



ファームウェア バージョン:	V2.40.01	
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:	2012/06/29	

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
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	2
WEB GUI 経由でのアップグレード方法	2
追加機能:	2
修正した問題点:	3
既知の問題:	4

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: v2.40.01	2012/06/29	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 GUI 経由でのアップグレードを行う方法」の2つがあります。

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 を使用することで、CLI の使用と管理者のワークステーションから NetDefend ファイアウォール間のファイル転送を安全に行なうことができます。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。

WEB GUI 経由でのアップグレード方法

WEB GUI 経由でのアップグレード方法は、ユーザマニュアルのファームウェアの更新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
V2.40.01	<ol style="list-style-type: none"> 1. VLAN インタフェースと同様に、イーサネットにおける IPv6 ルーティング、IP ルール、ポリシーベースルーティングに対応致しました。 2. HTTP posters の数の制限を削除致しました。 3. Ethernet MAC アドレス over HTTP(s)を使ったユーザ認証に対応致しました。 4. パスワード欄をアップデート致しました：パスワードが含まれているテキスト入力欄に移動した場合、パスワード欄がクリアされ、ユーザは直接新しいパスワードを入力することができます。 5. WebUI ページの“Reset”は通常のシャットダウン（CLI コマンドの“shutdown”と同じ動作）も含まれるように対応致しました。 6. iPhone での Cisco IPSec クライアントをサポート致しました。 7. より多くのカテゴリサイトに対応するため、Web コンテンツフィルタリングローカルキャッシュサイズを倍に致しました。 8. SSL VPN において CHAP、MS-CHAP、MS-CHAPv2、No Authentication をサポート致しました。 9. Web コンテンツフィルタリング設定において、filtering override を有効化すると override 間のタイムアウト値を入力することができるように対応致しました。

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
V2.40.01	<ol style="list-style-type: none"> 1. RADIUS アカウンティングを使った VPN 設定によっては、RADIUS アカウンティングサーバに入力/出力オクテット統計をレポートしなかった問題を修正致しました。 2. H.323 ALG が Alerting 状態の間、FACILITY メッセージを送信することができなかった問題を修正致しました。 3. LDAP から発信されるトラフィックがファイアウォールにより予期しない動作を引き起こすことがある問題を修正致しました。 4. SSL VPN は Proxy ARP された IP でリッスンするように構成されていた場合に、SSL VPN ポートあるにログインすることができなかった問題を修正致しました。 5. WebUI で Objects>>Services ページを閲覧するとファイアウォールが予期しない動作を行う問題を修正致しました。(DFL-260E/860E のみ) 6. SSL ネゴシエーションにおいて、ファイアウォールが不正なパケットを送信することがある問題を修正致しました。 7. HA を利用している場合に、SSL VPN クライアントをダウンロードするためにファイアウォールにログインすることができなくなる問題を修正致しました。 8. LDAP サーバの“パスワードアトリビュート”の値を空欄にすることができなかった問題を修正致しました。 9. インタフェースグループ内にインタフェースグループを追加することが可能だった問題を修正致しました。 10. イーサネットインターフェースのリンクがダウンした場合に ARP によってだけモニタされているルートはダウンとして認識しなかった問題を修正致しました。 11. “backup and restore”を使って High Availability を設定した場合に、正しくないインタフェース設定となるために設定を同期することができなくなる問題を修正致しました。 12. 大きな VLAN タグパケットがドロップされる問題を修正致しました。(DFL-260E/860E のみ) 13. SNMP で間違ったリンクスピードをレポートする問題を修正致しました。(DFL-260E/860E のみ) 14. インタフェースを誤ってリスタートさせる指示をすることがある問題を修正致しました。(DFL-260E/860E のみ) 15. 閏年の日が 2 月ではなく 1 月に追加されていた問題を修正致しました。 16. ログイベント“no_arp (ID:04100007) firewall action text was previously route_enabled”で“route_enabled”となっていた問題を“route_disabled”に修正致しました。 17. WebUI ALG SIP ダイアログのヘルプテキスト及び CLI コマンド“help ALG_SIP”にタイムユニット“秒”が追加されていた問題を修正致しました。 18. HA 環境においてアンチウィルスもしくは IDP ライセンスが期限切れとなった場合、非アクティブクラスタノードの予期しない動作の原因となる問題を修正致しました。 19. Web 認証を利用している場合に、ファイアウォールの予期しない動作を招くことがある問題を修正致しました。 20. SSH リモート管理を利用している場合に、CLI コマンド“dns -list”の出力テキストが正しいフォーマットではなかった問題を修正致しました。 21. オブジェクトがほとんど同じ名前が設定された場合に、ファイアウォールが下限と上限を正しく制御しなかった問題を修正致しました。 22. HA を利用している場合に、HA 設定 ReconfigFailoverTime が正しく動作せず、アクティブピアの設定を展開する際、ReconfigFailoverTime に到達する前にフェイルオーバーをしてしまう問題を修正致しました。 23. HA ウィザードをキャンセルした場合に、ファイアウォールの予期しない動作を招くことがある問題を修正致しました。(DFL-260E/860E のみ) 24. 稀に SIP セッションのクローズがファイアウォールの予期しない再起動の原因となる問題を修正致しました。 25. SSL VPN トンネルの安定性の問題を修正致しました。

26. 新しい設定を展開するとインタフェースのパフォーマンスに影響を与えてしまう問題を修正致しました。(DFL-260E/860E のみ)
27. HA クラスタにおいて共有 IP で SSL VPN を実行している場合に、再設定の間に非アクティブノードがアクティブになるために再設定時にクライアントが切断される問題を修正致しました。
28. SCP (Secure copy)の最近の変更によりオプションパラメータの終了を使うことにより、SCP コネクションが予期せずクローズされることでファイアウォールが誤った制御をしてしまう問題を修正致しました。
29. "add" CLI コマンドが場合によって、新しいオブジェクト設定にエラーをきたし、"set" CLI コマンドで正しくない値を入力することによりオブジェクト設定をユーザが編集することができてしまう問題を修正致しました。"-force"フラグを指定しない限り、変更でエラーが生じても設定を編集できないように変更致しました。
30. CLI"netobject"コマンドがIPv4 フォーマットでIPv6 アドレスを表示していた問題を修正致しました。
31. HA クラスタハートビートの送信を無効にすることができなかった問題を修正致しました。
32. 再設定され、新しい URL の解決に失敗した後、Web コンテンツフィルタサーバ接続が失速する問題を修正致しました。
33. ルーティング情報を含むログメッセージに正しくない値が利用されていた問題を修正致しました。
34. H.323 ALG を使っている場合に稀に予期しない動作をする問題を修正致しました。
35. 新しい設定を展開中に設定モジュールのエラーにより稀に予期しない動作を引き起こす問題を修正致しました。
36. CLI コマンド"ifstat"の出力にHA クラスタノードのインタフェースの共有 MAC アドレスが含まれていた問題を修正致しました。
37. 新しく追加されたユーザのパスワードが設定ファイル中で暗号化されていなかった問題を修正致しました。
38. 2 以上の ID を利用している場合に、OSPF MD5 認証が間違った動作をする問題を修正致しました。
39. RADIUS アカウンティングセッション ID 文字列が、後のセッションで再利用されることがある問題を修正致しました。
40. 新しい設定をアクティベートした後、CLI にプロンプトが表示されなくなる問題を修正致しました。
41. ファイアウォールの SSL VPN クライアントダウンロードページが開けない原因となる CVE-2011-3389 のセキュリティパッチに対応致しました。

既知の問題：

ファームウェアバージョン	既知の問題
V2.40.01	<ol style="list-style-type: none"> 1. SSL VPN インタフェースがアウトインターフェイス"any"オプションで設定されている場合に、SSL VPN が無効となる問題。 2. Oray.net Peanut Hull クライアントで使われる最新のプロトコルをサポートしていない問題。 3. HA モードにおいて透過モードが存在しない問題。 4. ALG が HA モードにおいてステートの同期が行えない問題。 5. HA モードにおいて、L2TP、PPTP、IPSec がステートの同期が行えない問題。 6. 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。 7. クラスタメンバーは非アクティブノードが OSPF ステートを学習することができるように、ブロードキャストインタフェースを共有しない場合に、VPN トンネルを介した OSPF フェイルオーバーはアクセラレート (<1s) フェイルオーバーよりも通常の OSPF フェイルオーバーを利用する問題。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。

- | | |
|--|-----------------------------------|
| | 8. IDP シグニチャステートが HA モードで同期しない問題。 |
|--|-----------------------------------|

Copyright 2006-2012 D-link Japan K.K.