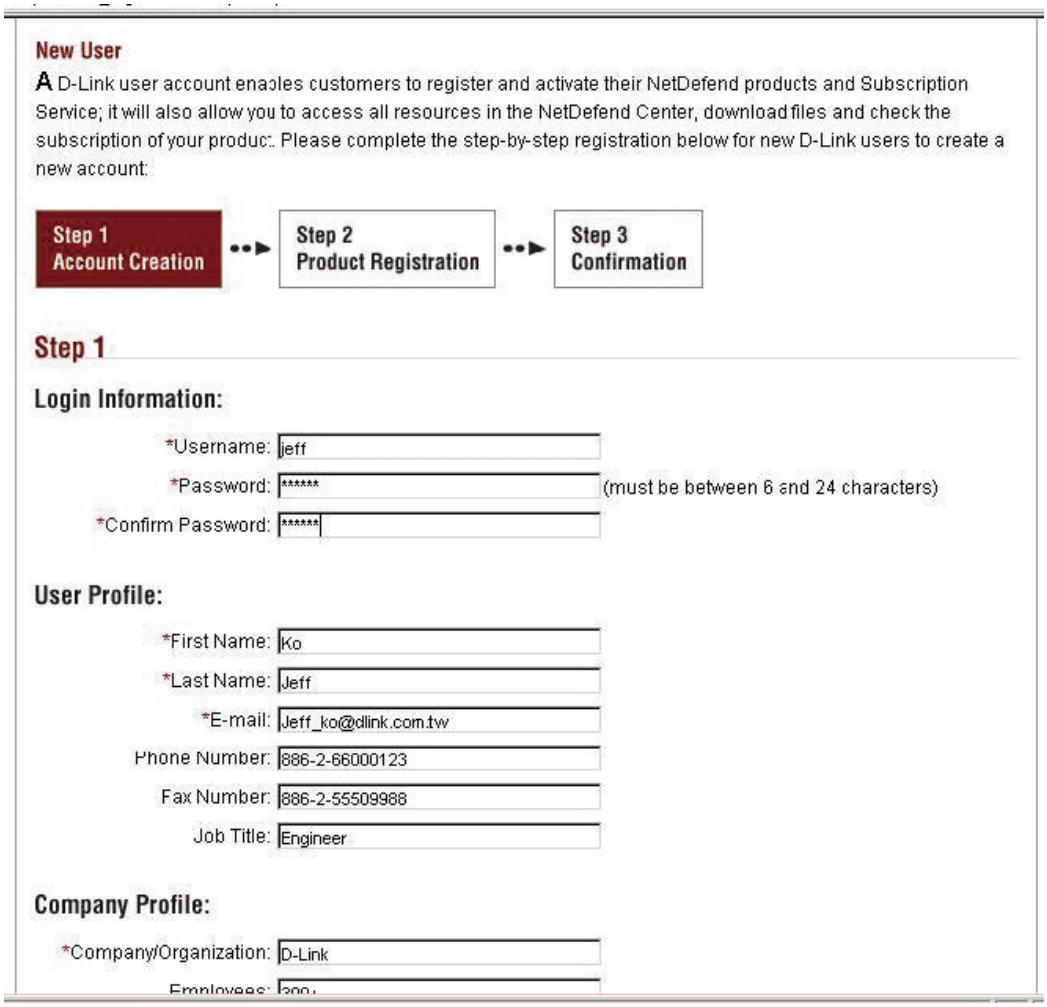
3. For security concern, your information provided in "My D-Link" is protected by HTTPS communication.

4. If you are already a D-Link member, and you want to register another firewall product, please input your username and password, then logon "My D-Link" directly.

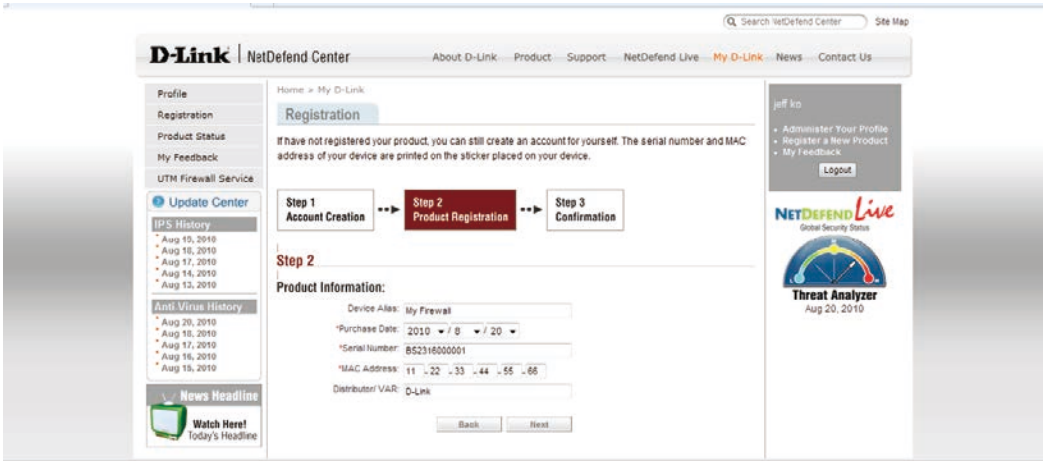


5. If you are new to "My D-Link" , please comprehend the registration information for My D-Link membership by following the steps below:

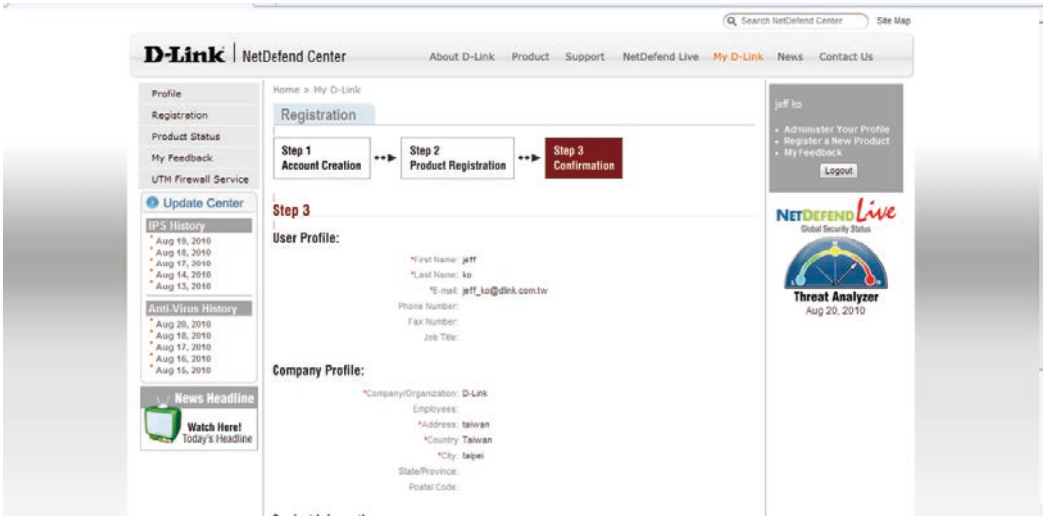
Step 1: Provide Login Information, User Profile and Company Profile. Please make sure you fill in the correct information for your membership.



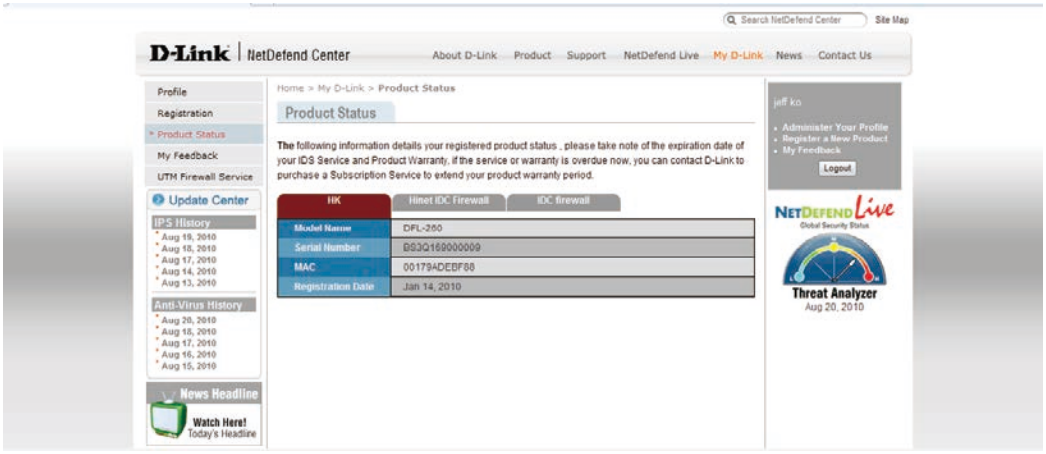
Step 2: Please fill in the MAC address and Serial Number of your appliance. To find the information, you can check the label at the bottom of the appliance.



Step 3: Please make sure you provide the correct information before submitting your registration.



6. After you complete the registration, you can check and review your registered Product Status anytime via NetDefend Security Portal.



D-Link NetDefend UTM Subscription

The standard NetDefend UTM (Unified Threat Management) Subscription provides your security device with UTM services for 90 days free trial starting from the day you activate or extend your service. Your NetDefend UTM Subscription should be renewed regularly to provide your security device with important updates and your network with the most up-to-date security service available from D-Link.

NetDefend UTM Subscription includes 3 optional services, IPS, Anti-Virus and Web Content Filtering. Customer can purchase either one of the 3 or any service combination.

D-Link NetDefend IPS Subscription

D-Link adopts the unique technology -Component-based signatures, which are built to recognize and protect against all varieties of known and unknown attacks, and address several aspects of an attack including payload, NOP sled, infection, exploit and more. In terms of signature coverage, the database includes attacks and data from a global attack sensor-grid and exploits collected from public sites such as the National Vulnerability Database and Bugtrax.

D-Link commits to deliver high quality IPS signatures by constantly creating and optimizing the signatures via D-Link Auto-Signature sensor system. Without overloading the existing security appliances, D-Link IPS signatures ensure a high ratio of detection accuracy and a lowest ratio of false positive.

D-Link NetDefend Anti-Virus Subscription

NetDefend UTM Firewall implements Stream Based Virus Scanning technology without caching the incoming files first, thus increase the inspection performance of UTM Firewall, and ease the nightmare of network bottleneck while enabling antivirus feature on UTM Firewall.

NetDefend UTM Firewall adopts the Signatures from the Well-Known Kaspersky Lab to enable customers the prompt signature update time and high quality antivirus signatures.

Built-in extreme performance AV acceleration engine together with stream-based virus scanning technology, NetDefend UTM Firewall blocks virus and malware before they ever reach the desktops or mobile devices, thus creates a safer network environment for SMB and enterprises.

D-Link NetDefend Web Content Filtering Subscription

Web surfing is becoming a critical concern of enterprise business, D-Link Web Content Filtering service enforces protection and management policy in terms of Internet resources access for your organization.

NetDefend Web Content Filtering Subscription helps organizations Monitor, Manage, and Control employee usage of and access to Internet resources. It puts management back in control, enabling a more business orientated and cost effective usage of the Internet.

Allow organizations to gain significant cost savings through:

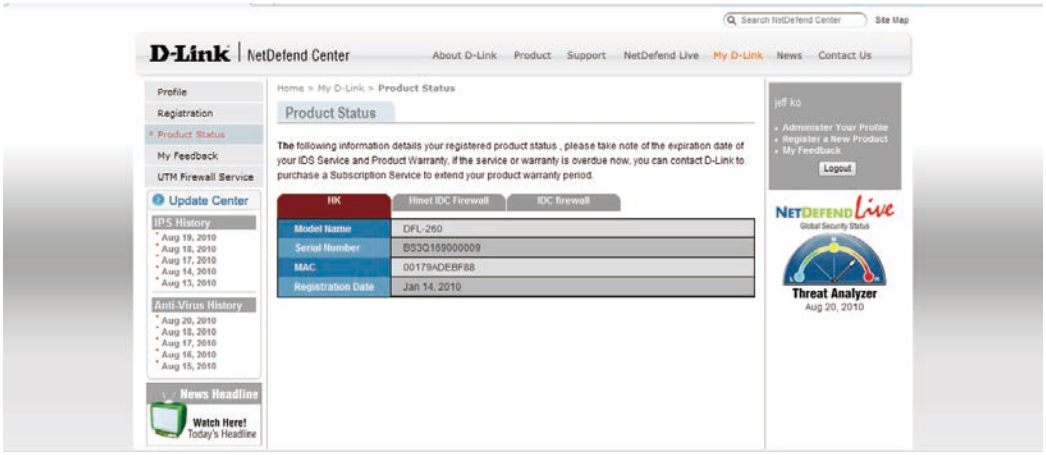
1) Areduction in wasted staff time (by reducing inappropriate web surfing).
2) Reduced Internet access costs and achieving bandwidth savings – by limiting and / or controlling non-business related use, and improve network response
3) Reducing legal exposure to work place relations (e.g. sexual harassment cases / child pornography and the adverse publicity that an incident would generate)
4) Reduced costs for recovering from an attack as less inappropriate content will be allowed to enter into the network.

Activate your update service of UTM firewall

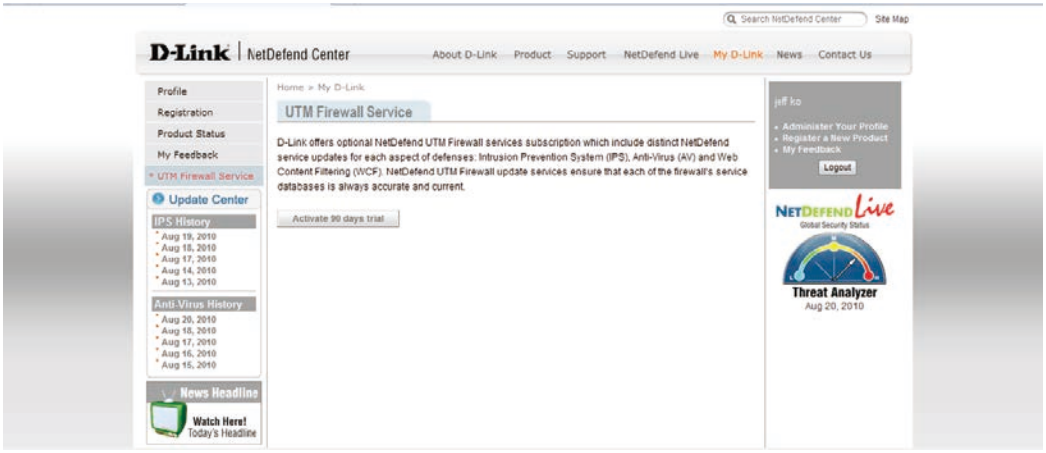
D-Linkprovides90daysfreetrial* forIPS,Anti-VirusandWCFservice. After 90 days trial period expired, you need to subscribe NetDefend UTM Subscription Package and enter authentication code onto the device GUI to renew your either one of NetDefend UTM Service or all service combination you purchased.

How to activate 90 days free trial Update Service of UTM firewall?

1. Please login your account on NetDefend Center, and click "UTM Firewall Service" of My D-Link, and click "Activate 90 days trial" button.



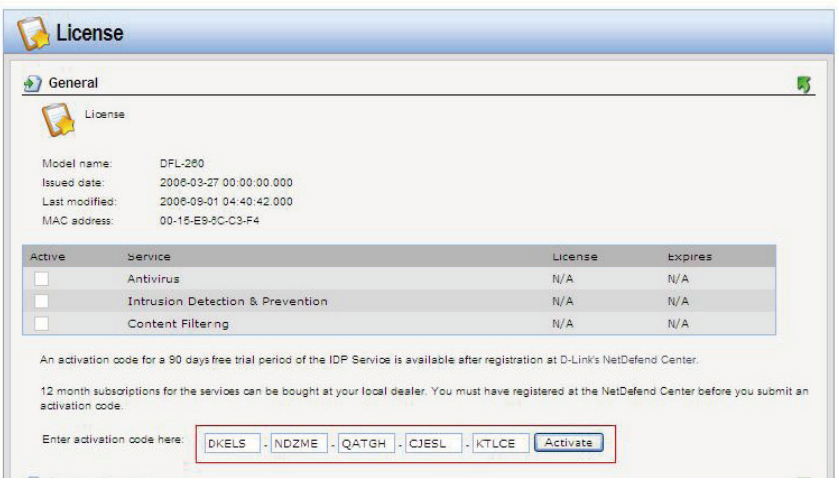
2. YouwillgetthealloftrialactivationcodesforUTMUpdateService.



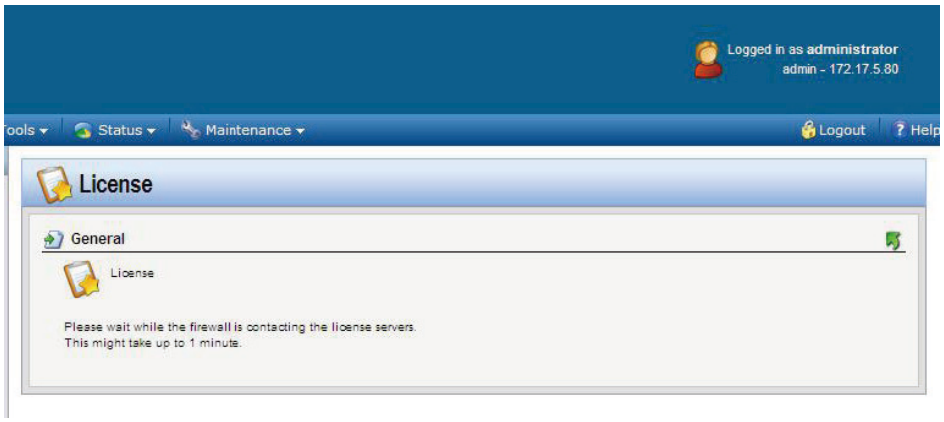
3. Login your firewall, point your mouse to "Maintenance " in the tool bar of firewall UI, and click "License" from the pull down menu. You can enter the trial activation code for UTM Update Service from here.

For Example: You want to activate IPS Update Service

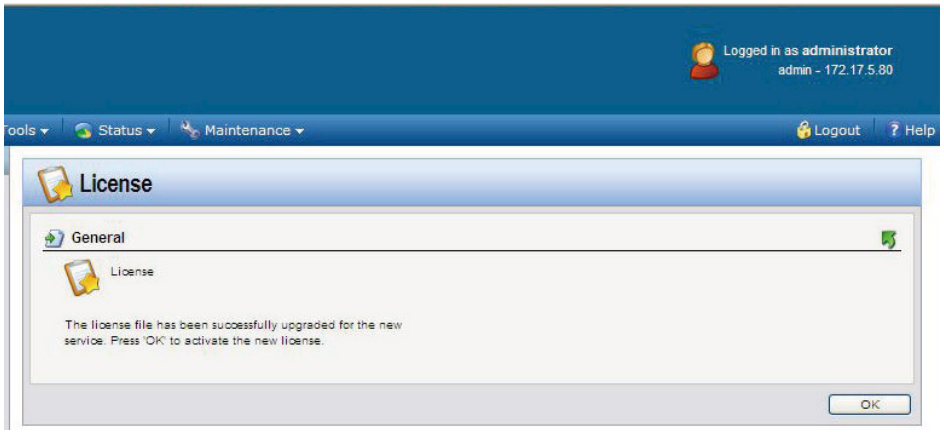
a. Enter the IPS trial activation code and click the "Activate" button



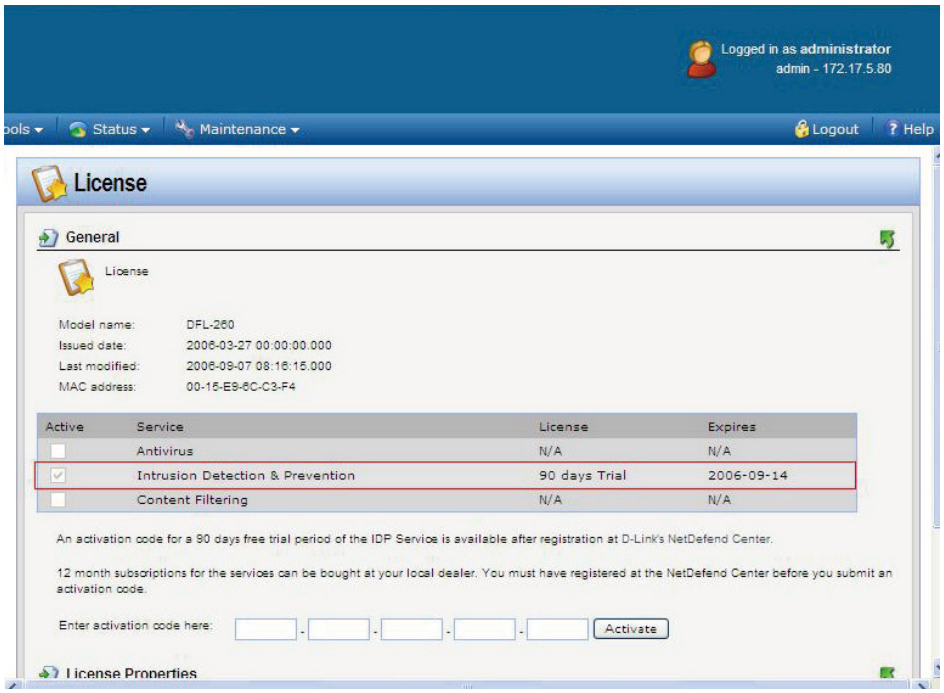
b. Firewall is contacting the License Server



c. Activate trial License successfully



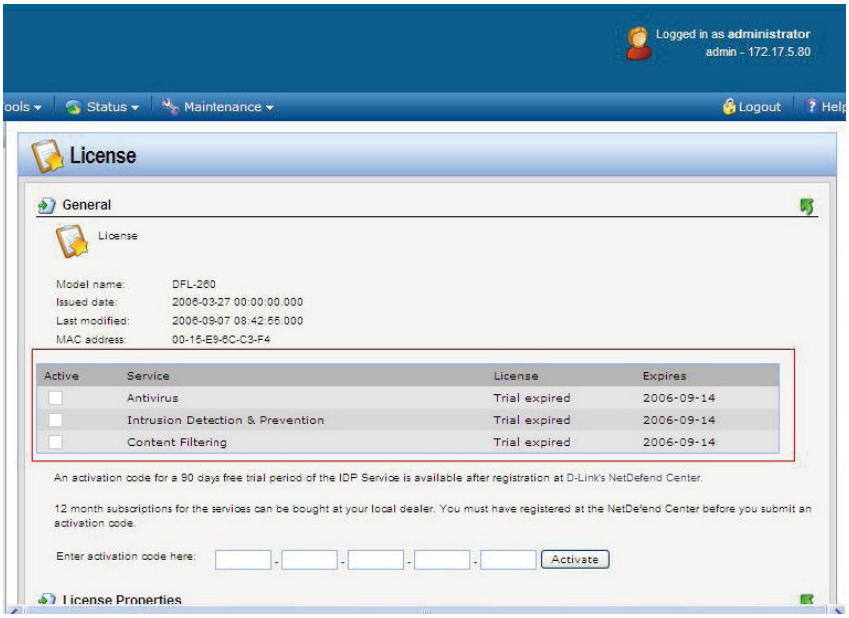
d. Trial IPS update service is enabled



* Your UTM subscription period is based on the type of package that has been purchased.

Extend your NetDefend UTM Update Service

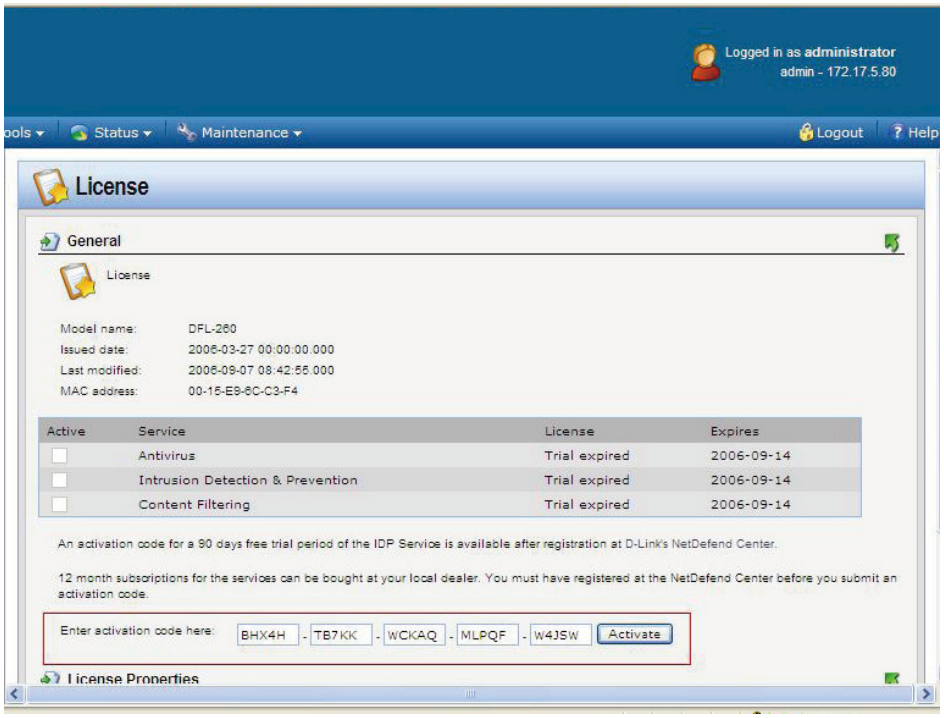
1. If your one or above of three update service is expired



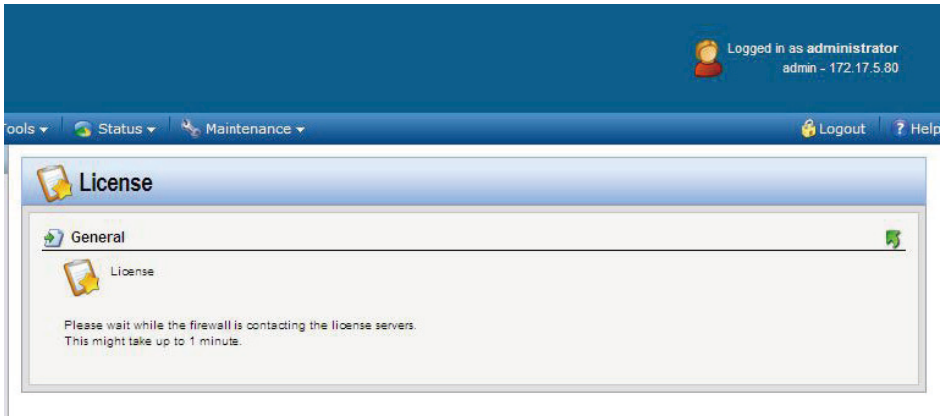
2. You can purchase NetDefend UTM Subscription to extend one of UTM Update service you needed from all authorized D-Link NetDefend resellers.

3. After receiving the service package, please find the authentication code on the license card.

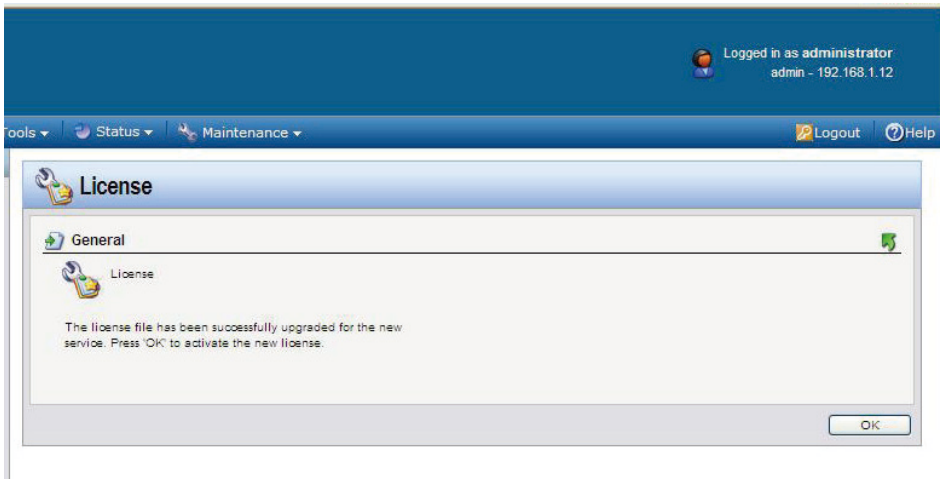
4. Login your firewall, point your mouse to “Maintenance” in the tool bar of firewall UI, and click “License” from the pull down menu. Enter the authentication code and click the “Activate” button



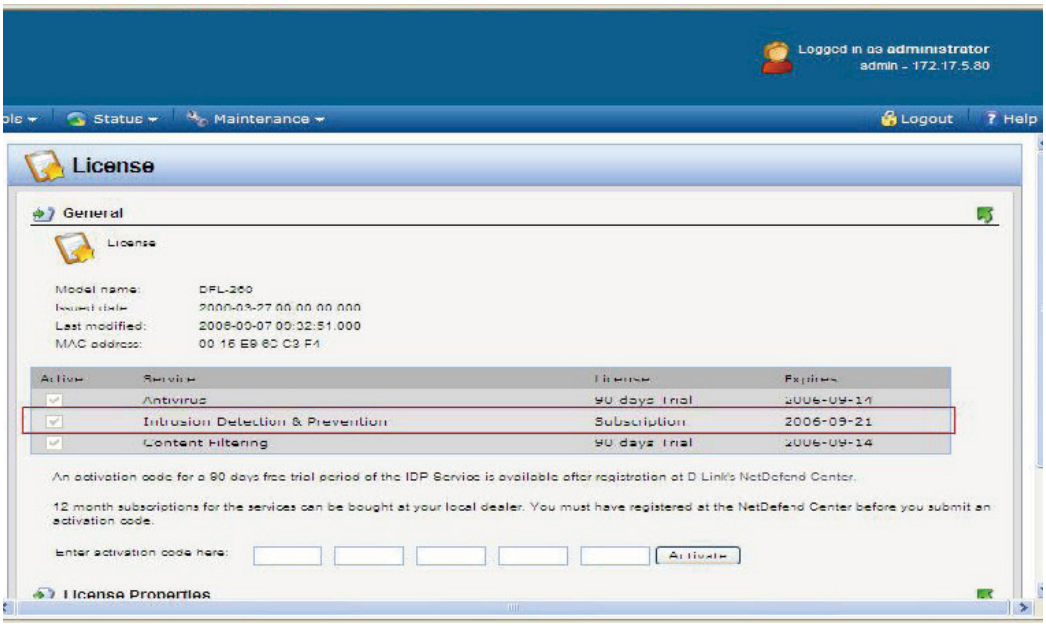
5. Firewall is contacting the License Server



6. Activate Subscription License successfully



7. IPS update service of NetDefend UTM Subscription you purchased is enabled.



付録 H Identity Awareness Agent (IDA) のインストールと管理

IDA Overview

Introduction

This guide describes the installation and administration of the Identity Awareness Agent (IDA) software. The IDA software is a component of the NetDefendOS identity awareness feature which is used for authentication of remote clients. This guide can be seen as an extension of the identity awareness description which can be found in the authentication section of the Administration Guide.

The Software is Separate to NetDefendOS

The IDA software is not supplied with NetDefendOS as it is a piece of self-contained software. Instead, it must be downloaded separately from the D-Link website. The IDA software version numbering is also different from NetDefendOS version numbering and new IDA versions may be released at any time.

The Software Runs On Windows Domain Servers

The IDA software runs on one or more Windows domain servers in an active directory, sending back authenticated client information to NetDefendOS so that further authentication is not necessary. The IDA can run on either a domain controller or domain member. Installation of the IDA software on multiple servers will provide redundancy.

Compatible Windows Servers

The IDA software can be installed on any of the following Windows server products:

- Windows 2003
- Windows 2008
- Windows 2008R2
- Windows 2012
- Windows 2016

IDA Installation Detailed guidelines for installation are described in the next chapter.

IDA Installation

The latest IDA software release can be downloaded from the D-Link website. The installation file is a self-extracting Windows executable. When the IDA software is installed, it runs as a Windows service called IDA.exe.

IDA Installation Requirements

The following should be noted when installing the IDA:

- When installing the IDA software, the user **must** have administrator privileges.
- When the IDA software is installed on a server that is not an Active Directory Domain Controller, it must be started using an account that has the privileges to allow the reading of the Security Event Log of the Domain Controller.
- It is recommended to run the IDA software at a lower priority than other processes.
- The IDA software must have permissions to do the following:
  - Read from the event log. To do this a user must be a member of the Event Log Readers user group. This group can be found in the Builtin Active Directory container.
  - Query the Active Directory for users and groups.
- The IDA software can also run as the Local System account.
  If the Remote Event Log Monitoring feature is required, an account for the computer where IDA is installed should be added to the Event Log Readers user group.

Deployment in Medium to Large Infrastructure Environments

If an environment has two domain controllers, it is recommended to install the IDA software on each domain controller and set them up to monitor the local Windows Event Log.

In an environment with a larger infrastructure, there is no need to install the IDA software on every single domain controller. Instead, remote Windows Event Log monitoring should be enabled.

If there are multiple sites in different geographic locations, it is highly recommended to have the IDA software installed in each local network.

Important: The Windows Server event IDs must be correct

The D-Link IDA software will only listen for certain event IDs so the Windows Server should be configured so that the correct IDs are generated. The IDs that the IDA listens for are as follows:

- **For Windows Server 2003**, the IDA listens for the following events:
  - **636** - A user has been added to a local domain group.
  - **637** - A user has been removed from a local domain group.
  - **673** - A user has logged in.
- **For Windows Server 2008 and later**, the IDA listens for the following events:
  - **103** - An RDP user has logged in and has been assigned a virtual IP.
  - **104** - An RDP user has logged out and the user's IP has been released.
  - **4732** - A user has been added to a local domain group.
  - **4733** - A user has been removed from a local domain group.
  - **4768** - A user has logged in.

IDAManagement

The IDAManagement Interface

The IDA service listens for authenticated users and sends their details to the configured NetDefend Firewall. The IDA service has its own management user interface and this interface has a number of tabs which are described below.

The General tab

This tab consists of the following settings:

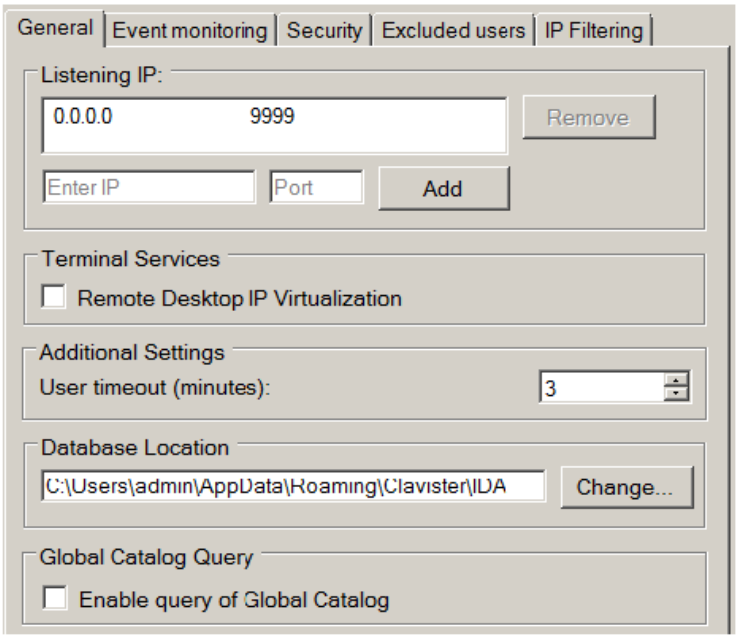
i. **Listening IP** - This is the IPv4 address and port number which the IDA will listen on for connections to NetDefendOS. By default, the IDA will listen on port 9999 of 0.0.0.0/0, which means any IPv4 address. Multiple IP values can be entered for this setting and must include the IP configured for the NetDefendOS Authentication Agent object of the connecting firewall.

ii**. Remote Desktop IP Virtualization** - This allows IDA to be used with a Windows Terminal Server ™ . This feature is described in detail later in this section.

iii. **User Timeout** - This is the time within which NetDefendOS must authenticate the user after they are authenticated by the Windows server.

iv. **Database Location** - The location of the database where login information is cached.

v. G**lobal Catalog Quer**y - By default, only the active directory is queried for the user. If this option is enabled and the active directory search fails then the global catalog will be queried.



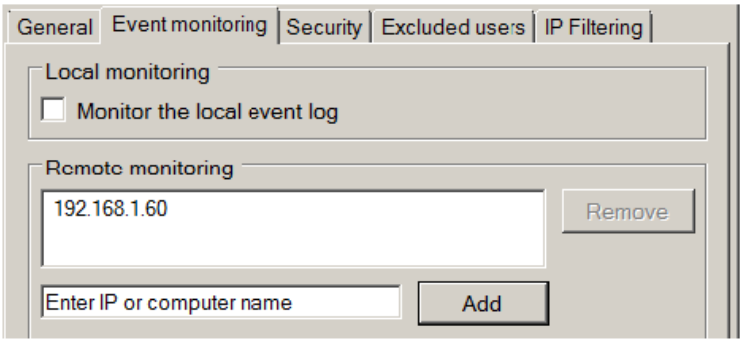
The Event Monitoring tab

This tab consists of the following settings:

i. **Monitor the local event log** - When enabled, this IDA installation will monitor the server on which it is installed for authentication events. Usually, this will be enabled since normally the agent will monitor events on its own server.

ii. **Remote monitoring** - This specifies the IP address of other domain servers which are to be monitored by this IDA installation. More than one IDP installation can monitor the same domain server and more than one IDP installation can send the same authentication event to NetDefendOS (duplicate received IDA events are recognized by NetDefendOS and ignored).

If the Monitor the local event log option is not enabled and no other server IP addresses are specified, the agent will send nothing back to NetDefendOS.

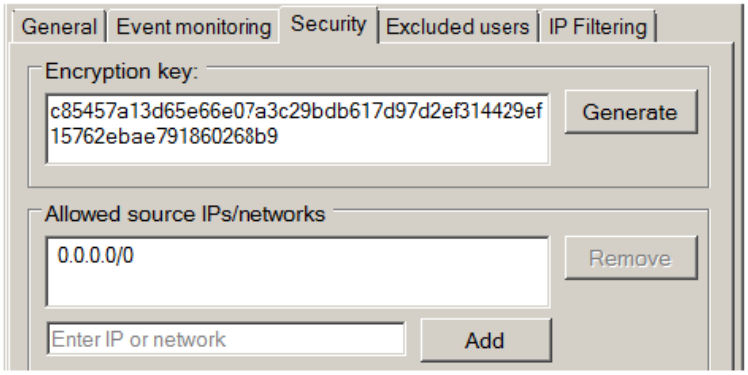


The Security tab

This tab consists of the following settings:

i. **Encryption key** - This is the key used to encrypt communication with NetDefendOS. By default, this value will be the same as the default value of the Pre-Shared Key property of the corresponding NetDefendOS Authentication Agent object. For improved security, it is recommended that this key is changed by the administrator, both for the IDA and the corresponding NetDefendOS Authentication Agent object.

ii. **Allowed IPs/networks** - This specifies the source IPv4 addresses from which the IDA will accept NetDefendOS connections. The default value of 0.0.0.0/0 means all IPv4 addresses are acceptable. The administrator can improve security by narrowing this to a specific network or IP address where the connecting NetDefend Firewall is located.

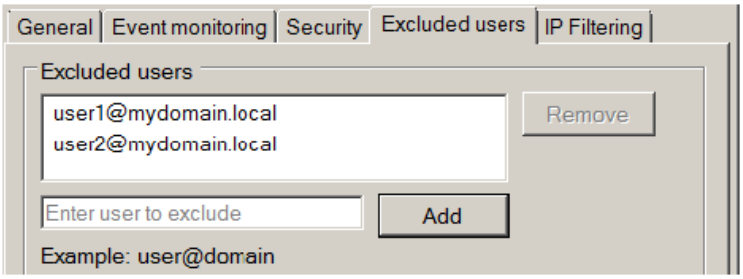


The Excluded Users tab

In this tab, it is possible to set up an exclusion list for the IDA so that users on the list will not have their authentication status sent back to NetDefendOS by the IDA service. The full User Principal Name (UPN) must be used to specify excluded users, for example:

```
myusername@mydomainname.local
```

Often, it is appropriate to include the administrator's own account on this exclusion list. The excluded users feature exists only in version 1.01.00 or later of the IDA software.



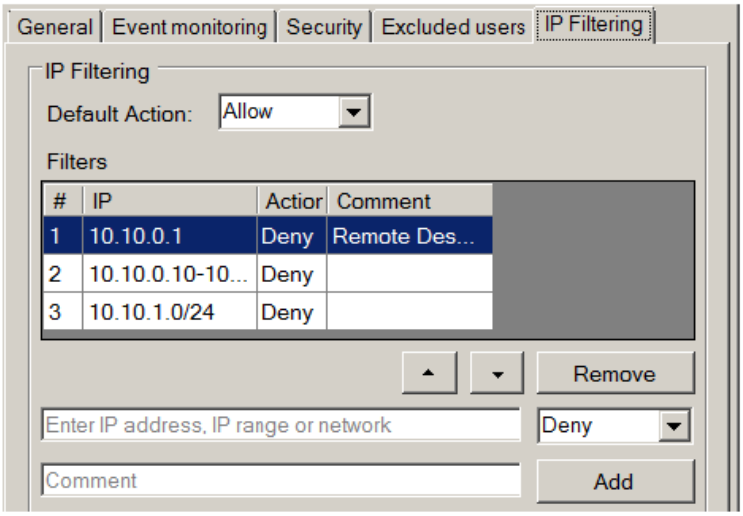
The IP Filtering tab

This tab allows the IP address of the authenticating client to be filtered using a list of filtering rules. Each rule added to the list by the administrator consists of an IP address, network or IP range, along with an action of either Allow or Deny.

When the IDA processes a new client login, it scans the rule list from top to bottom and stops scanning at the first match for the client's IP address. If the action for the matching rule is Allow, the login is sent to NetDefendOS as normal. If the action is Deny, the login is ignored and no message is sent to NetDefendOS.

If no match for the IP is found in the list, or the list is empty, the Default Action setting is applied. This setting is Allow by default.

An empty list (the default) with the Default Action set to Allow means that all client IP addresses are allowed.
This feature is only available in IDA version 1.05 or later.



An Example of IDA Redundancy

To illustrate how IDA redundancy could be implemented, consider a domain that has 4 servers called A, B, C and D. To implement minimal redundancy, the steps would be as follows:

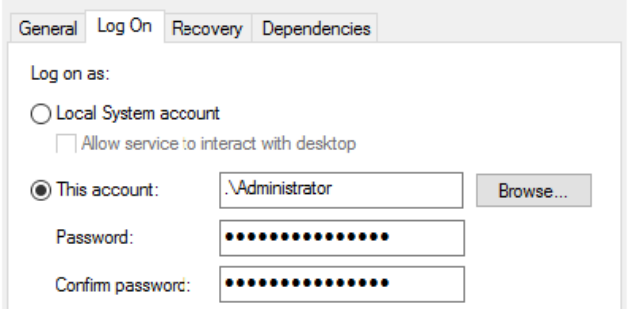
1. Install the IDA on server A and server B.
2. Enable the Event Monitoring for both installations so they are monitoring local server authentication events.
3. For server A, configure the Remote monitoring option with the IP addresses of servers B, C and D so that they are monitored too.
4. For server B, configure the Remote monitoring option with the IP addresses of servers A, C and D so that they are monitored too.

Now, if either server A or B should fail, authentication events will still be sent back to NetDefendOS. NetDefendOS will recognize any duplicate events sent by both server A and server

Using IDA with a Windows Terminal Server

In some environments, a Terminal Server may be used as well as a domain server. If this is the case, the IDA service is installed as before but the option Remote Desktop IP Virtualization should be enabled.

However, IP virtualization will not function with either Windows 2012 or 2016 Server if the IDA software is running as a Local System account. To solve this issue, change the settings in the Log On tab for the server to This Account and specify an account, as shown below:



The terminal server itself must have the following attributes:

- At least Windows Server 2008 ™ R2.
- The role Remote Desktop Session Host must be installed.
- The option IP virtualization per session must be enabled.

Note: DNS lookup is done using the terminal server IP

Any DNS lookups are performed using the IP of the Windows terminal server and not the session IP assigned to the client. Therefore, IP rules or IP policies may be needed to allow such DNS lookups through the firewall.

付録 I REAT API の使用方法

Introduction

The NetDefendOS software provides a REST API which allows certain aspects of its operation to be controlled by an external computer. At this time, only the NetDefendOS authentication subsystem can be controlled in this way.

The REST API functions by an external computer sending HTTP or HTTPS messages to the IP address of a NetDefendOS Ethernet interface over an IP network. NetDefendOS then processes the message and returns any reply in an HTTP/HTTPS message. Any data sent in messages uses the JSON format.

Note: JSON data is shown reformatted for readability
The JSON data sent back by NetDefendOS will be one continuous stream of characters without white space. The JSON output shown in this publication has been reformatted to make it more readable.

Enabling REST API Access in NetDefendOS

Allowing access by the REST API must be explicitly configured in NetDefendOS by creating a RemoteManagementREST object. The properties of this object determine what restrictions are placed on REST API access. These properties include the following:

- Protocol used (HTTP or HTTPS). Encrypting messages with HTTPS is recommended.
- The interface to accept connections from external clients on. The external computer will send REST API messages to the IP address of this interface.
- The source IP(s) to accept connections from external clients on.
- The access level permitted to clients (read only or read/write).
- The option to require REST API authentication using a *basic access authentication* schema with username/password credentials.

An Example of Enabling the REST API

Before the REST API can be used, it must be enabled by creating a REST API Management object in the NetDefendOS configuration and setting the properties of this object to the appropriate values. The example below shows how this is done.

Example 1.1. Enabling the REST API

This example will create a new *REST_managment* object called my- rest- api. This will allow read/write HTTPS communication only on the if3 interface and only from the network *mgmt-net*. Credentials will be required for access with a username of *my-admin-name* and password of *my-admin-pass.*

Command-Line Interface

```
Device:/> add RemoteManagement RemoteMgmtREST Name=my-rest-api Interface=if3 Network=mgmt-net HTTPS=Yes
          AccessLevel=ReadWrite BasicAUTH=Yes Username=my-admin-name Password=my-admin-pass
```

Web Interface

1. Go to: **System > Device > Remote Management**
2. Select **Add** > **REST API Management**
3. Enter **Name**: my-rest-api
4. Enable **HTTPS**
5. Enter **Interface**: if3
6. Enter **Network**: mgmt-net
7. Select **Access Level** to be Read/Write
8. Enable **Basic Auth**
9. Enter **Username**: my-admin-name
10. Enter **Password**: my-admin-pass
11. Click **OK**

Authentication

This section describes the usage of the NetDefendOS REST API with authentication. When the API is used with authentication, an external computer can perform the following management operations on a NetDefendOS configuration:

- List currently authenticated users.
- Retrieve information for a single currently authenticated user.
- Add a new authenticated user.
- End authentication of user.

A REST API Authentication Use Case

A typical use case for the REST API with authentication is where an external DHCP server is handing out IP addresses to clients on a private WiFi network in a public space such as a train station or airport. The clients might access resources such as the public Internet via a NetDefend Firewall.

As the DHCP server allocates IP addresses, it therefore needs to add and delete and possibly list the authenticated users in NetDefendOS. This can be done by using the REST API.

The sections that follow describe how to perform these operations.

Listing Currently Authenticated Users

To list information about all currently authenticated users, an HTTP GET must be sent to the URI */api/oper/userauth.* The GET can have only the following optional parameter:

- num - The maximum number of users to return (default value: 100).

To retrieve a list of all currently authenticated users, perform a GET towards the following URI:

```
/api/oper/userauth
```

NetDefendOS will send its reply back in JSON format. Below is an example of a reply to a GET:

```
{
 "error": false,
 "active_users_count": 2,
 "active_users": [
  {
   "username": "user1",
   "ip": "203.0.113.5",
   "groups": "group1,group2",
   "interface": "wan",
   "agent_type": "Identity Awareness",
   "session_timeout": 60,
   "idle_timeout": 60
  },
  {
   "username": "user2",
   "ip": "203.0.113.7",
   "groups": "group4,group5",
   "interface": "wan",
   "agent_type": "Identity Awareness",
   "session_timeout": 160,
   "idle_timeout": 60
  }
 ]
}
```

In the above JSON reply, there are 2 users listed with usernames user1 and user2. The user called *user1* has an IPv4 address of 203.0113.5 and belongs to the groups *group1* and *group2*. The user called *user2* has an IPv4 address of 203.0113.7 and belongs to the groups *group4* and *group5*.
Both users have connected to NetDefendOS through the *wan* interface.

The *agent-type* value indicates the origin of the authenticated user. If a user was added to the authenticated list with the REST API then its *agent-type* value will always be "Identity Awareness".

If there are no authenticated users, the response will be the following:

```
{
"error":false,
"active_users_count":0,"active_users":[]
}
```

Listing Information about a Single Authenticated User

To list information about a single currently authenticated user, an HTTP *GET* is sent to the path */api/oper/userauth* but with additional parameters to identify the user. The action can have the following parameters:

- **ip** - The IPv4 address of the user.
- **interface** - The NetDefendOS interface through which the client connected (optional).

For example, to list a single user, a *GET* could be sent to the following URI:

```
/api/oper/userauth?ip=203.0.113.5&interface=wan
```

Here, the IP address *203.0.113.5* is the IP address of the user and wan is the NetDefendOS interface that the user has connected to.
The JSON reply sent by NetDefendOS will have the following form:

```
{
 "error": false,
 "active_users": [
  {
    "username": "user1",
    "ip": "203.0.113.5",
    "groups": "group1,group2",
    "interface": "wan",
    "agent_type": "Identity Awareness",
    "session_timeout": 60,
    "idle_timeout": 60
   }
  ]
}
```

The output is similar in form to the output when a list of all authenticated users is retrieved.
If the specified user cannot be found, a JSON message like the following will be returned:

```
{
 "error":false,
 "active_users_count":5,
 "active_users":[]
}
```

Here, the *active_users* parameter has an empty value. Note also that the *active_users_count* value is the total number of currently authenticated users.

Adding a New Authenticated User

To add a new authenticated user, the action received by NetDefendOS should be an HTTP *POST* to the path */api/oper/userauth*. The action can have the following parameters:

- **ip** - The IPv4 address of the user.
- **username** - The username of the client.
- **interface** - The NetDefendOS interface through which the client connected (optional).
- **session_timeout** - The session timeout in seconds for this user.
- **groups** - A comma separated list of groups to which this user belongs. This is not optional and if there is no group membership then the parameter must be specified without a value.

For example, send a POST to the following URI:

```
/api/oper/userauth
```

The POST body should contain a string in the following form:

```
ip=192.168.1.10&interface=wan&session_timeout=60&idle_timeout=30&username=user3&
groups=group1,group2
```

Note that the above *POST* body has been split into 2 lines to fit this document's page width. In reality, these last two lines would be a single continuous line.

The parameter *idle_timeout* is optional. If this is not specified, the assumed value will be the same as *session_timeout*. Both *idle_timeout* and session_timeout have a maximum allowed value of one month.

In the above body, the username of the new authenticated user is specified as *user2* with an IP address of *192.168.1.10.* This user can only connect to NetDefendOS via the *wan* interface and they are a member of the groups called *group1* and *group2*. The client session timeout in seconds can be set as required. Here, it is 60 seconds.

The JSON reply sent by NetDefendOS will confirm that the user has been added and specify the parameter values used for the user. It will have the following form:

```
{
 "error": false,
 "user": {
  "username": "user1",
  "ip": "192.168.1.10",
  "groups": "group1, group2",
  "interface": "wan",
  "agent_type": "Identity Awareness",
  "session_timeout": 60,
  "idle_timeout": 60
 }
}
```

If there is an error, NetDefendOS will return a message indicating the problem. For example, if the interface name is incorrect, the following JSON message would be sent back to the client:

```
{
  "error":true,
"error_code":400,
  "error_message":"Property 'interface': Unknown interface name"
}
```

Ending Authentication of a User

In order to delete a user from the list of currently authenticated users, the REST API client must send an HTTP DELETE to the URI /api/oper/userauth . The action can have the following parameters:

- **ip** - The IPv4 address of the user.
- **interface** - The NetDefendOS interface through which the client connected (optional).

For example, to remove a user with the IP address 192.168.1.201, send a DELETE command to the URI:

```
/api/oper/userauth?ip=192.168.1.201
```

The Content-Type for this should be application/x-www-form-urlencoded.
The following JSON reply will be sent back by NetDefendOS if the deletion is successful:

```
{
"error": false
}
```

If the user was not found, NetDefendOS will return the following JSON message:

```
{
 "error": true,
 "error_code": 404,
 "error_message": "User does not exist"
}
```

The above message indicates that there is no user with the given IP address (and optionally the given interface) is currently authenticated.

Server Load Balancing

This section describes the usage of the REST API to control the server load balancing (SLB) feature in NetDefendOS. When the REST API is used with SLB, the load balanced servers can send back their loading information so NetDefendOS can allocate connections across the servers appropriately. This means that a new connection can be allocated to the server with the least load.

The need for this feature usually comes from the uneven server distribution that can arise due to "stickiness" with the NetDefendOS SLB feature. Stickiness can mean that connections from a particular client are always assigned to a particular server, even though SLB has tried to allocate the load evenly. The REST API for SLB means that NetDefendOS can be aware of the actual load experienced by a server and not just base allocation decisions on the number of connections allocated.

Configuring SLB to make use of the REST API consists of the following steps:

1. Create custom software which then runs on each of the servers to be balanced. This software uses the REST API to send back load information to NetDefendOS. The server load is expressed as a single integer percentage between zero and 100.

2. Enable REST API access by creating the appropriate Remote Management object in the NetDefendOS configuration. Doing this is described in Chapter 1: Introduction.

3. Create a NetDefendOSServer Load Balancing Rule object which uses Resource- usage as its distribution method. The Server Identifier string property of this rule must be included with the *POST* messages sent by servers so they can be associated with the rule in conjunction with the server's IP address.

Doing this is described further in the server load balancing section of the separate NetDefendOS Administration Guide.

Sending the Server Load to NetDefendOS with POST

To send the current server load to NetDefendOS, perform an HTTP *POST* towards the following URI:

```
/api/oper/slb
```

The POST message body can contain the following parameters:

l serverID - A string which is identical to the *Server Identifier* property of an *SLB Rule* in the receiving NetDefendOS configuration. This is mandatory. Along with the *serverIP* parameter, it associates an *SLB Rule* with the server .

- **serverIP** - The IP address of the sending server. This is mandatory. Along with the *serverID* parameter, it associates an *SLB Rule* with the server.

- **maintenance** - This can take the values yes or no. It indicates if the server is in service or not and provides a means for the server to temporarily make itself unavailable by using the value *yes*. A value of no means the server is available and this will make the server available to NetDefendOS for balancing if it is not already. The parameter can be missing when reporting a load and the online status is not changing.

- **load** - This is an integer which represents the current percentage of server load. This parameter can be omitted if the message is changing the *maintenance* value (either going offline, or coming back online). If it is omitted when the server is going online, NetDefendOS will assume a load of zero.

Note: maintenance and/or load must be present

All SLB POST messages must have either maintenance or load present, or both. The message is invalid if neither is present.
Both could be present when a server is both reporting its load and changing its status (such as when it comes online and reports its load).

For example, to send a load value of 31% for a server with an IP address of *192.168.1.10* and an associated SLB rule identifier of *serverA*, the *POST* body would contain the following:

```
serverID=serverA&serverIP=192.168.1.10&maintenance=no&load=31
```

Writing the Server Software

When writing the software that uses the REST API, the following should be noted about the way REST API *POST* messages are handled by NetDefendOS:

- NetDefendOS must receive at least one *POST* message per minute. If no message has been received for one minute, the server is considered to be unavailable and no connections are allocated to it. The next *POST* message it sends will make it available again (provided the maintenance is set to no).
- There is no upper limit how often a server can send a POST message. However, messages sent in excess of one every second will not improve load distribution and will only consume resources on the server and the firewall.
- It is recommended to only send a *POST* message when there is a significant change in the server load. A load change equal to or greater than 3% is recommended for a typical deployment.
- If the load remains stable then a *POST* message should be sent anyway at least every 15 seconds so that NetDefendOS continues to view the server as available and has an accurate view of the load.
- Until it receives at least one *POST* message from all servers after the last system start, NetDefendOS will use the round robin algorithm to allocate connections between servers. Once all servers have reported their loading, it will begin to allocate connections to the least loaded server.
- When the server sends back a load of 100%, connections could still be allocated to it if it has the least "estimated" load of all servers when all have reported 100% loading. When NetDefendOS allocates connections to servers it adjusts up its estimation of the loading to account for the connections added since the last time the server reported its load. In this way, NetDefendOS could estimate that a server's load is above 100%.

Error Messages from a POST Operation

If a *POST* is accepted, the JSON response sent back by NetDefendOS will be the following:

```
{
 "error":false
}
```

If there is an error, NetDefendOS will return a message indicating the problem. For example, the following JSON message might be returned to the client:

```
{
 "error":true,
 "error_code":400,
 "error_message":"Bad Request, malformed"
}
```

The following is a complete list of *POST* error messages:

- **malformed** - The body has an error in its syntax.
- **no server identifier parameter** - The serverID parameter is missing.
- **no server address parameter** - The serverIP parameter is missing.
- **missing parameter** - Either the load or maintenance parameter is missing.
- **load out of range** - The load value is not between 0 and 100.
- **unknown server** - No SLB rule matches the serverIP/serverID combination.

NetDefendOS Generated Log Event Messages

The following SLB REST API related log event messages are generated by NetDefendOS:

- ***Malformed request sent to the SLB handler in REST API.***
- ***The specified SLB server identifier and ip not configured.***
- ***SLB Server <server_ip> is not reporting load.***
- ***SLB Server <server_ip> is entering maintenance mode.***
- ***SLB Server <server_ip> is leaving maintenance mode.***

In the messages above, the parameter <server_ip> is the actual IP address of the server. These messages are fully described in the separate NetDefendOS Log Event Reference Guide.

Viewing Server Status

The load status that servers send back when using the REST API can be viewed in the NetDefendOS web interface by going to the **Server Load Balancing Status** page of the interface. An example screenshot of this page with the REST API in operation is shown below.

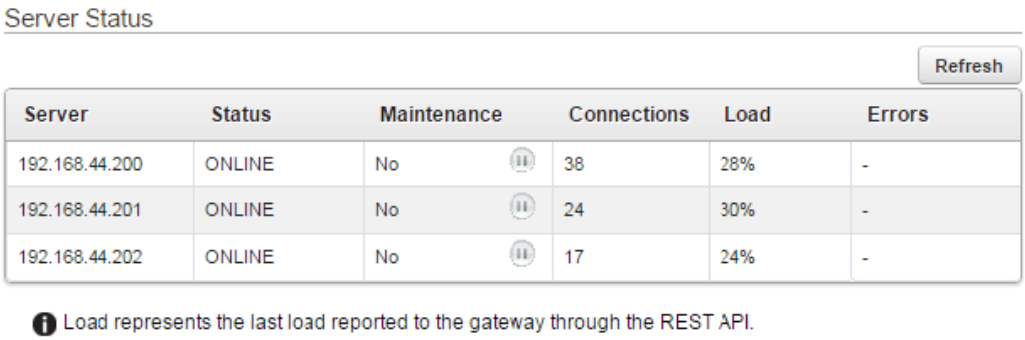


図 14-1　Path MTU Discovery 処理

If a server did not send a Post message within the last minute, the Errors column in the above screenshot would have shown the value REST for that server.

The Pause button in the Maintenance column of this WebUI display can be used to remove a server from being available for connection distribution. However, the server itself will not be aware when this is done and this is also independent from the API. Any existing connections to a server will not be closed by NetDefendOS when the pause button is pushed for that server.

However, note that new connections could still be allocated to a paused server in order to to comply with the requirement for SLB stickiness, if stickiness is enabled. Stickiness is explained further in the SLB section of the separate NetDefendOS Administration Guide.

Blacklist Control

This section describes the usage of the NetDefendOS REST API to change and list the contents of a configuration's blacklist. This section will not describe how the blacklist feature itself functions but only how the REST API is used to interact with it. A full description of the blacklist can be found in the separate NetDefendOS Administration Guide in the section titled Blacklisting Hosts and Networks.

The REST API allows an external computer to perform the following management operations on a NetDefendOS configuration:

- Add a new entry to the blacklist to block a single source IPv4 address (and optional service).
- Delete a blacklist entry previously added by the REST API.
- List all entries in the blacklist or entries of a specific alert type.

Note that the API can only delete blacklist entries that were first added by the API. Entries created by configured NetDefendOS features, such as IDP and threshold rules, cannot be altered by the API.

However, when retrieving a list of blacklist entries using the API, all entries are returned, including those not added by the API. It is possible when retrieving a list of entries to use a filter so that only the entries of a certain type are retrieved and doing this is described later in this section.

The typical use case for adding and deleting blacklist entries is when a separate network component identifies an IP address as the source of a threat and needs to have a NetDefend Firewall drop connections initiated by that address.

Visibility of REST API Changes for the NetDefendOS Administrator

Any changes made to the blacklist using the REST API are visible to the administrator when the blacklist is listed in a management interface such as the Web Interface (WebUI) or CLI.

In addition, a NetDefendOS user with administrator privileges has the ability to delete blacklist entries that were added using the REST API. However, the API cannot delete entries not created through the API.

Adding a New Blacklist Entry

To add a blacklist entry, the action received by NetDefendOS should be an HTTP *POST* to the path */api/oper/blacklist*. The action can have the following parameters:

- **host** - The single source IPv4 address to be blacklisted. (Required.) This must be a single IP address, not a range or network.
- **service** - The service associated with the entry. The value specified should be the name of a *Service* object defined in the NetDefendOS configuration. A "*400 Bad Request*" message is returned if it not a valid service name. (Optional with an default value of *all_services*.)
- **ttl** - The time-to-live in the blacklist in seconds. (Optional with a default value of 300 seconds.)
- **close_established** - Close any established connections that originate from this IP address. (Optional with an empty default value.)
- **rule_name** - The rule name associated with the entry. This arbitrary text data which can be used to store some value meaningful to the API client. It

has no meaning for NetDefendOS but will be stored in the blacklist and appear in a listing of entries. (Optional with an empty default value.)

- **description** - A textual description for the entry. (Optional with an empty default value.)

For example, to blacklist the IPv4 address *203.0.113.5*, send a *POST* to the following URI:

```
/api/oper/blacklist
```

The *POST* body should contain a string in the following form:

```
host=203.0.113.5
```

By default, this adds a blacklist entry with the service set to all_services. If, for example, the blacklist entry is only to apply to HTTP and HTTPS traffic then the *http- all* service would be specified as an additional parameters in the *POST* body:

```
host=203.0.113.5&service=http-all
```

The JSON reply sent by NetDefendOS will confirm that the entry has been added and specify all the parameter values used. It will have the following form:

```
{
 "error": false,
 "blacklist_entry": {
  "host": "203.0.113.5",
  "service": "http-all",
  "ttl": "300",
  "rule_name": "-",
  "description": "-"
 }
}
```

Deleting a Blacklist Entry

In order to delete a blacklist entry, the REST API client must send an HTTP *DELETE* to the URI */api/oper/blacklist*. The action can have the following parameters:

- **host** - The host IP address to blacklist. (Required.)
- **service** - The service associated with the entry. (Optional with a default value of *all_services*.)

As mentioned previously, a *DELETE* operation can only remove a blacklist entry that was previously added by the REST API. It cannot remove an entry that was added by a NetDefendOS feature such as IDP or threshold rules.

For example, to remove any entry with the IP address *203.0.113.5*, send a *DELETE* command to the URI:

```
/api/oper/blacklist?host=203.0.113.5
```

The *Content-Type* for this should be *application/x-www-form-urlencoded.*

The *service* parameter can be added to delete a previously added blacklist entry with a specific service. For example, to delete the entry with the IPv4 address *203.0.113.7* and service *http-all.*
send a *DELETE* command to the following URI:

```
/api/oper/blacklist?host=203.0.113.5&service=http-all
```

The following JSON reply will be sent back by NetDefendOS if the deletion is successful:

```
{
 "error": false
}
```

Note that every blacklist entry has a service associated with it and the delete operation will only delete an entry that has an exact match with the specified combination of IP address and service. If the *service* parameter is specified as *all_services* (the default) then this would not delete an entry that has a service of *http-all.*

Listing Blacklist Entries

To list all blacklist entries, an HTTP GET should be sent to the URI:

```
/api/oper/blacklist
```

The GET has only a single optional parameter with is *alert_type*. The *alert_type* restricts the listed entries to a particular source. All blacklist entries added using the REST API will have an *alert_type* value of "REST". If the *alert_type* parameter is not specified then all entries will be retrieved.

For example, to retrieve all entries created by the REST API then the alert-type filter should be set to the value "*REST*":

```
/api/oper/blacklist?alert_type=REST
```

All the possible values for the parameter alert_type can be found under the -alerttype option in the section for the command *blacklist* in the separate NetDefendOS CLI Reference Guide. It should be noted that the value "*ALL*" is not a valid *alert_type* with the REST API but this is the default if the *alert_type* parameter is not specified.

NetDefendOS will send back its reply to a *GET* command back in JSON format. Below is an example of a typical reply:

```
{
 "error": false,
 "blacklist_count": 2,
 "blacklist_hosts": [
 {
  "host": "203.0.113.5",
  "service": "",
  "ttl": "300",
  "alert_type": "REST",
  "rule_name": "-",
  "description": "api added"
 },
 {
  "host": "203.0.113.7",
  "service": "http-all",
  "ttl": "100",
  "alert_type": "REST",
  "rule_name": "-",
  "description": "api added"
 }
 ]
}
```

Neighbor Cache

Using the REST API, a summary of the devices directly connected to the firewall can be retrieved. This has similarities with a listing of the ARP cache but provides extra information about each device. The device information is sent back by NetDefendOS in JSON format. This same information can also be retrieved by using the neighborcache CLI command with various command options.

Sending the Neighbor Cache Request

To retrieve the neighbor cache information, an HTTP GET should be sent to the following URI:

```
/api/oper/neighbor_devices
```

The GET has no optional parameters.

The Statistics Retrieved

The following is a list of the possible values sent back in the JSON reply:

- **interface** - The name of the interface on which the external device is found.
- **ethernet_address** - The MAC address object of the external device.
- **ethernet_object** - Configuration object matching the MAC address (optional).
- **ethernet_vendor** - The vendor name matching the MAC address (optional).
- **ipv4** - The IPv4 address for this device (optional).
- **ipv6** - The IPv6 address for this device (optional).
- **authenticated_user** - The authenticated username for this IP address (optional).

- **hostname** - DHCP hostname (optional).
- **status** - Current status of the entry.
- **last_seen** - Number of seconds since last seen (optional). This value will appear only if the status is Inactive.

When one of the above values is indicated as optional, this indicates that the value will not be present if it is either unavailable or not relevant.

The *ethernet_object* is the name of the first *EthernetAddress* object found in the NetDefendOS address book that has a MAC address matching the MAC address of the external device. If no such object is found then the value will not be included in the JSON reply. The *EthernetAddress* object will have to be first created manually by the administrator with the relevant MAC address.

The hostname value may be included in the JSON reply if the external device was allocated its IP address by NetDefendOS acting as a DHCP server. The hostname will be the name sent by the external device in its DHCP request for an IP address. If it did not send a name in the request the hostname value will not be included.

An Example JSON Reply
Below is an example of a typical JSON reply:

```
{
 "error": false,
 "devices": [
 {
  "interface": "wan",
  "ethernet_address": "00-50-8B-D9-16-5E",
  "ethernet_vendor": "D-Link",
  "ipv4": "203.0.113.6",
  "status": "Active"
 },
 {
  "interface": "dmz",
  "ethernet_address": "F8-B2-53-CF-2B-CD",
  "ethernet_object": "my-pc",
  "ethernet_vendor": "Example Corp.",
  "ipv4": "10.6.19.1",
  "status": "Inactive",
  "last_seen": 2
  }
 ]
}
```

Statistics Retrieval

Using the REST API, the current values of a range of NetDefendOS operational parameters can be retrieved. The information is sent back by NetDefendOS in JSON format and consists of the values normally provided by the stats CLI command plus some additional information.

Sending the Statistics Request

To retrieve the statistical values, an HTTP GET should be sent to the following URI:

```
/api/stats
```

The GET has no optional parameters.

The Statistics Retrieved

The following is a list of the values sent back in the JSON reply:

- System uptime since the last restart.
- Time of last system event such as a version updgrade.
- Current CPU load as a percentage.
- Memory installed, free and maximum free (bytes).
- Number of allocated and active connections.
- Current packet fragments that are allocated, lingering and active.
- Buffer sizes that are allocated, free and total allocation (bytes).
- Packet fragment buffer size allocated and total allocation (bytes).

- Number of cores used for polling.
- If the unit is under InControl management.

An Example JSON Reply

Below is an example of a typical JSON reply:

```
{
 "error": false,
 "uptime": {
  "seconds_total": 191,
  "days": 0,
  "hours": 0,
  "minutes": 3,
  "seconds": 11
 },
 "last_event": "2018-02-06 18:23:49: Firmware upgrade
       request from WebUI by admin (192.168.1.11).",
 "cpu_load": 14,
 "memory": {
  "installed": 2137166035,
  "free": 1807419356,
  "largest_free": 1696489544
 },
 "connections": {
 "allocated": 256000,
 "active": 7
 },
 "fragments": {
  "allocated": 1024,
  "active": 0,
  "lingering": 0
 },
 "buffers": {
  "allocated": 24617,
  "free": 23590,
  "memory": 33058800,
  "out_of_buffers": 0
 },
 "fragbufs": {
  "allocated": 32,
  "memory": 322048
 },
 "active_poll_cores": 1,
 "incontrol_status": "Not Configured
}
```

About Information

Using the REST API, a program running on an external computer is able to retrieve the version of NetDefendOS that is currently running, as well as information about the underlying computing platform. The reply is sent back by NetDefendOS in JSON format.

Sending the About Request

To retrieve the information, an HTTP GET should be sent to the following URI:

```
/api/about
```

The GET has no optional parameters.

The About Information Returned

The following is a list of the values sent back in the JSON reply:

- **error** - This is false if the request was successful.
- **version** - The full version number of the NetDefendOS software.

- **version_numbers** - The version number broken down into its parts.
- **buildtype** - This usually has the value Release unless the version a technical preview.
- **vendor**- The system vendor. This will usually be D-Link.
- **product** - The name of the system software. This will usually be NetDefendOS.
- **model** - The platform on which the software is running.
- **device_name** - The name that has been assigned to the device. The default name will be Device if it has not been changed.

An Example JSON Reply

Below is an example of a typical JSON reply:

```
{
 "error": false,
 "version": "12.00.12.03-12345",
 "version_numbers": [
  12,
  0,
  12,
  3,
  12345
 ],
 "buildtype": "Release",
 "vendor": "D-Link",
 "product": "NetDefendOS",
 "model": "DFL-260E",
 "device_name": "MyDevice"
}
```