ファームウェアバージョン：	V11.10.01.06	
プラットフォーム/ハードウェア：	DFL-260E	A1
	DFL-860E	A1
	DFL-1660	A1
	DFL-2560	A1
	DFL-2560G	A1/A2
発行日：	2018/1/5	

本リリースノートには、DFL シリーズのファームウェア更新に関する重要な情報が含まれています。ご使用の DFL シリーズに対応するリリースノートであることを確認してください。

DFL シリーズに関する詳細な情報が必要な場合は“ユーザマニュアル”を参照してください。

目次：

変更履歴とシステム要件： 2
アップグレードの手順に関して： 2
WEB GUI 経由でのアップグレード方法 2
参考：SCP プロトコルを使用して CLI 経由でのアップグレード方法 4
追加機能： 5
機能の変更点： 9
MIB の変更点： 9
修正した問題点： 9
既知の問題： 24

変更履歴とシステム要件：

ファームウェアバージョン	リリース日付	モデル	ハードウェアバージョン
ランタイム: v11.10.01.06	2018/1/5	DFL-260E	A1
		DFL-860E	A1
		DFL-1660	A1
		DFL-2560	A1
		DFL-2560G	A1、A2

アップグレードの手順に関して：

ファームウェアのアップグレード方法には下記の「SCP プロトコルを使用して CLI 経由でのアップグレードを行う方法」と「WEB GIU 経由でのアップグレードを行う方法」の 2 つがあります。

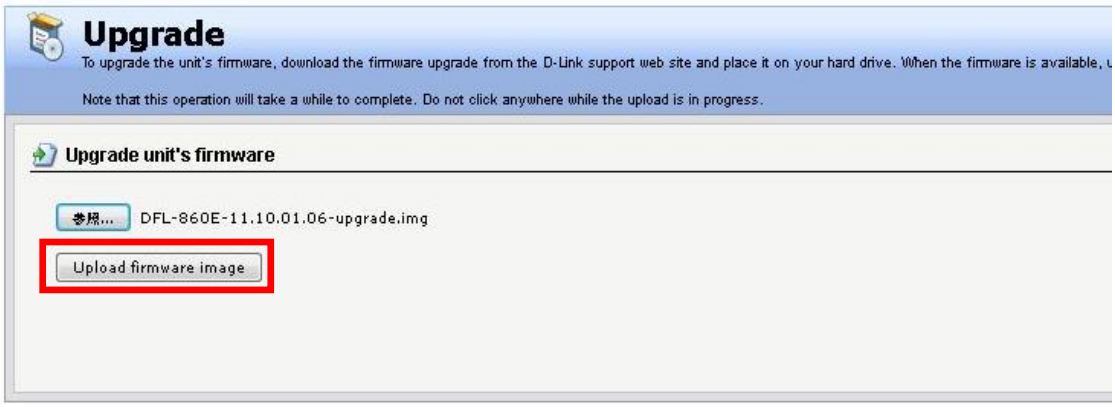
※V2.40.02 及びこれより古いファームウェアでは、アップグレード時にコンフィグレーションが正しく更新されないことがある問題が存在します。必ず、アップグレード前に現在のコンフィグを保存し、アップグレード後にリストアを行ってください。
この問題は本ファームウェアにおいて修正されていますが、V2.40.02 より古いファームウェア（V2.40.01.08 を含む）からどのバージョンのファームウェアにアップグレードする場合においても、内在する問題となります。
該当バージョン以外のファームウェアバージョンにおきましても、念のためアップグレード前にコンフィグの保存を行うことを推奨します。

本バージョンでは、日本語 GUI 言語ファイルが用意されていません。本ファームウェアバージョンにアップグレード後は、ログイン画面で English を選択してご使用ください。

WEB GUI 経由でのアップグレード方法

1. 本製品と設定用の PC を接続後、WEB ブラウザを立ち上げ、アドレスバーに WEB GUI の管理画面を表示します。デフォルトのシステム IP アドレスは 192.168.10.1 です。
2. WEB GUI のログイン画面が表示されたら、ユーザ名とパスワードを入力し、ログインしてください。デフォルトのユーザ名およびパスワードは「admin」です。
3. ログイン後、上部のメニューから ***Maintenance > Backup*** の順にクリックします。
4. 「Configuration Backup」の「Backup Configuration」ボタンをクリックします。
5. 任意のフォルダにコンフィグのバックアップファイルを保存します。
6. 上部のメニューから、***Maintenance > Upgrade*** の順にクリックします。
7. 「Upgrade unit's firmware」の「参照」ボタンをクリックします。

8. ローカルのハードディスク上に保存したファームウェアファイルを選択し、「Upload firmware image」をクリックします。



9. アップグレード後、DFL への接続が切断されるので、WEB GUI のアドレスに再接続（画面を更新）します。

10. メインページの「NetDefendOS Version」にて、最新バージョンになっていることを確認します。

注意：ファームウェアのアップデート中に、電源を切らないでください。アップデート中に電源を切ると、起動に失敗し、正常に起動できなくなることがあります。故障の原因となりますので、ご注意ください。

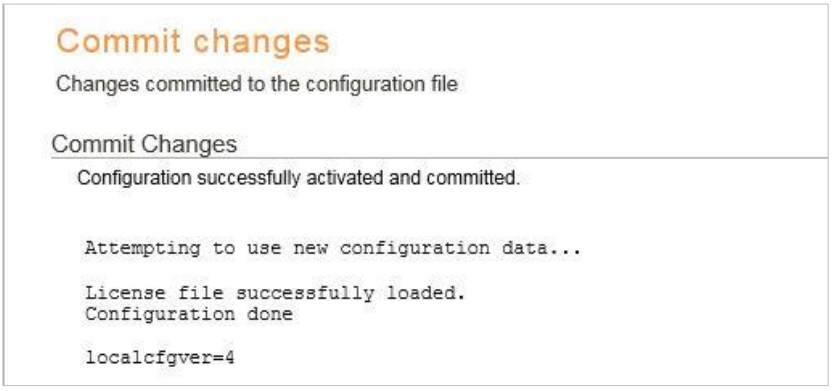
11. ***System > Maintenance > Device Maintenance > Backup & Restore*** の順にクリックします。

12. 「Configuration Restore」の「参照」ボタンをクリックし、コンフィグのバックアップファイルを指定します。

13. 「*Restore Configuration*」ボタンをクリックすると、ファイルがアップロードされます。

14. 「*Activate*」ボタンをクリックし、コンフィグのアクティブ化と保存を行います。

15. 以下の画面が表示されれば、コンフィグのリストアが完了です。



参考：SCP プロトコルを使用して CLI 経由でのアップグレード方法

SCP(Secure Copy)はファイル転送用のコミュニケーション・プロトコルとして広く使用されています。NetDefendOS と共に SCP クライアントを提供していませんが、ほぼ全てのワークステーションのプラットフォームに対応する無料の SCP クライアントを手に入れることができます。
SCP は CLI の処理を補足するもので、管理者のワークステーションと NetDefend ファイアウォール間のファイル転送を安全に行うことができます。NetDefendOS で使用する多様なファイルは SCP を使用してアップロード及びダウンロードを行なうことができます。

この機能の詳細の情報は、ユーザマニュアルの Secure Copy（SCP）に関して記載されている章をご確認下さい。

追加機能：

ファームウェアバージョン	追加機能
V11.10.01.06	1. WEB ユーザインタフェースを新しいインタフェースに刷新致しました。 2. アプリケーションの制御機能を追加致しました。 3. IPv6 について、システム間の相互運用性とプロトコル準拠に関する改善を行いました。 4. Windows Active Directory ドメイン認証ユーザのアクセス制御に対応致しました。 5. SSL VPN クライアントのルート情報の設定に対応致しました。デフォルトの all-nets に加え、明示的なルート情報をクライアントに適用することができます。 6. WEB コンテンツフィルタリングで HTTPS トラフィックに対応致しました。 7. L2TPv3 サーバの構成に対応致しました。 8. HTTP ALG 機能について、HTTPS の URL フィルタリングに対応致しました。 9. メモリログページの検索フィルタをデフォルトで非表示とし、フリーテキスト検索フィールドのみ表示するように致しました。ヘッダーをクリックしてすべてのフィルタを表示することができます。 10. 表示コンテンツが多い WEB UI のページについて、ブラウジング速度を改善致しました。 11. DHCP サーバから IP アドレスが再利用され、古いユーザが MAC 認証によりログインした場合、DHCP サーバが古いユーザに対しログアウトメッセージを送信するように対応致しました。 12. High Availability ノードにおける役割変更において、ネットワーク通信が途切れずシームレスな遷移となるように改善致しました。 13. iPhone アプリで保持されるアーカイブファイル「.ipa」を識別可能な MIME タイプとして追加致しました。 14. DFL-2560/2560G/870 について、CPU 負荷の抑制と IPsec セットアップの高速化のため、IKE ネゴシエーションのハードウェアアクセラレーションに対応致しました。 15. HTTPS 接続について、Administrator ページ、SSL VPN Portal、TLS ALG、Use Authentication Rules で使用される X509 ルート証明書チェーンの設定に対応致しました。 16. ICMPv6 Neighbor Discovery Options の最大数の制御に対応し、ネットワークセキュリティを向上致しました。 17. CLI の Ping コマンドで使用する「-recvif」パラメータについて、「-srcif」というパラメータ名に変更致しました。 18. HTTP ALG に「Force SafeSearch」オプションを追加致しました。本オプションを有効化すると、HTTP ALG 経由の Google、Bing、Yahoo への検索において、これら検索エンジンが提供するセーフサーチ機能を使用するようになります。 19. L2TPv3 クライアントに対応致しました。 20. CLI の"connections"コマンドに新しい引数"-ipver="を追加致しました。この引数により、表示する通信（IPv4 もしくは IPv6）を指定することができます。 21. IPsec トンネルに構成する暗号化アルゴリズムとして、SHA256 と SHA512 に対応致しました。 22. High Availability 利用時に、IKE ネゴシエーションで確立された IPSec トンネルの同期に対応致しました。HA 機能のサポート対象は DFL-1660、DFL-2560、DFL-2560G、DFL-870 のみです。 23. IKE/IPsec の仮想ルーティングに対応致しました。 24. スタティックリンクアグリゲーションおよび IEEE 802.1AX-2008/802.3ad リンクアグリゲーションに対応致しました。 25. アンチウイルスエンジンについて、Kaspersky のストリーミングベースの最新技術に対応致しました。悪意のあるスクリプトや、システムを介して転送される URL とファイルに対する保護を改善致しました。 26. IPv6 ネイティブ接続回線を持たない環境で、IPv4 を利用したトンネルブローカーに対するトンネルを確立することで、IPv6 ホストへのアクセスや IPv6 サービスの提供を可能にする 6 in 4 トンネリング機能に対応致しました。

27. 802.1q ad の追加により、802.1ad Service VLAN 上で 802.1q VLAN を使用した QinQ の設定が可能になりました。
28. Status -> Tool に Packet Capture 機能（PCAP ツール）を追加致しました。
29. Diagnostic Console ページを追加致しました。これにより、システムの重大ログを収集し、システム内部の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。Diagnostic Console は、Status -> Maintenance -> Diagnostic Console から利用可能です。
30. VLAN インタフェースで DHCP クライアントに対応致しました。
31. VLAN で PPPoE クライアントに対応致しました。
32. Radius で Framed-IP-Network 属性値に対応致しました。Framed-IP 属性値と結合されルーティングを生成します。これにより、L2TPv2/IPsec の RADIUS 認証を使用した VPN トンネルのセットアップが可能になります。
33. コマンドラインインタフェース（CLI）で、Memory Log の表示とフィルタに対応致しました。
34. User Identity Awareness Agent のプロトコルを更新し、１ユーザに対してサポートされるグループメンバシップ数を増やしました。注意：NetDefendsOS ver10.21.02 以上では、User Identity Awareness Agent ver1.01.00 以上を使用する必要があります。
35. ZoneDefense 機能で Universal MIB を使用するスイッチに対応致しました。
36. 製品品質の改善のため、製品使用に関する匿名の情報がメーカーに送信されるようになりました。ファームウェアバージョン、UTM データベースバージョン、連続稼働時間、メモリ使用率といった情報が暗号化されて送信されます。送信される診断データの種類は設定可能であり、完全に無効化にすることもできます。
37. RADUIS サーバの構成において、RADIUS リクエストのソース IP の手動設定に対応致しました。
38. DHCPv6 サーバに対応致しました。
39. RADIUS リレーに対応致しました。
40. ファイアウォールの ARP キャッシュ内の MAC アドレスに基づいてユーザを認証する新しい認証エージェントが追加されました。サポートされる認証ソースは外部 RADIUS/LDAP データベースです。
41. バックアップ RADIUS サーバへの接続に失敗した場合、プライマリ RADIUS サーバへの接続試行を行うオプションを追加致しました。
42. WEB コンテンツフィルタリングのカテゴリ 31 について、"Spam"から"Remote control/desktop"に変更致しました。
43. CLI において、IPsec 証明書キャッシュの情報をより詳細に表示するように更新致しました。
44. CLI コマンド"routes"のエイリアスとして"route"も利用できるように対応致しました。
45. WEB ユーザインタフェースのメインのステータスページで「System Information」一覧に現在の High Availability ステータスを表示するように対応致しました。
46. WEB UI と CLI のリモート管理において、RADIUS を認証ソースとして使用することに対応致しました。
47. IPsec インタフェースの監視に対応致しました。本機能では、ホストの ICMP Ping を監視し、ホストが返答を停止した場合にトンネルの IKE SA と IPsec SA を削除の上、新しいネゴシエーションがトリガされます。ICMP Ping メッセージは毎秒送信され、設定したパケット数がロストした場合、トンネル監視により再ネゴシエーションがトリガされます。
48. SNMP 管理インタフェースへの認証と暗号化を行う SNMPv3 に対応致しました。デフォルトのローカルユーザデータベースが SNMPv3 認証の認証ソースとして使用され、サポートされる暗号方式は AES です。
49. パスワード総当たり攻撃に対する保護がローカルユーザデータベースで常にアクティブとなるように対応致しました。機能のアクティビティ監視に役立つ、ログイベント及び一時的にブロックされたユーザの一覧を追加致しました。
50. Startup Wizard に透過モードの設定を追加致しました。
51. Daylight Saving Time（サマータイム）に、ロケーション名を指定する自動モードを追加致しました。
52. IPv6 ルータ、イーサネットのネットワークプレフィックス、VLAN 及びリンクアグ

	リゲーションインタフェースの検出に対応致しました。DHCPv6 クライアントのシステムやアドレス自動構成を使用して利用することができます。 53. URL フィルタリングプロファイルと WEB コンテンツフィルタリングプロファイルを 1 つの WEB プロファイルに統合し、IP ポリシー構成をシンプル化しました。アップグレードした場合、既存の URL フィルタリングプロファイルと WEB コンテンツフィルタリングプロファイルは新しいタイプに変換されます。 54. レイヤ 2 透過モードとレイヤ 3 スタティックルートモードの両方のシナリオで、ブロードキャストパケットを転送する IP ポリシーを適用できるように対応致しました。 55. HTTP ALG と Light Wight HTTP ALG について、IPv6 IP ポリシーとルールに対応致しました。 56. ループバックインタフェースで IPv6 通信に対応し、より詳細な IPv6 ルーティングシナリオを適用することができるようになりました。 57. WEB UI の「Date and Time」画面において、時刻同期を強制するボタンを追加致しました。NTP を使用した時刻同期が有効な場合にボタンが表示されます。また、ステータス表示として、同期アクティビティや次の同期試行時間も表示されます。 58. Light-Weight HTTP ALG について、WEB サイトがブロックされた際に表示されるバナーページのカスタマイズに対応致しました。 59. HTTP Poster について、ポストが成功したかどうかを示すログの出力に対応致しました。 60. Light Weight HTTP ALG で IPv6 トラフィックに対応致しました。 61. IP アドレスベースのポリシーの代わりに、FQDN アドレスオブジェクトを使用する IP ポリシーに対応致しました。 62. IP ポリシーについて、IP アドレスの地理的ロケーションに基づいたポリシーを作成する GEO IP に対応致しました。 63. Mail Alerting 機能により、異常な動作を検知し即時にアクションを実行することが可能となりました。 64. WEB ユーザインタフェースで TLS 1.2 に対応致しました。 65. Voice over IP を設定する VoIP プロファイルを追加致しました。 66. SSL/TLS ALG で SHA-256 ハッシュアルゴリズムに対応致しました。 67. 新しい IP ポリシーとして、SLB ポリシー、マルチキャストポリシー、ステートレスポリシーを追加致しました。 68. ログをより直観的な表示に改善致しました。クリティカル/重要なイベントが直観的に把握できるように、重要度別にログの記録を色分けしました。 69. WEB UI において、スクリプトファイルの直接アップロードに対応致しました。 70. DFL-1660/2560/2560G/870 で SHA-256/SHA-512 ハッシュアルゴリズムのハードウェアアクセラレーションに対応致しました。 71. IPsec エンジンで IKEv2 に対応致しました。IKEv2 は Windows 8.1、Windows 10、Mac OS X 10.11 のローミングクライアントでテストされています。 72. IMAP 経由で送信された E メール添付ファイルのアンチウイルススキャンに対応致しました。プロトコルフィールドで IMAP が設定されたサービスを使用する IP ポリシーで有効化することができます。 73. POP3/IMAP の Anti-SPAM で、しきい値レベルのフル構成と、Reply Address Domain Verification、DNS ブラックリスト、Distributed Checksum Clearinghouses（DCC）などのメカニズムに対応致しました。 74. アンチウイルス機能において、HTTP もしくは FTP 経由で転送されるネストされた ZIP ファイル（例：ZIP ファイルの中に ZIP ファイルを含めるケース）について、10 レベルの Zip-in-Zip に対応致しました。 75. IMAP プロトコルで転送された不要な E メール添付ファイルのブロックに対応致しました。 76. IPv6 トラフィック転送時における、High Availability セットアップの冗長性に対応致しました。対象製品は DFL-1660/2560/2560G/870 です。DFL-260E/860E は High Availability をサポートしていません。 77. 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で使用可能な DHCPv6 Client を追加致しました。 78. エンドポイントの通信において、最適なパケットサイズを使用し中間ルータでのフラグメンテーションを防ぐ IPv4 Path MTU Discovery に対応致しました。

79. TLS-ALG と WEB UI の HTTPS 管理で使用される暗号化スイートとして、AES 128/AES 128 SHA-1 に対応致しました。現在使用している SSL 設定を再検討の上、安全でない暗号化方式を無効化することを推奨します。
80. MD5 暗号ハッシュ機能の既知の脆弱性により、IPsec と SSH において、HMAC-MD5 ベースの認証アルゴリズムはデフォルトの設定では無効化致しました。
81. SHA-1 暗号ハッシュ機能の既知の脆弱性により、IPsec において、HMAC-SHA1 ベースの認証アルゴリズムはデフォルトの設定では無効化致しました。
82. アンチウイルスのキャッシュに対応し、Anti-Virus Block ページを改善致しました。
83. IP ポリシーについて、プロトコルの設定を改善致しました。
84. Lightweight HTTP ALG に対応致しました。
85. IP ポリシーで使用される事前定義されたサービス一覧のプロトコル設定を更新致しました。
86. TLS ライブラリを更新しセキュリティを改善致しました。
87. 例外レポートの自動送信機能を追加致しました。インシデント発生後にシステムが起動すると、匿名の暗号化されたクラッシュレポートが自動的に D-Link に送信されます。クラッシュレポートは、D-Link 側で重大な問題を特定し、修正を迅速に提供する上で役に立ちます。本機能は Diagnostics Settings から無効化できます。
88. RADIUS リレーの"Override User Data Interface"設定により、ユーザ認証を伴うトラフィックに対し、インタフェースの手動設定に対応致しました。
89. RADIUS 及び LDAP 認証で通信する場合に使用するソース IP の設定に対応致しました。
90. IKE 認証で SHA-2 署名の証明書（SHA-256、SHA-384、SHA-512 ハッシュアルゴリズムを含む）に対応致しました。
91. CA サーバ上で証明書の CRL にアクセス不可であった場合の動作を設定できるように対応致しました。CRL がアクセス不可であっても証明書の使用を許可する "conditional"オプションが追加されています。
92. 証明書で使用する CRL 配布ポイント（CDP）の設定に対応致しました。
93. システムが送信する IKE パケットの IP ヘッダーに含まれる Differentiated Services（DSCP）フィールド値の設定に対応致しました。
94. WEB ユーザインタフェースもしくは SCP 経由でデバイスから直接 MIB ファイルをダウンロードできるように対応致しました。
95. 再設定や再起動時でも、SNMP のインタフェースインデックスとインタフェース OID の永続性を保持するように対応致しました。
96. ドメイン名、IPv4/IPv6 アドレスに対しトレースルートを実行する CLI コマンド "traceroute"を追加致しました。
97. CLI コマンド"ping"で IPv6 アドレスやドメイン名への Ping に対応致しました。
98. アクティブな L2TP クライアントセッション一覧を表示する CLI コマンドを追加致しました。
99. CLI コマンド”ifstat”が引数なしに実行された場合に、設定されたインタフェースのリンクステータスを表示するように対応致しました。
100. CLI コマンド'ike -show'で、既存インタフェース、リモート/ローカルエンドポイントの他に、ローカル/リモート ID を表示するように対応致しました。
101. アクティブな PPTP クライアントセッション一覧を表示する CLI コマンドを追加致しました。
102. IKE/IPsec の SNMP により利用可能な統計カウンタについて、トラブルシューティングや監視に役立つ、広範囲の統計値を含むように改善致しました。
103. フラグメント化した SYN パケットと（もしくは）ペイロードデータを送信する SYN パケットをドロップする機能を追加致しました。初期設定は drop and log です。
104. アンチウイルスサブシステムで ZIP 爆弾攻撃に対する保護を改善致しました。Compression Ratio Action の"Scan"は削除されました。既存の設定は"Drop"に変換されます。また、Compression Ratio 設定は 500 より大きい値で設定することはできません。
105. WEB コンテンツフィルタリングと Email Control プロファイルにカテゴリを追加し、より細かな制御を可能にしました。
106. IPsec トンネルで IPv6 に対応致しました。
107. FQDN/DNS アドレスのグループを作成・使用することができるようになりました。
108. ローカルユーザデータベース内のユーザパスワードが、事前定義された複雑なルー

	ルに適合するようにポリシーで強制できるようになりました。 109. 複数の IPsec 構成モードプールに対応致しました。各 IPsec インタフェースは、自身のプールや他のインタフェースの共有プールを使用して設定することができます。プールは IPv4 または IPv6 アドレスを配布するように設定することができます。 110. 複数の IPv4 と IPv6 アドレスを解決可能なホスト名は、IPsec のリモートエンドポイントとして使用することができます。 111. User Authentication Rule の Multiple Username Logins 設定に新しいオプションを追加致しました。例外なしで、ユーザ名毎に一つのログインセッションのみ許可する設定（strict 設定）が可能です。 112. IPsec 設定の WEB UI におけるオプション構成を更新致しました。

機能の変更点：

ファームウェアバージョン	変更点
V11.10.01.06	1. CVE-2014-3566 の脆弱性に対応するため SSLv3 を無効化致しました。

MIB の変更点：

ファームウェアバージョン	変更点
V11.10.01.06	1. メモリ使用率と TCP バッファ使用率をサポート致しました。 2. 製品毎に提供されていた MIB ファイルを共通化致しました。 3. Fastpath オブジェクトを追加致しました。 4. Crypto オブジェクトを追加致しました。 5. DHCPv6 オブジェクトを追加致しました。 6. AppControl オブジェクトを追加致しました。 7. Anti-Spam オブジェクトを追加致しました。

※V11.10.01.06 では、管理インタフェースから MIB ファイルをダウンロードすることが可能です。（***Status > Maintenance > Resources***）

修正した問題点：

ファームウェアバージョン	修正した問題点
V11.10.01.06	1. CLI コマンド'vlan'による出力結果が、VLAN ID でソートされない問題を修正致しました。また、‘num’と‘page’パラメータにより、長い出力結果を分割することができるようになりました。 2. CLI コマンド'blacklist'の出力結果でポート番号と宛先 URL が正しくセットされない問題を修正致しました。 3. Log and Event Receivers Category '36（USAGE）'の削除済み設定により、空のログデータが送信される問題を修正致しました。このカテゴリを除外するように設定が更新されました。 4. High Availability クラスタノードにおいて、LDAP サーバのクエリに共有 IP が使用されない問題を修正致しました。 5. HTTP ベーシック認証の Realm 値がオプション設定とならない問題を修正致しました。 6. WEB UI における OSPF メモリ最大使用量の単位を”kilobytes”から”bytes”に修正致しました。 7. IPsec トンネルに設定された Local Gateway が CLI コマンド"ipsectunnels -iface"の出力結果に表示されない問題を修正致しました。 8. DFL-860E の DMZ/WAN1/WAN2、DFL-260E の DMZ/WAN のインタフェースのリンク

	ステータスが、Reconfigure 処理中に一時的に消える問題を修正致しました。 9. SMTP ALG 及び POP3ALG において添付ファイルの名前が必須となる問題を修正致しました。 10. SIP ALG で"420 Bad Extension"レスポンスを使用しないことがある問題を修正致しました。 11. NAT デバイス配下のビルトイン L2TP クライアントが正常に動作しない問題を修正致しました。 12. 新しいバージョンにアップグレードする際、コンフィグが正常に更新されないことがある問題を修正致しました。 13. Internet Explorer8 以前のブラウザバージョンを使用して HTTPS web 認証接続を行った場合、ユーザログイン後に画面が表示されない問題を修正致しました。 14. OSPF を実行しているノードにおいて多数のネイバを使用しているとき、稀にメモリが破損する可能性がある問題を修正致しました。 15. CLI 上での各種 SSH 関連コマンドの実行後に、出力結果が表示されない問題を修正致しました。 16. Routemon で一部インタフェースのリンクステータスを検出できない問題を修正致しました。（DFL-260E/DFL-860E のみ） 17. インタフェースのリンクステータス情報が Reconfigure 後に消えてしまう問題を修正致しました。（DFL-260E/DFL-860E のみ） 18. IDP が設定されているケースにおいて、一部のトラフィックで遅延が発生する可能性がある問題を修正致しました。 19. 同じ NAT ゲートウェイ配下に存在する複数の L2TP/IPsec クライアントに接続できない問題を修正致しました。 20. "Interface Alias"で"Comment"を選択した際に SNMP の Interface Alias 欄が空となる問題を修正致しました。 21. 同じローカル IP アドレスを持つ L2TP クライアントが NAT デバイス配下で IPsec トンネルを確立した場合に、通信に問題が発生することがある問題を修正致しました。 22. High Availability 構成における Reconfigure 処理時に、OSPF ルートデータベースが更新されない問題を修正致しました。 23. Web ユーザインタフェースが Internet Explorer10 と 100%の互換性がない問題を修正致しました。基本構成の更新により、すべての主要なブラウザにおいて正確なページのレンダリングが可能となりました。 24. Dynamic Routing Rules において、"OSPF Tag range"または"Router Type"でフィルタしている場合に OSPF ルートを正しくエクスポート/インポートできない問題を修正致しました。 25. SSL VPN や IPv6 Neighbor Discovery などの一部のログメッセージカテゴリが、ログメッセージ除外リストに含まれていない問題を修正致しました。 26. XAuth 認証の IPsec を使用している場合に ESP delete notification 送信されないことがある問題を修正致しました。 27. IP プロトコル 33 と 48 が誤ったプロトコル名でログ出力され、IP プロトコル 131 と 142 のプロトコル名が出力されない問題を修正致しました。現在の IANA 定義に基づいて IP プロトコルリストを更新しました。 28. Syslog Receiver 設定において、RFC5424 に基づく Syslog メッセージ送信のオプションを追加致しました。 29. 設定ページで「OK」ボタンを押下する前に 16 進数の Pre-Shared Key に対して検証が行われない問題を修正し、16 進数の文字列のみを受け付けるように対応致しました。 30. User Authentication Rule の作成時、ルール名を付けずに作成可能で、保存時にエラーが表示される問題を修正致しました。ルール追加時は名前の設定が必要となります。 31. CLI コマンド"dns"で 0～2 のインデックス値でサーバが表示される問題について、インデックス 1～3 でサーバが表示されるように修正致しました。 32. TCP_FIN ステートの通信の統計値に TCP_OPEN が含まれる問題を修正致しました。 33. VLAN インタフェースの統計が Reconfigure 処理毎にリセットされる問題を修正致しました。 34. DHCP リレーを設定していないインタフェース上で受信した DHCP リレーパケットがドロップされることがある問題を修正致しました。 35. グローバル設定で IPv6 を無効化している状態で VLAN の IPv6 を有効化した場合に、

	設定の警告が生成されない問題を修正致しました。 36. Reconfigure アクションの実行後、リンクステータスを使用したルートモニタリングにより無効化されたルートの復旧が行われない問題を修正致しました。 37. SSH CLI セッションにおいて、大量の貼り付けデータやセッションに送信された大量データを処理できない問題を修正致しました。 38. HA クラスタ構成環境において、IDP でスキャンされた通信が破損することがある問題を修正致しました。 39. WEB UI の L2TP/PPTP クライアントページにおいて、Originator IP Type や Originator IP の設定項目が存在しない問題を修正致しました。 40. システムによって自動的に作成されたインタフェースルートのインデックスについて、CLI を使用して変更できない問題を修正致しました。 41. タイムアウトした場合、UAC と UAS に対する通知を行わずに SIP セッションが終了する問題を修正致しました。セッション終了前の通知として、UAC にタイムアウトメッセージを送信し UAS にキャンセルメッセージを送信するように修正しています。 42. IPv6 エニーキャストソースアドレスが無効として処理される問題を修正致しました。RFC 4291 に基づいて"IPv6 Anycast Source"という新規設定が追加され、必要に応じて動作を変更できるようになっています。 43. CLI コマンド"arpsnoop"と"ndsnoop"が実行された時にステータスフィードバックが出力されない問題を修正致しました。 44. CLI コマンド"dhcpserver"を-mappings オプションと一緒に使用する場合に-num や –fromentry オプションに従わない問題を修正致しました。 45. 有効な Neighbor Solicitation の受信後に ND キャッシュの更新に失敗する場合がある問題を修正致しました。 46. WEB UI の IPv6 ネットワークアドレス検証で 100 以上のネットワークサイズの利用に対応できない問題を修正致しました。 47. L2TP/PPTP クライアントのリモートエンドポイントのアドレス帳から DNS オブジェクトを使用できない問題を修正致しました。 48. クラスタ設定を展開する際、稀にファイアウォールのメモリ消費量が増加することがある問題を修正致しました。 49. Status -> Run-time information -> Connections ページで選択したフィルタオプションの一部が適用できない問題を修正致しました。 50. 選択したルーティングテーブルが”main“ルーティングテーブルと異なる場合、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パラメータによって指定されたルーティングテーブルに IPv6 インタフェースルートが追加されない問題を修正致しました。 51. Identity Awareness Agent によって認証されたユーザは HA クラスタの非アクティブノードに同期されない問題を修正致しました。 52. PPTP クライアントが多数同時接続しようとした場合にユーザがログアウトする問題を修正致しました。 53. SIP ベンダーAastra が SIP ALG でサポートされていない問題を修正致しました。 54. SIP ALG の CLI コマンド"sip -registration flush"および"sip -statistics flush"が動作しない問題を修正致しました。 55. 到達不可な RADIUS アカウンティングサーバが稀に不明な動作を引き起こす可能性がある問題を修正致しました。 56. L2TP セッションがクローズするときにログが生成されない問題を修正致しました。 57. 有効な Neighbor Discovery パケットにより、インタフェースドロップ統計の値が増加する問題を修正致しました。 58. HA フェイルオーバ後に非アクティブなノードが古いルートステータスでスタックする問題を修正致しました。本問題による影響として、非アクティブノードのルートが実際には Up 状態であるにも関わらず Down 状態としてレポートされることがありました。 59. HTTP ALG における SNMP ステータスのインデックス値が Reconfigure 処理時にリセットされることで、ポーリング時に一つの HTTP ALG のみ表示される問題を修正致しました。 60. 一部のインタフェースタイプに対する SNMP プロパティのインタフェースエイリアスのポーリングにおいて、該当のインタフェースに設定されたコメントを返さない問

	題を修正致しました。 61. コンフィグファイルの最後に余分な改行が含まれている場合、コンフィグのバックアップやリストアが失敗する問題を修正致しました。 62. インタフェース上で DHCP クライアントが使用されているとき、ブロードキャストアドレスがセットされない問題を修正致しました。 63. HA ハンドオーバー時に、稀に非アクティブな HA ノードが自身の共有 IP に対して Neighbor Solicitation を誤って送信する問題を修正致しました。 64. HA クラスタで Switch Routes を設定しようとする際にエラーや警告が生成されない問題を修正致しました。 65. 外部からの SSL VPN 通信において、SSL VPN インタフェースの宛先ポート、宛先 IP、名前のログが存在しない問題を修正致しました。 66. 監視する HTTP ホストのリクエスト URL プロパティにおいて、実際の URL の前に "http://"プレフィックスが必要となる問題を修正致しました。本修正により、設定されていない場合には"http://"が自動的に追加されます。 67. ユーザからの"expected response"値にスペース、タブ、LF（ラインフィード）、CR（キャリッジリターン）などの特殊記号が含まれる場合、ファイアウォールは HTTP Monitoring レスポンスの適合に失敗する問題を修正致しました。 68. HTTP 監視ホストの DNS 解決が失敗した場合に、各ルートが常に”up”と宣言され、それ以上の通信の試行が行われない問題を修正致しました。 69. 複数のアクティブな IPsec トンネルが存在し、ダイナミックルートの追加が有効なシステムにおいて、Reconfigure 処理毎にメモリ使用率が増加する問題を修正致しました。 70. RADIUS の認証と（もしくは）アカウンティングにより、システムが不安定になることがある問題を修正致しました。 71. 多数のユーザがシステムにログインした後にメモリ利用率が増大する問題を修正致しました。 72. 実際のサービスがそれぞれ重複していない場合であっても、別のサービスグループのメンバとして構成されるときに、重複サービスについて警告が表示される問題を修正致しました。 73. Authentication Agent でエージェント名を指定せずにオブジェクトを追加できる問題を修正致しました。 74. "DirectedBroadcasts" drop ログメッセージにおいて、ブロードキャストを送信するホストのソース IP と、使用予定となっていた宛先 IP/network/broadcast に関する情報が含まれていない問題を修正致しました。 75. IPv6 Ping メッセージ送信時に IPv6 がグローバルで有効になっているかどうかをチェックしないため、動作可否に関わらずユーザが Ping を送信する可能性がある問題を修正致しました。 76. IPv6 ルートを追加し、IPv6 が有効化されていない場合に警告メッセージが通知されない問題を修正致しました。 77. 不正あるいは期限切れの RADIUS Accounting レスポンスによりメモリ使用量の増加を引き起こすことがある問題を修正致しました。 78. "pcapdump"機能において、キャプチャ対象がベースインタフェースの場合、VLAN 経由の外向きパケット通信をキャプチャできない問題を修正致しました。 79. IPsec トンネル経由で送信された ICMP パケットの最後の部分がドロップされることがある問題を修正致しました。 80. IPv6 グループが稀に誤った IPv6 アドレス範囲を作成することがある問題を修正致しました。 81. サービスグループにポートが重複するサービスを追加した場合に表示される警告メッセージについて、問題の内容と対処方法が明確になるように修正致しました。 82. タイムアウトによりログアウトしたユーザが、複数回ログアウトするように見える事象が稀に発生する問題を修正致しました。 83. Web コンテンツフィルタリングサービスのカテゴリ分類を示す円グラフで、Hit 数が多い場合にパーセンテージが正しく計算されない問題を修正致しました。 84. 2 つ以上の SSL VPN インタフェースに対し、同じサーバ IP とポートを設定できない問題を修正致しました。 85. SMTP ログレシーバにより IDP イベントがレポートされる際に、ファイアウォールで予期せぬ動作が発生することがある問題を修正致しました。

	86. NAT 配下において L2TP/IPsec 透過モードトンネルを使用している L2TP クライアントで、L2TP トンネルの再確立が行われないことがある問題を修正致しました。 87. VLAN インタフェースの MTU が正しく計算されず、不要な ICMPv6 PacketTooBig エラーメッセージが生成される問題を修正致しました。 88. invalid_ip_checksum ログメッセージで、チェックサムが正しく表示されない問題を修正致しました。 89. Ping コマンドの実行の際、ラウンドトリップ時間が正しくレポートされない事象が稀に発生する問題を修正致しました。 90. ファイアウォールから SCP 経由でハイフンを含むファイル名（例：my-cap.cap）のファイルをダウンロードすると、"Permission denied"エラーメッセージが表示され失敗する問題を修正致しました。 91. CLI コマンド"pipes -show"の実行後に出力結果が表示されない問題を修正致しました。 92. システムが不要な TCP ACK パケットを送信することがある問題を修正致しました。 93. CLI コマンド"pcapdump"実行時、バッファが一杯の場合に警告メッセージが表示されない問題を修正致しました。 94. カスタムタイムアウト設定の説明における"timeout"について、"idle lifetime"に修正致しました。 95. HA セットアップで"arp -notify"コマンドが使用された場合、システムが共有 MAC アドレスではなくプライベート MAC アドレスを不正に使用する問題を修正致しました。 96. SLB HTTP モニタリングの設定で、設定をブランクにしたままでもエラーを表示せず処理されるように修正致しました。 97. IDP ルールの HTTP Normalization 設定に対する変更が無視される問題を修正致しました。 98. IP がブラックリストに含まれた後にブラックリストからリリースされた場合、スタティックな DHCP リースがスタティックとして扱われない問題を修正致しました。スタティックリースは常にスタティックであり、ブラックリスト更新中に一時的に割り当てられた関連リースはリースプールから削除されます。 99. WEB UI の IDP ログステータスページで、ルールが構成済みであるにも関わらず常に"No IDP or Threshold rules are currently logging."と表示される問題を修正致しました。 100. HA クラスタのメンバの一つで UTM サービスが期限切れとなった場合、アクティブノードから非アクティブノードへのデータベース送信の永久ループが発生する問題を修正致しました。 101. Log and Event Receivers 設定で"main"以外のルーティングテーブルがサポートされない問題を修正致しました。 102. インタフェースにより、ハードウェア統計が CLI で正しく表示されない、かつリセットできないことがある問題を修正致しました。 103. XAuth 認証を使用する IPsec トンネルに関連する構成の変更を行った時に、稀に予期せぬ再起動が発生することがある問題を修正致しました 104. High Availability クラスタにおいて、ノードの少なくとも一つでアンチウイルスサブスクリプションが期限切れとなり IDP データベースが同期された場合、ノードで Reconfigure 処理のループが発生する問題を修正致しました。 105. 多数のアドレスが含まれる NAT プールを使用する際、パフォーマンスに悪影響をもたらす問題を修正致しました。 106. ALG が使用されていない場合、Update サーバへの Ping が正しく送信されない問題を修正致しました。 107. WEB UI ページのログインユーザ表示で、ユーザ名やグループではなく、"Logged in as"というラベルが付けられている問題を修正致しました。 108. Advanced Settings の IP 設定において、マルチキャストソースアドレスをブロックするアドレス範囲に含まれるアドレスが多すぎる問題について、アドレス範囲を適切な 224.0.0.0-239.255.255.255 に修正致しました。 109. LDAP 認証において、スペースを含む表示ユーザ名が使用されており、それが AD に対するユーザ名として使用されている場合、認証が失敗する問題を修正致しました。 110. High Availability 環境でシステムがアクティブになる際、システムで IPv6 アドレスが正しくアドバタイズされない問題を修正致しました。

	111. ファイアウォールを介して高負荷の IPsec トラフィックが送信された場合、稀にパフォーマンス低下に伴うハードウェアアクセラレーションの失敗に関するログが生成される問題を修正致しました。（DFL-260E/860E のみ） 112. CLI コマンドの出力表示やタブ使用に関する問題を修正致しました。 113. 内部 SSH サーバによりメモリ使用量が増加することがある問題を修正致しました。 114. 識別子名を設定していない IPv6Network のインタフェース上で Router Advertisement を有効にすると、設定エラーが発生する問題を修正致しました。 115. IPsec ログにおいて local_peer と remote_peer プロパティが切り捨てられる問題を修正致しました。 116. ファイアウォール起動時と HA アクティブ化の際に、常に IDP と AV データベースの自動更新が行われる問題について、設定時間のみに自動更新が実施されるように修正致しました。 117. ログイベント"too_many_flows_aged"と"failed_to_select_policy_rule"が両方とも同じログ ID 「01803001」を使用する問題を修正致しました。 118. OpenLDAP サーバに対する LDAP クエリが想定通りに動作しない問題を修正致しました。LDAP サーバにおいて'Combined Username'と'Optional Attribute'という新しい設定を利用することにより、OpenLDAP への LDAP クエリがどのように送信されるかを指定することができます。 119. HTTPS ALG を使用している場合に一部の Web ページへのアクセスや読み込みができない問題を修正致しました。 120. POP3 ALG ログメッセージに正しくない E メールアドレスが含まれることがある問題を修正致しました。 121. SMTP/POP3 ALG でデータのヘッダーから正しくフィールドが読み取れない事象が稀に発生する問題を修正致しました。 122. リンク障害からの復旧後、DHCP クライアントが自身の IP アドレスリースを更新しない問題を修正致しました。 123. ファイアウォールが SynRelay として構成されているとき、ピアの両方が NAT ゲートウェイ配下に配置され透過モードを使用している IPsec トンネル内において、TCP トラフィックが想定通りに動作せず、SYN-ACK がクライアントに到達しない問題を修正致しました。 124. Remote Management の SNMP 設定において、コミュニティストリングが 32 文字以上の場合に切り捨てられる問題を修正致しました。 125. Unsolicited ARP Replies 設定に従って Unsolicited ARP リプライが正しく処理されない問題を修正致しました。 126. User Authentication Rule における Multiple Username Logins 設定が、認証サーバからのタイムアウトを使用する選択をしている場合に正しく動作しない問題を修正致しました。 127. 同一インタフェース上で同じ IP を持つ 2 つの SSL VPN インタフェースが構成されている場合、異なるポートが使用されていても、2 つのインタフェースのうち一つのみですべてのクライアントの通信をトリガする問題を修正致しました。 128. SIP PBX の設定により、ファイアウォールが INVITE リクエストをドロップすることがある問題を修正致しました。 129. ソースとして LDAP を使用する認証済みユーザのパスワードにおいて、一部文字がサポートされていない問題を修正致しました。 130. 複数のスタティック DHCP ホストで同じ IP や MAC アドレスを警告メッセージなしに設定できる問題を修正致しました。 131. DFL-260E/860E の暗号化アクセラレータが高いパフォーマンス負荷状況で応答なしの状態になることがある問題を修正致しました。 132. CLI コマンド"dhcpserver"でクライアント識別子が表示されない問題を修正し、MAC と識別子の両方に対応致しました。 133. ユニキャストリプライの受信が可能であるにも関わらず、システムが DHCP Discover と DHCP Request メッセージ内に BROADCAST フラグをセットする問題を修正致しました。 134. CLI コマンド update center で引数を指定しない場合にエラーが返される問題を修正致しました。デフォルトアクションではすべてのデータベースのステータスを表示します。 135. DHCP の更新により L2TP/PPTP トラフィックに使用されるインタフェースに変更

	があった場合にL2TP/PPTPクライアントが正しくないソースIPを使用する問題を修正致しました。 136. IPsec Status ページから"List all active IKE SAs"をクリックした際にナビゲーションメニューが消える問題を修正致しました。 137. 出力インタフェースの IP アドレスの動的更新より前にオープンした通信について、NAT されたトラフィックで古いソース IP アドレスが使用される問題を修正致しました。 138. DHCP サーバに設定できる最小リース時間を 0 秒から 30 秒に修正致しました。 139. Ndsnoop コマンドの出力で、ファイアウォールの MAC アドレスが 00-00-00-00-00-00 と表示されることがある問題を修正致しました。 140. リモート管理インタフェースで悪意のある SNMP パケットを解析すると、システムが正しく動作しないことがある問題を修正致しました。 141. Web インタフェース上の IDP ログイベントで Advisory リンクが表示されない問題を修正致しました。また、IDP ログイベントを大量に表示するとき、システムが応答不可となる問題を修正致しました。 142. HTTP バナーファイルで、%REDIRHOST%の前にスペースが配置され不正な URL となる問題を修正致しました。 143. サービスのカスタムタイムアウトが、IP ポリシーで使用された場合に動作しない問題を修正致しました。 144. CLI コマンド"userauth -remove"で認証ユーザを強制ログアウトした際にログイベントが生成されない問題を修正致しました。 145. 65535 個のブロック処理の後、TFTP ALG によるパケットの転送が停止する問題を修正致しました。 146. CLI コマンド"ippool"と"idppipes"でデフォルトアクションが設定されておらず、引数が必須となる問題を修正致しました。本修正により、引数なしでの実行は"-show"オプションで実行することと同じ動作となります。また、他のコマンドとの整合性のため、"ippool"の"-max"オプションは"-num"オプションに置き換えられました。 147. ファイアウォールを経由するトレースルートの実行時に、開始クライアントへ正しく応答が返らない問題を修正致しました。 148. 新しい TLS プロトコルにおいて、ALG が SSLv2 互換性モードを処理できない問題を修正致しました。 149. 拒否されたパケットが存在しないにも関わらず、拒否された DHCP リレーパケットの統計が増加する問題を修正致しました。 150. CLI コマンド"ipsecstats -ike"で不要な"more entries not displayed"列が大量に出力される問題を修正致しました。 151. ブラックリストに含まれる IP アドレスが稀に誤った動作をすることがある問題を修正致しました。 152. 誤った PPPoE インタフェース名が closed/open イベントにログ出力されることがある問題を修正致しました。 153. 再起動せずにポートベース VLAN を削除することができない問題を修正致しました。 154. ポートベース VLAN によるパケット転送が、スイッチのルートに基づいて正しく行われない問題を修正致しました。 155. LDAP などの外部データベースから返されるグループ名にスペースが含まれることをサポートしない問題を修正致しました。 156. 手動で追加されたルートのデフォルトメトリックを 100 から 0 に修正致しました。 157. 透過モードの IPsec トラフィックにおいて、スタティック宛先アドレスの変換に失敗する問題を修正致しました。 158. IDP Rule の Rule Actions 設定において、有効化された"Protect"と"Dynamic Black Listing"を"Audit"アクションに変更した場合、"Dynamic Black Listing"が有効化されたままになる問題を修正致しました。 159. NAT デバイス配下で同じリモート ID を使用する IPsec 透過モードクライアントが、同時接続に失敗する問題を修正致しました。 160. IPsec インタフェースに設定する IPsec ルールが最大数に達した場合に管理者に通知する警告テキストを追加致しました。 161. RADIUS 認証が有効である場合に、SSL VPN Portal が SSL VPN クライアントと同じ認証方式を使用しないことがある問題を修正致しました。

	162. High Availability と OSPF を使用しているとき、同期インタフェースで稀に OSPF パケットのフラッディングが発生することがある問題を修正致しました。 163. RADIUS サーバからの応答に RADIUS アトリビュートが含まれる場合、RADIUS アカウンティングセッションがクローズする問題を修正致しました。 164. ピア Xauth 認証が必要なケースで、フェーズ 1 キー再生成ネゴシエーションが削除される問題を修正致しました。 165. 稀に IPsec 構成によってファイアウォールがバッファを使い果たすことがある問題を修正致しました。 166. 設定したパイプに収まらないパケットを処理する際に、Traffic Shaping サブシステムが CPU リソースを多大に消費する問題を修正致しました。 167. ブラックリストにおける大量のホストの処理を最適化致しました。 168. WEB UI オブジェクトで Clone オプションが常に利用可能とならない問題を修正致しました。 169. ネゴシエーションで最後の IKE メッセージが受信される前に、新しい IPsec セキュリティアソシエーションの ESP パケットを受信することにより、生存期間の間、ファイアウォールはそのセキュリティアソシエーションの ESP パケットをドロップする問題を修正致しました。 170. IKEsnoop メッセージ内の ISAKMP クッキーが正しく表示されず、'Delete SPIs'の出力と'IKE delete'メッセージ内のクッキーにおいて不一致が生じることがある問題を修正致しました。 171. XAuth 認証を使用する IPsec トンネルにおいて、ネゴシエーション後に稀にメモリ消費が増大することがある問題を修正致しました。 172. IP ポリシー構成時のソースアドレス変換で'Auto'を設定すると、正しく動作しない問題を修正致しました。 173. IPsec トンネル経由のフラグメント化されたトラフィックがドロップされることがある問題を修正致しました。 174. HTTPS 証明書を選択せずに HTTPS 管理を設定した場合でも、エラーが生成されない問題を修正致しました。 175. Router Advertisement 関連の設定で、一貫性のない名前を使用している問題を修正致しました。名前の修正及び configuration converter の追加により、既存の動作はアップグレード後も同様に動作します。 176. ネイバと通信する OSPF で IPsec インタフェースを使用できない問題を修正致しました。 177. プライマリルートが失敗したルートモニターセットアップにおいて、セカンダリルートを使用した通信が Reconfigure 処理時にクローズする問題を修正致しました。 178. RADIUS サーバの認証ユーザがタイムアウトするときに稀にメモリ消費が増大することがある問題を修正致しました。 179. VLAN インタフェースで実行するように OSPF を構成する際、OSPF マルチキャストパケットを受け付ける VLAN のイーサネットベースインタフェースの受信モードパラメータをセットせず、OSPF 通信が失敗することがある問題を修正致しました。 180. WEB ユーザインタフェースの選択ボックスの幅が不十分であり、長いオブジェクト名が完全に表示されない問題を修正致しました。 181. CLI コマンド"time -sync"によるエラーメッセージの説明が不十分である問題を修正致しました。 182. IPv6 コアルートの設定時、常に警告が生じる問題を修正致しました。 183. 一部ログで UTF-8 文字列が正しく表示されない問題を修正致しました。 184. CLI コマンド"ping"を使用してファイアウォールから送信された UDP パケットが常に同じ Fragmentation ID もしくは Identification フィールドを含む問題を修正致しました。 185. CLI コマンド"time -sync"による出力がすべてのアクティブな CLI セッションで表示される問題を修正致しました。コマンドの出力結果は、本コマンドを実行したセッションのみで表示されるようになります。 186. Syslog Receiver 設定オブジェクト内の Facility パラメータの説明における誤りを修正致しました。 187. あまり一般的でない証明書について、設定に追加できないことがある問題を修正致しました。 188. トラフィックがプロキシを介して送信される場合に HTTPS で Web コンテンツフィ

	ルタリングが動作しない問題を修正致しました。 189. 一部の Advanced settings 選択肢で説明が存在しない問題を修正致しました。 190. DHCP サーバの Custom Option パラメータは空欄にすることが可能にも関わらず、Save & Activate 中にエラーメッセージが表示される問題を修正致しました。 191. IPsec トンネルにおいて、リモートエンドポイントとして DNS 名を設定した IP4Address オブジェクトを使用する場合、IPsec トラフィックで問題が発生することがある問題を修正致しました。 192. WEB UI の Connections ページの行の背景色が、フィルタ適用後に変更されない問題を修正致しました。 193. "Ordering"を"Default"に設定したルーティングテーブルのルーティングルールを使用しているトラフィックが、正しくルートされないことがある問題を修正致しました。 194. HTTP ALG で WEB コンテンツフィルタリングを設定している場合、一部 HTTP サイトへのアクセスが失敗する問題を修正致しました。 195. TCPSequenceNumbers 設定で"ValidateLogBad"、"ValidateReopen"、"ValidReopenLog"、"ReopenValidate"、"ReopenValidLog"オプションが動作せず、システムが"ValidateLogBad"の設定で動作する問題を修正致しました。 196. パケットによる通信の再オープンが許可されており、転送される想定にも関わらず、パケットに不正な TCP シーケンス番号が含まれドロップされる旨のログが生成される問題を修正致しました。 197. OSPF の"point-to-multipoint"インタフェースで 2 つ以上のネイバ設定が許可されない問題を修正致しました。 198. OSPF の"point-to-multipoint"インタフェースがユニキャストではなくマルチキャストを使用するネイバを検知する問題を修正致しました。 199. OSPF の"point-to-multipoint"インタフェースがインタフェース IP に対し無効な"dummy"ルートを作成する問題を修正致しました。 200. "ifstat -restart"コマンド実行後、手動で割り当てられた MAC アドレスのイーサネットインタフェースが元の MAC アドレスに戻る問題を修正致しました。 201. 特定のルーティングテーブルを使用する SSL VPN インタフェースが既に構成されている場合、設定変更後の再起動実施時にファイアウォールが予期せぬ動作をすることがある問題を修正致しました。 202. システムの負荷が重い場合、稀に NetDefendOS の Web 認証が失敗することがある問題を修正致しました。 203. ファイアウォールの SNMP 統計で、アクティブな IPsec トンネルが"down"としてレポートされることがある問題を修正致しました。 204. SSL VPN インタフェースの設定時、Outer Interface としてインタフェースグループを使用することができない問題を修正致しました。 205. 新しいリースに対し、CLI コマンド"ippool -renew"を使用することができない問題を修正致しました。 206. 既存の証明書と同じ名前で証明書を保存しようとする際、エラーメッセージが表示されない修正致しました。 207. OSPF 内の E-flag が正しくセットされず、通信の問題が発生することがある問題を修正致しました。 208. IPsec インタフェースの Dead Peer Detection 設定がリモートクライアントに対して動作しないことがある問題を修正致しました。 209. 必要な権限を持たないユーザがログインした場合にメッセージが適切に表示されない問題を修正致しました。 210. Advanced TCP 設定において、CC（Connection Count）オプションが、WEB UI 上で誤った名前"TCP Option Connection Timeout"となっていた問題を修正致しました。 211. アドレス変換やアンチウイルスなどのコンテンツ検査機能を使用する通信において、ファイアウォールが不正なチェックサムの TCP パケットを生成することがある問題を修正致しました。この場合、稀に TCP 通信の低速化または停止を招きます。 212. 設定時の警告メッセージ"Shared IP address cannot be equal to iface IP address"において、該当インタフェースの名前が含まれない問題を修正致しました。 213. CLI コマンド"appcontrol -show_lists"の実行時、適切な情報が表示されない問題を修正致しました。 214. アンチウイルスなどのレイヤ 7 の機能の一部において、ICMP エラーがサービスで

	許可されているにも関わらず、ICMP エラーが転送されない問題を修正致しました。 215. IPsec と L2TP について、"IPsec Before Rules"または"L2TP Before Rules"オプションを使用する（ルールセットをバイパスさせる）とき、Syslog に default-rule として出力される問題を修正致しました。 216. WEB UI の Address book のフォルダにコメントが表示されない問題を修正致しました。 217. DHCP リレーのポート 68 で DHCPACK メッセージを受信した場合、当該メッセージが転送されない問題を修正致しました。 218. High Availability のセットアップにおいて、OSPF 経由のスタティックルートの挿入/削除が動作しない問題を修正致しました。 219. IPsec トンネルの NAT-T 設定が OFF に設定されていても NAT-T Vendor ID が送信される問題を修正致しました。 220. "Relay Filter"を設定した DHCP サーバにおいて、DHCP クライアントからのユニキャスト DHCP Request/Renewal メッセージを大量にドロップする問題を修正致しました。 221. RST フラグを持つ TCP セグメントに ACK 番号 0x00000000 が含まれない問題を修正致しました。 222. NAT-T に関連する相互運用性の問題により、IPsec トラフィックをドロップすることがある問題を修正致しました。 223. 大きなサイズの LSA を受信後、利用可能な十分なメモリがあるにも関わらず OSPF モジュールがメモリエラーをレポートする問題を修正致しました。 224. ログメッセージ内のユーザの access_level が正しく表示されない場合がある問題を修正致しました。 225. IPsec トンネルセットアップの際、サポートされない ISAKMP と IPsec Security Association 属性を受信した場合、設定した属性も送信されるにも関わらずセットアップが失敗する問題を修正致しました。 226. Web コンテンツフィルタリングで一部 URL が誤って禁止される問題を修正致しました。 227. ICMPv6 のエラーメッセージ"Packet too big"が NetDefendOS を通過せずにトラフィックがブロックされることがある問題を修正致しました。 228. アンチウイルスを使用している場合、'sysmsgs'コマンドを実行すると、稀に内部メディアについて"FAT chain inconsistence"とレポートすることがある問題を修正致しました。 229. Web ユーザインタフェースでブラウザを正しく識別せず、サポートされないブラウザバージョンを使用している旨のメッセージが表示される場合がある問題を修正致しました。 230. 誤った IPsec 認証アルゴリズム（SHA）が、同じトンネルの IKE アルゴリズムに設定されていると、IPsec トンネル設定に追加されることがある問題を修正致しました。（例：IKE アルゴリズムに SHA1 が設定されている場合、その SHA1 が自動的に IPsec アルゴリズムにも設定される） 231. CLI コマンド'ipsecglobalstats'の実行によりレポートされる"Active flows"の数が、短い生存期間の通信であったとしても常に最大値に達することがある問題を修正致しました。 232. 構成変更に伴う IP ルールや IP ポリシーについての警告メッセージが存在しない問題を修正致しました。 233. ZoneDefense が unblocking イベントに関してログ出力しない問題を修正致しました。 234. IPsec SA の暗号鍵再生成時、IKE SA がない状態でファイアウォールが IPsec "initial contact"通知を送信する問題を修正致しました。これにより、鍵生成リクエストが処理される前にレスポンダによる IPsec SA の削除が行われ、鍵生成に代わって新しい IKE と IPsec SA が確立されるため、トンネルを介したトラフィック送信が中断されることになります。 235. Update Center の Hourly 設定の設定可能範囲を 1-11 から 1-12 に修正致しました。 236. Update Center で"Hourly"インターバルを使用する場合、アップデートが設定値ではなく 1 時間ごとに実施される問題を修正致しました。 237. CLI コマンド”blacklist –show”コマンドですべてのブラックリスト及びホワイトリストのホストが表示される問題を修正し、デフォルトで 20 のブラックリスト及びホワ

	イトリストのホスト、または-num 引数で指定した数のホストを表示するように致しました。 238. NAT-pool の IP 範囲設定で、アドレスが 0.0.0.0 から開始する場合、非常に広範囲な IPv4 アドレス(> 65535)を受け入れる問題を修正致しました。 239. Web 認証使用時、パスワードに含まれるスペースが'+'記号に変換される問題を修正致しました。 240. アンチウイルスや IDP データベースが手動で削除された場合、管理 WEB UI の Update Center セクションにおいて日付が正しく表示されない問題を修正致しました。 241. CLI コマンド”pcapdump –show”ですべてのキャプチャされたパケットが表示される問題を修正致しました。デフォルトで 20 パケットもしくは-num 引数で指定されたパケット数を表示するように対応致しました。 242. IPsec プロポーザルが適合しているにも関わらず、IPsec トンネルセットアップで失敗することがある問題を修正致しました。 243. IDP 使用時、システムのメモリ消費が増大する問題を修正致しました。 244. ライセンス期限切れにより IDP スキャンが無効化された際にログ出力や通知が表示されない問題を修正致しました。 245. 複数のオプションを含む受信 ICMPv6/Neighbor Advertisement がファイアウォールによって中断される問題を修正致しました。 246. 同じ NAT デバイス配下の複数のクライアントへの L2TP/IPsec トラフィックが稀に混合してしまう問題を修正致しました。 247. フルシステムバックアップファイルが SSL VPN に関連するファイルを含まない問題を修正致しました。 248. NAT ゲートウェイ配下の L2TP 通信において、1 番目のクライアントが 2 番目のクライアント接続により稀に切断されることがある問題を修正致しました。 249. High Availability において、コンフィグの同期を完了させるためにノードの再起動が必要となることがある問題を修正致しました。 250. ブラックリストログに誤ったプロトコルとポートが表示されることがある問題を修正致しました。 251. SIP のメモリ使用率が正しく表示されない問題を修正致しました。 252. アクティブなノードで CLI コマンド"dhcpserver -releaseip"が実行された時に、DHCP サーバリースが非アクティブな HA ノードから削除されない問題を修正致しました。 253. HA クラスタでサポートされない PPPoE を設定しようとする場合に、明確なエラーメッセージを表示するように修正致しました。 254. WEB UI の DataGrids のインデックス列において、最大 999 項目までの表示が有効であった仕様を、5 桁まで有効となるように修正致しました。 255. IPv4 ヘッダーから Don't Fragment フラグを取り去るときにファイアウォールが Identification フィールドの一意性を検証しない問題を修正致しました。検証しない場合、他のノードについてリアセンブルの問題を引き起こす可能性があります。本修正により、Don't Fragment フラグが取り除かれた場合、0 の値の Identification フィールドは適切な値に置き換わります。 256. IPsec のパフォーマンスが時間の経過に伴い低下する問題を修正致しました。（DFL-260E と DFL-860E のみ） 257. カスタムタイムアウト値を持つサービスオブジェクトから生成された通信タイムアウトが、High Availability クラスタのピア間で正しく同期されない問題を修正致しました。 258. IPsec トラフィックを管理するパケットバッファが最適化されない問題を修正致しました。 259. HTTP ALG で、"Accept-Encoding"ヘッダーに含まれるサポートされないキーワードがアンダースコアに置き換えられ、制限の厳しい Web でリクエストに失敗する可能性がある問題を修正致しました。本修正により、すべてのキーワードはスペースに置き換わります。 260. アンチウイルススキャンを行うように設定した HTTP ALG を使用する場合、一部のファイルのダウンロードに失敗する問題を修正致しました。 261. Email Control のブラックリストとホワイトリストのフィルタが正しく一致しないことがある問題を修正致しました。

	262. IPsec トンネルの NAT-Traversal が OFF に設定されている場合でもファイアウォールが IPsec プロポーザルで UDP encapsulation mode を送信する問題を修正致しました。 263. Auditor 権限のユーザでログインしているときに snoop コマンドを利用できる問題について、管理者アクセス権限を持つユーザのみで利用できるように修正致しました。 264. HTTP ALG によって生成される"Malformed Request"エラーページに"Reclassification Request Failed"のエラーページが含まれる問題を修正致しました。 265. POP3 ALG を使用する場合に E メールコンテンツが誤ってブロックされることがある問題を修正致しました。 266. UDP を使用するプロトコルの脆弱性により DDoS 攻撃で攻撃の影響を増幅させる可能性がある問題を修正致しました。 267. POP3 または SMTP のコンテンツ検査を使用しているとき、ネストされた複数の部分から成る E メールが破損する問題を修正致しました。 268. 稀にファイアウォールで実行中のコンフィグバックアップをダウンロードすることができない問題を修正致しました。 269. ID 616、617、618 の HA ログメッセージが、イベントの説明について誤ったシンタックスを使用している問題を修正致しました。 270. SMTP ALG において、Outlook Mail クライアントで送信されたメールがスパムとしてマークされる問題を修正致しました。 271. PPPoE 設定が変更された際に古い PPPoE セッションが終了しない問題を修正致しました。 272. 古い IP ルールの利用を無効化することにより、Threshold、Pipe、IDP、ルーティングルールまで無効化される問題を修正致しました。 273. 古い IP ルールの利用を無効化しても、IP ルールセットに含まれる IP ルールが無効化されない問題を修正致しました。 274. IPsec トンネルのセットアップ速度が遅くなり、IPsec トンネルを多数含む大規模なセットアップにおいて CPU 負荷が高くなる問題を修正致しました。 275. ファイアウォールで生成されたパケットが、Switch Route を介してルーティングされた場合に誤ったハードウェアアドレスを取得する問題を修正致しました。 276. アンチウイルスで Reconfigure 処理によりシグネチャ更新が中断された場合、ユニットの構成終了後に手動でアップデートを行い、ダウンロードを再開させる必要がある問題を修正致しました。 277. 11.00 未満のバージョンから 11.00 以上のバージョンにアップグレードする場合、稀に設定エラーで失敗することがある問題を修正致しました。 278. アンチウイルスデータベースを更新する際の通信エラーにより全ての更新プロセスが再実行される問題を修正致しました。 279. WEB UI の read-only オブジェクトをクローン（コピー）した場合、元のオブジェクトからいくつかの値がコピーされない問題を修正致しました。 280. Clone 機能がサポートするオブジェクトを更新致しました。 281. IKE Security Association の期限が切れようとしているとき、システムが Dead Peer Detection メッセージに応答しないことがある問題を修正致しました。 282. Safari ブラウザを使用している場合にコンフィグバックアップをアップロードすることができない問題を修正致しました。 283. 一部の HTTP バナーファイルで"%URL%"変数が正しく置き変わらないことがある問題を修正致しました。 284. SAT ルールを使用している場合、IPsec 透過モードにおける TCP パケットのチェックサムに誤りがあり、トラフィックがドロップすることがある問題を修正致しました。（DFL-2560 と DFL-2560G のみ） 285. POP3 通信が稀に応答しなくなることがある問題を修正致しました。 286. NATPool サブシステムで、構成済み IP 範囲がフルに使用されない問題を修正致しました。 287. クライアントが以前割り当てられていた IP アドレスを取得しようとするときに、DHCP サーバで、受信 DHCPREQUEST メッセージをフィルタする構成済みリレーフィルタが使用されない問題を修正致しました。 288. ライフタイムを過ぎた後も、IP アドレスが DNS キャッシュに残ることがある問題を修正致しました。 289. ユーザ認証時、グループメンバシップのリストが 255 文字に制限され、一部ユーザ

	権限に対応できない問題を修正致しました。 290. HTTP ALG において、SSL サーバ証明書でバージョン番号がない場合に受信できない問題を修正し、番号がない場合は version1 に変換されるように対応致しました。 291. XAuth 認証を使用する IPsec トンネルにおいて Dead Peer Detection が開始されない事象が稀に発生する問題を修正致しました。 292. Main ルールセット以外のルールセットで FQDN オブジェクトを使用する場合、IP アドレスが FQDN オブジェクトに追加・削除された際に、破損した情報の重複ログイベントが生成される問題を修正致しました。 293. メモリにロードされたアンチウイルスシグネチャの誤った番号がレポートされることがある問題を修正致しました。 294. ライフタイムの間に IKE SA が IKE 鍵を再生成している場合、"ike -show -tunnel=<tunnel_name>"コマンドの出力が正しくフィルタされない問題を修正致しました。 295. 一部の非標準 IMAP 拡張がサポートされていない問題を修正致しました。 296. WEB UI でアドレスグループ上にマウスカーソルを合わせたとき、各アドレスオブジェクトのアドレスがツールチップ（補足情報画面）に表示されない問題を修正致しました。 297. リモートエンドポイントタイプの IP 範囲やネットワークで設定された、透過モードの IPsec トンネルが、NAT 配下のピアに対してのネゴシエーションに失敗する問題を修正致しました。 298. ARP モニタリングが無効化されている場合でも、手動 ARP ルックアップ間隔が指定されたとき、ルートフェイルオーバ時の ARP モニタリングが無効化されない問題を修正致しました。 299. ホストモニタリングの設定で稀に設定エラーが発生する問題を修正致しました。また、ホストモニタリングに HTTP を使用し HTTP 応答がフラグメント化された特殊なケースにおいて、システムが正しい応答のマッチングに失敗する問題を修正致しました。 300. トラフィックが何らかの理由で IPsec トンネル経由での転送を停止した場合、トンネルモニタリング機能と CLI コマンド"ike -delete"は、IKE SA（IKEv1 のみ）に属さない一部の IPsec SA を削除することに失敗する問題を修正致しました。 301. ESP トラフィックが誤って IPsec トンネルにルーティングされることがある問題を修正致しました。 302. IMAP を使用した E メールのダウンロード方式の一部が想定通りに動作しない問題を修正致しました。 303. SMTP と HTTP ALG に対するアンチウイルススキャンにより、時間の経過に伴いシステムのメモリ消費が増大する問題を修正致しました。 304. アクティベーションの前に不正な FQDN アドレスを検出することができない問題を修正致しました。 305. CLI コマンド“blacklist”において、-time オプションで 0 秒を指定し IP アドレスを 0 秒間ブロックした場合、ブラックリスト一覧で負の値が生成され、次の再構成イベントまでホストがブロックされる問題を修正致しました。本修正により、ブラックリストの設定中は 0 秒間の IP ブロックを実行できないように対応致しました。 306. Reconfigure 処理後に Brute force 履歴が失われる問題を修正致しました。 307. SCP 経由の証明書ダウンロードが正常に行われない問題を修正致しました。 308. 不正な MIME 形式の E メールが正しく転送されない問題を修正致しました。 309. 認証ソースとして RADIUS を使用し、User Authentication SSL VPN Rule で複数ログインを許可しているとき、同じインタフェースと IP からの SSL VPN Portal への複数ログインが許可されない問題を修正致しました。 310. Authentication Agent と REST API ユーザに関するログイベントが生成されない問題を修正致しました。 311. 一部の ICMP と ICMPv6 エラーの TCP パケットに不完全な SEQ/ACK 番号が含まれる問題を修正致しました。 312. E メールの MIME ボディが空の場合、POP3 コンテンツスキャンを通過しないことがある問題を修正致しました。 313. IPv6 トラフィックにおいて HTTP ALG が使用されているとき、Path MTU Discovery が動作しないことがある問題を修正致しました。 314. 稀に POP3 ALG でメールフェッチのタイムアウトが発生する問題を修正致しまし

	た。 315. 送信済みフォルダにメールのコピーを保存するように設定された一部の E-Mail クライントにおいて、IMAP ALG 経由で E メールが送信できない問題を修正致しました。 316. メッセージ添付を含む E メールの一部が IMAP もしくは POP3 コンテンツスキャナーにより正しく転送されない問題を修正致しました。 317. CLI による各 NAT Pool の概要で関連する flow の数が正しくない問題を修正致しました。 318. ステートフル NAT Pool において、構成済み最大ステート値に基づいてステート数が制限されない問題を修正致しました。 319. RFC 1939 で示されるように最終オクテットで始まる行を"byte-stuffed"（バイトで埋める）処理をする、という要件を満たさないメッセージについて、POP3 コンテンツスキャナーで処理できない問題を修正致しました。 320. NetDefendOS 11.04.00 ではスケジュール機能を設定できても適用することができない問題を修正致しました。 321. WEB ポータルへのユーザ認証で BASIC 認証を使用するとき、正しい post-login ページが表示されない問題を修正致しました。 322. IPsec 暗号化/復号化用のハードウェアアクセラレーションを使用するプラットフォームにおいて、不完全な ESP パケットによりトンネルが正常に確立されないことがある問題を修正致しました。 323. IMAP スキャンで全てのデータが利用可能でないとき想定しない動作となる問題を修正致しました。 324. E メールヘッダーが IMAP ALG 経由でダウンロードされない問題を修正致しました。 325. Reconfigure 処理後、通信がタイムアウトした際にステートフル NAT プールの一部のステートがスタックし、削除できない問題を修正致しました。 326. UI エレメントが存在せず、単一のポリシーに対し SAT ポリシーを構成することができない問題を修正致しました。 327. Update Center が破損した IDP シグネチャデータベースを削除できない問題を修正致しました。 328. 復号化に失敗した ESP パケットについて、ログメッセージに失敗の理由が正しく生成されない問題を修正致しました。 329. POP3 コンテンツスキャンによる解析が一部の E メールで正常に行われず検出エラーが発生する問題を修正致しました。 330. 明示的な Content-Type ヘッダーが存在しない場合、POP3 コンテンツスキャナーによる、メッセージの最後のボディ部分の脅威検出が失敗する問題を修正致しました。 331. ファイアウォールが稀に無効な DNS クエリを生成する問題を修正致しました。 332. HTTP Poster による IP アドレスの自動更新が正常に動作しない問題を修正致しました。 333. 接続 WEB サーバがコンテンツ圧縮を使用している場合、アンチウイルススキャンを設定した HTTP ALG で適切にスキャンできない問題を修正致しました。本問題では、アンチウイルスエンジンによる検出結果が、ファイルが感染した/（感染したにも関わらず）クリーンである、というように誤った内容になります。 334. システム起動時から 24 時間以内に Reconfigure 処理が行われると、Update Center サブシステムが CSPN サーバの更新リストの取得に失敗する問題を修正致しました。 335. CLI コマンド"dhcprelay"でエントリを無制限に表示する問題を修正致しました。本修正により、デフォルトで 20 エントリを表示し、必要に応じて-num オプションでエントリ数を指定できるようになりました。 336. 証明書の Import/export と検証について、より整合性のある方法に修正致しました。本修正により、証明書とプライベートキーは、PEM エンコード形式の crt/key ファイル拡張子でエクスポートされるようになりました。インポート可能な証明書は PEM または DER エンコード形式の証明書です。 337. セットアップウィザードの時刻設定にて Set Date and Time ページにリダイレクトされる問題を修正致しました。Set Date and Time は削除され、セットアップウィザード内で設定できるようになりました。 338. PPPoE トンネル経由で構成された外部ルートに関して、トンネルが IP を取得した後にアンチウイルスのデータベースが自動的に更新されない問題を修正致しました。 339. HTTP ALG において、成功していない HTTP コードを正しく処理できず、トラフィックの送信が妨げられる問題を修正致しました。

	340. パケット転送時、SYN リレー機能で ICMPv6 エラー”Packet Too Big”内の TCP ヘッダーを正しくリストアできない問題を修正致しました。 341. PPPoE インタフェースへ送信されるパケットがパケットキャプチャ機能でキャプチャされない問題を修正致しました。 342. 7-bit 転送エンコードを含む HTTP パーシステントコネクションの HTTP ALG を使用すると、同じ 7-bit 転送エンコードを使用して、後に続くすべてのメッセージを処理する問題を修正致しました。 343. HTTP を使用した音楽ストリームで Web コンテンツフィルタリングまたは File Control を設定している場合、一部ストリームがドロップする問題を修正致しました。 344. メインルーティングテーブルに含まれないインタフェースについて、IPv4 DHCP サーバの応答が送信されない問題を修正致しました。 345. High Availability における Out-of-buffers カウンタが正しく増加しないことがある問題を修正致しました。 346. TLS ALG において、一部アプリケーションがタイムアウトする問題に対応するため、Idle Timeout 値を 30 秒から 5 分に修正致しました。 347. 無効な MIME フォーマットが含まれる E メールが IMAP コンテンツスキャナーの通過に失敗する問題を修正致しました。 348. DNS サーバへのルートが不明な場合、最初の試行失敗の後、DNS キャッシュがバックオフし、FQDN アドレスを解決できない問題を修正致しました。 349. 再送信された TCP SYN パケットがドロップの信号を送る ACK と一緒に応答される問題を修正し、誤った ACK 応答を削除致しました。 350. IMAP を使用する E メール制御の一部機能が、プライベートネットワークで使用された場合に動作しない問題を修正致しました。 351. Connection Close を受信後、リストの次のサーバを試行せずに同じ Updatecenter WCF サーバが再度試行される問題を修正致しました。 352. IMAP の事前認証が想定通りに動作しない問題を修正致しました。 353. Initial_Contact 通知受信時、IKE SA を使用しない IPsec SA が削除されない問題を修正致しました。 354. HTTP ヘッダーフィールド'Content-type'でサポートされる文字数が 64 文字のため、HTTP ALG 使用時にアクセス不可な URL が存在する問題について、サポート文字数を 256 文字に修正致しました。 355. HTTP を使用したホストモニタリングで、受信データと ExpectedResponse パラメータが正しく合致しない問題を修正致しました。 356. PPPoE インタフェースのソースインタフェースとして Link Aggregation インタフェースを選択できない問題を修正致しました。 357. ステートフル NAT プールにおいて、新しいステートに対し、最後に使用された IP を使用しないことがある問題を修正致しました。 358. データの転送中、どちらか片側で予期せず IMAP 通信がクローズした場合、ファイアウォールで適切に処理できない問題を修正致しました。 359. 大きなサイズの添付ファイルを含む E メールの場合、稀にアンチウイルススキャナーを通過しない問題を修正致しました。 360. POP3 に対するアンチスパムのタグ付けが稀に想定通りに動作しない問題を修正致しました。 361. E メールの圧縮添付ファイルによって予期せぬ動作が発生することがある問題を修正致しました。 362. 稀にアンチウイルススキャナーが ZIP ファイルのスキャンに失敗する問題を修正致しました。 363. マルチキャストアドレス変換を使用しているとき、ファイアウォールによる UDP フラグメントのデータ変換が正しく行われない問題を修正致しました。 364. 圧縮ファイルに対するウイルススキャンが正しく動作しない問題を修正致しました。 365. ファイアウォールによる自動 IPv6 フラグメントの送信が可能だった問題を修正致しました。 366. すべての IPsec トンネルインタフェース設定を削除すると、1 分程度の Reconfigure 処理が発生する問題を修正致しました。 367. 非マルチパートメッセージが IMAP コンテンツスキャナーによって正しくスキャンされない問題を修正致しました。

	368. IMAP を使用しているとき、スパムメールが正しくタグ付けされない問題を修正致しました。 369. 同じメールに対して異なる方式でスパムが検出された場合、IMAP ALG のスパムカウンタが正しくカウントされない問題を修正致しました。本修正により、スパムカウンタは検出スパムメール毎にカウントされます。 370. DHCP Relays 設定の MaxAutoRoutes 項目を MaxConcurrentRelays という名前に変更し、機能を明確に表すように修正致しました。 371. LDAP 応答を受信したとき、memberOf 属性に含まれるユーザグループの最初の 256 文字のみ使用される問題を修正致しました。 372. ルートフェイルオーバにおいて ARP モニタリングが使用され、その後無効化された場合、システムが再起動するまで ARP モニタリングクエリを送信し続ける問題を修正致しました。 373. POP3 メッセージトランザクションが正しく処理されないことがある問題を修正致しました。 374. ウイルスを含む E メール添付が稀に POP3 ALG もしくは SMTP ALG によって検知されない問題を修正致しました。 375. 非常に大きなサイズのエピローグを含む E メール（破損していることが多い）が IMAP コンテンツスキャナーの通過に失敗する問題を修正致しました。 376. ZoneDefense を設定しているとき、不明な設定に関する警告が表示される問題を修正致しました。 377. スケジュールされたアンチウイルスの更新が、処理に失敗または停止する場合がある問題を修正致しました。更新に時間がかかる場合に適切に処理できるように、スケジュールエンジンが更新されました。 378. IMAP コンテンツスキャン時、暗号化された長いサブジェクトヘッダーを持つ E メールメッセージが破損することがある問題を修正致しました。 379. Mail Alerting が設定され、新しい設定をアクティブ化する際に設定の警告が表示されないことがある問題を修正致しました。 380. ローカルユーザデータベースのユーザがログインしたときに追加されたルートが、システムの再構成後に破損または追加されない問題を修正致しました。

既知の問題：

ファームウェアバージョン	既知の問題
V11.10.01.06	1. HA モードにおいて、透過モードのステート同期が行われずループが発生する問題。 2. アプリケーションレイヤゲートウェイでステート同期行われない問題。クラスタが他のピアにフェイルオーバするとき、ALG によって処理されるすべてのトラフィックがフリーズします。ただし、クラスタが 30 秒程度で元のピアへフェイルバックした場合、フリーズしたセッション（及び関連する送信）は再度処理を開始します。新しい設定がアップロードされる度、このようなフェイルオーバ（及びフェイルバック）が発生します。 3. HA クラスタの非アクティブノードが、IPsec、PPTP、L2TP および GRE トンネル経由で到達不可となる問題。これらのトンネルはアクティブノードへ/から確立します。 ・非アクティブな HA メンバはトンネルを介してログイベントを送信できません。 ・非アクティブな HA メンバはトンネルを介して管理/監視できません。 ・OSPF：クラスタメンバがブロードキャストインタフェースを共有せずに、非アクティブノードが OSPF ステートについて学習する場合、トンネル経由の OSPF フェイルオーバはアクセラレータされたフェイルオーバ（<1s）ではなく、通常の OSPF フェイルオーバを使用します。デフォルト設定で 20-30 秒、より積極的な同期 OSPF タイミングでも 3-4 秒かかります。 4. L2TP 及び PPTP トンネルでステートが同期されない問題。フェイルオーバ時には、トンネルが動作していないとみなされた後に、次のクライアントでトンネルを再確立します。タイムアウトは一般的に 30～120 秒の範囲です。 5. IDP シグニチャステートが HA モードで同期しない問題。 6. トランスポートモードの 2 つの DFL ファイアウォール間で、IPsec L2TP/L2TPv3 ト

	ンネルを確立できない問題。 対処方法：クライアントサイトの WAN IP アドレスに対して“local endpoint”を指定する