FortiGate™

バージョン 4.0 MR2

管理ガイド

本書は FortiOS 4.0 MR2 のリリース直前に発行されました。したがって、その内容は発行日に基づく情報に限られます。本書は 2010 年 5 月に改訂される予定です。詳細については techdoc@fortinet.com までお問い合わせください。

FORTINET®

FortiGate 管理ガイド

バージョン 4.0 MR2

2009 年 3 月 26 日

01-420-89802-20100326

商標

目次

はじめに

小規模企業向けの FortiGate ® -50 シリーズから大規模企業、サービスプロバイダ、およびキャリア向けの FortiGate-5000 シリーズまで、FortiGate 製品ラインは、FortiOS セキュリティ オペレーティング システムを FortiASIC プロセッサやその他のハードウェアと組み合わせて、次のような一連の高性能なセキュリティおよびネットワーク機能を提供します。

- ファイアウォール、VPN、およびトラフィック シェーピング
- 不正侵入防御システム (IPS)
- アンチウイルス / アンチスパイウェア / アンチマルウェア
- Web フィルタリング
- アンチスパム
- アプリケーション制御 (たとえば、IM や P2P)
- VoIP サポート (H.323、SIP、および SCCP)
- レイヤ 2/3 ルーティング
- 複数の冗長 WAN インタフェース オプション

FortiGate アプライアンスは、ネットワークの可用性やアップタイムを低下させることなく、ネットワーク、コンテンツ、およびアプリケーション レベルの脅威 (サイバー犯罪者が好む複雑な攻撃を含む) に対するコスト効果に優れた包括的なプロテクションを提供します。FortiGate プラットフォームには、ネットワーク アップタイムを最大化するための高可用性 (アクティブ / アクティブ、アクティブ / パッシブ) や、異なるセキュリティ ポリシーが必要なさまざまなネットワークを分離するためのバーチャル ドメイン機能などの高度なネットワーク機能が搭載されています。

この章には、以下のトピックが含まれています。

フォーティネット製品

セキュリティ ゲートウェイやそのほかの製品で構成されたフォーティネットの製品ポートフォリオでは、ASIC で高速化されたハイ パフォーマンス、統合複合脅威プロテクション、および常に更新される詳細な脅威インテリジェンスが強力に統合されています。こうしたユニークな統合ソリューションを通じて、あらゆる規模の企業、管理されたサービスプロバイダ、および通信キャリアを対象に、ネットワーク / コンテンツ / アプリケーション セキュリティと柔軟でスケーラブルな拡張パスを提供します。フォーティネット製品ファミリの詳細については、www.fortinet.com/products を参照してください。

作業を開始する前に

このFortiGate バージョン4.0 MR2 管理ガイドでは、FortiGate™ Webベース マネージャとFortiOSのオプションに関するシステム管理者のための詳細情報と、それらの使用方法について説明します。ここでは、使用しているモデルの『FortiGate インストール ガイド』にある指示に従ってFortiGate ユニットがすでに正常にインストールされていることを前提にしています。

この段階では、次の状態になっています。

- Web ベース マネージャまたは CLI による管理者アクセス権限を持っています。
- FortiGate ユニットはネットワークに設置されています。
- 動作モードが設定されています。
- システム時刻、DNS 設定、管理者パスワード、およびネットワーク インタフェースは設定されています。
- ファームウェア、FortiGuard アンチウイルス、および FortiGuard アンチスパムの更新は完了しています。

インストールの基本が完了すれば、このドキュメントを使用できます。このドキュメントでは、Web ベース マネージャを使用して次の操作を行う方法について説明します。

- FortiGate ユニットを保守する（バックアップを含む）
- インストール中に設定された基本的な項目を再設定する
- 高度な機能を設定する

このガイドにはまた、FortiGate のコマンド ライン インタフェース（CLI）に関する一部の情報も含まれています。ただし、すべてのコマンドは含まれていません。CLI の詳細については、『FortiGate CLI リファレンス』を参照してください。

このドキュメントは、エンド ユーザではなく、管理者を対象に作成されています。

このガイドの構成

この項では、このガイドの構成についての簡単な説明と、章ごとの概要について説明します。最初の数章では、製品を使用し始めたり、新機能を学習したりするのに役立つ概要について説明します。これらの章に続いて、このガイドでは Web ベース マネージャの機能が Web ベース マネージャ（または GUI）のメニューと同じ順序で説明され、最後には詳細な索引が付いています。

この管理ガイドでは、ある章または項が VDOM またはグローバル設定のどちらのものかを示すためにバーチャル ドメイン（VDOM）およびグローバル アイコンが表示されます。VDOM およびグローバル設定は、バーチャル ドメインを使って動作させている FortiGate ユニットにのみ適用されます。バーチャル ドメインを有効にしていない場合は、区別はありません。

このドキュメントの最新バージョンは、「フォーティネット テクニカル ドキュメント」Web サイトの「FortiGate」ページから入手できます。このドキュメントの情報は、FortiGate Web ベース マネージャのオンラインヘルプにも別の形式で記載されています。

また、FortiOS 製品の詳細については、同じ FortiGate ページだけでなく Fortinet Knowledge Base でも参照できます。

この管理ガイドは以下の章で構成されています。

- Web ベース マネージャでは、FortiGate Web ベース マネージャの機能について紹介した後、FortiGate に接続する方法について説明します。また、Web ベース マネージャ オンラインヘルプの使用方法についても説明します。

- システム ダッシュボードでは、FortiGate ユニットのダッシュボードである [System Status] ページについて説明します。シリアル番号、アップタイム、FortiGuard ライセンス情報、システム リソースの使用方法、警告メッセージ、ネットワーク統計などの、FortiGate ユニットの現在のシステム ステータスを一目でわかるように表示できます。このページからは CLI にもアクセスできます。また、ユニットのファームウェア、ホスト名、システム時刻の変更などの、ユーザが実行できるステータスの変更についても説明します。最後に、モデル番号に 50 と 60 の付いたモデルを除くすべての FortiGate モデルで使用できるトポロジ ビューアについて説明します。
- ファームウェア管理方法では、ファームウェア バージョンのアップグレードと管理について説明します。この項には、現在の設定を正しくバックアップする方法や、アップグレードが失敗した場合に実行すべきことに関する重要な情報が含まれているため、FortiGate ファームウェアをアップグレードする前にこの項を確認してください。
- バーチャル ドメインの使用では、VDOM を使用して FortiGate ユニットを複数の仮想 FortiGate ユニットとして動作させることにより、 複数のネットワークのそれぞれに個別のファイアウォールとルーティングのサービスを提供することができます。
- システム – ネットワークでは、FortiGate ユニットで物理インタフェース、仮想インタフェース、および DNS を設定する方法について説明します。
- システム – DHCP サーバでは、FortiGate インタフェースを DHCP サーバまたは DHCP リレー エージェントとして設定する方法について説明します。
- システム – 設定では、HA と仮想クラスタリングの設定、SNMP と差し替えメッセージの設定、および動作モードの変更を行うための手順について説明します。
- システム – 管理者では、管理者アカウントの追加と編集、管理者の管理者プロファイルの定義、FortiGuard Management Service または FortiManager を使用した集中管理の設定、言語、タイムアウト、Web 管理ポートなどの一般的な管理設定の定義などを行うための方法について説明します。
- システム – 証明書では、IPSec VPN や管理者認証などのさまざまな FortiGate の機能で使用される X.509 セキュリティ証明書を管理する方法について説明します。
- システム – メンテナンスでは、管理コンピュータまたは USB ディスクを使用してシステム設定をバックアップおよび復元する方法のほか、リビジョン管理を使用したり、FortiGuard サービスや FortiGuard Distribution Network (FDN) の更新を有効にしたり、バーチャル ドメインの最大数を増やすためにライセンス キーを入力したりする方法について詳しく説明します。
- ルータ – スタティックでは、スタティック ルートの定義、およびルート ポリシーの作成を行う方法について説明します。スタティック ルートを使用すると、パケットは、工場出荷時に設定されているデフォルト ゲートウェイ以外の宛先に転送されます。
- ルータ – ダイナミックでは、ルータの [Dynamic] メニューについて説明します。これには、[Dynamic] メニュー内で使用できるメニューおよび設定が含まれます。
- ルータ – モニタでは、[Routing Monitor] リストを解釈する方法について説明します。このリストには、FortiGate ルーティング テーブル内のエントリが表示されます。
- ファイアウォール ポリシーでは、FortiGate インタフェース、ゾーン、および VLAN サブインタフェースの間の接続とトラフィックを制御するためにファイアウォール ポリシーを追加する方法について説明します。この章ではまた、ネットワーク トラフィックに DoS センサを適用するために DoS ポリシーを追加する方法、および実際にパケットを受信したり、それ以外の方法で処理することなく、攻撃のパケットをスニッフィングすることによって FortiGate ユニットを不正侵入検知システム (IDS) アプライアンスとして動作させるためにスニッファ ポリシーを追加する方法についても説明します。
- ファイアウォール アドレスでは、ファイアウォール ポリシーのアドレスおよびアドレス グループを設定する方法について説明します。
- ファイアウォール サービスでは、使用可能なサービスと、ファイアウォール ポリシーのサービス グループを設定する方法について説明します。
- ファイアウォール スケジュールでは、ファイアウォール ポリシーのワンタイム スケジュールと反復スケジュールを設定する方法について説明します。

- ファイアウォール仮想 IP では、仮想 IP アドレスと IP プールを設定および使用する方法について説明します。
- ファイアウォール負荷分散では、FortiGuard 負荷分散を使用して受信トラフィックを使用可能なサーバ間で分散させる方法について説明します。
- 統合脅威管理 (UTM) では、[UTM] メニューについて説明します。これには、アンチウイルス、情報漏洩防止、および Web コンテンツ フィルタリングが含まれます。
- IPsec VPN では、[IPsec VPN] メニューについて説明します。これには、このメニューに関する情報と、このメニュー内で使用可能な設定が含まれます。
- PPTP VPN では、Web ベース マネージャを使用して、PPTP クライアントの IP アドレスの範囲を指定する方法について説明します。
- SSL VPN では、[SSL VPN] メニューについて説明した後、基本的な SSL VPN 設定に関する情報を提供します。
- ユーザでは、ユーザ認証を介してネットワーク リソースへのアクセスを制御する方法について説明します。
- WAN 最適化および Web キャッシュでは、FortiGate ユニットを使用して、ワイド エリア ネットワーク (WAN) またはインターネット上の各拠点の間を通過するトラフィックのパフォーマンスとセキュリティを向上させる方法について説明します。
- エンドポイントでは、FortiGate のエンドポイント NAC を使用して、ネットワーク内で FortiClient Endpoint Security (Enterprise Edition) を強制的に使用させる方法について説明します。
- 無線コントローラでは、FortiGate ユニットを、FortiWiFi ユニットの無線アクセス ポイント (AP) 機能を管理する無線ネットワーク コントローラとして機能するように設定する方法について説明します。
- ログおよびレポートでは、[Log&Report] メニューについて説明します。これには、レポートやロギングの情報が含まれます。

ドキュメントの規則

フォーティネット テクニカル ドキュメントでは、次に説明する規則を使用します。

IP アドレス

フォーティネットまたは他の任意の組織に属するパブリック IP アドレスの公開を防止するために、フォーティネット テクニカル ドキュメントで使用されている IP アドレスは架空のものであり、フォーティネットに固有のドキュメント ガイドラインに従っています。使用されているアドレスは、http://ietf.org/rfc/rfc1918.txt?number=1918 で入手可能な「RFC 1918: プライベート インターネットのためのアドレス割り当て」で定義されているプライベート IP アドレスの範囲に従っています。

注意、注記、およびヒント

フォーティネット テクニカル ドキュメントでは、注意、注記、およびヒントのための次のガイダンスとスタイルを使用します。

注意: データの損失や装置への損傷などの、予期しない結果または望まない結果を発生させる恐れのあるコマンドまたは手順について警告します。

注記: ショートカットなどの代替手段や、任意の設定項目などを中心として、作業ステップを進めるにあたり有用な情報を提供します。

ヒント： 設置環境の作業に合わせるためなど、有用な追加情報がハイライト表示されます。

表記規則

フォーティネットのドキュメントでは、次の表記規則を使用します。

表 1: フォーティネット テクニカル ドキュメントの表記規則

規則	例
ボタン、メニュー、テキスト ボックス、フィールド、またはチェック ボックスのラベル	*[Minimum log level]* から、*[Notification]* を選択します。

CLI の入力 *	`config system dns`
	`  set primary <address_ipv4>`
	`end`

CLI の出力	`FGT-602803030703 # get system settings`
	`comments : (null)`
	`opmode : nat`

強調	HTTP 接続はセキュリティ保護されて***いない***ため、第三者によって傍受される可能性があります。
ファイルの内容	`<HTML><HEAD><TITLE>` ファイアウォール認証 `</TITLE></HEAD>` `<BODY><H4>` このサービスを利用するには、認証を行わなければなりません。 `</H4>`
ハイパーリンク	フォーティネット テクニカル サポートWebサイト (https://support.fortinet.com) を参照してください。
キーボード入力	リモート VPN ピアまたはクライアントの名前 (`Central_Office_1` など) を入力します。
ナビゲーション	*[VPN]*、*[IPSEC]*、*[Auto Key (IKE)]* の順に選択します。
出版物	詳細については、『*FortiGate 管理ガイド*』を参照してください。 **注記：** リンクは通常、最新バージョンに移動します。以前のリリースにアクセスするには、http://docs.fortinet.com/ を参照してください。このリンクは、このドキュメントの各ページの一番下に表示されます。

* コマンド構文を表すために使用される規則については、21 ページの「CLI コマンド構文」を参照してください。

CLI コマンド構文

このガイドでは、コマンド ライン インタフェース (CLI) でコマンドを入力するときに使用する構文を説明するために次の規則を使用します。

構文の有効な置換を示すには、かっこ、中かっこ、およびパイプを使用します。`<address_ipv4>` などの制約表記は、どのデータ型または文字列パターンが入力可能な値の入力であるかを示します。

詳細については、『*FortiGateCLI リファレンス*』を参照してください。

表 2: コマンド構文

規則	説明
角かっこ `[ ]`	必須ではないワードまたはワード列。たとえば、 `[verbose {1 | 2 | 3}]` は入力を省略することができ、または `verbose` というワードとそれにつづくオプションを `verbose 3` のように入力することもできます。

表 2: コマンド構文

山かっこ < >		データ型により入力値が変わるワード。 入力を定義するために、山かっこの中には内容を示した名前のあとにアンダースコア(_)が続き、サフィックスは データ型を示します。たとえば、 `<retries_int>` は、リトライ回数を入力することを示しており、たとえば `5` のように入力します。 データ型には次のものがあります。 ・ `<xxx_name>`: 設定の別の部分を参照する名前(たとえば、`policy_A`)。 ・ `<xxx_index>`: 設定の別の部分を参照するインデックス番号(たとえば、最初のスタティック ルートを指す `0`)。 ・ `<xxx_pattern>`: 文字列のパターンに一致しうる正規表現またはワイルドカードを含むワード(たとえば、`@example.com` で終わるすべての電子メール アドレスに一致する `*@example.com`)。 ・ `<xxx_fqdn>`: 完全修飾ドメイン名 (FQDN)(たとえば、`mail.example.com`)。 ・ `<xxx_email>`: 電子メール アドレス(たとえば、`admin@mail.example.com`)。 ・ `<xxx_ipv4>`: IPv4 アドレス(たとえば、`192.168.1.99`)。 ・ `<xxx_ipv4range>`: IPv4 アドレスの範囲。 ・ `<xxx_v4mask>`: ドット区切り 10 進数の IPv4 ネットマスク(たとえば、`255.255.255.0`)。 ・ `<xxx_ipv4mask>`: スペースで区切られたドット区切り 10 進数の IPv4 アドレスとネットマスク(たとえば、`192.168.1.99 255.255.255.0`)。 ・ `<xxx_ipv4/mask>`: スラッシュで区切られたドット区切り 10 進数の IPv4 アドレスと CIDR 表記のネットマスク(たとえば、`192.168.1.99/24`)。 ・ `<xxx_ipv6>`: IPv6 アドレス。 ・ `<xxx_v6mask>`: ドット区切り 10 進数の IPv6 ネットマスク。 ・ `<xxx_ipv6mask>`: スペースで区切られたドット区切り 10 進数の IPv6 アドレスとネットマスク。 ・ `<xxx_str>`: 別のデータ型 ***ではない***文字列(たとえば、`P@ssw0rd`)。スペースまたは特殊文字を含む文字列は引用符で囲むか、またはエスケープ シーケンスを使用する必要があります。 ・ `<xxx_int>`: 別のデータ型 ***ではない***整数(たとえば、分数としての `15`)。
中かっこ { }		ワードまたはワード列を垂直バーまたはスペースにより区切られたオプションの中から選択する 1 組のオプションが角かっこ [ ] で囲まれていない限り、少なくともいずれかのオプションを入力する必要があります。
	縦棒 | で区切られたオプション	相互に排他的なオプション。たとえば、 `{enable | disable}` は、`enable` または `disable` のどちらかを入力する必要があるが、両方を入力してはいけないことを示します。

	スペースで区切られたオプション	相互に排他的ではないオプション。たとえば、
		`{http https ping snmp ssh telnet}`
		は、これらのオプションのすべてまたはサブセットを任意の順序で、スペースで区切られたリストで入力できることを示します。たとえば、次のようにします。
		`ping https ssh`
		注記: オプションを変更するには、リスト全体を入力し直す必要があります。たとえば、前の例に `snmp` を追加するには、次のように入力します。
		`ping https snmp ssh`
		このオプションがオプションの既存のリストを置き換えるのではなく、そのリストに追加されるか、そのリストから取り除かれる場合、またはそのリストがカンマで区切られている場合は、例外が注記されます。

フォーティネット製品の登録

機能の設定やカスタマイズを開始する前に、少し時間を取って、フォーティネット テクニカル サポート Web サイト (https://support.fortinet.com) でフォーティネット製品を登録してください。

ファームウェアの更新、テクニカル サポート、FortiGuard アンチウイルスやその他の FortiGuard サービスなど、多くのフォーティネット カスタマ サービスには製品登録が必要です。

詳細については、Fortinet Knowledge Base の記事「登録に関するよく寄せられる質問」を参照してください。

フォーティネット製品の使用許諾契約書

「*フォーティネット製品の使用許諾契約書*」を参照してください。

カスタマ サービスおよびテクニカル サポート

フォーティネット テクニカル サポートは、お使いのフォーティネット製品の迅速なインストール、容易な設定、およびネットワーク内での確実な動作が行えるよう、支援するサービスを提供しています。

フォーティネットが提供しているテクニカル サポート サービスの詳細については、フォーティネット テクニカル サポート Web サイト (https://support.fortinet.com) を参照してください。

設定ファイル、ネットワーク構成図、その他の具体的な情報を提供することによって、テクニカル サポート チケットの解決にかかる時間を大幅に改善できます。必要な情報のリストについては、Fortinet Knowledge Base の記事「FortiGate トラブルシューティング ガイド — テクニカル サポートの要件」を参照してください。

トレーニング

フォーティネット トレーニング サービスは、世界中の顧客およびパートナーのニーズに応えるためのさまざまなトレーニング プログラムを提供しています。フォーティネット トレーニング サービス Web サイト (http://campus.training.fortinet.com) を参照するか、または training@fortinet.com に電子メールを送信してください。

フォーティネット ドキュメント

「フォーティネット テクニカル ドキュメント」Web サイト (http://docs.fortinet.com) では、フォーティネットの出版物の最新版のほか、テクニカル ノートなどの追加のテクニカル ドキュメントを提供しています。

「フォーティネット テクニカル ドキュメント」Web サイトに加えて、フォーティネット テクニカル ドキュメントはフォーティネット ツールおよびドキュメント CD や Fortinet Knowledge Base でも入手できます。

ツールおよびドキュメント CD

お使いの製品のドキュメントは、お使いの製品に付属するフォーティネット ツールおよびドキュメント CD で入手できます。この CD に収録されているドキュメントは、製品出荷時の最新版です。フォーティネット ドキュメントの最新版については、「フォーティネット テクニカル ドキュメント」Web サイト (http://docs.fortinet.com) を参照してください。

Fortinet Knowledge Base

Fortinet Knowledge Base は、トラブルシューティングの記事やハウツー記事、例、FAQ、テクニカル ノート、用語集などのフォーティネット テクニカル ドキュメントをマニュアル以外にも提供しています。Fortinet Knowledge Base には、http://kb.fortinet.com でアクセスしてください。

フォーティネット テクニカル ドキュメントに関するコメント

このドキュメントやその他のフォーティネット テクニカル ドキュメントに誤り、または脱落がありましたら、techdoc@fortinet.com までお知らせください。

Web ベース マネージャ

この項では、FortiGate ユニットの使いやすい Web ベース マネージャ管理インタフェース (グラフィカル ユーザ インタフェースまたは GUI とも呼ばれる) の機能について説明します。

Web ブラウザを実行している任意の管理コンピュータから HTTP 接続またはセキュアな HTTPS 接続を使用して、FortiGate Web ベース マネージャに接続し、FortiGate ユニットを設定および管理できます。管理コンピュータの推奨される最小の画面解像度は 1280 × 1024 です。Web ベース マネージャによって表示される一部の情報は、最も一般的な Web ブラウザの最新バージョンでのみサポートされている機能を使用しています。これらの Web ブラウザの古いバージョンは、必ずしも Web ベース マネージャで正しく動作するとは限りません。

FortiGate ユニットは、任意の FortiGate インタフェースから HTTP 接続および HTTPS 接続の Web ベースで管理できるように設定できます。Web ベース マネージャに接続するには、FortiGate の管理者アカウントとパスワードが必要です。Web ベース マネージャは複数の言語をサポートしていますが、最初に使用するときは、デフォルトで英語で表示されます。

[System]、*[Dashboard]*、*[Status]* の順に選択すると、システム ダッシュボードに FortiGate ユニットのステータスに関する詳細情報を表示できます。ダッシュボードには、現在の FortiOS のファームウェア バージョン、アンチウイルスおよび IPS 定義のバージョン、動作モード、接続されているインタフェース、システム リソースなどの情報が表示されます。また、FortiGate ユニットが FortiAnalyzer ユニットや FortiManager ユニット、またはその他の集中管理サービスに接続されているかどうかも表示されます。

Web ベース マネージャのメニュー、リスト、および設定のページを使用して、ほとんどの FortiGate 設定を設定できます。Web ベース マネージャを使用して行われた設定変更は、FortiGate ユニットをリセットしたりサービスを中断したりしなくても、直ちに有効になります。設定はボタン バーにある [Backup Configuration] ボタンを使用して、いつでもバックアップできます。ボタン バーは、Web ベース マネージャの右上隅にあります。保存された設定は、いつでも復元できます。

Web ベース マネージャにはまた、詳細な状況依存のオンラインヘルプも含まれています。ボタン バーにある *[オンラインヘルプ]* を選択すると、現在の Web ベース マネージャ ページに関するヘルプが表示されます。

FortiGate のコマンド ライン インタフェース (CLI) を使用すると、Web ベース マネージャから設定できるのと同じ FortiGate 設定のほか、CLI のみの追加の設定を設定できます。システム ダッシュボードによって、Web ベース マネージャを終了することなく使用できる、CLI コンソールへの容易なエントリ ポイントが提供されます。

この項には以下のトピックが含まれています。

- 一般的な Web ベース マネージャ タスク
- FortiGate オンラインヘルプの使用
- Web ベース マネージャ ページ Web ベース マネージャ ページ

一般的な Web ベース マネージャ タスク

このトピックでは、次の一般的な Web ベース マネージャ タスクについて説明します。

- Web ベース マネージャへの接続
- 現在の設定の変更
- FortiGate の管理者パスワードの変更
- Web ベース マネージャの言語の変更
- FortiGate ユニットへの管理アクセスの変更
- Web ベース マネージャのアイドル タイムアウトの変更

- VDOM の切り替え
- Web ベース マネージャから FortiGate の CLI への接続
- カスタマ サポートへの接続

Web ベース マネージャへの接続

Web ベース マネージャに接続するには、次のものが必要です。

- 使用している FortiGate ユニットのクイックスタート ガイドとインストール ガイドの指示に従ってネットワークに接続された FortiGate ユニット
- 接続できる FortiGate インタフェースの IP アドレス
- FortiGate ユニットに接続できるネットワークへのイーサネット接続を備えたコンピュータ
- サポートされている Web ブラウザ。Knowledge Base の記事「*フォーティネット製品の Web ベース マネージャ (GUI) の Web ブラウザでサポートされている Microsoft Windows Web ブラウザ*」および「フォーティネット ハードウェアの Web ベース マネージャ (GUI) で使用される Mac OS ブラウザ」を参照してください。

Web ベース マネージャに接続するには

1 Web ブラウザを起動し、https:// の後に、接続できる FortiGate ユニット インタフェースの IP アドレスを付加して参照します。

たとえば、IP アドレスが 192.168.1.99 の場合は、https://192.168.1.99 を参照します。(https:// の "s" を付け忘れないでください)。

セキュアな HTTPS 認証方法をサポートするために、FortiGate ユニットには自己署名済みセキュリティ証明書が付属しています。リモート クライアントが FortiGate ユニットへの HTTPS 接続を開始すると常に、この証明書がそのリモート クライアントに提供されます。接続すると、FortiGate ユニットによって、ブラウザに 2 つのセキュリティ警告が表示されます。

最初の警告では、FortiGate ユニットの自己署名済みセキュリティ証明書を受け付け、必要に応じてインストールするよう求められます。この証明書を受け付けない場合は、FortiGate ユニットによって接続が拒否されます。この証明書を受け付けた場合は、ログイン ページが表示されます。入力された資格情報は、FortiGate ユニットに送信される前に暗号化されます。この証明書を完全に受け付けることを選択すると、今後この警告は表示されなくなります。

ログイン ページが表示される直前に、2 番目の警告によって、FortiGate 証明書の識別名が元の要求とは異なることが通知されます。この警告は、FortiGate ユニットが接続をリダイレクトするために発生します。これは情報メッセージです。*[OK]* を選択して、ログインを続行します。

2 *[Name]* フィールドに、「admin」または設定されている管理者の名前を入力します。

3 *[Password]* フィールドに、管理者アカウントのパスワードを入力します。

4 *[Login]* を選択します。

現在の設定の変更

現在の設定を変更する場合 (管理者のパスワードの変更など) は、項目を強調表示してから、該当するアイコンを選択する必要があります。使用可能なアイコンにはすべて、これ以外の方法ではアクセスできないためです。アイコンにアクセスするためのこの方法を、次の手順で説明します。現在の設定を変更する場合は常に、26 ページの「リスト内の項目を変更するためのアイコンにアクセスするには」の手順を使用します。

リスト内の項目を変更するためのアイコンにアクセスするには

1 [Check box] カラムの、変更する設定の行内で、チェック ボックスを選択してこの行を強調表示します。

グレーになっていたアイコンがアクセス可能になります。ページによっては、行を強調表示したときに、一部のアイコンがアクセス可能にならないことがあります。

2 1 つまたは複数のアイコンがアクセス可能になったら、変更を行うために使用するアイコン（[編集] アイコンなど ）を選択します。

変更を行い、ページ上のリストに戻ると、チェック ボックスの選択および行の強調表示は解除されています。

FortiGate の管理者パスワードの変更

デフォルトでは、admin 管理者アカウントを使用し、パスワードを入力することなく Web ベース マネージャにログインできます。誰かに FortiGate にログインされ、設定オプションを変更されることがないように、admin 管理者アカウントにパスワードを追加する必要があります。セキュリティを強化するために、admin 管理者アカウントのパスワードや、後で追加するその他の任意の管理者アカウントのパスワードを定期的に変更してください。

管理者のパスワードを変更するには、*[System]*、*[Admin]*、*[Administrators]* の順に選択し、*[編集]* アイコンへのアクセスを有効にしてからパスワードを変更します。*[OK]* を選択して、新しいパスワードを保存します。

また、*[Create New]* を選択することによって新しい管理者アカウントを追加することもできます。管理者の追加、管理者アカウントのパスワードの変更、および関連する設定の詳細については、169 ページの「システム – 管理者」を参照してください。

注記：管理者アカウントのパスワードを忘れたか、または失うかして FortiGate ユニットにログインできない場合は、Fortinet Knowledge Base の記事「失われた FortiGate 管理者アカウントのパスワードの復旧」を参照してください。

Web ベース マネージャの言語の変更

Web ベース マネージャに表示する言語を、英語、簡体字中国語、日本語、韓国語、スペイン語、繁体字中国語、フランス語のいずれかに変更できます。最適な結果を得るには、管理コンピュータのオペレーティング システムで使用されている言語を選択する必要があります。

言語を変更するには、*[System]*、*[Admin]*、*[Settings]* の順に選択し、*[Display Settings]* で *[Language]* ドロップダウン リストから目的の言語を選択して、*[Apply]* を選択します。Web ベース マネージャ ページに、選択された言語が表示されます。

FortiGate ユニットへの管理アクセスの変更

管理者は、管理アクセスを使用することにより、FortiGate ユニットに接続して設定を表示したり変更したりできます。FortiGate ユニットのデフォルト設定では、FortiGate ユニットのクイックスタート ガイドとインストール ガイドで説明されている、そのユニットの 1 つ以上のインタフェースへの管理アクセスが許可されます。

管理アクセスは、次の操作によって変更できます。

- いずれかの FortiGate インタフェースからの管理アクセスを有効または無効にする
- Web ベース マネージャへの HTTPS 管理アクセスのセキュリティ保護を有効または無効にする (推奨される)
- Web ベース マネージャへの HTTP 管理アクセスを有効または無効にする (推奨されない)
- CLI へのセキュアな SSH 管理アクセスを有効または無効にする (推奨される)
- CLI への SSH または Telnet 管理アクセスを有効または無効にする (推奨されない)

管理アクセスを変更するには、*[System]*、*[Network]*、*[Interface]* の順に選択して *[編集]* アイコンにアクセスし、そのインタフェースの 1 つ以上の管理アクセスの種類を選択します。*[OK]* を選択して、変更を保存します。

管理アクセスの変更の詳細については、101 ページの「インタフェースへの管理アクセスの設定」を参照してください。

Web ベース マネージャのアイドル タイムアウトの変更

デフォルトでは、管理セッションの動作していない時間が 5 分続くと、Web ベース マネージャはその管理セッションを接続解除します。このアイドル タイムアウトは、Web ベース マネージャにログインしたまま無人の状態になっている PC から Web ベース マネージャが誰かに使用されないようにするために推奨されます。ただし、このアイドル タイムアウトは、次の手順を使用して変更できます。

アイドル タイムアウトを変更するには、*[System]*、*[Admin]*、*[Settings]* の順に選択し、*[Idle Timeout]* で分単位の時間を入力してから、*[Apply]* を選択して変更を保存します。

VDOM の切り替え

VDOM が有効になっている場合は、左のカラムに [Current VDOM] という名前のメニューが表示されます。このメニューの横には、ドロップダウン リストが表示されます。このドロップダウン リストには、その FortiGate ユニット上で設定されているすべての VDOM が含まれています。これによって、VDOM に簡単に、すばやくアクセスできるようになっています。

[Current VDOM] メニューを使用してある VDOM に切り替えるには、*[Current VDOM]* の横にあるドロップダウン リストから、切り替え先の VDOM を選択します。その VDOM に自動的にリダイレクトされます。

Web ベース マネージャから FortiGate の CLI への接続

[CLI Console] ウィジェットを使用して、Web ベース マネージャのダッシュボードから FortiGate の CLI に接続できます。CLI を使用すると、Web ベース マネージャから使用可能なすべての設定オプションを設定できます。一部の設定オプションは、CLI からのみ使用できます。また CLI を使用すると、診断コマンドを入力したり、Web ベース マネージャからは使用できないその他の高度な操作を実行したりすることもできます。FortiGate の CLI の詳細については、『*FortiGateCLI リファレンス*』を参照してください。

CLI コンソールに接続するには、*[System]*、*[Dashboard]*、*[Status]* の順に選択し、[CLI Console] ウィジェットのウィンドウの内部を選択します。CLI に自動的にログインされます。詳細については、50 ページの「[CLI Console]」を参照してください。

カスタマ サポートへの接続

[カスタマ サポートへの接続] ボタンを押すと、新しいブラウザ ウィンドウが開いて「Fortinet Support」Web ページが表示されます。このページからは、次の操作を行うことができます。

- Fortinet Knowledge Base にアクセスする
- カスタマ サポートにログインする (Support Login)
- フォーティネット製品を登録する (Product Registration)
- フォーティネットの Product End of Life を表示する
- Fortinet Training and Certification について検索する
- FortiGuard Center にアクセスする。

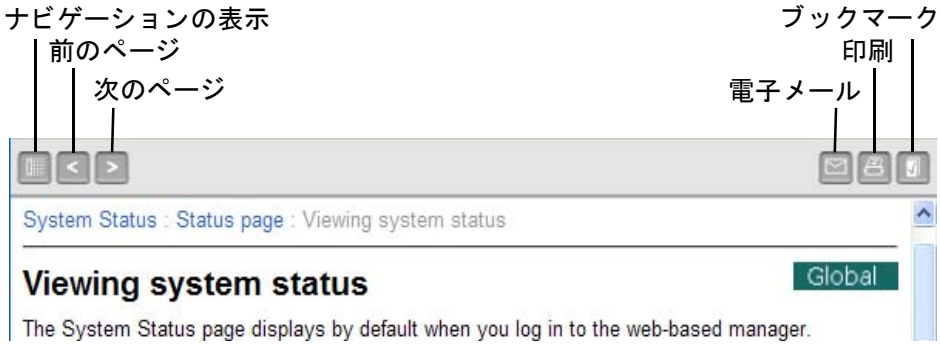
製品の更新、テクニカル サポート、および FortiGuard サービスを受けるには、フォーティネット製品を登録する必要があります。フォーティネット製品を登録するには、「Product Registration」にアクセスしてその指示に従います。

FortiGate オンラインヘルプの使用

[オンラインヘルプ] ボタンを押すと、現在の Web ベース マネージャ ページに関する状況依存のオンラインヘルプが表示されます。表示されるオンラインヘルプ ページはコンテンツ ウィンドウと呼ばれ、現在の Web ベース マネージャ ページに関連した情報と手順が含まれています。また、ほとんどのヘルプ ページには、関連するトピックへのハイパーリンクも含まれています。オンラインヘルプ システムには、追加情報の検索に使用できるリンクもいくつか含まれています。

FortiGate の状況依存のオンラインヘルプ トピックには、Web ベース マネージャ ページが VDOM 固有の設定またはグローバル設定のどちら用かを示す [VDOM] または [Global] アイコンも含まれています。VDOM およびグローバル設定は、バーチャル ドメインが有効な状態で動作している FortiGate ユニットにのみ適用されます。FortiGate ユニットをバーチャル ドメインが無効な状態で動作させている場合は、[VDOM] および [Global] アイコンを無視できます。バーチャル ドメインの詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

図 1: 状況依存のオンラインヘルプ ページ (コンテンツ ウィンドウのみ)



[ナビゲーションの表示]	オンラインヘルプ ナビゲーション ウィンドウを開きます。ナビゲーション ウィンドウから、オンラインヘルプの目次、索引、および検索を使用して、オンラインヘルプ内のすべての情報にアクセスできます。オンラインヘルプは、FortiGateWeb ベース マネージャおよび『*FortiGate 管理ガイド*』と同じように構成されています。
[前のページ]	オンラインヘルプ内の前のページを表示します。
[次のページ]	オンラインヘルプ内の次のページを表示します。
[電子メール]	オンラインヘルプをはじめ任意のフォーティネット テクニカル ドキュメント製品に関するコメントまたは修正項目がある場合は、Fortinet Technical Documentation (techdoc@fortinet.com) に電子メールを送信します。
[印刷]	現在のオンラインヘルプ ページを印刷します。
[ブックマーク]	役立つオンラインヘルプ ページを見つけやすくするために、このオンラインヘルプ ページのエントリをブラウザのブックマークまたはお気に入りリストに追加します。すべてのブラウザでサポートされているわけではありません。

オンラインヘルプの目次または索引を表示したり、検索機能を使用したりするには、Web ベース マネージャの右上隅のボタン バーにある [オンラインヘルプ] を選択します。オンラインヘルプから、[ナビゲーションの表示] を選択します。

図 2: ナビゲーション ウィンドウとコンテンツ ウィンドウを含むオンラインヘルプ ページ

[Contents]	オンラインヘルプの目次を表示します。目次内を移動して、オンラインヘルプ内の情報を検索できます。オンラインヘルプは、FortiGateWeb ベースマネージャおよび『*FortiGate 管理ガイド*』と同じように構成されています。『FortiOS 管理ガイド』。
[Index]	オンラインヘルプの索引を表示します。索引を使用して、オンラインヘルプ内の情報を検索できます。
[Search]	オンラインヘルプの検索を表示します。詳細については、30 ページの「オンラインヘルプの検索」を参照してください。
[目次の表示]	索引、検索、またはハイパーリンクを使用してオンラインヘルプ内の情報を検索した場合、目次が表示されないか、または目次と現在のヘルプ ページの同期がとれていない可能性があります。[目次の表示] を選択すると、目次内の現在のヘルプ ページの場所を表示できます。

オンラインヘルプの検索

オンラインヘルプの検索を使用して、FortiGate オンラインヘルプ システムのテキスト全体の中から 1 つの単語または複数の単語を検索できます。次の点に注意してください。

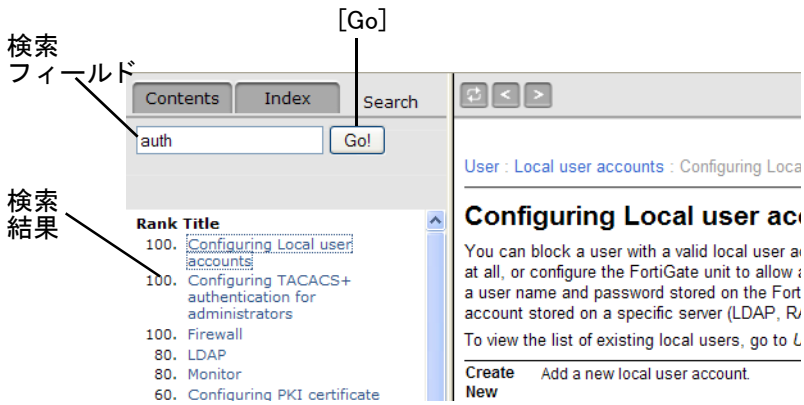
- 複数の単語を検索すると、入力したすべての単語を含むヘルプ ページのみが検索されます。入力した単語のいずれかだけを含むヘルプ ページは検索されません。
- 検索で見つかったヘルプ ページは、関連性の順番にランク付けされます。ランク付けが高ければ高いほど、そのヘルプ ページに検索対象の 1 つまたは複数の単語に関する有用な情報や詳細な情報が含まれている可能性が高くなります。ヘルプ ページのタイトルに検索単語が含まれているヘルプ ページには、最も高いランクが付けられます。
- 検索のワイルドカード文字としてアスタリスク (*) を使用して、任意の数の文字を置き換えることができます。たとえば、**auth*** を検索すると、**auth**、**authenticate**、**authentication**、**authenticates** などを含むヘルプ ページが検索されます。
- 場合によっては、検索で完全一致しか見つからないことがあります。たとえば、**windows** を検索した場合は、**window** という単語を含むページが検索されない可能性があります。ワイルドカード * を使用すれば (たとえば、**window*** を検索する)、この事態を回避できます。

オンラインヘルプ システム内を検索するには

1 任意の Web ベース マネージャ ページから、オンラインヘルプ ボタンを選択します。
2 *[ナビゲーションの表示]* を選択します。
3 *[Search]* を選択します。
4 検索フィールドに検索対象の 1 つ以上の単語を入力してから、キーボード上の *Enter* キーを押すか、または *[Go]* を選択します。

検索結果ウィンドウに、入力したすべての単語を含むすべてのオンラインヘルプ ページの名前が表示されます。リストから名前を選択して、そのヘルプ ページを表示します。

図 3: オンラインヘルプ システムの検索



キーボードを使用したオンラインヘルプ内の移動

表 3 のキーボード ショートカットを使用して、オンラインヘルプ内の情報を表示したり、検索したりすることができます。

表 3: オンラインヘルプ ナビゲーション キー

キー	機能
Alt+1	目次を表示します。
Alt+2	索引を表示します。
Alt+3	[検索] タブを表示します。
Alt+4	前のページに移動します。
Alt+5	次のページに移動します。
Alt+7	オンラインヘルプをはじめ任意のフォーティネット テクニカル ドキュメント製品に関するコメントまたは修正項目がある場合は、Fortinet Technical Documentation (techdoc@fortinet.com) に電子メールを送信します。
Alt+8	現在のオンラインヘルプ ページを印刷します。
Alt+9	役立つオンラインヘルプ ページを見つけやすくするために、このオンラインヘルプ ページのエントリをブラウザのブックマークまたはお気に入りリストに追加します。

Web ベース マネージャ ページ

Web ベース マネージャのインタフェースは、メニューとページで構成されています。ページの多くには、複数のタブが含まれています。メニュー項目 (*[System]* など) を選択すると、Web ベース マネージャが展開されて、そのメイン メニューに関連付けられたサブ メニューが表示されます。別のサブ メニューを表示するには、そのタブを選択します。

このマニュアルの手順では、たとえば、次のようにメニュー項目、サブ メニュー項目、およびタブを指定することによってページが表示されます。

1 *[System]*、*[Network]*、*[Interface]* の順に選択します。

このトピックには、以下の内容が含まれています。

- Web ベース マネージャ メニューの使用
- Web ベース マネージャ リストの使用
- Web ベース マネージャ リストに対するページ コントロールの使用
- 表示されるカラムのカラム設定を使用した制御
- カラム設定と組み合わせたフィルタの使用

Web ベース マネージャ メニューの使用

Web ベース マネージャ メニューを使用すると、すべての主要な FortiGate 機能のための設定オプションにアクセスできます (31 ページの図を参照)。

[システム]	ネットワーク インタフェース、バーチャル ドメイン、DHCP サービス、管理者、証明書、高可用性 (HA)、システム時刻などのシステム設定を設定したり、システム オプションを設定したりします。
[ルータ]	FortiGate のスタティック ルーティングやダイナミック ルーティングを設定したり、ルータ モニタを表示したりします。
[ファイアウォール]	ネットワーク保護機能に適用されるファイアウォール ポリシーやプロテクション プロファイルを設定します。また、仮想 IP アドレスや IP プールも設定します。
[UTM]	アンチウイルス保護やアンチスパム保護、Web フィルタリング、不正侵入防御、情報漏洩防止、およびアプリケーション制御を設定します。

[VPN]	IPSec と SSL の仮想プライベート ネットワークを設定します。PPTP は CLI で設定されます。
[ユーザ]	ユーザ認証が必要なファイアウォール ポリシーで使用するユーザ アカウントを設定します。また、RADIUS、LDAP、TACACS+、Windows AD などの外部の認証サーバも設定します。ファイアウォール、IPSec、SSL、IM、および禁止ユーザの監視を設定します。
[エンドポイント]	エンドポイントを設定したり、FortiClient の設定情報を表示したり、ソフトウェアの検出パターンを設定したりします。
[WAN 最適化 & キャッシュ]	ワイド エリア ネットワーク (WAN) 上の拠点の間を通過するトラフィックや、インターネットから Web サーバへのトラフィックのパフォーマンスとセキュリティを向上させるために、WAN 最適化と Web キャッシュを設定します。
[ワイアレス コントローラ]	FortiGate ユニットを、FortiWiFi ユニットの無線アクセス ポイント (AP) 機能を管理する無線ネットワーク コントローラとして機能するように設定します。
[ログ & レポート]	ロギングやアラート メールを設定します。ログ メッセージやログ レポートを表示します。
[現在の VDOM]	FortiGate ユニットで VDOM が有効になっている場合にのみ表示されます。VDOM 間をすばやく切り替えることができます。VDOM 間を切り替えるには、[現在の VDOM] の横にあるドロップダウン リストから VDOM を選択します。

Web ベース マネージャ リストの使用

Web ベース マネージャ ページの多くには、リストが含まれています。ネットワーク インタフェース、ファイアウォール ポリシー、管理者、ユーザなどのリストがあります。

リストへの読み取り / 書き込みアクセスを許可する管理者プロファイルを持つ管理者としてログインした場合は、そのリストに応じて、通常は次のことが可能になります。

- [Create New] を選択して、リストに新しい項目を追加する。
- ページ上のリスト内の項目の設定を修正または変更する。
- リストから項目を削除する。その項目を削除できない場合は、[削除] アイコンが使用可能になりません。項目は通常、別の設定に追加されている場合は削除できません。まず項目が追加されている設定を見つけ、その設定から項目を削除する必要があります (図 を参照)。

リストへの読み取り専用アクセスを許可する管理者プロファイルを持つ管理者としてログインした場合は、そのリスト上の項目を表示することだけが可能になります (図 を参照)。

詳細については、179 ページの「管理者プロファイル」を参照してください。

Web ベース マネージャ リストへのフィルタの追加

Web ベース マネージャで複雑なリストに表示される情報を制御するためのフィルタを追加できます。フィルタを含むリストの例については、次の Web ベース マネージャ ページを参照してください。

- セッション リスト (51 ページの「現在のセッション リストの表示」を参照)
- ファイアウォール ポリシーおよび IPv6 ポリシー リスト (267 ページの「ファイアウォール ポリシー リストの表示」、278 ページの「DoS ポリシー リストの表示」、および 282 ページの「スニファ ポリシー リストの表示」を参照)
- ファイアウォール ユーザ監視リスト (464 ページの「ファイアウォール ユーザ モニタ リスト」を参照)
- IPSec VPN モニタ (422 ページの「VPN のモニタ」を参照)
- 既知のエンドポイントのエンドポイント NAC リスト (475 ページの「エンドポイントの監視」を参照)
- ログとレポート ログ アクセス リスト (496 ページの「ログ メッセージへのアクセスおよび表示」を参照)

フィルタは、自分にとって重要な情報に焦点を絞ることができるように、リストに表示されるエントリの数を削減するために有効です。

たとえば、*[System]*、*[Dashboard]*、*[Status]* の順に選択し、*[Statistics]* セクションで *[Sessions]* 行の *[Details]* を選択すると、FortiGate ユニットが現在処理している通信セッションを表示できます。使用頻度の高い FortiGate ユニットは、数百 ～ 数千の通信セッションを処理している可能性があります。特定のセッションを見つけやすくするためのフィルタを追加できます。たとえば、特定のファイアウォール ポリシーによって許可されているすべての通信セッションを探しているとします。特定のポリシー ID またはポリシー ID の範囲に対応するセッションのみを表示するためのポリシー ID フィルタを追加できます。

Web ベース マネージャ リストにフィルタを追加するには、任意のフィルタ アイコンを選択して *[Edit Filters]* ウィンドウを表示します。*[Edit Filters]* ウィンドウから、フィルタ処理する任意のカラム名を選択し、そのカラムに対してフィルタを設定できます。また、1 つ以上のカラムに対するフィルタを一度に追加することもできます。フィルタ アイコンは、フィルタ処理されていないカラムでは灰色のままになり、フィルタ処理されたカラムでは緑色に変化します。

個々のカラムに表示される情報の種類に応じて、異なるフィルタのスタイルを使用できます。いずれの場合も、フィルタ処理する対象と、フィルタに一致する情報を表示するかどうかを指定するか、またはフィルタに一致しない情報を表示しないことを選択することによってフィルタを設定します。

ファイアウォール ポリシー、IPv6 ポリシー、定義済みシグネチャ、およびログとレポート ログ アクセス リストでは、フィルタをカラム設定と組み合わせることにより、リストで表示される情報をさらにきめ細かく制御できます。詳細については、35 ページの「カラム設定と組み合わせたフィルタの使用」を参照してください。

注記：フィルタの設定は FortiGate の設定に格納され、次回、フィルタを追加したいずれかのリストにアクセスしたときにも保持されます。

数値を含むカラムに対するフィルタ

カラムに数値（たとえば、IP アドレス、ファイアウォール ポリシー ID、ポート番号）が含まれている場合は、1 つの数値または数値の範囲でフィルタ処理できます。たとえば、発信元アドレスのカラムを、1 つの IP アドレスまたはアドレスの範囲内のすべてのアドレスに対するエントリのみを表示するように設定できます。範囲を指定するには、範囲の一番上と一番下の値をハイフンで区切ります（たとえば、25-50）。

テキスト文字列を含むカラムに対するフィルタ

カラムにテキスト文字列（たとえば、名前やログ メッセージ）が含まれている場合は、テキスト文字列でフィルタ処理できます。また、テキスト文字列と正確に一致する（等しい）情報、テキスト文字列を含む情報、またはテキスト文字列に等しくないか、テキスト文字列を含まない情報をフィルタ処理することもできます。さらに、テキスト文字列の大文字 / 小文字に一致するかどうかも指定できます。

テキスト文字列は空白にすることも、非常に長くすることもできます。また、テキスト文字列に <、&、> などの特殊文字を含めることもできます。ただし、フィルタ処理では、< の後にスペースがない限り、< に続く文字を無視します（たとえば、`<string` を無視しますが、`< string` は無視しません）。フィルタ処理ではまた、一致した開始と終了の < と > の文字と、その内部にあるすべての文字も無視します（たとえば、`<string>` を無視しますが、`>string>` は無視しません）。

特定の項目のみを含むことができるカラムに対するフィルタ

特定の項目（たとえば、ログ メッセージの重大度や定義済みシグネチャのアクション）のみを含むことができるカラムの場合は、リストから 1 つの項目を選択できます。この場合は、選択された 1 つの項目に対してのみフィルタ処理できます。

カスタム フィルタ

その他のカスタム フィルタも使用できます。日付の範囲や時間の範囲に従って、ログ メッセージをフィルタ処理できます。また、複数の重大度レベルを持つログ メッセージを表示するためのレベル フィルタを設定することもできます。

Web ベース マネージャ リストに対するページ コントロールの使用

Web ベース マネージャには、標準的なブラウザ ウィンドウに表示できるより多くの項目を含むリストを容易に表示できるようにするためのページ コントロールが含まれています。ページ コントロールを含む Web ベース マネージャ ページには、次のものがあります。

- セッション リスト（51 ページの「現在のセッション リストの表示」を参照）
- ルータ モニタ（261 ページの「ルータ - モニタ」を参照）
- ファイアウォール ユーザ監視リスト（464 ページの「ファイアウォール ユーザ モニタ リスト」を参照）
- IPSec VPN モニタ（422 ページの「VPN のモニタ」を参照）
- 禁止ユーザ リスト（466 ページの「NAC 隔離および禁止ユーザ リスト」を参照）
- ログとレポート ログ アクセス リスト（496 ページの「ログ メッセージへのアクセスおよび表示」を参照）
- 既知のエンドポイントのエンドポイント NAC リスト（475 ページの「エンドポイントの監視」を参照）

[最初のページ]	リスト内の項目の最初のページを表示します。
[前ページ]	リスト内の項目の前のページを表示します。
[現在のページ]	表示されているリスト項目の現在のページ番号。ページ番号を入力して Enter キーを押すと、そのページにある項目を表示できます。たとえば、5 ページ分の項目があるときに「3」を入力すると、項目の 3 ページ目が表示されます。
[総ページ数]	表示できるリスト項目のページ数。
[次ページ]	リスト内の項目の次のページを表示します。
[最後のページ]	リスト内の項目の最後のページを表示します。

表示されるカラムのカラム設定を使用した制御

カラム設定を使用すると、一部の Web ベース マネージャ リストを、自分にとって重要な情報が見つけやすくなり、重要性の低い情報が表示されないか、または目立たなくなるようにフォーマットできます。

複雑なリストを含む Web ベース マネージャ ページでは、カラム設定を変更することにより、そのリストのために表示される情報カラムを制御したり、それらの情報カラムが表示される順序を制御したりすることができます。カラム設定で制御できる Web ベース マネージャ ページには、次のものがあります。

- ネットワーク インタフェース リスト（89 ページの「インタフェースの設定」を参照）
- ファイアウォール ポリシーおよび IPv6 ポリシー（267 ページの「ファイアウォール ポリシー リストの表示」を参照）
- ファイアウォール ユーザ監視リスト（464 ページの「ファイアウォール ユーザ モニタ リスト」を参照）
- IPSec VPN モニタ（422 ページの「VPN のモニタ」を参照）
- 既知のエンドポイントのエンドポイント NAC リスト（475 ページの「エンドポイントの監視」を参照）
- ログとレポート ログ アクセス リスト（496 ページの「ログ メッセージへのアクセスおよび表示」を参照）

注記： リストのカラム設定に対して行った変更はすべて FortiGate の設定に格納され、次回、このリストにアクセスしたときに表示されます。

カラム設定をサポートしているリストでカラム設定を変更するには、*[Column Settings]* を選択します。*[Available fields]* から、表示されるカラム見出しを選択した後、右矢印を選択してそれらのカラム見出しを [Show these fields in this order] リストに移動します。同様に、カラム見出しを非表示にするには、左矢印を使用してそれらのカラム見出しを *[Available fields]* リストに戻します。カラムが表示される順序を変更するには、*[Move Up]* と *[Move Down]* を使用します。

たとえば、インタフェース リストのカラム見出しを、各インタフェースの [*IP/Netmask*]、*[MAC]* アドレス、*[MTU]*、およびインタフェースの *[Type]* のみが表示されるように変更できます。

カラム設定と組み合わせたフィルタの使用

ファイアウォール ポリシー、IPv6 ポリシー、定義済みシグネチャ、ファイアウォール ユーザ監視、IPSec モニタ、およびログとレポート ログ アクセス リストでは、フィルタをカラム設定と組み合わせることにより、リストで表示される情報をさらにきめ細かく制御できます。

たとえば、*[Intrusion Protection]*、*[Signature]*、*[Predefined]* の順に選択して、不正侵入防御の定義済みシグネチャ リストを、選択されたアプリケーションの脆弱性から保護するシグネチャの名前のみが表示されるように設定できます。これを行うには、*[Column Settings]* を設定して *[Applications]* と *[Name]* のみが表示されるようにします。次に、選択されたアプリケーションのみが表示されるように *[Applications]* にフィルタを適用します。また、定義済みシグネチャ リストでは、異なるカラムでリストを並べ替えることもできます。各アプリケーションのすべてのシグネチャが一緒にグループ化されるように、アプリケーションごとにリストを並べ替えることができます。

詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。

システム ダッシュボード

この項では、システム ダッシュボードと、そのページである [Status] および [Usage] について説明します。シリアル番号、アップタイム、FortiGuard ライセンス情報、システム リソースの使用方法、警告メッセージ、ネットワーク統計などの、FortiGate ユニットの現在のシステム ステータスを一目でわかるように表示できます。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にした場合は、ステータス ページがグローバルに使用可能になり、システム ステータス設定は FortiGate ユニット全体に対してグローバルに設定されます。VDOM が有効になっている場合は、トポロジ ビューアは使用できません。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には、以下のトピックが含まれています。

注記： [System Dashboard] ページを表示するには、ブラウザで Java スクリプトがサポートされている必要があります。

FortiOS 4.0 MR2 には、トポロジ ビューアが含まれていません。FortiOS 4.0 MR2 にアップグレードすると、トポロジ ビューアの設定はすべて失われます。

ダッシュボードの概要

[Dashboard] メニューを使用すると、ダッシュボードを追加したり、カスタマイズしたりできます。ダッシュボードは、複数のウィジェットからの（トラフィック活動などの）情報を表示するために使用できるメニューです。これらの情報は有効であり、ファームウェアを更新したり、FortiGate ユニットを再起動したり、ログとアーカイブの統計をすばやく表示したりする場合に役立ちます。

ダッシュボードを追加したりカスタマイズしたりして、特定のダッシュボードに特定の情報（ログ情報など）が含まれるようにすると、該当するダッシュボードに直接移動してその特定の情報を表示できるようになります。たとえば、アーカイブ ダッシュボード（[Dashboard]、[Archives] の順に選択）には [DLP Archive Usage] および [Log and Archive Statistics] ウィジェットが含まれているため、ユーザはログ アーカイブ情報のみを表示できます。

どちらかのメニューが表示されているときにウィジェットをカスタマイズまたは追加する場合、管理者には読み取りおよび書き込み特権が必要です。[Status] や [Usage] で情報を表示する場合、管理者には読み取り特権が必要です。管理者およびそのプロファイルの詳細については、179 ページの「管理者プロファイル」を参照してください。

このトピックには、以下の内容が含まれています。

ダッシュボードの追加

ダッシュボードは最初、デフォルト メニューである [Status] および [Usage] から追加されます。[Status] または [Usage] のどちらのメニューが表示されている場合も、ダッシュボードの追加、削除、または名前変更を行うことができます。[Reset Dashboards] を選択することによって、[Dashboard] メニューをデフォルト設定にリセットできます。

[Dashboard] メニューにダッシュボードを追加するには

1 *[Dashboard]*、*[Status]* の順に選択します。

2 *[ダッシュボード]* アイコンを選択します。

3 次のオプションを含むドロップダウン リストが表示されます。

[Add Dashboard]	[Dashboard] メニューに新しいダッシュボードを追加します。
[Rename Dashboard]	現在のダッシュボードの名前を変更します。既存のデフォルト メニューである [Status] および [Usage] の名前を変更できます。
[Delete Dashboard]	表示されている現在のダッシュボードを削除します。
[Reset Dashboards]	[Dashboard] メニュー全体を、元のデフォルト設定にリセットします。

4 *[Add Dashboard]* を選択します。

5 *[Add Dashboard]* ウィンドウの *[Name]* フィールドに、ダッシュボードの名前を入力します。

6 *[OK]* を選択します

新しいダッシュボードに自動的にリダイレクトされます。ダッシュボードへのウィジェットの追加を開始できます。

ダッシュボードへのウィジェットの追加

[Dashboard] メニューにダッシュボードを追加した後は、そのダッシュボードに複数のウィジェットを追加できます。ほとんどのウィジェットは特定の情報を表示するようにカスタマイズ可能であり、さらに一部のウィジェットではより詳細な情報を表示できます。

ダッシュボードにウィジェットを追加するには、*[ウィジェット]* アイコンを選択してから、[Click active module name to add module to the page] ウィンドウでウィジェットを選択します。

ウィジェットのカスタマイズに使用可能なウィジェットの設定	
[Widget Title]	表示の名前を示します。
[Open/Close arrow]	表示を開くか、または閉じる場合に選択します。
[History]	展開された一連のデータを表示する場合に選択します。 すべてのウィジェットで使用できるわけではありません。
[Edit]	表示の設定を変更する場合に選択します。
[Refresh]	表示されている情報を更新する場合に選択します。
[Close]	表示を閉じる場合に選択します。操作を確認するよう求められます。

注記：[Status] に表示される情報は、プライマリ ユニットだけでなく HA クラスタ全体に適用されます。これには、アクセスされた URL、送受信された電子メール、捕捉されたウイルスなどの情報が含まれます。

VDOM ダッシュボードとグローバル ダッシュボード

VDOM 管理者は、自分の VDOM のための VDOM 固有のダッシュボードを表示したり設定したりできます。VDOM ダッシュボードを表示するには、VDOM から *[System]*、*[Dashboard]*、*[Status]* の順に選択します。VDOM ダッシュボードでは、[System Information]、[Unit Operation]、[System Resources]、[Log and Archive Statistics]、[CLI Console]、[Top Sessions]、および [Traffic History] ダッシュボード ウィジェットが使用可能です。

これらの使用可能なウィジェットは、グローバル ダッシュボードの同じウィジェットとは次のように異なります。

[System Information]	バーチャル ドメインを有効または無効にすることができません。現在の管理者の一覧がありません。
[CLI Console]	ユーザは現在の VDOM にログインしているため、グローバル設定にはアクセスできません。
[Unit Operation]	ユニットの再起動とシャットダウンが使用できません。 管理サービスまたは FortiAnalyzer ユニットを設定できません。 ネットワーク ポートに関する情報がありません。
[Top Sessions]	この VDOM のセッションのみを表示します。
[Traffic History]	この VDOM に属するインタフェースまたは VLAN しか選択できません。

super_admin 管理者プロファイルを持つグローバル管理者は、グローバル ダッシュボードしか表示できません。

[System Information]

[System Information] を見つけるには、*[System]*、*[Dashboard]*、*[Status]* の順に選択します。

ダッシュボードに [System Information] ウィジェットを追加するには、*[System]*、*[Dashboard]*、*[Status]* の順に選択し、*[Add Content]* を選択して、リストから *[System Information]* を選択します。

[Serial Number]	FortiGate ユニットのシリアル番号。このシリアル番号は FortiGate ユニットに固有であり、ファームウェアをアップグレードしても変わりません。
[Uptime]	FortiGate ユニットが起動されてからの時間を、日数、時間数、および分数で表したもの。
[System Time]	FortiGate ユニットの内部クロックに基づく現在の日付と時刻。 この時間を変更するか、または FortiGate ユニットが NTP サーバから時間を取得するように設定するには、*[Change]* を選択します。詳細については、41 ページの「システム時刻の設定」を参照してください。

[HA Status]	このユニットの高可用性のステータス。 [Standalone] は、このユニットが HA モードで動作していないことを示します。 [Active-Passive] または [Active-Active] は、このユニットが HA モードで動作していることを示します。 このユニットの HA ステータスを設定するには、[Configure] を選択します。詳細については、137 ページの「HA」を参照してください。
[Host Name]	現在の FortiGate ユニットのホスト名。 ホスト名を変更するには、*[Change]* を選択します。 詳細については、41 ページの「FortiGate ユニットのホスト名の変更」を参照してください。 FortiGate ユニットが HA モードに設定されている場合、このフィールドは表示されません。
[Cluster Name]	この FortiGate ユニットの HA クラスタの名前。詳細については、137 ページの「HA」を参照してください。 このフィールドを表示するには、FortiGate ユニットが HA モードで動作している必要があります。
[Cluster Members]	HA クラスタ内の FortiGate ユニット。各メンバに関して、ホスト名、シリアル番号、そのユニットがクラスタ内の上位（マスタ）ユニットまたは下位（スレーブ）ユニットのどちらであるかといった情報が表示されます。詳細については、137 ページの「HA」を参照してください。 このフィールドを表示するには、FortiGate ユニットが、バーチャル ドメインが無効になっている HA モードで動作している必要があります。
[Virtual Cluster 1] **[Virtual Cluster 2]**	仮想クラスタ 1 および仮想クラスタ 2 内の各 FortiGate ユニットの役割。詳細については、137 ページの「HA」を参照してください。 これらのフィールドを表示するには、FortiGate ユニットが、バーチャル ドメインが有効になっている HA モードで動作している必要があります。
[Firmware Version]	FortiGateユニットにインストールされている現在のファームウェアのバージョン。ファームウェア バージョンの形式は ファームウェアを変更するには、*[Update]* を選択します。 詳細については、42 ページの「FortiGate の変更」を参照してください。
[System Configuration]	設定ファイルがバックアップされた期間。[Backup] を選択して、現在の設定をバックアップすることができます。[Backup] を選択すると、[Backup] ページに自動的にリダイレクトされます。設定ファイルを復元する場合は、[Restore] を選択します。[Restore] を選択すると、[Restore] ページに自動的にリダイレクトされます。
[FortiClient Version]	エンドポイント制御に使用されている FortiGate ユニットにアップロードされる FortiClient の現在のバージョン。このフィールドは、FortiClient のイメージを FortiGate ユニットにアップロードできる場合に表示されます。詳細については、473 ページの「FortiClient インストーラ ダウンロードおよび必須バージョンの設定」を参照してください。
[Operation Mode]	現在の FortiGate ユニットの動作モード。FortiGate ユニットは、NAT モードまたはトランスペアレント モードで動作できます。NAT モードとトランスペアレント モードとを切り替えるには、*[Change]* を選択します。詳細については、166 ページの「動作モードの変更」を参照してください。 バーチャル ドメインが有効になっている場合、このフィールドには、現在のバーチャル ドメインの動作モードが表示されます。各バーチャル ドメインは、NAT モードまたはトランスペアレント モードのどちらでも動作できます。 バーチャル ドメインが有効になっている場合、グローバル システム ステータス ダッシュボードにはこのフィールドが含まれません。
[Virtual Domain]	FortiGate ユニット上のバーチャル ドメインのステータス。バーチャル ドメイン機能のステータスを変更するには、*[Enable]* または *[Disable]* を選択します。 バーチャル ドメインを有効または無効にすると、セッションが終了するため、ログインし直す必要があります。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。
[Current Administrators]	現在 FortiGate ユニットにログインしている管理者の数。 現在ログインしている各管理者に関するより詳細な情報を表示するには、*[Details]* を選択します。追加情報には、ユーザ名、接続の種類、接続元の IP アドレス、およびログインした時刻が含まれます。
[Current User]	FortiGate ユニットにログインするために使用した管理者アカウントの名前。PKI またはリモート認証によってはなく、パスワードによってローカルに認証されている場合は、*[Change Password]* を選択してこのアカウントのパスワードを変更できます。パスワードを変更するとログアウトされるため、新しいパスワードを使用してログインし直す必要があります。詳細については、172 ページの「管理者アカウントのパスワードの変更」を参照してください。

システム時刻の設定

FortiGate ユニットのシステム時刻は、[System Information] ウィジェットで変更できます。また、[System Information] ウィジェットの [System Time] 領域に現在の時刻を表示することもできます。

1 *[System]*、*[Dashboard]*、*[Status]* の順に選択します。
2 *[System Information]* ウィジェットで、*[System Time]* 行にある *[Change]* を選択します。
3 タイム ゾーンを選択した後、日付と時刻を手動で設定するか、または NTP サーバとの同期を設定します。

[System Time]	現在の FortiGate システムの日付と時刻。
[Refresh]	現在の FortiGate システムの日付と時刻の表示を更新します。
[Time Zone]	現在の FortiGate システムのタイム ゾーンを選択します。
[Automatically adjust clock for daylight saving changes]	タイム ゾーンで夏時間と標準時間が切り替わる際に FortiGate のシステム クロックを自動的に調整したい場合に選択します。
[Set Time]	FortiGate システムの日付と時刻を、[Hour]、[Minute]、[Second]、[Year]、[Month]、および [Day] フィールドに入力した値に設定する場合に選択します。
[Synchronize with NTP Server]	NTP (Network Time Protocol) サーバを使用してシステムの日付と時刻を自動的に設定する場合に選択します。サーバと同期間隔を指定する必要があります。 FortiGate ユニットは、NTP バージョン 4 を使用します。NTP バージョン 4 では現在、RFC は使用できません。NTP バージョン 3 の RCF は RFC 1305 です。NTP の詳細については、http://www.ntp.org を参照してください。
[Server]	NTP サーバの IP アドレスまたはドメイン名を入力します。使用できる NTP サーバを検索するには、http://www.ntp.org を参照してください。
[Sync Interval]	FortiGate ユニットが NTP サーバと時刻の同期をとる頻度を指定します。たとえば、1440 分に設定すると、FortiGate ユニットは 1 日に 1 回時刻の同期をとります。

FortiGate ユニットのホスト名の変更

FortiGate のホスト名は、[Status] ページと FortiGate の CLI プロンプトに表示されます。また、このホスト名は、SNMP システム名としても使用されます。SNMP については、142 ページの「SNMP」を参照してください。

デフォルトのホスト名は、FortiGate ユニットのシリアル番号です。たとえば、シリアル番号 FGT8002805030003 は、FortiGate-800 ユニットになります。

管理者プロファイルでシステム設定への書き込みアクセスが許可されている管理者は、FortiGate ユニットのホスト名を変更できます。

ホスト名が 16 文字より長い場合は、切り詰められて表示され、最後の文字が "~" になります。完全なホスト名は *[System]*、*[Status]*、*[Dashboard]* の順に選択すると表示されますが、CLI や、ホスト名が使用されているその他の場所では切り詰められたホスト名が表示されます。FortiGate ユニットが HA クラスタの一部である場合は、そのユニットをクラスタ内の他のユニットから区別できるように一意のホスト名を使用しなくてはなりません。

FortiGate ユニットのホスト名を変更するには

1 *[System]*、*[Dashboard]*、*[Status]* の順に選択します。
2 [System Information] セクションの *[Host Name]* フィールドで、[Change] を選択します。
3 *[New Name]* フィールドに、新しいホスト名を入力します。
4 *[OK]* を選択します

新しいホスト名が [Host Name] フィールドと CLI プロンプトに表示されます。また、SNMP システム名にも追加されます。

FortiGate の変更

注意：古いファームウェア イメージをインストールすると、一部のシステム設定が失われる可能性があります。ファームウェア イメージを変更する前に、常に設定をバックアップしてください。

管理者プロファイルでメンテナンス読み取りおよび書き込みアクセスが許可されている FortiGate 管理者は、FortiGate ファームウェアを変更できます。ファームウェア イメージは、ローカル ハード ディスク、ローカル USB ディスク、FortiGuard ネットワークを含むいくつかのソースから転送できます。ファームウェア変更では、新しいバージョンにアップグレードするか、または以前のバージョンへの復帰を行います。ファームウェアを変更するための適切な手順に従ってください。

USB ディスクおよび FortiGuard ネットワークを使用する方法の詳細については、199 ページの「システム – メンテナンス」を参照してください。ファームウェアの管理の詳細については、61 ページの「ファームウェア管理方法」を参照してください。

[Upgrade]（または、ファームウェアをダウングレードする場合は [Downgrade]）を選択すると、[Firmware Upgrade/Downgrade] ページに自動的にリダイレクトされます。

[Firmware Upgrade/Downgrade] ページ

FortiGate ユニット上のファームウェアをアップグレードまたはダウングレードするための設定を提供します。

[Upgrade From]	使用可能なソースのドロップダウン リストから、ファームウェア ソースを選択します。 可能性のあるソースには、ローカル ハード ディスク、USB、および FortiGuard ネットワークがあります。 このフィールドは、すべてのモデルで表示されるわけではありません。
[Upgrade File]	ローカル ハード ディスク上のファームウェア イメージの場所を参照します。 このフィールドは、ローカル ハード ディスクと USB にのみ使用できます。
[Allow Firmware Downgrade]	古いファームウェア イメージのインストール（ダウングレード）を確認する場合に選択します。 このフィールドは、ファームウェアをダウングレードしようとした場合にのみ表示されます。
[More Info]	FortiGuard ネットワークを経由したファームウェアの更新に関する詳細情報を表示するために、FortiGuard Center に移動します。

注記：FortiGate モデルのファームウェアの更新にアクセスするには、FortiGate ユニットをカスタマ サポートに登録する必要があります。詳細については、http://support.fortinet.com を参照するか、またはカスタマ サポートにお問い合わせください。

[License Information]

[License Information] には、テクニカル サポート契約と FortiGuard サブスクリプションのステータスが表示されます。FortiGate ユニットは、FortiGuard Distribution Network (FDN) に接続しようとするときに、ライセンス情報のステータス インジケータを自動的に更新します。FortiGuard サブスクリプションのステータス インジケータは、FDN に接続可能であり、最後の接続試行中にライセンスが有効であった場合は緑色、FortiGate ユニットが FDN に接続できない場合は灰色、FDN に接続可能だが、ライセンスの期限が切れている場合はオレンジ色になります。

新しい FortiGate ユニットは、電源が投入されると FortiGuard サービスを自動的に検索します。このユニットが集中管理用に設定されている場合は、設定されている FortiManager システム上で FortiGuard サービスを検索します。FortiGate ユニットは、シリアル番号を FortiGuard サービス プロバイダに送信します。このサービス プロバイダは次に、この FortiGate ユニットが登録済みであり、かつ FortiGuard サブスクリプションと FortiCare サポート サービスの有効な契約が締結されているかどうかを判断します。この FortiGate ユニットが登録済みであり、かつ有効な契約が締結されている場合は、ライセンス情報が更新されます。

この FortiGate ユニットが登録されていない場合は、super_admin プロファイルを持つすべての管理者に、登録フォームへのアクセスを提供するリマインダ メッセージが表示されます。

30 日以内に契約の期限が切れる場合は、super_admin プロファイルを持つすべての管理者に、契約の追加フォームへのアクセスを提供する通知メッセージが表示されます。単純に、新しい契約番号を入力して *[Add]* を選択します。また、Fortinet サポートは契約満了リマインダも送信します。

必要に応じて、登録の通知または契約の問い合わせを無効にすることができます。

登録の通知を無効にするには

```
config system global
  set registration-notification disable
end
```

契約満了の通知を無効にするには

```
config system global
  set service-expire-notification disable
end
```

いずれかの設定オプションを選択すると、[Maintenance] ページが表示されます。詳細については、199 ページの「システム – メンテナンス」を参照してください。

[Support Contract]	終了日や登録ステータスなどの、現在の Fortinet サポート契約に関する詳細を表示します。 ・ *[Not Registered]* が表示されている場合は、*[Register]* を選択してユニットを登録してください。 ・ *[Expired]* が表示されている場合は、*[Renew]* を選択して、テクニカル サポート契約の更新に関する情報を表示してください。お近くの販売代理店にご相談ください。 ・ *[Registered]* が表示されている場合は、この FortiGate ユニットを登録したサポートの名前も表示されます。 ・ *[Login Now]* を選択すると、この FortiGate ユニットを登録した Fortinet サポートのアカウントにログインすることができます。
[FortiGuard Services]	
[AntiVirus]	FortiGuard アンチウイルスのバージョン、ライセンス発行日、およびサービス ステータス。ライセンスの期限が切れている場合は、*[Renew]* を選択してライセンスを更新できます。
[AV Definitions]	FortiGuard アンチウイルス定義の現在インストールされているバージョン。これらの定義を手動で更新するには、*[Update]* を選択します。詳細については、59 ページの「[P2P Usage]」を参照してください。
[Extended set]	拡張された FortiGuard アンチウイルス定義の現在インストールされているバージョン。 これらの定義を手動で更新するには、*[Update]* を選択します。詳細については、59 ページの「[P2P Usage]」を参照してください。 拡張されたアンチウイルス データベースは、すべてのモデルで使用できるわけではありません。
[Intrusion Protection]	FortiGuard 不正侵入防御システム (IPS) ライセンスのバージョン、ライセンス発行日、およびサービス ステータス。ライセンスの期限が切れている場合は、*[Renew]* を選択してライセンスを更新できます。
[IPS Definitions]	IPS 攻撃定義の現在インストールされているバージョン。これらの定義を手動で更新するには、*[Update]* を選択します。詳細については、59 ページの「[P2P Usage]」を参照してください。
[Web Filtering]	FortiGuard Web フィルタリング ライセンスのステータス、終了日、およびサービス ステータス。ライセンスの期限が切れている場合は、*[Renew]* を選択してライセンスを更新できます。
[Email Filtering]	FortiGuard 電子メール フィルタリングまたはアンチスパム ライセンスのステータス、ライセンス終了日、およびサービス ステータス。ライセンスの期限が切れている場合は、*[Renew]* を選択してライセンスを更新できます。
[Email Filtering Rule Set]	FortiGuard 電子メール フィルタリング ルール セットの現在インストールされているバージョン。これらのルール セットを手動で更新するには、*[Update]* を選択します。詳細については、59 ページの「[P2P Usage]」を参照してください。

[Analysis & Management Service]	FortiGuard Analysis Service および FortiGuard Management Service ライセンス、ライセンス終了日、および到達可能性ステータス。詳細については、208 ページの「FortiGuard Analysis and Management Service オプションの設定」を参照してください。
[Services Account ID]	別のサービス アカウント ID を入力するには、*[Change]* を選択します。この ID は、FortiGuard Management Service や FortiGuard Analysis Service などのサブスクリプション サービスのライセンスを検証するために使用されます。詳細については、208 ページの「FortiGuard Analysis and Management Service オプションの設定」を参照してください。
[Virtual Domain]	
[VDOMs Allowed]	このユニットが現在のライセンスでサポートしているバーチャル ドメインの最大数。 ハイエンドの FortiGate モデルの場合は、*[Purchase More]* リンクを選択してフォーティネット テクニカル サポートからライセンス キーを購入することにより、VDOM の最大数を増やすことができます。詳細については、199 ページの「VDOM ライセンスの追加」を参照してください。
[Endpoint Security]	
[FortiClient Software Windows Installer]	エンドポイント NAC 用の FortiGuard から入手可能な最新バージョンの FortiClient アプリケーションに関する情報を表示します。FortiClient アプリケーション インストーラを PC にダウンロードするには、*[Download]* を選択します。詳細については、473 ページの「FortiClient インストーラ ダウンロードおよび必須バージョンの設定」を参照してください。
[Application Signature package]	現在のエンドポイント NAC アプリケーション検知の定義済みシグネチャ パッケージのバージョン番号。詳細については、471 ページの「Configuring アプリケーション センサーの設定」を参照してください。

FortiGuard 定義の手動による更新

FortiGuard アンチウイルス データベース、不正侵入防御の定義、およびアンチスパム ルール セットは、[System Status] ページの [License Information] セクションからいつでも更新できます。

FortiGuard アンチウイルス定義、IPS 定義、またはアンチスパム ルール セットを手動で更新するには

1 最新の更新ファイルを Fortinet サポート サイトからダウンロードし、それを Web ベース マネージャへの接続に使用するコンピュータにコピーします。
2 Web ベース マネージャを起動し、*[System]*、*[Dashboard]*、*[Status]* の順に選択します。
3 [License Information] セクションにある、[FortiGuard Subscriptions] の [AV Definitions]、[IPS Definitions]、または [AS Rule Set] フィールドで、[Update] を選択します。
4 [Browse] を選択して更新ファイルを見つけるか、またはパスとファイル名を入力します。
5 *[OK]* を選択して、更新ファイルを FortiGate ユニットにコピーします。
FortiGate ユニットは AV 定義を更新します。この処理には 1 分程度かかります。
6 *[System]*、*[Dashboard]*、*[Status]* の順に選択して、選択した定義またはルール セットのバージョン情報が更新されていることを確認します。

[Unit Operation]

注意：FortiGate ユニットの電源を突然切断すると、ユニットの設定が壊れることがあります。ここで、または CLI で再起動およびシャットダウン オプションを使用すると、設定が失われないようにするための適切なシャットダウン手順が確実に実行されます。

[Unit Operation] ウィジェットでは、FortiGate ユニットのフロント パネルの図に、このユニットのイーサネット ネットワーク インタフェースのステータスが表示されます。ネットワーク インタフェースが緑色になっている場合、そのインタフェースは接続されています。インタフェースの上にマウス ポインタを置くと、名前、IP アドレス、ネットマスク、およびインタフェースの現在のステータスが表示されます。

[Reboot] または *[ShutDown]* を選択すると、ポップアップ ウィンドウが開き、システム イベントの理由を入力できるようになります。ディスク ロギング、イベント ロギング、および管理イベントが有効になっている場合は、入力した理由がディスク イベント ログに追加されます。イベント ロギングの詳細については、496 ページの「ログ メッセージへのアクセスおよび表示」を参照してください。

FortiGate ユニットでは、1 つの管理方法と 1 つのロギング / 分析方法のみを表示できます。それぞれの図は、どの方法を選択したかに基づいて変化します。何も選択していない場合、図は表示されません。

[INT / EXT / DMZ / HA / WAN1 / WAN2 / 1 / 2 / 3 / 4]	FortiGate ユニット上のネットワーク インタフェース。これらのインタフェースの名前と数は、モデルによって異なります。 インタフェース名の下のアイコンは、各インタフェースのアップ / ダウン ステータスを色で示します。緑色はインタフェースが接続されていることを、灰色は接続されていないことを示しています。 インタフェースの設定やステータスを表示するには、そのインタフェースのアイコンの上にマウスを移動させます。ポップアップ ウィンドウに、インタフェースのフル ネーム、インタフェースのエイリアス (設定されている場合)、IP アドレスとネットマスク、リンクのステータス、インタフェースの速度、および送受信されたパケットの数が表示されます。
[AMC-SW1/1, ...] **[AMC-DW1/1, ...]**	FortiGate ユニットで AMC (Advanced Mezzanine Card) モジュールがサポートされ、かつネットワーク インタフェースを含む AMC モジュール (たとえば、ASM-FB4 には 4 つのインタフェースが含まれています) をインストールしている場合は、これらのインタフェースがインタフェースのステータス表示に追加されます。これらのインタフェースには、モジュールとインタフェースに基づいた名前が付けられます。たとえば、AMC-SW1/3 は SW1 モジュール上の 3 番目のネットワーク インタフェースであり、AMC-DW2/1 は DW2 モジュール上の最初のネットワーク インタフェースです。 AMC モジュールはハード ディスクもサポートしています (たとえば、ASM-S08 モジュール)。ハード ディスクがインストールされている場合、ASM-S08 には、ハード ディスクがどの程度使用されているかを示す水平バーとパーセンテージも表示されます。 FortiGate ユニットがトランスペアレント モードで動作している場合は、FortiGate インタフェースをブリッジするために ASM-CX4 および ASM-FX2 モジュールを追加することもできます。 AMC モジュールの詳細については、219 ページの「AMC モジュールの設定」を参照してください。
[FortiAnalyzer]	FortiGate ユニットの図と FortiAnalyzer の図の間のリンク上にあるアイコンは、それらの OFTP 接続のステータスを示します。赤色のアイコンの上にある "X" は、接続されていないことを示しています。緑色のアイコンの上にあるチェック マークは、OFTP 通信が行われていることを示しています。 FortiGate ユニット上で FortiAnalyzer ユニットへのリモート ロギングを設定するには、FortiAnalyzer の図を選択します。詳細については、491 ページの「FortiAnalyzer ユニットへのリモート ロギング」を参照してください。
[FortiGuard Analysis Service]	FortiGate ユニットの図と FortiGuard Analysis Service の図の間のリンク上にあるアイコンは、それらの OFTP 接続のステータスを示します。赤色のアイコンの上にある "X" は、接続されていないことを示しています。緑色のアイコンの上にあるチェック マークは、OFTP 通信が行われていることを示しています。 FortiGuard Analysis Service へのリモート ロギングを設定するには、FortiGuard Analysis Service の図を選択します。詳細については、『*FortiGuard Analysis and Management Service 管理ガイド*』を参照してください。
[FortiManager]	FortiGate ユニットの図と FortiManager の図の間のリンク上にあるアイコンは、接続のステータスを示します。赤色のアイコンの上にある "X" は、接続されていないことを示しています。緑色のアイコンの上にあるチェック マークは、この 2 つのユニットの間で通信が行われていることを示しています。 FortiGate ユニット上で集中管理を設定するには、FortiManager の図を選択します。詳細については、183 ページの「集中管理」を参照してください。
[FortiGuard Management Service]	FortiGate ユニットの図と FortiGuard Management Service の図の間のリンク上にあるアイコンは、接続のステータスを示します。赤色のアイコンの上にある "X" は、接続されていないことを示しています。緑色のアイコンの上にあるチェック マークは、通信が行われていることを示しています。 FortiGate ユニット上で集中管理を設定するには、FortiGuard Management Service の図を選択します。詳細については、183 ページの「集中管理」を参照してください。

[Reboot]	FortiGate ユニットをシャットダウンして再起動する場合に選択します。ログに記録される再起動の理由を入力するよう求められます。
[Shutdown]	FortiGate ユニットをシャットダウンする場合に選択します。確認するよう求められます。また、ログに記録されるシャットダウンの理由を入力することも求められます。

[System Resources]

[System Resources] ウィジェットには、CPU やメモリ (RAM) の使用率などの、FortiGate ユニットの基本的なリソースの使用状況が表示されます。[System Status] ページに表示されていないシステム リソースはすべて、[History] アイコンを選択することでグラフとして表示できます。

最新の CPU とメモリの使用率を表示するには、[更新] アイコンを選択します。

[History]	CPU、メモリ、セッション、およびネットワークの最新の 1 分間の使用率をグラフィカルに表示します。このページにはまた、最新の 20 時間のウイルスおよび不正侵入検知も表示されます。詳細については、46 ページの「動作履歴の表示」を参照してください。
[CPU Usage]	ダイヤル ゲージおよびパーセンテージとして表示された現在のCPUステータス。 Web ベース マネージャには、コア プロセスの CPU 使用率のみが表示されます。管理プロセス (たとえば、Web ベース マネージャへの HTTPS 接続のためのプロセス) の CPU 使用率は除外されます。 表示される CPU 使用率は、CLI コマンド `get system performance status` を使用し、`user`、`system`、および `nice` のパーセンテージを追加した場合と同等です。Web ベースの CPU 使用率とこの CLI コマンドは、どちらも同じ CPU 情報にアクセスします。
[Memory Usage]	ダイヤル ゲージおよびパーセンテージとして表示された現在のメモリ (RAM) ステータス。 Web ベース マネージャには、コア プロセスのメモリ使用率のみが表示されます。管理プロセス (たとえば、Web ベース マネージャへの HTTPS 接続のためのプロセス) のメモリ使用率は除外されます。
[FortiAnalyzer Usage]	円グラフとパーセンテージで表示される、この FortiGate ユニットのクォータで使用されている FortiAnalyzer ディスク領域の現在のステータス。 [System Resources] の [Edit] メニューを使用すると、この情報が表示されないように選択できます。 FortiAnalyzer ユニットへのロギングを設定している場合にのみ表示されます。
[Disk Usage]	円グラフとパーセンテージで表示される、使用されている FortiGate ユニットのディスク領域の現在のステータス。 FortiGate ユニット上にハード ディスクが存在する場合にのみ表示されます。

動作履歴の表示

[System Resource History] ページには、時間の経過に伴う各種のシステム リソースや保護の動作を表す 6 つのグラフが表示されます。

グラフの垂直軸にユニットが表示されていない場合、そのグラフはパーセンテージで表されています。

各グラフの更新間隔は 3 秒です。

動作履歴を表示するには、*[System]*、*[Dashboard]*、*[Status]* の順に選択してから、[System Resources] ウィジェットの右上隅にある [History] を選択します。

[Time Interval]	グラフの下部の軸に沿って表示する時間間隔を選択します。
[CPU Usage History]	指定された時間間隔毎の CPU 使用率 (%)。
[Memory Usage History]	指定された時間間隔毎のメモリ使用率 (%)。
[Session History]	指定された時間間隔毎のセッション数。
[Network Utilization History]	指定された時間間隔毎のネットワーク使用率。
[Virus History]	指定された時間間隔毎に検出されたウイルスの数。
[Intrusion History]	指定された時間間隔毎に検出された侵入の試みの数。

警告メッセージ コンソール

警告メッセージは、ファームウェア変更、ネットワーク セキュリティ イベント、ウイルス検知イベントなどの、FortiGate ユニット上のシステム イベントを追跡するのに役立ちます。

各メッセージには、イベントが発生した日付と時刻が表示されます。

[History]	すべての警告メッセージを表示します。
[Edit]	警告メッセージ コンソールを設定します。
[Refresh]	表示されている情報を更新します。
[Close]	モジュールを閉じます。
[Acknowledge this message]	このメッセージを削除する場合に選択します。 [History] ウィンドウに、 各警告メッセージのための [確認] アイコンも表示されます。

警告メッセージ コンソールには、次の種類のメッセージを表示できます。

System restart	システムが再起動されました。再起動は、オペレータが操作したため、または電源がオフ / オンされたために生じた可能性があります。
System shutdown	管理者が、Web ベース マネージャまたは CLI から FortiGate ユニットをシャットダウンしました。
Firmware upgraded by <admin_name>	指定の管理者が、アクティブまたは非アクティブ パーティションのどちらかで、ファームウェアをより新しいバージョンにアップグレードしました。
Firmware downgraded by <admin_name>	指定の管理者が、アクティブまたは非アクティブ パーティションのどちらかで、ファームウェアをより古いバージョンにダウングレードしました。
FortiGate has reached connection limit for <n> seconds	アンチウイルス エンジンが、表示されている時間、メモリ不足に陥ったため、保護モードに入りました。この状況下では、モデルや設定にもよりますが、コンテンツをブロックするか、またはスキャンなしで通過させることも選択できます。
Found a new FortiAnalyzer Lost the connection to FortiAnalyzer	FortiGate ユニットが、FortiAnalyzer ユニットを発見したか、または FortiAnalyzer ユニットへの接続を失ったことを示します。詳細については、491 ページの「FortiAnalyzer ユニットへのリモート ロギング」を参照してください。
New firmware is available from FortiGuard	更新されたファームウェア イメージをこのFortiGateユニットにダウンロードできます。

警告メッセージ コンソールを設定することにより、コンソールに表示されるメッセージの種類を制御できます。

警告メッセージ コンソールを設定するには

1 *[System]*、*[Dashboard]*、*[Status]* の順に選択します。
2 警告メッセージ コンソールのタイトル バーにある *[編集]* アイコンを選択します。
3 警告メッセージ コンソールに表示される警告の種類を選択します。
デフォルトでは、すべての警告の種類が有効になっています。
4 *[OK]* を選択します。

[Log and Archive Statistics]

[Log and Archive Statistics] ウィジェットを使用すると、DLP アーカイブやネットワーク トラフィックのほか、攻撃の試み、捕捉されたウイルス、捕捉されたスパム電子メールなどのセキュリティの問題に関して、FortiGate ユニットで何が発生しているかを一目でわかるように表示できます。

トラフィックの量や種類だけでなく、システムに対して行われた攻撃の試みについて、すばやく知ることができます。特に気になる領域を調べるには、*[Details]* を選択して、その領域の最新の動作の詳細なリストを表示します。

[Log and Archive Statistics] ウィジェットに表示される情報は、ログ メッセージから導き出されます。ログ メッセージによって収集された情報を使用して、時間の経過に伴うネットワーク動作や攻撃の傾向を調べることができます。実際に [Log and Archive Statistics] ウィジェットのデータを収集するには、以下に示すさまざまな設定が必要です。

[Since]	カウントが最後にリセットされた日付と時刻。 カウントは、FortiGate ユニットの再起動時、または *[Reset]* を選択したときにリセットます。
[Reset]	[Log and Archive Statistics] のカウントを 0 にリセットします。
[DLP Archive]	FortiGate ユニットを通過し、DLP によってアーカイブされた HTTP、HTTPS、電子メール、FTP IM、および VoIP（セッション制御とも呼ばれる）トラフィックの概要。*[Details]* ページには、選択された種類のトラフィック（最大 64 項目）の最新の項目のリストが表示され、アーカイブされたトラフィックが格納されている FortiAnalyzer ユニットへのリンクが示されます。FortiAnalyzer ユニットへのロギングが設定されていない場合、*[Details]* ページには、*[Log & Report]*、*[Log Config]*、*[Log Settings]* へのリンクが表示されます。 FortiGate ユニットを、このウィジェットの DLP アーカイブ データを収集するように設定するには、ログ データをアーカイブするように DLP センサを設定します。詳細については、404 ページの「DLP アーカイブ」を参照してください。 また、ファイアウォール ポリシーにもプロファイルを追加する必要があります。ファイアウォール ポリシーが、選択されたプロトコルのセッションを受信すると、[Statistics] ウィジェットにメタデータが追加されます。 電子メールの統計は、電子メール プロトコルに基づいています。POP3 と IMAP のトラフィックは受信された電子メールとして、SMTP は送信された電子メールとして登録されます。FortiGate ユニットが SSL コンテンツのスキャンと検査をサポートしている場合、受信電子メールには POP3S と IMAPS も含まれ、送信電子メールには SMTPS も含まれます。受信または送信電子メールでこれらのプロトコルが使用されていない場合、これらの統計は不正確です。SSL コンテンツのスキャンと検査の詳細については、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。 IM の統計は AIM、ICQ、MSN、および Yahoo! プロトコルに基づいており、IM DLP ルールの DLP センサで *[Archive]* を選択することによって設定されます。 VoIP の統計は SIP、SIMPLE、および SCCP セッション制御プロトコルに基づいており、セッション制御 DLP ルールの DLP センサで *[Archive]* を選択することによって設定されます。
[Log]	FortiGate ユニットでログに記録されたトラフィック、ウイルス、攻撃、スパム電子メール メッセージ、およびブロックされた URL の概要。また、DLP およびイベント ログ メッセージに一致したセッションの数も表示されます。*[Details]* ページには最新 20 項目のリストが表示され、時間、発信元、宛先などの情報が示されます。 *[DLP data loss detected]* には、DLP センサ プロファイルに一致したセッションの数が実際に表示されます。DLP は DLP センサに一致したすべてのセッションに関するメタデータを収集し、このメタデータを DLP ログに記録します。DLP ログ メッセージが記録されるたびに、[DLP data loss detected] の数値が増えます。概要または完全なアーカイブに DLP を使用している場合は、[DLP data loss detected] の数値が非常に大きくなることがあります。この数値は、データが消失または漏洩したことを示していない可能性があります。

[Statistics] ウィジェットでの DLP アーカイブ情報の表示

[System Status] ページの [Statistics] ウィジェットから、FortiGate ユニットを通過する HTTP、HTTPS、FTP、および IM トラフィックに関する統計を表示できます。各トラフィックの種類の横にある *[Details]* リンクを選択することにより、詳細情報を表示できます。[Statistics] セクションのヘッダにある *[Reset]* を選択すると、DLP アーカイブおよびアタック ログ情報をクリアし、カウントを 0 にリセットすることができます。

DLP アーカイブ情報を表示するには、*[System]*、*[Dashboard]*、*[Status]* の順に選択して [Statistics] ウィジェットを表示し、行内の *[Details]* を選択します。次の表は、*[Details]* を選択したときに表示される情報をプロトコルごとに示しています。

表 4: DLP アーカイブ情報の表示

HTTP	**[Date and Time]** — URL がアクセスされた時刻。 **[From]** — URL のアクセス元の IP アドレス。 **[URL]** — アクセスされた URL。
電子メール	**[Date and Time]** — 電子メールが FortiGate ユニットを通過した時刻。 **[From]** — 送信者の電子メール アドレス。 **[To]** — 受信者の電子メール アドレス。 **[Subject]** — 電子メールの件名。
FTP	**[Date and Time]** — アクセスの時刻。 **[Destination]** — アクセスされた FTP サーバの IP アドレス。 **[User]** — FTP サーバにログインしたユーザ ID。 **[Downloads]** — ダウンロードされたファイルの名前。 **[Uploads]** — アップロードされたファイルの名前。
IM	**[Date / Time]** — アクセスの時刻。 **[Protocol]** — この IM セッションで使用されているプロトコル。 **[Kind]** — このトランザクションの IM トラフィックの種類。 **[Local]** — このトランザクションのローカル アドレス。 **[Remote]** — このトランザクションのリモート アドレス。 **[Direction]** — このファイルが送信されたか、または受信されたかを示します。

アタック ログの表示

[Status] ページの [Statistics] セクションから、FortiGate ユニットが阻止したネットワーク攻撃に関する統計を表示できます。捕捉されたウイルス、検出された攻撃、検出されたスパム電子メール、およびブロックされた URL に関する統計を表示できます。また、DLP ルールに一致したセッションに関する情報も表示できます。各攻撃の種類の横にある [Details] リンクを選択することにより、詳細情報を表示できます。

[Statistics] セクションのヘッダにある [Reset] を選択すると、DLP アーカイブおよびアタック ログ情報をクリアし、カウントを 0 にリセットすることができます。

アタック ログ情報を表示するには、*[System]*、*[Dashboard]*、*[Status]* の順に選択して [Statistics] ウィジェットを表示し、行内の *[Details]* を選択します。次の表は、*[Details]* を選択したときに表示される情報をプロトコルごとに示しています。

表 5: アタック ログ情報の表示

AV	**[Date and Time]** — ウイルスが検出された時刻。 **[From]** — 送信者の電子メール アドレスまたは IP アドレス。 **[To]** — 対象とされた受信者の電子メール アドレスまたは IP アドレス。 **[Service]** — サービスの種類 (POP、HTTP など)。 **[Virus]** — 検出されたウイルスの名前。
IPS	**[Date and Time]** — 攻撃が検出された時刻。 **[From]** — 攻撃の発信元。 **[To]** — 攻撃の対象とされたホスト。 **[Service]** — サービスの種類。 **[Attack]** — 検出され、防御された攻撃の種類。
電子メール	**[Date and Time]** — スパムが検出された時刻。 **[From -> To IP]** — 送信者および対象とされた受信者の IP アドレス。 **[From -> To Email Accounts]** — 送信者および対象とされた受信者の電子メール アドレス。 **[Service]** — サービスの種類 (SMTP、POP、IMAP など)。 **[SPAM Type]** — 検出されたスパムの種類。
URL	**[Date and Time]** — URL へのアクセスの試みが検出された時刻。 **[From]** — URL の表示を試みたホスト。 **[URL Blocked]** — ブロックされた URL。

表 5: アタック ログ情報の表示

DLP	**[Date and Time]** — URL へのアクセスの試みが検出された時刻。 **[Service]** — サービスの種類（HTTP、SMTP、POP、IMAP など）。 **[Source]** — セッションの発信元アドレス。 **[From]** — URL の表示を試みたホスト。 **[URL Blocked]** — ブロックされた URL。 **[From]** — 送信者の電子メール アドレスまたは IP アドレス。 **[To]** — 対象とされた受信者の電子メール アドレスまたは IP アドレス。

[CLI Console]

[Status] ページには、CLI コンソールを含めることができます。このコンソールを使用するには、コンソールを選択して、現在 Web ベース マネージャで使用している管理者アカウントに自動的にログインします。テキストを CLI コンソールからコピーしたり（Ctrl-C）、CLI コンソールに貼り付けたり（Ctrl-V）することができます。

[CLI Console] ウィジェットのタイトル バーには、*[カスタマイズ]* と *[デタッチ]* の 2 つのコントロールが配置されています。

[デタッチ] は、[CLI Console] ウィジェットを、サイズ変更したり画面上の位置を変更したりできるポップアップ ウィンドウに移動します。デタッチされた CLI コンソールには、*[カスタマイズ]* と *[アタッチ]* の 2 つのコントロールがあります。[アタッチ] は、[CLI Console] ウィジェットを元の [System Status] ページに戻します。

[カスタマイズ] を使用すると、テキストや背景のフォントや色を定義することによって、コンソールの外観を変更できます。

[Preview]	CLI コンソールの外観への変更のプレビュー。
[Text]	このラベルの横にある現在の色見本を選択してから、右にあるカラー パレットから色を選択して、CLI コンソール内のテキストの色を変更します。
[Background]	このラベルの横にある現在の色見本を選択してから、右にあるカラー パレットから色を選択して、CLI コンソール内の背景の色を変更します。
[Use external command input box]	通常のコンソール エミュレーション領域の下にコマンド入力フィールドを表示する場合に選択します。このオプションが有効になっている場合は、コンソール エミュレーション領域または外部コマンド入力フィールドのどちらかに入力することによって、コマンドを入力できます。
[Console buffer length]	コンソール バッファでメモリ内に保持する行数を入力します。有効な数値の範囲は 20 ～ 9999 です。
[Font]	CLI コンソールの表示フォントを変更するには、リストからフォントを選択します。
[Size]	フォントのサイズを選択します。デフォルトのサイズは 10 ポイントです。

[Top Sessions]

[Top Sessions] には、現在 FortiGate ユニット上に最も多いセッションが開かれている IP アドレスを示す棒グラフまたは表のどちらかが表示されます。これらのセッションは、発信元または宛先 IP アドレスやポート アドレスごとに並べ替えられます。使用されている並べ替えの条件は、右上隅に表示されます。

[Top Sessions] ウィジェットはFortiGateユニットをポーリングしてセッション情報を取得するため、これが FortiGate ユニットのパフォーマンスに若干影響を与えます。このため、ダッシュボード上にこの表示が示されていない場合、データは収集されておらず、システム パフォーマンスも影響を受けていません。この表示が示されている場合、情報はメモリ内にのみ格納されます。

注記： FortiGate ユニットを再起動すると、[Top Sessions] の統計はゼロにリセットされます。

現在のセッション リスト、つまり現在 FortiGate ユニットによって処理されているすべてのセッションのリストを表示するには、*[Details]* を選択します。詳細については、51 ページの「現在のセッション リストの表示」を参照してください。

グラフ内のバーで表されているセッションに関する詳細を表示するには、そのバーをクリックします。

[Top Sessions] ウィジェットに表示される情報を変更するには、[編集] アイコンを選択し、必要な変更を行います。

[Sort Criteria]	[System Status] に表示される [Top Sessions] の並べ替えに使用される方法を選択します。次のいずれかを選択します。 ・ [Source Address] ・ [Source Address] ・ [Port Address]
[Display User Name]	この発信元 IP アドレスに関連付けられたユーザ名を含めるときに選択します (このユーザ名が使用可能な場合)。表形式の場合、このデータは別の列に表示されます。 *[Display User Name]* は、並べ替えの条件が *[Source Address]* の場合にのみ使用できます。
[Resolve Host Name]	IP アドレスをホスト名に解決する場合に選択します。 *[Resolve Host Name]* は、並べ替えの条件が *[Destination Port]* の場合は使用できません。
[Resolve Service]	ポート アドレスを、一般に関連付けられているサービス名に解決する場合に選択します。サービスに関連付けられていないポート アドレスはすべて、引き続きポート アドレスとして表示されます。たとえば、ポート 443 は HTTPS に解決されます。 *[Resolve Service]* は、並べ替えの条件が *[Destination Port]* の場合にのみ使用できます。
[Display Format]	[Top Sessions] の情報の表示方法を選択します。次のいずれかを選択します。 ・ [Chart] ・ [Table]
[Top Sessions to Show]	表示するセッションの数を選択します。5、10、15、または 20 セッションの表示を選択します。
[Refresh Interval]	表示が更新される頻度を選択します。更新間隔の範囲は 10 ～ 240 秒です。*[0]* を選択すると、表示の自動更新が無効になります。手動更新のオプションは、[Top Sessions] のタイトル バーでも引き続き選択できます。 更新間隔を短くすると、FortiGate ユニットのパフォーマンスに影響を与えることがあります。この場合は、更新間隔を増やすか、または自動更新を無効にしてみてください。

現在のセッション リストの表示

現在のセッション リストには、現在 FortiGate ユニットによって処理されているすべてのセッションが表示されます。現在のセッション リストには、セッションごとに次の情報が表示されます。

- セッション プロトコル (tcp や udp など)
- 発信元アドレスとポート
- 宛先アドレスとポート
- このセッションに適用されるポリシーの ID (存在する場合)
- このセッションの期限が切れるまでの期間
- このセッションが属するバーチャル ドメイン

[Virtual Domain]	特定のバーチャル ドメインによって処理されているセッションのリストを表示するには、そのバーチャル ドメインを選択します。すべてのバーチャル ドメインによって処理されているセッションを表示するには、[All] を選択します。 このオプションは、バーチャル ドメインが有効になっている場合にのみ使用できます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。
[Refresh]	セッション リストを更新します。
[First Page]	現在のセッションの表示されている最初のページに移動する場合に選択します。
[Previous Page]	現在のページの直前にあるセッションのページに移動する場合に選択します。

[Page]	セッション リストの表示を開始するセッションのページ番号を入力します。たとえば、5 ページ分のセッションがあるときに「3」を入力すると、セッションの 3 ページ目が表示されます。 "/" の次の数値は、セッションのページ数です。
[Next Page]	セッションの次のページに移動する場合に選択します。
[Last Page]	現在のセッションの表示されている最後のページに移動する場合に選択します。
[Total]	セッションの総数。
[Clear All Filters]	設定されている表示フィルタをすべてリセットする場合に選択します。
[Return]	[Top Sessions] の表示に戻ります。
[Filter Icon]	[#] と [Expiry] を除くすべての列の項目名の左側にあるアイコン。選択すると、[Edit Filter] ダイアログが表示され、列ごとに表示フィルタを設定できるようになります。32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。
[Protocol]	接続のサービス プロトコル (たとえば、udp、tcp、icmp)。
[Source Address]	接続の発信元 IP アドレス。
[Source Port]	接続の発信元ポート。
[Destination Address]	接続の宛先 IP アドレス。
[Destination Port]	接続の宛先ポート。
[Policy ID]	このセッションを許可しているファイアウォール ポリシーの番号か、またはセッションに FortiGate インタフェースが 1 つしか関係していない場合 (たとえば、管理セッション) は空白。
[Expiry (sec)]	接続が期限切れになるまでの時間 (秒単位)。
[Duration]	各セッションの有効期間 (秒単位)。この有効期間は、このセッションがアクティブであった期間です。
[Delete]	アクティブな通信セッションを停止します。管理者プロファイルで、システム設定への読み取りおよび書き込みアクセスが許可されている必要があります。

現在のセッション リストを表示するには

1 *[System]*、*[Dashboard]*、*[Status]* の順に選択します。

2 *[Top Sessions]* ウィジェットで、ウィジェットの下部にある *[Details]* を選択します。

現在のセッション リストが表示されます。必要に応じて、*[デタッチ]* を選択してデタッチしたり、ブラウザ ウィンドウを拡張してリスト全体を確認したりします。

3 *[Return]* を選択して、[Top Sessions] の棒グラフ表示に戻ります。

[Top Viruses]

[Top Viruses] には、FortiGate ユニットによって最も頻繁に検出されたウイルス脅威を表す棒グラフが表示されます。

[Top Viruses] の表示は、デフォルトのダッシュボード表示には含まれていません。ドロップダウン メニューから、*[Add Content]*、*[Top Viruses]* の順に選択することによって表示できます。

[History] アイコンを選択すると、ウィンドウが開き、検出された最大 20 個の最新のウイルスが、ウイルス名、最後に検出された時刻、検出された回数などの情報とともに表示されます。システムでは最大 1024 のエントリが格納されますが、Web ベース マネージャには最大 20 個のみが表示されます。

このウィジェットのタイトル バー領域にある *[編集]* アイコンを選択すると、このウィジェットのいくつかの設定を設定できます。設定を保存するには、*[OK]* を選択する必要があります。

[Top Viruses] のカスタム表示

[Custom Widget Name]	このウィジェットの新しい名前を入力します。このフィールドはオプションです。

[Refresh Interval]	表示の更新間隔 (秒単位) を選択します。範囲は 10 ～ 240 秒です。[0] を選択すると、更新が無効になります。また、モジュール ヘッダにある *[更新]* アイコンを使用して更新することもできます。
[Top Viruses To Show]	上位 *5*、*10*、*15*、または *20* 個のウイルスの表示を選択します。

[Top Attacks]

[Top Attacks] には、FortiGate ユニットによって検出された最も多数の攻撃を表す棒グラフが表示されます。

[Top Attacks] の表示は、デフォルトのダッシュボード表示には含まれていません。ドロップダウン メニューから、*[Add Content]*、*[Top Attacks]* の順に選択することによって表示できます。

[History] アイコンを選択すると、ウィンドウが開き、検出された最大 20 個の最新の攻撃が、攻撃名、最後に検出された時刻、検出された回数などの情報とともに表示されます。FortiGate ユニットでは最大 1024 のエントリが格納されますが、Web ベース マネージャには最大 20 個のみが表示されます。

このウィジェットのタイトル バー領域にある *[編集]* アイコンを選択すると、このウィジェットのいくつかの設定を設定できます。設定を保存するには、*[OK]* を選択する必要があります。

[Top Attacks] のカスタム表示

[Custom Widget Name]	このウィジェットの新しい名前を入力します。このフィールドはオプションです。
[Refresh Interval]	表示の更新間隔 (秒単位) を選択します。範囲は 10 ～ 240 秒です。[0] を選択すると、更新が無効になります。また、モジュール ヘッダにある *[更新]* アイコンを使用して更新することもできます。
[Top Attacks To Show]	上位 *5*、*10*、*15*、または *20* 個の攻撃の表示を選択します。

[Traffic History]

[Traffic History] ウィジェットには、選択された 1 つのインタフェース上の最新の 1 時間、1 日、および 1 か月のトラフィックが表示されます。この機能は、対処が必要なトラフィックのピークを見つけたり、その頻度、期間、その他の情報を取得したりするのに役立ちます。

一度に監視できるインタフェースは 1 つだけです。*[Edit]* を選択し、ドロップダウン メニューからインタフェースを選択して *[Apply]* を選択することによって、監視されているインタフェースを変更できます。*[Apply]* を選択すると、すべてのトラフィック履歴データがクリアされます。

[Interface]	監視されているインタフェース。
[kbit/s]	トラフィックのグラフの単位。トラフィック量がどれだけ少なくても、多くてもトラフィック レベルを表示できるように、縮尺はトラフィック レベルに基づいて変化します。
[Last 60 Minutes] **[Last 24 Hours]** **[Last 30 Days]**	FortiGate のこのインタフェース上で各種の期間にわたって監視されているトラフィックを示す 3 つのグラフ。 あるグラフでは、他のグラフに比べて、特定の傾向を突き止めやすい場合があります。
[Traffic In]	このインタフェース上で FortiGate ユニットに受信されるトラフィックが、薄い赤色の線で示されます。
[Traffic Out]	このインタフェース上で FortiGate ユニットから送信されるトラフィックが、濃い緑色の線で示され、薄い緑色で塗りつぶされます。

このウィジェットのタイトル バー領域にある *[編集]* アイコンを選択すると、このウィジェットのいくつかの設定を設定できます。設定を保存するには、*[OK]* を選択する必要があります。

[Traffic History] のカスタム表示

[Custom Widget Name]	このウィジェットの新しい名前を入力します。このフィールドはオプションです。
[Select Network Interface]	ドロップダウン リストからインタフェース (FortiGate ユニットのインタフェース) を選択します。選択したインタフェースには、そのインタフェース上で発生するトラフィックが表示されます。
[Enable Refresh]	情報の更新を有効にする場合に選択します。

[Top Policy Usage]

[Top Policy Usage] には、FortiGate ユニットを通過するトラフィック量がファイアウォール ポリシーによって分類されて、グラフまたは表のどちらかで表示されます。

グラフまたは表の表示から、次の操作を行うことができます。

- グラフ内の各バーの上にマウス ポインタを置くことによって、ファイアウォール ポリシーに関する詳細を表示する。
- グラフ上のファイアウォール ポリシーを選択して、そのファイアウォール ポリシーを表示したり、必要に応じて変更したりする。

[Top Policy Usage] のデータは、すべてのファイアウォール ポリシーごとに収集されます。[Top Policy Usage] を設定して、最大 20 のファイアウォール ポリシーのデータを表示できます。セッションを受け付けたファイアウォール ポリシーのみが、グラフまたは表に表示されます。

[Reset]	すべてのカウントを 0 にリセットします。
[Edit]	モジュールを設定します。
[Refresh]	表示されている情報を更新します。
[Close]	モジュールを閉じます。
[Policy ID]	ファイアウォール ポリシー識別子。
[Total Bytes] または [Total Packets]	*[Sort Criteria]* の設定に応じてバイト数またはパケット数で表された、ファイアウォール ポリシーの累積のトラフィック量。

[Top Policy Usage] モジュールを設定するには

1 *[System]*、*[Dashboard]*、*[Usage]* の順に選択します。

2 [Top Policy Usage] モジュールのタイトル バーにある *[編集]* アイコンを選択します。

3 次の情報を入力し、*[OK]* を選択します。

ダッシュボード — [Top Policy Usage] のカスタム表示

[Custom Widget Name]	このウィジェットの新しい名前を入力します。このフィールドはオプションです。
[Sort Criteria]	ポリシーを *[Bytes]* または *[Packets]* のどちらの数で並べ替えるかを選択します。
[VDOM]	監視する VDOM を選択するか、または *[Global]* を選択します。このオプションは、グローバル管理者のみが使用できます。VDOM 管理者には、自分の VDOM のみが表示されます。
[Display Format]	*[Chart]* または *[Table]* の表示を選択します。
[Top Entries To Show]	上位 *5*、*10*、*15*、または *20* 個のアプリケーションの表示を選択します。
[Refresh Interval]	表示の更新間隔 (秒単位) を選択します。範囲は 10 ～ 240 秒です。[0] を選択すると、更新が無効になります。また、モジュール ヘッダにある *[更新]* アイコンを使用して更新することもできます。

[DLP Archive Usage]

[DLP Archive Usage] には、FortiGate ユニットがコンテンツ アーカイブ (DLP アーカイブ) に送信したデータ量が表示されます。この情報は、DLP ルール、ファイアウォール ポリシー、プロテクション プロファイル、またはプロトコルによって分類できます。

表の表示から、次の操作を行うことができます。

- グラフ内の各バーの上にマウス ポインタを置くことによって、データに関する詳細を表示する。
- グラフ上のバーを選択して、データに関するより詳細な情報を表示する。

[DLP Archive Usage] のデータは、DLP センサ プロファイルをファイアウォール ポリシーに追加することによって収集されます。DLP センサに一致したセッションに関する情報のみが、グラフまたは表に追加されます。ファイアウォール ポリシーによって受け付けられたが、DLP センサが設定されたプロテクション プロファイルが含まれていないセッションは、表示されるデータに含まれません。

[Reset]	すべてのカウントを 0 にリセットします。
[Edit]	モジュールを設定します。
[Refresh]	表示されている情報を更新します。
[Close]	モジュールを閉じます。
[DLP Rule] または [Policy] または [Profile] または [Protocol]	*[Report By]* の設定に応じて、DLP ルール、ファイアウォール ポリシー、プロファイル、またはプロトコル。
[Bytes] または [Messages]	*[Sort Criteria]* の設定に応じてバイト数またはメッセージ数で表された、アーカイブされたデータの量。

このウィジェットのタイトル バー領域にある *[編集]* アイコンを選択すると、このウィジェットのいくつかの設定を設定できます。設定を保存するには、*[OK]* を選択する必要があります。

[DLP Archive Usage] のカスタム表示

[Custom Widget Name]	このウィジェットの新しい名前を入力します。このフィールドはオプションです。
[Report By]	[DLP Rule]、[Profile]、[Policy]、[Protocol] のいずれかを選択します。
[Sort Criteria]	結果を *[Bytes]* または *[Messages]* のどちらの数で並べ替えるかを選択します。
[Protocol]	含めるプロトコルを選択します。
[VDOM]	監視する VDOM を選択するか、または *[Global]* を選択します。このオプションは、グローバル管理者のみが使用できます。VDOM 管理者には、自分の VDOM のみが表示されます。 このフィールドは、*[Report By]* が *[Protocol]* の場合は使用できません。
[Top Entries To Show]	上位 *5*、*10*、*15*、または *20* 個の項目の表示を選択します。
[Refresh Interval]	表示の更新間隔 (秒単位) を選択します。範囲は 10 ～ 240 秒です。[0] を選択すると、更新が無効になります。また、モジュール ヘッダにある *[更新]* アイコンを使用して更新することもできます。

[RAID Monitor]

[RAID Monitor] の表示には、RAID アレイと各 RAID ディスクの現在の状態が表示されます。RAID アレイの設定については、223 ページの「RAID アレイの設定」を参照してください。

[RAID Monitor] の表示は、 デフォルトのダッシュボード表示には含まれていません。ドロップダウン メニューから、 *[Add Content]*、 *[RAID Monitor]* の順に選択することによって表示できます。

[RAID Monitor] は、FortiGate ユニットに複数のディスクがインストールされていない限り表示されません。

[Configure]	RAID アレイを設定するか、または劣化したアレイを再構築する場合に選択します。詳細については、223 ページの「RAID ディスクの設定」を参照してください。
[Array Status]	
アレイ ステータス アイコン	RAID アレイのステータスを示します。 チェックマークの付いた緑色は、正常な RAID アレイを示します。 黄色の三角形は、このアレイが劣化した状態にあるが、引き続き機能していることを示します。劣化したアレイは正常なアレイより低速です。劣化した状態を修正するには、アレイを再構築します。 レンチは、アレイが再構築されていることを示します。 アレイ ステータス アイコンの上にマウスを移動させると、このアレイのステータスのテキスト メッセージが表示されます。
ディスク ステータス アイコン	アレイ内のディスクごとに 1 つのアイコンがあります。 チェックマークの付いた緑色は、正常なディスクを示します。 ×印の付いた赤色は、このディスクに障害が発生し、注意が必要なことを示します。 ディスク ステータス アイコンの上にマウスを移動させると、このディスクのステータスとストレージ容量が表示されます。
[RAID Level]	この RAID アレイの RAID レベル。RAID レベルは、RAID アレイの設定の一部として設定されます。詳細については、224 ページの「RAID レベル」を参照してください。
[Disk Space Usage]	
ステータス バー	このバーは、 現在使用されている RAID アレイのパーセンテージを示します。
[Used]/[Free]/[Total]	これらの 3 つの数値は、使用されている RAID アレイのストレージ容量、空きストレージ容量、および RAID アレイ内の合計ストレージ容量を示します。これらの値は GB で表されます。 *[Used]* に *[Free]* を加えると *[Total]* に等しくなります。
同期中ステータス	RAID アレイの同期の進行状況を表示します。同期には数時間かかることがあります。 同期中、RAID アレイのステータスは、同期がバックグラウンドで実行されていることを示します。 同期の進行状況バーは、RAID アレイが同期されている場合にのみ表示されます。 この進行状況バーを更新するには、このウィジェットのタイトル バーにある [更新] アイコンの選択が必要になる場合があります。
再構築ステータス	RAID アレイの再構築の進行状況を表示します。アレイの再構築には数時間かかることがあります。 再構築中、アレイは劣化した、脆弱な状態にあります。再構築中にディスク障害が発生すると、データが消失します。 再構築が完了するまで、RAID アレイが信頼性の低下したモードで実行されていることを示す警告が表示されます。 この進行状況バーを更新するには、このウィジェットのタイトル バーにある [更新] アイコンの選択が必要になる場合があります。

RAID ディスクの設定

RAID アレイを設定するには、*[System]*、*[Dashboard]*、*[Status]* の順に選択し、[RAID Monitor] ウィジェットで *[Configure]* を選択します。

[RAID level]	RAID のレベルを選択します。オプションには次のものがあります。 **[RAID-0]** —（ストライピング）より高いパフォーマンス、冗長性はなし **[RAID-1]** —（ミラーリング）ストレージ容量は半分になるが、完全な冗長性 **[RAID-5]** — パリティ チェック付きストライピング、および冗長性 使用可能な RAID レベル オプションは、使用可能なハード ディスクの数によって異なります。RAID 0 または RAID 1 には、2 台以上のディスクが必要です。RAID 5 には、3 台以上のディスクが必要です。 RAID レベルの変更は、[Apply] が選択されたときに有効になります。 RAID レベルを変更すると、アレイに格納されているログ情報がすべて消去され、FortiGate ユニットが再起動されます。ユニットは、RAID アレイを再設定している間オフラインのままになります。再起動された後、完全な動作状態にするには、アレイを同期する必要があります。 RAID レベルの詳細については、224 ページの「RAID レベル」を参照してください。
[Status]	RAID アレイのステータスまたは稼働状態。このステータスは、次のいずれかになります。 **[OK]** — 標準のステータスであり、すべてが正常です。 **[OK (Background-Synchronizing) (%)]** — RAID レベルを変更した後、ディスクを同期しています。同期の進行状況バーに進行状況が表示されます。 **[Degraded]** — アレイ内の 1 台以上のディスクが故障しているか、削除されたか、または正常に機能していません。この状態では冗長性がないことについての警告が表示されます。また、劣化したアレイは正常なアレイより低速でもあります。アレイを修正するには、*[Rebuild RAID]* を選択します。 **[Degraded (Background-Rebuilding) (%)]** — [Degraded] と同じですが、RAID アレイがバックグラウンドで再構築されています。再構築が完了するまで、アレイは引き続き脆弱な状態にあります。
[Size]	ギガバイト（GB）単位の RAID アレイのサイズ。アレイのサイズは、選択された RAID レベルと、アレイ内のディスクの数によって異なります。
[Rebuild RAID]	アレイに新しいディスクが追加された後、または故障したディスクが交換された後にアレイを再構築する場合に選択します。 ディスクが少なすぎる状態で RAID アレイを再構築しようとすると、再構築エラーが表示されます。機能しているディスクを挿入した後、再構築が開始されます。 このボタンは、RAID アレイが劣化した状態にあり、かつ再構築するための十分なディスクが存在する場合にのみ使用できます。 再構築がすでに進行中のときに、再構築を再起動することはできません。 **注記：** ディスクが故障すると、機能しているディスクの数が、RAID レベルの動作にとって十分でなくなる可能性があります。この場合は、RAID アレイを再構築するために、故障したディスクを機能しているディスクに交換してください。
[Disk#]	このディスクのアレイ内の位置。これは、そのディスクの物理スロットに対応します。 ディスクが FortiGate ユニットから削除された場合、そのドライブ ベイに新しいディスクが挿入されるまで、そのディスクはアレイのメンバではないとしてマークされますが、その位置は保持されます。
[Status]	このディスクのステータス。オプションには、[OK] と [unavailable] があります。 ディスクは、削除されるか、または故障すると [unavailable] になります。
[Member]	選択されたディスクが RAID アレイに含まれているかどうかを表示します。 チェックマークの付いた緑色のアイコンは、このディスクがアレイに含まれていることを示します。 ×印の付いた灰色のアイコンは、このディスクが RAID アレイに含まれていないことを示します。 ディスクは、RAID アレイ内のメンバでない場合でも、ダッシュボードの表示には正常として表示される可能性があります。 ディスクは、使用可能であっても、RAID アレイで使用されていない可能性があります。たとえば、RAID 1 アレイ内に 3 台のディスクが存在する場合は、2 台のみが使用されます。
[Capacity]	このドライブが RAID アレイに提供しているストレージ容量。 このディスクの完全なストレージ容量が、自動的に RAID アレイに使用されます。 RAID アレイの合計ストレージ容量は、ディスクの容量と数、およびアレイの RAID レベルによって異なります。

[Top Application Usage]

[Top Application Usage] には、FortiGate ユニットを通過するトラフィック量がアプリケーションの種類によって分類されて、グラフまたは表のどちらかで表示されます。グラフには、アプリケーションが使用の順番に表示されます。

グラフまたは表の表示から、次の操作を行うことができます。

- 各バーの上にマウス ポインタを置くことにより、トラフィック量を表示する。
- グラフ上のアプリケーションの種類を選択することにより、そのアプリケーションを使用した発信元アドレスや、各発信元アドレスからのセッションによって転送されたデータ量に関する情報を表示する。

[Top Application Usage] のデータ収集は、アプリケーション制御のブラック / ホワイト リストをプロテクション プロファイルに追加することによって開始されます。アプリケーション制御に一致したアプリケーションに関する情報のみが、グラフまたは表に追加されます。ファイアウォール ポリシーによって受け付けられたが、アプリケーション制御が設定されたプロテクション プロファイルが含まれていないセッションは、表示されるデータに含まれません。

[Reset]	すべてのカウントを 0 にリセットします。
[Edit]	モジュールを設定します。
[Refresh]	表示されている情報を更新します。
[Close]	モジュールを閉じます。
[Applications]	使用の順番でのアプリケーション名。
[Bytes] または [Messages]	*[Sort Criteria]* の設定に応じてバイト数またはメッセージ数で表されたトラフィック量。

[Top Application Usage] モジュールを設定するには、*[System]*、*[Dashboard]*、*[Usage]* の順に選択し、[Top Application Usage] モジュールのタイトル バーにある *[編集]* アイコンを選択します。

[Top Application Usage] のカスタム表示

[Custom Widget Name]	このウィジェットの新しい名前を入力します。このフィールドはオプションです。
[Sort Criteria]	アプリケーションを *[Bytes]* または *[Messages]* のどちらの数で並べ替えるかを選択します。
[Application Details]	このウィジェットに表示されるアプリケーション情報に関する詳細情報。
[Report By]	*[Source Address]* または *[Destination Address]* を選択します。
[Display User Name]	IP アドレスの代わりにユーザ名 (既知の場合) を表示するには、このチェック ボックスをオンにします。
[Resolve Host Name]	IP アドレスを表示する代わりに、逆 DNS 参照を使用してホスト名を決定する場合に選択します。
[VDOM]	監視する VDOM を選択するか、または *[Global]* を選択します。このオプションは、グローバル管理者のみが使用できます。VDOM 管理者には、自分の VDOM のみが表示されます。
[Display Format]	*[Chart]* または *[Table]* の表示を選択します。
[Top Entries To Show]	上位 *5*、*10*、*15*、または *20* 個のアプリケーションの表示を選択します。
[Refresh Interval]	表示の更新間隔 (秒単位) を選択します。範囲は 10 ～ 240 秒です。[0] を選択すると、更新が無効になります。また、モジュール ヘッダにある *[更新]* アイコンを使用して更新することもできます。

[Disk Status]

[Disk Status] ウィジェットを使用すると、現在 FortiGate ユニットにインストールされている各ディスクのステータスを表示できます。このステータスには、使用されている領域の容量と、使用可能な空き領域の容量が含まれます。*[System]*、*[Maintenance]*、*[Disk]* の順に選択することによって、ディスクのステータスに関するより詳細な情報を参照できます。[Disk] ページには、ディスクの稼働状態、RAID イベント、ディスクの視覚的な表現、およびディスクの管理の設定に関連した情報が表示されます。管理の設定の例としては、たとえば、3 つのパーティションをそれぞれ、ファームウェア用、ログ用、WAN オプション ストレージ用に設定するといった場合があります。ディスク管理の詳細については、216 ページの「[Disk]」 を参照してください。

[P2P Usage]

[P2P Usage] には、サポートされている各インスタント メッセージング クライアントの合計バイト数と合計帯域幅が表示されます。これらのクライアントは、WinNY、BitTorrent、eDonkey、Guntella、および KaZaa です。[P2P Usage] では、ウィジェットのデフォルトの名前しか変更できません。

[P2P Usage] ウィジェットの名前のみを変更できます。名前を変更するには、タイトル バーにある *[編集]* アイコンを選択し、*[Custom Widget Name]* フィールドに名前を入力します。*[OK]* を選択して、変更を保存します。

[Per-IP Bandwidth Usage]

[Per-IP Bandwidth Usage] ウィジェットを使用すると、IP アドレスごとのセッション データを表示できます。このデータには、トラフィックを開始した各 IP アドレス (と現在の帯域幅消費) が表示され、これは [Top Sessions] ウィジェット同じです。トラフィックを開始したユーザの IP アドレスを表示する代わりに、編集ウィンドウで *[Resolve Host Name]* を選択することによって、そのユーザの名前を表示することを選択できます。

このウィジェットのタイトル バー領域にある *[編集]* アイコンを選択すると、このウィジェットのいくつかの設定を設定できます。設定を保存するには、*[OK]* を選択する必要があります。

[Per-IP Bandwidth Usage] のカスタム表示

[Custom Widget Name]	このウィジェットの新しい名前を入力します。このフィールドはオプションです。
[Resolve Host Name]	IP アドレスの代わりに名前を表示する場合に選択します。
[Display Format]	[Chart] または [Table] のどちらかを選択します。[Chart] を選択すると、情報が棒グラフとして表示されます。[Table] を選択すると、情報が表内に表示されます。
[Top Entries to Show]	表またはグラフ内に表示される上位エントリを選択します。
[Refresh Interval]	表示の更新間隔 (秒単位) を選択します。範囲は 10 ～ 240 秒です。[0] を選択すると、更新が無効になります。また、モジュール ヘッダにある *[更新]* アイコンを使用して更新することもできます。

[VoIP Usage]

[VoIP Usage] ウィジェットでは、現在のアクティブな VoIP 通話 (over SIP および SCCP プロトコルを使用) のほか、破棄された通話、失敗した通話、または応答のなかった通話を表示できます。実際に成功した通話数や、このウィジェット内の情報を最後にクリアしてからの合計の通話数を容易に確認できます。

[VoIP Usage] ウィジェットの名前のみを変更できます。名前を変更するには、タイトル バーにある *[編集]* アイコンを選択し、*[Custom Widget Name]* フィールドに名前を入力します。*[OK]* を選択して、変更を保存します。

[IM Usage]

[IM Usage] ウィジェットには、インスタント メッセージング クライアントと、ネットワーク上で実行されているそれらのクライアントの動作に関する詳細が表示されます。このウィジェット内から、ユーザ、チャット、メッセージ、クライアント間のファイル転送、および実行されたすべての音声チャットに関連した情報を表示できます。[IM Usage] は、これらの情報を IM、Yahoo!、AIM、および ICQ に関して提供します。

[IM Usage] ウィジェットの名前のみを変更できます。名前を変更するには、タイトル バーにある *[編集]* アイコンを選択し、*[Custom Widget Name]* フィールドに名前を入力します。*[OK]* を選択して、変更を保存します。

[FortiGuard]

FortiGuard Center から受信された FortiGuard 警告情報のみを表示する、個別の [Alert Message Console] ウィジェットを設定できます。新しく作成された [Alert Message Console] ウィジェットの名前を変更し、*[FortiGuard security alerts]* オプションを選択することにより、警告の受信とこのウィジェット上への表示を有効にすることができます。

FortiGuard は、FortiGuard Center の現在のニュースや RSS フィードに関連した情報を提供します。このバージョンの [Alert Message Console] ウィジェットには、FortiGuard サブスクライバに最新のニュースや脅威について通知する、FortiGuard Center からの RSS フィードが表示されます。

[FortiGuard] ウィジェットを有効にするには、追加された [Alert Message Console] ウィジェットで、タイトル バー領域にある *[編集]* アイコンを選択します。表示される *[Custom Alert Display]* のリストで、*[FortiGuard security alerts]* の横にあるチェック ボックスをオンにします。

ファームウェア管理方法

この項には、現在の設定を正しくバックアップする方法や、アップグレードが失敗した場合に実行すべきことに関する重要な情報が含まれているため、アップグレードする前にこの項を確認することをお勧めします。

また、新しいファームウェア メンテナンス リリースがリリースされた場合は、『FortiOS ハンドブック』の「新機能」の章も確認する必要があります。この章には、現在の設定では問題が発生する可能性のある変更や新機能に関する貴重な情報が含まれています。

ファームウェア イメージに加えて、フォーティネットではパッチ リリース、つまり重要な問題を解決するためのメンテナンス リリース ビルドをリリースしています。ファームウェアをアップグレードする前に、パッチ リリースのリリース ノートを確認することを強くお勧めします。以下の手順に従ってください。

- パッチ リリースのリリース ノートをダウンロードして確認します。
- パッチ リリースをダウンロードします。
- 現在の設定をバックアップします。
- 64 ページの「アップグレードの前のファームウェアのテスト」の手順を使用して、パッチ リリースをインストールします。
- パッチリリースインストール前の状態の設定が適用されていることを確認します。

リリース ノートを確認せずにパッチ リリースをインストールしたり、ファームウェアをテストしたりすると、設定が変更されたり、予期しない問題が発生したりすることがあります。

また、FortiOS 4.0 では、トランスペアレント モードのときに NAT を使用するように FortiGate を設定することもできます。詳細については、Fortinet Knowledge Center の記事「トランスペアレント モードでの NAT の設定」を参照してください。

FortiGate ユニット上でバーチャル ドメイン (VDOM) を有効にすると、システム ファームウェアのバージョンがグローバルに設定されます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には、以下のトピックが含まれています。

注記：[Backup and Restore] ページで使用可能な設定 (FortiManager ユニットへのリモートでのバックアップなど) の詳細については、199 ページの「システム - メンテナンス」を参照してください。

設定のバックアップ

注意：パッチ リリースのインストール、ファームウェアのアップグレード / ダウングレード、または工場出荷のデフォルト値への設定のリセットの前には、常に設定をバックアップしてください。

設定を、ローカル PC、FortiManager ユニット、FortiGuard Management サーバ、または USB キーにバックアップできます。また、FortiGuard Analysis and Management Service が有効になっている場合は、FortiGuard Management サーバにもバックアップできます。ローカルのハードドライブがある場合は、そのドライブにも設定ファイルをバックアップできます。そのドライブ上でパーティションが有効になっている場合は、バックアップするすべての設定ファイルが、ログとシステム データ用に作成されている特定のパーティションに格納されます。

FortiOS 4.0 にアップグレードする前に、FortiGate ユニットのすべての設定をバックアップすることをお勧めします。これにより、FortiOS 3.0 MR7 へのダウングレードが必要になり、これらの設定を復元することになっても、すべての設定が引き続き使用可能なことが保証されます。

Web ベース マネージャでの設定のバックアップ

設定を、FortiManager ユニットや FortiGuard Management サーバなどのさまざまな場所にバックアップできます。次の手順は、Web ベース マネージャで現在の設定を正しくバックアップする方法を示しています。

Web ベース マネージャで設定ファイルをバックアップするには

1 *[System]*、*[Dashboard]*、*[Status]* の順に選択します。

2 [System Information] ウィジェットで、*[System Configuration]* 行にある *[Backup]* を選択します。

[Backup] ページに自動的にリダイレクトされます。

3 設定ファイルが格納される場所を選択します。

4 設定ファイルを暗号化するには、[Encrypt configuration file] の横にあるチェック ボックスをオンにします。

VPN証明書を保存するために設定ファイルを暗号化する場合は、*[Encrypt configuration file]* チェック ボックスをオンにして、パスワードを入力した後、パスワードを再度入力して確認します。

5 *[Backup]* を選択します。

6 ファイルを保存します。

CLI を使用した設定のバックアップ

TFTP または FTP サーバ、あるいは USB キーを使用して、設定ファイルをバックアップできます。また、FortiGuard Analysis and Management Service が設定されている場合は、FortiGuard Management サーバにも設定をバックアップできます。

CLI で設定をバックアップする場合は、設定全体をバックアップするか (`execute backup full-config`)、または設定の一部をバックアップするか (`execute backup config`) を選択できます。バーチャル ドメインが設定されている場合は、特定の管理者がバックアップを許可される対象についての制限があります。詳細については、『*FortiGateCLI リファレンス*』を参照してください。

次の手順は、CLI で現在の設定をバックアップする方法を示しており、読者が次のコマンドに精通していることを前提にしています次の手順で使用されている個々のコマンドの詳細については、『*FortiGateCLI リファレンス*』を参照してください。

CLI を使用して設定ファイルをバックアップするには

1 設定ファイルを USB キーにバックアップするには、次のコマンドを入力します。

```
execute backup config usb <backup_filename> <encrypt_passwd>
```

2 設定ファイルを TFTP または FTP サーバにバックアップするには、次のコマンドを入力します。

```
execute backup config {tftp | ftp} <backup_filename>
<tftp_server_ipaddress> <ftp server [:ftp port] <ftp_username>
<ftp_passwd> <encrypt_passwd>
```

3 設定を FortiGuard Management サーバにバックアップするには、次のコマンドを入力します。

```
execute backup config management-station <comment>
```

CLI を使用して設定ファイル全体をバックアップするには

設定ファイル全体をバックアップするには、次のコマンドを入力します。

```
execute backup full-config {tftp | ftp | usb} <backup_filename>
<backup_filename> <tftp_server_ipaddress> <ftp server [:ftp
port] <ftp_username> <ftp_passwd> <encrypt_passwd>
```

USB キーへの設定のバックアップ

FortiGate ユニットに USB ポートが装備されている場合は、現在の設定を USB キーにバックアップできます。設定ファイルを USB キーにバックアップする場合は、その USB キーが FAT16 ディスクとしてフォーマットされていることを確認してください。FAT16 フォーマットは、サポートされている唯一のパーティションの種類です。詳細については、202 ページの「USB ディスクのフォーマット」を参照してください。

先に進む前に、FortiGate ユニットの USB ポートに USB キーが挿入されていることを確認してください。

設定を USB キーにバックアップするには

1 *[System]*、*[Dashboard]*、*[Status]* の順に選択します。

2 [System Information] ウィジェットで、*[System Configuration]* 行にある *[Backup]* を選択します。

[Backup] ページに自動的にリダイレクトされます。

3 *[USB Disk]* を選択します。

VPN証明書を保存するために設定ファイルを暗号化する場合は、*[Encrypt configuration file]* チェック ボックスをオンにして、パスワードを入力した後、パスワードを再度入力して確認します。

4 *[Backup]* を選択します。

5 ファイルを保存します。

CLI または Web ベース マネージャのいずれかから設定ファイルを正常にバックアップしたら、FortiOS 4.0 へのアップグレードに進みます。

アップグレードの前のファームウェアのテスト

新しいファームウェア バージョン、あるいはメンテナンスまたはパッチ リリースにアップグレードする前に、インストールする必要のあるファームウェアをテストすることもできます。ファームウェアをテストすることによって、新機能や既存の機能の変更に精通できるだけでなく、現在の設定がこのファームウェアで動作するかどうかも確認できます。ファームウェア イメージをテストするには、システムの再起動からインストールした後、それをシステム メモリに保存します。ファームウェアがシステム メモリに保存された後、FortiGate ユニットは、そのファームウェアを現在の設定で使用して動作します。

次の手順では、ファームウェアが完全にはインストールされません。FortiGate ユニットは、次回の再起動時に、その FortiGate ユニットに最初にインストールされていたファームウェアを使用して動作します。ファームウェアを完全にインストールするには、65 ページの「FortiGate ユニットのアップグレード」の手順を使用します。

次の手順は、通常のファームウェア イメージまたはパッチ リリースのどちらに対しても実行できます。

次の手順では、ファームウェア イメージがすでに管理コンピュータにダウンロードされていることを前提にしています。

アップグレードの前にファームウェア イメージをテストするには

1 新しいファームウェア イメージ ファイルを、TFTP サーバのルート ディレクトリにコピーします。

2 TFTP サーバを起動します。

3 CLI にログインします。

4 次のコマンドを入力して、TFTP サーバを実行しているコンピュータに ping を発行します。

```
execute ping <server_ipaddress>
```

TFTP サーバを実行しているコンピュータに ping を発行すると、FortiGate ユニットと TFTP サーバが正常に接続されていることが確認されます。

5 次のコマンドを入力して、FortiGate ユニットを再起動します。

```
execute reboot
```

6 FortiGate ユニットが再起動すると、一連の起動メッセージが表示されます。次のメッセージが表示されたら、直ちにいずれかのキーを押して、システムの起動を中断します。

```
Press any key to display configuration menu…
```

いずれかのキーを押すまでに 3 秒しかありません。すぐにキーを押すさないと FortiGate ユニットが再起動するため、ログインし、手順 5. ～ 6. をもう一度繰り返さなければならなくなります。

起動プロセスを正常に中断できた場合は、次のメッセージが表示されます。

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

7 G を押して、TFTP サーバから新しいファームウェア イメージを取得します。

次のメッセージが表示されます。

```
Enter TFTP server address [192.168.1.168] :
```

8 TFTP サーバのアドレスを入力し、Enter キーを押します。

次のメッセージが表示されます。

```
Enter Local Address [192.168.1.188] :
```

9 FortiGate ユニットの内部の IP アドレスを入力します。

この IP アドレスは、FortiGate ユニットを TFTP サーバに接続します。この IP アドレスは TFTP サーバと同じネットワーク上に存在する必要がありますが、ネットワーク上の別のデバイスの IP アドレスを使用しないようにしてください。

次のメッセージが表示されます。

```
Enter File Name [image.out] :
```

10 ファームウェア イメージ ファイルの名前を入力し、*Enter* キーを押します。

TFTP サーバによってファームウェア イメージ ファイルが FortiGate ユニットにアップロードされ、次のメッセージが表示されます。

```
Save as Default firmware/Backup firmware/Run image without
  saving: [D/B/R]
```

11 R を押します。

FortiGate ファームウェア イメージがインストールされ、システム メモリに保存します。FortiGate ユニットが起動され、新しいファームウェア イメージが現在の設定で実行されます。

ファームウェアのテストを完了したら、FortiGate ユニットを再起動して、元のファームウェアの使用を再開できます。

FortiGate ユニットのアップグレード

アップグレードが成功し、FortiGate ユニットにハード ドライブが装備されている場合は、*[System]*、*[Maintenance]*、*[Backup and Restore]* の順に選択して表示されるページにある *[Boot alternate firmware]* オプションを使用できます。このオプションを使用すると、2 つのファームウェア イメージ (たとえば、FortiOS 3.0 MR7 と FortiOS 4.0) をダウングレードまたはアップグレードに使用できます。

アップグレードが成功しなかった場合は、68 ページの「以前のファームウェア イメージへの復帰」に進んでください。

次の手順は、パッチ リリースをインストールするときにも使用できます。パッチ リリースとは、特定の問題を解決するが、新機能や既存の機能の変更は含まれていないファームウェア イメージのことです。パッチ リリースは、最新のファームウェア バージョンにアップグレードされているかどうかにかかわらずインストールできます。

Web ベース マネージャでの FortiOS 4.0 へのアップグレード

注意 : パッチ リリースのインストール、ファームウェアのアップグレード / ダウングレード、または工場出荷のデフォルト値への設定のリセットの前には、常に設定をバックアップしてください。

次の手順は、Web ベース マネージャで FortiOS 4.0 にアップグレードする方法を示しています。CLI を使用して FortiOS 4.0 にアップグレードすることをお勧めします。CLI のアップグレード手順では、現在のファイアウォール設定がすべて工場出荷のデフォルト設定に戻ります。

Web ベース マネージャで FortiOS 4.0 にアップグレードするには

1 ファームウェア イメージ ファイルを管理コンピュータにダウンロードします。

2 Web ベース マネージャにログインします。

3 *[System]*、*[Status]* の順に選択し、*[System Information]* ウィジェットを見つけます。

4 *[Firmware Version]* の横にある *[Update]* を選択します。

5 ファームウェア イメージ ファイルのパスとファイル名を入力するか、または *[Browse]* を選択してファイルを見つけます。

6 *[OK]* を選択します。

FortiGate ユニットは、ファームウェア イメージ ファイルをアップロードし、新しいファームウェア バージョンにアップグレードした後、再起動して FortiGate ログインを表示します。この処理には数分かかることがあります。

アップグレードが正常にインストールされた場合は、次の操作を行います。

- FortiGate ユニットに ping を発行して、引き続き接続されていることを確認します。
- ブラウザのキャッシュをクリアし、Web ベース マネージャにログインします。

Web ベースマネージャに再ログイン後、引き継ぐべき設定を保存する必要があります。設定には、FortiOS 3.0 MR7 から引き継がれているものと、引き継がれていないもの (特定の IPS グループ設定など) があります。引き継がれた設定を保存するには、*[System]*、*[Maintenance]*、*[Backup and Restore]* の順に選択します。

注記 : FortiOS4.0 にアップグレードした後、FortiGuard Distribution Network (FDN) から最新の FortiGuard シグネチャを取得するために [Update Now] を実行してください。ファームウェアに含まれているシグネチャが、FDN で現在入手可能なシグネチャより古い可能性があるためです。

CLI を使用した FortiOS 4.0 へのアップグレード

注意 : パッチ リリースのインストール、ファームウェアのアップグレード / ダウングレード、または工場出荷のデフォルト値への設定のリセットの前には、常に設定をバックアップしてください。

次の手順では、TFTP サーバを使用してファームウェアをアップグレードします。CLI のアップグレード手順では、現在のファイアウォール設定がすべて工場出荷のデフォルト設定に戻ります。

CLI でファームウェアをアップグレードする方法の詳細については、Fortinet Knowledge Base の記事「CLIの手順でTFTPを使用したFortiGateファームウェアのロード」を参照してください。

次の手順では、ファームウェア イメージがすでに管理コンピュータにダウンロードされていることを前提にしています。

CLI を使用して FortiOS 4.0 にアップグレードするには

1 新しいファームウェア イメージ ファイルを、TFTP サーバのルート ディレクトリにコピーします。

2 TFTP サーバを起動します。

3 CLI にログインします。

4 次のコマンドを入力して、TFTP サーバを実行しているコンピュータに ping を発行します。

```
execute ping <server_ipaddress>
```

TFTP サーバを実行しているコンピュータに ping を発行すると、FortiGate ユニットと TFTP サーバが正常に接続されていることが確認されます。

5 次のコマンドを入力して、ファームウェア イメージを TFTP サーバから FortiGate ユニットにコピーします。

```
execute restore image <name_str> <tftp_ipv4>
```

ここで、<name_str> はファームウェア イメージ ファイルの名前であり、<tftp_ipv4> は TFTP サーバの IP アドレスです。たとえば、ファームウェア イメージ ファイルの名前が image.out であり、TFTP サーバの IP アドレスが 192.168.1.168 の場合は、次のコマンドを入力します。

```
execute restore image.out 192.168.1.168
```

FortiGate ユニットから、次のようなメッセージが表示されます。

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

6 y を押します。

FortiGate ユニットは、ファームウェア イメージ ファイルをアップロードし、新しいファームウェア バージョンにアップグレードした後、再起動します。この処理には数分かかります。

7 CLI に再接続します。

8 次のコマンドを入力して、ファームウェア イメージが正常にインストールされたことを確認します。

```
get system status
```

9 CLI からアンチウイルスおよび攻撃定義を更新するには、次のコマンドを入力します。

```
execute update-now
```

代わりに、Web ベース マネージャからアンチウイルスおよび攻撃定義を更新する場合は、Web ベース マネージャにログインし、*[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択します。

アップグレードの確認

Web ベース マネージャに再ログインすると、FortiOS 3.0 MR7 の設定のほとんどが引き継がれています。たとえば、*[System]*、*[Network]*、*[Options]* の順に選択すると、FortiOS 3.0 MR7 の設定から引き継がれた DNS 設定を確認できます。

どの設定が引き継がれたかを確認する必要があります。また、管理アクセスの設定も引き継がれたことを確認する必要があります。設定を確認することにより、FortiOS 4.0 の新機能や変更に精通することができます。

設定は、次の操作によって確認できます。

- Web ベース マネージャで、各メニューおよびタブを操作する
- CLI で show シェル コマンドを使用する

以前のファームウェア イメージへの復帰

アップグレードが正常にインストールされなかった場合は、以前のファームウェア イメージ（または、FortiOS 3.0 などのバージョン）への復帰が必要になることがあります。次の手順は、Web ベース マネージャまたは CLI のどちらかを使用して以前のファームウェア イメージに正しくダウングレードする方法を示しています。また、以前の設定を復元する方法に関する手順も含まれています。

このトピックには、以下の内容が含まれています。

Web ベース マネージャでの以前のファームウェアへのダウングレード

注意：パッチ リリースのインストール、アップグレード / ダウングレード、または工場出荷のデフォルト値へのリセットの前には、常に設定をバックアップしてください。

以前のファームウェアにダウングレードする場合は、次の設定のみが保持されます。

- 動作モード
- インタフェース IP/ 管理 IP
- ルートの静的テーブル
- DNS 設定
- VDOM のパラメータ / 設定
- 管理者ユーザのアカウント
- セッション ヘルパ
- system accprofile

FortiOS 4.0 で追加の設定を作成した場合は、ダウングレードの前に現在の設定をバックアップするようにしてください。詳細については、62 ページの「設定のバックアップ」を参照してください。

Web ベース マネージャでダウングレードするには

1 *[System]*、*[Dashboard]*、*[Status]* の順に選択し、*[System Information]* ウィジェットを見つけます。

2 *[Firmware Version]* の横にある *[Update]* を選択します。

3 ファームウェア イメージ ファイルのパスとファイル名を入力するか、または *[Browse]* を選択してファイルを見つけます。

4 *[OK]* を選択します

次のメッセージが表示されます。

```
This version will downgrade the current firmware version.Are you
sure you want to continue?
```

5 *[OK]* を選択します

FortiGate ユニットは、ファームウェア イメージ ファイルをアップロードし、古いファームウェア バージョンに戻した後、設定をリセットし、再起動して FortiGate ログインを表示します。この処理には数分かかります。

6 Web ベース マネージャにログインします。

[System]、*[Dashboard]*、*[Status]* の順に選択して、*[System Information]* に表示されているファームウェア バージョンが正しいファームウェアに変更されていることを確認します。

ダウングレードの確認

以前のファームウェアに正常にダウングレードした後、接続と設定を確認します。Web ベース マネージャに接続できない場合は、管理アクセスの設定と内部ネットワークの IP アドレスが正しいことを確認してください。ダウングレードによって、設定がデフォルト設定に変更される可能性があります。

CLI を使用した以前のファームウェアへのダウングレード

注意：パッチ リリースのインストール、アップグレード / ダウングレード、または工場出荷のデフォルト値へのリセットの前には、常に設定をバックアップしてください。

以前のファームウェアにダウングレードする場合は、次の設定のみが保持されます。

- 動作モード
- インタフェース IP/ 管理 IP
- ルートの静的テーブル
- DNS 設定
- VDOM のパラメータ / 設定
- 管理者ユーザのアカウント
- セッション ヘルパ
- system accprofile

FortiOS 4.0 で追加の設定を作成した場合は、ダウングレードの前に設定をバックアップするようにしてください。詳細については、62 ページの「設定のバックアップ」を参照してください。

次の手順では、ファームウェア イメージがすでに管理コンピュータにダウンロードされていることを前提にしています。

CLI を使用してダウングレードするには

1. 新しいファームウェア イメージ ファイルを、TFTP サーバのルート ディレクトリにコピーします。
2. TFTP サーバを起動します。
3. CLI にログインします。
4. 次のコマンドを入力して、 TFTP サーバを実行しているコンピュータに ping を発行します。

   ```
   execute ping <server_ipaddress>
   ```

   TFTP サーバを実行しているコンピュータに ping を発行すると、FortiGate ユニットと TFTP サーバが正常に接続されていることが確認されます。
5. 次のコマンドを入力して、ファームウェア イメージを TFTP サーバから FortiGate ユニットにコピーします。

   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```

   ここで、<name_str> はファームウェア イメージ ファイルの名前であり、<tftp_ipv4> は TFTP サーバの IP アドレスです。たとえば、ファームウェア イメージ ファイルの名前が image.out であり、TFTP サーバの IP アドレスが 192.168.1.168 の場合は、次のコマンドを入力します。

   ```
   execute restore image tftp image.out
   192.168.1.168
   ```

   FortiGate ユニットから、次のメッセージが表示されます。

   ```
   This operation will replace the current firmware version!Do you
   want to continue? (y/n)
   ```

6 y を押します。

FortiGate ユニットによってファームウェア イメージ ファイルがアップロードされます。ファイルがアップロードされた後、次のようなメッセージが表示されます。

```
Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

7 y を押します。

FortiGate ユニットは、古いファームウェア バージョンに戻し、設定を工場出荷のデフォルト値にリセットして、再起動します。この処理には数分かかります。

FortiGate ユニットによってファームウェアがアップロードされたら、FortiGate ユニットはデフォルト IP アドレスを含めてデフォルト設定に戻されているため、IP アドレスを再設定する必要があります。IP アドレスの設定については、インストール ガイドを参照してください。

8 CLI に再接続します。

9 次のコマンドを入力して、ファームウェア イメージが正常にインストールされたことを確認します。

```
get system status
```

以前の設定を復元するには、71 ページの「設定の復元」を参照してください。

設定の復元

以前のファームウェアにダウングレードした後、設定が引き継がれていない可能性があります。FortiOS 4.0 にアップグレードする前に保存した設定ファイルを使用して、以前のファームウェアの設定を復元できます。

次の手順は、最新のパッチ リリースまたはメンテナンス リリースをインストールした後に設定を復元するときにも使用できます。

Web ベース マネージャでの設定の復元

次の手順では、Web ベース マネージャで以前のファームウェア設定を復元します。

Web ベース マネージャで設定を復元するには

1 Web ベース マネージャにログインします。

2 *[System]*、*[Dashboard]*、*[Status]* の順に選択し、[System Information] ウィジェットを見つけます。

3 [System Configuration] 行で *[Restore]* を選択して、*[Local PC]*、*[FortiManager]*、または *[FortiGuard]*（FortiGate ユニットに FortiGuard Analysis and Management Service が設定されている場合）のいずれかから設定を復元します。

[Restore] ページに自動的にリダイレクトされます。

4 ファイルの場所を入力するか、または *[Browse]* を選択してファイルを見つけます。

必要に応じて、設定ファイルのパスワードを入力します。

5 *[Restore]* を選択します。

FortiGate ユニットによって設定が復元されます。FortiGate ユニットが再起動するため、この処理には数分かかることがあります。

Web ベース マネージャにログインし、さまざまなメニューやタブを操作することによって、設定が復元されていることを確認できます。

CLI での設定の復元

次の手順では、CLI で以前のファームウェア設定を復元します。

CLI で設定を復元するには

1 バックアップされた設定ファイルを、 TFTP サーバのルート ディレクトリにコピーします。

2 TFTP サーバを起動します。

3 CLI にログインします。

4 次のコマンドを入力して、 TFTP サーバを実行しているコンピュータに ping を発行します。

```
execute ping <server_ipaddress>
```

TFTP サーバを実行しているコンピュータに ping を発行すると、FortiGate ユニットと TFTP サーバが正常に接続されていることが確認されます。

5 次のコマンドを入力して、バックアップされた設定ファイルをコピーして FortiGate ユニット上に復元します。

```
execute restore allconfig <name_str> <tftp_ipv4> <passwrd>
```

ここで、<name_str> はバックアップされた設定ファイルの名前、<tftp_ipv4> は TFTP サーバの IP アドレス、<passwrd> は設定をバックアップしたときに入力したパスワードです。たとえば、バックアップされた設定ファイルが confall、TFTP サーバの IP アドレスが 192.168.1.168、パスワードが ghrffdt123 の場合は、次のコマンドを入力します。

```
execute restore allconfig confall 192.168.1.168 ghrffdt123
```

FortiGate ユニットから、次のメッセージが表示されます。

```
This operation will overwrite the current settings and the
system will reboot!
Do you want to continue? (y/n)
```

6 y を押します。

FortiGate ユニットによって、バックアップされた設定ファイルがアップロードされます。ファイルがアップロードされた後、次のようなメッセージが表示されます。

```
Getting file confall from tftp server 192.168.1.168
##
Restoring files...
All done.Rebooting...
```

この処理には数分かかることがあります。

CLI の show シェル コマンドを使用して設定が復元されていることを確認するか、または Web ベース マネージャにログインします。

バーチャル ドメインの使用

この項では、バーチャル ドメイン (VDOM) とそのいくつかの利点、および VDOM を使用して FortiGate ユニットを複数の仮想ユニットとして動作させる方法について説明します。

FortiGate ユニット上で VDOM を有効にすると、バーチャル ドメインの設定を FortiGate ユニットにさまざまに行います。

バーチャル ドメインの操作を開始するには、77 ページの「バーチャル ドメインの有効化」を参照してください。

この項には、以下のトピックが含まれています。

バーチャル ドメイン

バーチャル ドメイン (VDOM) は、FortiGate ユニットを、複数の独立したユニットとして機能する 2 つ以上の仮想ユニットに分割するための方法です。これにより、FortiGate ユニット 1 台で、組織内の複数の部門や個別の組織それぞれにサービスを提供したり、サービス プロバイダのマネージド セキュリティ サービスの基盤として機能させたりするなど、優れた柔軟性を発揮します。

VDOM の利点

VDOM の利点には、次のいくつかがあります。

- 管理の容易性
- 継続的なセキュリティのメンテナンス
- 物理的なスペースと電力の削減

管理の容易性

VDOM は個別のセキュリティ ドメインであり、これによって個別のゾーン、ユーザ認証、ファイアウォール ポリシー、ルーティング、および VPN 設定が可能になります。また、VDOM を使用すると、一度に多数のルートまたはファイアウォール ポリシーを管理する必要がなくなるため、複雑な設定の管理を簡略化することもできます。詳細については、74 ページの「VDOM の設定」を参照してください。

デフォルトでは、各 FortiGate ユニットに、ルートという名前の VDOM が存在します。この VDOM には、FortiGate の物理インタフェース、モデム、VLAN サブインタフェース、ゾーン、ファイアウォール ポリシー、ルーティング設定、および VPN 設定のすべてが含まれています。

また、その VDOM に制限された管理者アカウントを割り当てることもできます。VDOM が特定の組織にサービスを提供するように作成されている場合は、この機能により、その組織は独自の設定を管理できるようになります。

SNMP、ロギング、アラート メール、FDN ベースの更新、NTP ベースの時刻設定などの管理システムは、管理 VDOM 内のアドレスとルーティングを使用してネットワークと通信します。これらの管理システムは、管理バーチャル ドメインと通信するネットワーク リソースにのみ接続できます。管理 VDOM は、デフォルトでルートに設定されていますが、変更することもできます。詳細については、84 ページの「管理 VDOM の変更」を参照してください。

継続的なセキュリティのメンテナンス

VDOM に入ったパケットは、その VDOM に閉じ込められます。VDOM 内に、VDOM 内の VLAN サブインタフェース間またはゾーン間を結ぶためのファイアウォール ポリシーを作成できます。パケットがバーチャル ドメインの境界を内部で横断することはありません。パケットが VDOM 間を移動するには、物理インタフェース上のファイアウォールを通過する必要があります。次に、パケットは異なるインタフェース上の別の VDOM に到着しますが、別のファイアウォールを通過してからでないとそこに入ることはできません。どちらの VDOM も同じ FortiGate ユニット上に存在します。VDOM 間リンクは、Internal インタフェースであるという点でこの動作を変更します。ただし、通過するパケットには物理インタフェース上とまったく同じセキュリティの手段がとられます。

VDOM が設定されていない場合、管理者は FortiGate ユニット全体にわたる設定に容易にアクセスできます。これにより、セキュリティ上の問題や、広範囲に及ぶ設定エラーが発生することがあります。しかし、管理者の権限は 1 つの VDOM に限定されます。1 つの VDOM 上の管理者は、別の VDOM に関する情報を変更できません。設定が変更されたり、エラーがあったりしたとしても、その VDOM にのみ適用されるため、潜在的なダウンタイムが制限されます。

FortiGate ユニットの他の機能はグローバルであり、そのユニット上のすべての VDOM に適用されます。つまり、不正侵入防御設定、アンチウイルス設定、Web フィルタ設定、プロファイル設定などはすべて、1 つしか存在しません。VDOM ではまた、ファームウェア バージョンのほか、アンチウイルスおよび攻撃データベースも共有されます。動作モード（NAT/ ルートまたはトランスペアレント）は、VDOM ごとに個別に選択できます。共有される設定の完全なリストについては、76 ページの「グローバル設定」を参照してください。

物理的なスペースと電力の削減

VDOM の数を増やすために、追加のハードウェアや出荷は必要なく、既存のネットワークへの変更もごくわずかです。追加の物理的なスペースも必要ありません。使用している VDOM のために購入したライセンスのサイズによってのみ制限されます。

ほとんどの FortiGate ユニットは、デフォルトで、NAT/ ルートとトランスペアレント モードの任意の組み合わせによる最大 10 個の VDOM をサポートします。ハイエンドの FortiGate モデルの場合は、VDOM の最大数を 25、50、100、または 250 に増やすためのライセンス キーを購入できます。詳細については、79 ページの「VDOM ライセンス」を参照してください。

バーチャル ドメイン設定が有効になっており、デフォルトの super_admin としてログインした場合は、*[System]*、*[Dashboard]*、*[Status]* の順に選択し、*[License Information]* ウィジェットにある *[Virtual Domain]* を参照することにより、FortiGate ユニット上でサポートされているバーチャル ドメインの最大数を確認できます。

VDOM の詳細については、『*FortiGate VLAN および VDOM ガイド*』を参照してください。

注記： FortiAnalyzer ユニット上での設定中、VDOM は、FortiAnalyzer ユニットのライセンスによって許可されている FortiGate ユニットの最大数に向けてカウントされます。登録されるデバイスの総数は、FortiAnalyzer ユニットの *[Dashboard]* ページの *[License Information]* で確認できます。

VDOM の設定

VDOM を設定して使用するには、バーチャル ドメイン設定を有効にする必要があります。詳細については、77 ページの「バーチャル ドメインの有効化」を参照してください。

VDOM は、VLAN サブインタフェース、ゾーン、ファイアウォール ポリシー、ルーティング設定、および VPN 設定を追加することによって設定できます。また、ルート VDOM から他の VDOM に物理インタフェースを移動したり、ある VDOM から別の VDOM に VLAN サブインタフェースを移動したりすることもできます。VLAN の詳細については、『*FortiGate VLAN および VDOM ガイド*』を参照してください。

以下の設定は、1 つのバーチャル ドメインに限定され、複数のバーチャル ドメインで共有されることはありません。VDOM の標準管理者には、これらの設定のみが表示されます。また、デフォルトの super_admin もこれらの設定にアクセスできますが、最初に設定対象の VDOM を選択する必要があります。

表 6: VDOM の設定

設定オブジェクト	詳細情報の参照先
システム	
ネットワーク - ゾーン	106 ページの「ゾーンの設定」
ネットワーク - DNS データベース	113 ページの「FortiGate DNS サービスの設定」
ネットワーク - Web プロキシ	117 ページの「Explicit Web プロキシの設定」
ネットワーク - ルーティング テーブル (トランスペアレント モード)	120 ページの「ルーティング テーブル (トランスペアレント モード)」
ネットワーク - モデム	107 ページの「モデム インタフェースの設定」
無線 - 設定	126 ページの「無線の設定」
無線 MAC フィルタ	128 ページの「無線 MAC フィルタ」
無線モニタ	129 ページの「無線モニタ」
無線 - 悪意のある AP	130 ページの「悪意のある AP の検出」
DHCP - サービス	134 ページの「DHCP サービスの設定」
DHCP - アドレス リース	136 ページの「アドレス リースの表示」
設定 - 差し替えメッセージ	153 ページの「差し替えメッセージ」
設定 - 動作モード (NAT/ ルートまたは トランスペアレント)	166 ページの「動作モードの変更」
設定 - 管理 IP (トランスペアレント モード)	166 ページの「動作モードの変更」
ルータ	
スタティック	229 ページの「ルータ - スタティック」
ダイナミック	247 ページの「ルータ - ダイナミック」
モニタ	261 ページの「ルータ - モニタ」
ファイアウォール	
ポリシー	265 ページの「ファイアウォール ポリシー」
アドレス	295 ページの「ファイアウォール アドレス」
サービス	301 ページの「ファイアウォール サービス」
スケジュール	309 ページの「ファイアウォール スケジュール」
仮想 IP	313 ページの「ファイアウォール仮想 IP」
仮想 IP グループ	326 ページの「仮想 IP グループ」
仮想 IP、IP プール	327 ページの「IP プールの設定」
負荷分散	339 ページの「ファイアウォール負荷分散」
UTM	
アンチウイルス ファイル フィルタ	358 ページの「アンチウイルス」
不正侵入防御	363 ページの「不正侵入防御」
Web フィルタ	374 ページの「Web フィルタ」
電子メール フィルタ	386 ページの「電子メール フィルタ」
情報漏洩防止	395 ページの「情報漏洩防止」
アプリケーション制御	405 ページの「アプリケーション制御」

表 6: VDOM の設定（続き）

設定オブジェクト	詳細情報の参照先
VoIP	409 ページの「VoIP」
VPN	
IPSec	411 ページの「IPsec VPN」
SSL	427 ページの「SSL VPN」
ユーザ	
ローカル	448 ページの「ローカル ユーザ アカウント」
リモート	449 ページの「リモート認証」
ディレクトリ サービス	454 ページの「ディレクトリ サービス」
PKI	456 ページの「PKI 認証」
ユーザ グループ	457 ページの「ユーザ グループ」
オプション	184 ページの「設定」
モニタ	186 ページの「管理者の監視」
WAN 最適化と Web キャッシュ	437 ページの「WAN 最適化および Web キャッシュ」
エンドポイント NAC	469 ページの「エンドポイント」
無線コントローラ	479 ページの「無線コントローラ」
ログとレポート	
ロギング設定	490 ページの「FortiGate ユニットでのログの保存方法」
アラート メール	495 ページの「アラート メール」
イベント ログ	496 ページの「ログ メッセージへのアクセスおよび表示」
ログ アクセス	496 ページの「ログ メッセージへのアクセスおよび表示」
DLP アーカイブ	404 ページの「DLP アーカイブ」
レポート アクセス	504 ページの「FortiAnalyzer レポート スケジュール」

グローバル設定

次の設定は、すべてのバーチャル ドメインに影響します。バーチャル ドメインが有効になっている場合は、デフォルトの super_admin プロファイルを持つアカウントだけがグローバル設定にアクセスできます。

表 7: グローバル設定

設定オブジェクト	詳細情報の参照先
システム	
ステータス - システム時刻	41 ページの「システム時刻の設定」
ステータス - ホスト名	41 ページの「FortiGate ユニットのホスト名の変更」
ステータス - ファームウェア バージョン	42 ページの「FortiGate の変更」([System Status] ページ）または 61 ページの「ファームウェア管理方法」
ネットワーク インタフェースと VLAN サブインタフェース	89 ページの「インタフェースの設定」（グローバル設定の一部としてインタフェースを設定しますが、各インタフェースと VLAN サブインタフェースは VDOM に属します。グローバル設定の一部としてインタフェースを VDOM に追加します。）
ネットワーク オプション - DNS	113 ページの「DNS サーバ」
ネットワーク オプション - [Detect Interface Status for Gateway Load Balancing]	101 ページの「ゲートウェイ負荷分散のためのインタフェース ステータス検出の設定」

表 7: グローバル設定（続き）

設定オブジェクト	詳細情報の参照先
管理者 – 管理者	169 ページの「管理者」 （グローバル管理者を追加できます。また、管理者を VDOM に追加することもできます。VDOM 管理者は、管理者アカウントを追加または設定できません。）
管理者 – プロファイル	179 ページの「管理者プロファイル」
管理者 – 集中管理の設定	183 ページの「集中管理」
管理者 – 設定 – アイドルおよび認証タイムアウト	184 ページの「設定」および 447 ページの「ユーザ認証の設定」
管理者 – 設定 – Web ベース マネージャの言語	184 ページの「設定」
管理者 – 設定 – LCD パネルの PIN（該当する場合）	184 ページの「設定」
無線 – 設定	126 ページの「無線の設定」
無線 – MAC フィルタ	128 ページの「無線 MAC フィルタ」
無線 – モニタ	129 ページの「無線モニタ」
無線 – 悪意のある AP	130 ページの「悪意のある AP の検出」
設定 – HA	137 ページの「HA」
設定 – SNMP	142 ページの「SNMP」
設定 – 差し替えメッセージ	153 ページの「差し替えメッセージ」
証明書	191 ページの「システム – 証明書」
設定のバックアップと復元	39 ページの「[System Information]」および 201 ページの「[Firmware]」
メンテナンス – リビジョン制御	200 ページの「[Configuration Revision]」
メンテナンス – スクリプト	215 ページの「スクリプト ファイルの作成」
メンテナンス – FDN 更新設定	203 ページの「FortiGuard Distribution Network」
ログとレポート	
ログ設定	490 ページの「FortiGate ユニットでのログの保存方法」
アラート メール	495 ページの「アラート メール」

バーチャル ドメインの有効化

デフォルトの管理者アカウントを使用して、FortiGate ユニット上で複数の VDOM での動作を有効にすることができます。

バーチャル ドメインを有効にするには

1 super_admin プロファイル アカウントで Web ベース マネージャにログインします。

2 *[System]*、*[Dashboard]*、*[Status]* の順に選択します。

3 *[System Information]* で、*[Virtual Domain]* の横にある *[Enable]* を選択します。

FortiGate ユニットからログオフされます。ここで、管理者として再度ログインできます。

あるいは、CLI を使用して、次のコマンドを入力します。

```
config system global, set vdom-admin
```

バーチャル ドメインが有効になると、 Web ベース マネージャと CLI が次のように変更されます。

- グローバル設定と VDOM ごとの設定が分離されます。詳細については、74 ページの「VDOM の設定」および 76 ページの「グローバル設定」を参照してください。
- [Current VDOM] という新しいメニュー表示されます。これを使用して、VDOM から VDOM に移動できます。詳細については、85 ページの「VDOM 間の切り替え」を参照してください。

- *[System]* オプションの下に、新しい *[VDOM]* エントリが表示されます。
- VDOM 内では、使用できるダッシュボード メニュー オプションが減り、新しい *[Global]* オプションが表示されます。*[Global]* を選択すると、現在の VDOM が終了します。
- グローバル レベルでは、動作モード オプションは存在しません。
- グローバル レベルのオプションを表示したり設定したりできるのは、super_admin プロファイル アカウントだけです。
- super_admin プロファイル アカウントは、すべての VDOM の設定を設定できます。
- 各 VDOM に対して、1 人以上の管理者を設定できます。ただし、これらの管理者アカウントは、自分に許可されていない VDOM の設定を編集できません。

バーチャル ドメインが有効になっている場合は、現在のバーチャル ドメインが画面の左下に *[Current VDOM]: <バーチャル ドメインの名前>* という形式で表示されます。

VDOM とグローバル設定の設定

VDOM は、受信トラフィック用と送信トラフィック用の少なくとも 2 つの物理インタフェースまたは仮想サブインタフェースが含まれていなければ意味がありません。関連付けられているタスクを行えるかは、管理者の権限によって異なります。super_admin プロファイル アカウントを使用している場合は、すべてのタスクを実行できます。標準管理者アカウントを使用している場合、実行できるタスクは、読み取り専用権限または読み取り / 書き込み権限のどちらを持っているかによって異なります。表 6 は、各役割で実行できるタスクを示しています。

表 8: 管理者の VDOM の権限

タスク	標準管理者アカウント		super_admin プロファイル管理者アカウント
	読み取り専用権限	読み取り / 書き込み権限	
グローバル設定の表示	可	可	可
グローバル設定の設定	不可	不可	可
VDOM の作成または削除	不可	不可	可
複数の VDOM の設定	不可	不可	可
VDOM へのインタフェースの割り当て	不可	不可	可
VLAN の作成	不可	可 - 1 つの VDOM に対して	可 - すべての VDOM に対して
VDOM への管理者の割り当て	不可	不可	可
追加の管理者アカウントの作成	不可	可 - 1 つの VDOM に対して	可 - すべての VDOM に対して
プロテクション プロファイルの作成および編集	不可	可 - 1 つの VDOM に対して	可 - すべての VDOM に対して

この項には、以下のトピックが含まれています。

VDOM ライセンス

デフォルトでは、すべての FortiGate ユニット（FortiGate-30B を除く）で 10 個の VDOM がサポートされます。*[System]*、*[Maintenance]*、*[License]* タブが表示されない場合は、使用している FortiGate モデルで 10 個を超える VDOM がサポートされていません。

ハイエンドの FortiGate モデルでは、許可される VDOM の最大数を 25、50、100、250、または 500 に増やすための VDOM ライセンス キーのカスタマ サービスからの購入がサポートされています。VDOM を 250 以上設定すると、システム パフォーマンスが低下します。

表 9: FortiGate モデルでサポートている VDOM

FortiGate モデル	VDOM のサポート	VDOM のデフォルトの最大数	VDOM ライセンスの最大数
30B	なし	0	0
ローエンドおよびミッドレンジ モデル	あり	10	10
ハイエンド モデル	あり	10	500

注記：FortiGate ユニットには、設定されているすべての VDOM の間で分割された、限られたリソースしかありません。これらのリソースには、システム メモリや CPU が含まれます。250 以上の VDOM を実行している場合は、プロキシ、Web フィルタリング、アンチウイルスなどの統合脅威管理（UTM）機能を実行できません。FortiGate ユニットは、基本的なファイアウォール機能しか提供できません。

VDOM ライセンス キーを取得するには

1 管理者アカウントを使用して FortiGate ユニットにログインします。

super_admin プロファイル アカウントなどのその他のアカウントにも、VDOM ライセンスをインストールするための十分な特権がある場合があります。

2 *[System]*、*[Dashboard]*、*[Status]* の順に選択します。

3 39 ページの「[System Information]」に示す FortiGate ユニット のシリアル番号を記録します。

4 [License Information] ウィジェットで、*[Virtual Domains]* 行にある *[Purchase More]* を選択します。

フォーティネット カスタマ サポートの Web サイトに移動するため、そこでログインし、25、50、100、250、または 500 の VDOM のためのライセンス キーを購入できます。

5 ライセンス キーを受け取ったら、*[System]*、*[Maintenance]*、*[License]* の順に選択します。

6 *[License Key]* フィールドに、フォーティネット カスタマ サポートから受け取った 32 文字のライセンス キーを入力します。

7 *[Apply]* を選択します。

新しい VDOM ライセンスを確認するには、*[Global Configuration]* で *[System]*、*[Dashboard]*、*[Status]* の順に選択します。*[License Information]* 領域の *[Virtual Domains]* にある *[VDOMs Allowed]* に、許可されている VDOM の最大数が表示されます。

注記：登録された FortiGate ユニット上で作成された VDOM は、接続されている FortiAnalyzer ユニットによって実際のデバイスとして認識されます。FortiAnalyzer ユニットには、登録済みデバイスの総数の VDOM が含まれています。たとえば、3 つの FortiGate ユニットが FortiAnalyzer ユニットに登録され、合計で 4 つの VDOM を含んでいる場合、FortiAnalyzer ユニット上に登録されている FortiGate ユニットの総数は 7 ユニットです。詳細については、『*FortiAnalyzer 管理ガイド*』を参照してください。

新しい VDOM の作成

デフォルトでは、すべての FortiGate ユニットに、VDOM が有効になっていると表示されるルート VDOM が含まれています。追加の VDOM を使用するには、まずそれらの VDOM を作成する必要があります。

複数の VDOM を使用している場合は、割り当てるリソースを VDOM によって多くしたり、少なくしたりすると有効です。この VDOM のリソース管理によって、FortiGate ユニットのパフォーマンスが向上します。詳細については、86 ページの「個々の VDOM のリソース使用量の設定」を参照してください。

VDOM 名には、次のような制限があります。

- 英字、数字、"-"、および "_" のみが許可されます。
- 名前に含めることができるのは 11 文字以下です。
- 名前にスペースを含めることはできません。
- VDOM の名前を、インタフェース、ゾーン、スイッチ インタフェース、または他の VDOM と同じにすることはできません。

VDOM 名の `vsys_ha` と `vsys_fgfm` は、FortiGate ユニットによって使用されています。新しい VDOM に `vsys_ha` または `vsys_fgfm` という名前を付けようとすると、FortiGate ユニットによってエラーが生成されます。

注記：250 以上の VDOM を作成する場合は、限られたリソースのために、プロキシ、Web フィルタリング、アンチウイルスなどの UTM 機能を有効にすることはできません。同様に、多数の VDOM を作成すると、パフォーマンスが低下することがあります。複数の VDOM でのパフォーマンスを向上させるには、86 ページの「個々の VDOM のリソース使用量の設定」を参照してください。

新しい VDOM を作成するには

1 super_admin プロファイル管理者としてログインします。
2 VDOM が有効になっていることを確認します。詳細については、77 ページの「バーチャル ドメインの有効化」を参照してください。
3 *[System]*、*[VDOM]*、*[VDOM]* の順に選択します。
4 *[Create New]* を選択します。
5 [New Virtual Domain] ページで、新しい VDOM の名前（最大 11 文字）を入力します。この名前は変更できません。
6 必要に応じて、この VDOM に関するコメント（最大 63 文字）を入力します。
7 *[OK]* を選択します

VDOM の無効化

複数の VDOM が設定されている場合は、削除して後で再作成するのではなく、1 つの VDOM を一時的に無効にすると有効です。

この無効化は、初期の設定中や、装置の変更中のほか、DoS 攻撃の最中でも使用できます。

無効になっている VDOM は、*[Enable]* チェック ボックスがオフになっています。このチェック ボックスが灰色で表示されている VDOM は管理 VDOM であり、無効にすることはできません。

再び有効にするには、単純に *[Enable]* チェック ボックスをオンにしてプロンプトに応答します。

VDOM を無効にするには

1 super_admin プロファイル管理者としてログインします。
2 *[System]*、*[VDOM]*、*[VDOM]* の順に選択します。
3 無効にする VDOM の *[Enable]* チェック ボックスをオフにします。
4 確認を求められたら、選択を確認します。

VDOM とグローバル設定の操作

管理者としてログインしたときにバーチャル ドメインが有効になっていると、*[System]* の下の *[VDOM]* オプションの表示で示されているように、FortiGate ユニットは自動的にグローバル設定に入ります。

バーチャル ドメインを操作するには、*[System]*、*[VDOM]*、*[VDOM]* の順に選択します。

[VDOM] ページ

作成したすべての VDOM と、デフォルトのルート VDOM を表示します。このページでは、新しい VDOM を編集、削除、または作成することができます。また、このページでは、別の VDOM に切り替えることもできます。

[Create New] 新しい VDOM を追加する場合に選択します。新しい VDOM 名を入力し、*[OK]* を選択します。
VDOM の名前を、既存の VDOM、VLAN、またはゾーンと同じにすることはできません。VDOM 名の長さは最大 11 文字であり、スペースを含めることはできません。

[Edit] この VDOM の説明を変更する場合に選択します。VDOM の名前は変更できません。既存の VDOM を編集する場合は、[Edit Virtual Domain] ページに自動的にリダイレクトされます。

[Delete] この VDOM を削除する場合に選択します。

[Switch Management [<management_vdom>]] 管理 VDOM を、リストで選択されている VDOM に変更します。これにより、この管理 VDOM が [Switch Management] の横の角かっこの中に表示されます。たとえば、[Switch Management [vdom_1]] となります。デフォルトの管理 VDOM はルートです。
詳細については、84 ページの「管理 VDOM の変更」を参照してください。

[Name] この VDOM の名前。

[Operation Mode] VDOM の動作モード ([NAT] または [Transparent])。
VDOM がトランスペアレント モードにある場合は、SNMP で、その VDOM の管理アドレス、アドレスの種類、およびサブネット マスク
を表示できます。詳細については、142 ページの「SNMP」を参照してください。

[Interfaces] この VDOM に関連付けられているインタフェース (仮想インタフェースを含む)。
すべての VDOM には、その VDOM 用に名前が付けられた SSL VPN 仮想インタフェースが含まれています。ルート VDOM の場合、このインタフェースは ssl.root です。

[Enable] このカラムは、次の 3 つの状態のいずれかになります。
- 緑色のチェックマークは、この VDOM が有効になっており、その VDOM を変更するために *[Enter]* アイコンを選択できることを示します。
- オフのチェックマークは、この VDOM が無効になっていることを示します。無効になっている場合は、その VDOM の設定が保持されます。*[Enter]* アイコンは使用できません。
- 灰色で表示されているチェックマークは、この VDOM が管理 VDOM であることを示します。削除することも、無効に変更することもできません。この VDOM は、常にアクティブです。

[Comments] この VDOM が作成されたときに、管理者によって追加されたコメント。

[New Virtual Domain] ページ

新しい VDOM を設定するための各設定を提供します。既存の VDOM を編集する場合は、[Edit Virtual Domain] ページに自動的にリダイレクトされ、ここでシステム リソースの最大量および保証された量を変更できます。

[Name] この VDOM の名前を入力します。

[Enable] この VDOM を有効にする場合に選択します。

[Comments] この VDOM に関する説明を入力します。このフィールドはオプションです。

[Edit Virtual Domain] ページ

システム リソースの最大量を変更するための設定を提供します。

[Name] この VDOM の名前。VDOM を編集している場合は、VDOM 名を変更できません。1

[Enable] この VDOM が有効になっているか、無効になっているかを示します。VDOM を編集している場合は、VDOM を有効にするか、無効にするかを変更できません。

[Comments]	必要に応じて、このフィールドにある説明を変更します。このフィールドはオプションです。
[Resource Usage]	[Maximum] および [Guaranteed] フィールドの数値を入力します。システム リソースの制限を変更する方法の詳細については、86 ページの「個々の VDOM のリソース使用量の設定」を参照してください。

VDOM へのインタフェースの追加

VDOM には、少なくとも 2 つの有効なインタフェースが含まれている必要があります。これらのインタフェースは、物理インタフェースでも、VLAN サブインタフェースなどの仮想インタフェースでもかまいません。デフォルトでは、すべての物理インタフェースがルート バーチャル ドメインに含まれています。インタフェースの種類の詳細については、89 ページの「インタフェースの設定」を参照してください。

VLAN サブインタフェースは一般に、物理インタフェースとは別の VDOM に含める必要があります。これを行うには、スーパー管理者が最初に VDOM を作成し、VLAN サブインタフェースを作成した後、その VLAN を正しい VDOM に割り当てる必要があります。

VDOM は、VDOM 内ではなく、グローバル設定でのみ追加できます。VLAN サブインタフェースの作成については、95 ページの「VLAN インタフェースの追加」を参照してください。

VDOM 間リンク

VDOM 間リンクとは、物理インタフェースを使用しなくても 2 つの VDOM 間で内部的に通信できるようにするためのインタフェースのペアです。VDOM 間リンクは物理インタフェースと同じセキュリティを備えていますが、FortiGate ユニット上の物理インタフェースの数には制限されない、より柔軟な設定が可能になります。すべての仮想インタフェースと同様に、リンクの速度はCPU負荷によって異なりますが、一般には物理インタフェースより高速です。VDOM 間リンクには、MTU の設定は存在しません。DHCP のサポートには、VDOM 間リンクが含まれています。

パケットは、VDOM 間リンクを最大 3 回通過できます。これは、ループを防ぐためです。トラフィックが暗号化または暗号化解除されると、パケットの内容が変更されるため、これにより VDOM 間カウンタがリセットされます。ただし、IPIP または GRE トンネルを使用している場合は、カウンタがリセットされません。

HA モードでは、VDOM 間リンクの両端が同じ仮想クラスタ内に存在する必要があります。VDOM 間リンクでは IPSec 経由の DHCP がサポートされていますが、通常の DHCP サービスは使用できません。

VDOM 間リンクを表示するには、*[System]*、*[Network]*、*[Interface]* の順に選択します。VDOM 間リンクが作成されると、2 つの内部の VDOM に対応する仮想インタフェースのペアが自動的に作成されます。各仮想インタフェースには、その VDOM 間リンクの名前に "0" または "1" を付加した名前が付けられます。そのため、VDOM 間リンクの名前が "vlink" の場合、これらのインタフェースは "vlink0" と "vlink1" になります。仮想インタフェースを表示するには、VDOM リンクの横にある展開の矢印を選択します。

注記：VDOM 間リンクは、トランスペアレント モードにあるドメインを参照できません。

VDOM 間リンクを作成するには

1 管理者としてログインします。

2 *[System]*、*[Network]*、*[Interface]* の順に選択します。

3 *[Create New]* ボタンにある矢印を選択します。

4 *[VDOM link]* を選択します。

[New VDOM Link] 画面が表示されます。

5 新しい VDOM リンクの名前 (最大 11 文字) を入力します。

この名前にスペースや特殊文字を含めることはできません。ハイフン（"-"）とアンダーライン（"_"）が許可されます。この名前の後に "0" または "1" が付加されて実際のインタフェースになることに注意してください。

6 VDOM リンク "0" を設定します。

7 このインタフェースの接続先の VDOM をメニューから選択します。

8 このインタフェースの IP アドレスとネットマスクを入力します。

9 管理アクセス方法 (1 つまたは複数) を選択します。PING、TELNET、および HTTP は安全性の低い方法であることに注意してください。

10 必要に応じて、このインタフェースの説明を入力します。

11 VDOM リンク "1" について、手順 7. ～ 10. を繰り返します。

12 *[OK]* を選択して設定を保存し、*[System]*、*[Interface]* 画面に戻ります。

VDOM へのインタフェースの割り当て

VDOM がいずれかの設定で使用されている場合は、その VDOM を削除できません。たとえば、その VDOM にインタフェースが割り当てられている場合は、その VDOM を削除できません。インタフェースが次のいずれかの設定に含まれている場合は、VDOM からそのインタフェースを削除できません。

- DHCP サーバ
- ゾーン
- ルーティング
- 負荷分散
- DoS ポリシーおよびワンアームド スニッファ ポリシーを含むファイアウォール ポリシー
- proxy arp (CLI を使用してのみアクセス可能)

これらの設定を削除する前に、後日この VDOM を作成したくなったときに復元できるように、設定をバックアップすることをお勧めします。

先に進む前に、このリスト内の項目を削除するか、またはインタフェースを削除できるように変更してください。インタフェースに結合されたオブジェクトが存在しなくなると、そのインタフェースの [Edit] 画面上の [VDOM] フィールドは、灰色で表示されたロックされた状態から変更されます。

注記：*[削除]* アイコンが表示されたら、インタフェースまたはサブインタフェースを再割り当てしたり、削除したりすることができます。このアイコンが存在しない場合は、このインタフェースがどこかの設定で使用されていることを示します。

ヒント： VDOM を削除する代わりに、無効にすることができます。設定が保持されるため、削除した場合の、後で再設定するために必要な時間が節約されます。詳細については、81 ページの「VDOM とグローバル設定の操作」を参照してください。

次の手順は、既存のインタフェースを、あるバーチャル ドメインから別のバーチャル ドメインに再割り当てする方法を説明しています。ここでは、VDOM が有効になっており、複数の VDOM が存在することを前提にしています。

VDOM にインタフェースを割り当てるには

1 管理者としてログインします。

2 *[System]*、*[Network]*、*[Interface]* の順に選択します。

3 再割り当てするインタフェースの *[Edit]* を選択します。

4 そのインタフェースの新しいバーチャル ドメインを選択します。

5 必要に応じてその他の設定を設定し、*[OK]* を選択します。

詳細については、92 ページの「インタフェースの設定」を参照してください。

このインタフェースが VDOM に割り当てられます。このインタフェースの既存のファイアウォール仮想 IP アドレスは削除されます。このインタフェースを参照しているルートをすべて手動で削除し、新しい VDOM 内にこのインタフェースの新しいルートを作成する必要があります。そうしないと、ネットワーク トラフィックが正しくルーティングされません。スタティック ルートの作成の詳細については、229 ページの「ルータ – スタティック」を参照してください。

VDOM への管理者の割り当て

独自のリソースを管理している組織にサービスを提供する VDOM を作成している場合は、その VDOM の管理者アカウントを作成する必要があります。

VDOM 管理者は、その VDOM 内の設定を変更できますが、FortiGate ユニット上の他の VDOM に影響する変更を行うことはできません。

VDOM に割り当てられた標準管理者は、その VDOM に属するインタフェース上の Web ベース マネージャまたは CLI にのみログインできます。スーパー管理者は、管理アクセスを許可する FortiGate ユニット上の任意のインタフェースを使用して Web ベース マネージャまたは CLI に接続できます。コンソール インタフェースに接続することによってログインできるのは、スーパー管理者またはルート ドメインの標準管理者だけです。

注記： VDOM に管理者アカウントが割り当てられている場合は、そのアカウントが別の VDOM に割り当てられるか、または削除されるまで、その VDOM を削除できません。

VDOM に管理者を割り当てるには

1 super_admin としてログインします。

2 バーチャル ドメインが有効になっていることを確認します。詳細については、77 ページの「バーチャル ドメインの有効化」を参照してください。

3 *[System]*、*[Admin]*、*[Administrators]* の順に選択します。

4 新しい管理者アカウントを作成するか、または既存の管理者アカウントの *[編集]* アイコンを選択します。

5 [Virtual Domain] リストに移動します。

6 この管理者が管理する VDOM を選択します。

管理者は、super_admin 管理者でない限り、そのアカウントが作成されたときに特定の VDOM に割り当てられます。詳細については、171 ページの「管理者アカウントの設定」を参照してください。

7 必要に応じて、その他の設定を設定します。

詳細については、171 ページの「管理者アカウントの設定」を参照してください。

8 *[OK]* を選択します

管理 VDOM の変更

FortiGate ユニット上の管理 VDOM からは、次に示すような、いくつかのデフォルトの種類のトラフィックが発信されます。

- SNMP
- ロギング
- アラート メール
- FDN ベースの更新
- NTP ベースの時刻設定

管理 VDOM を変更する前に、[System Dashboard] 画面でバーチャル ドメインが有効になっていることを確認してください。詳細については、77 ページの「バーチャル ドメインの有効化」を参照してください。

特定の時点で管理 VDOM になれる VDOM は 1 つだけです。

グローバル イベントは、管理 VDOM に設定された VDOM とともにログに記録されます。

注記：RADIUS 認証を使用している管理者がいる場合は、管理 VDOM を変更できません。

管理 VDOM を変更するには

1 *[System]*、*[VDOM]*、*[VDOM]* の順に選択します。

2 VDOM のリストから、新しい管理 VDOM になる VDOM を選択します。
このリストは、*[Apply]* ボタンのすぐ左にあります。

3 *[Apply]* を選択して、変更を行います。
プロンプトで、変更を確認します。
これで、管理トラフィックは新しい管理 VDOM から発信されます。

VDOM 間の切り替え

FortiGate ユニット上で VDOM を有効にした後に表示される [Current VDOM] メニューを使用して、VDOM 間を容易に切り替えることができます。[Current VDOM] メニューには、メニューの名前の横にドロップダウン リストが配置されています。このドロップダウン リストには、作成したすべての VDOM（デフォルトのルート VDOM と [Global] を含む）が含まれています。

別の VDOM に切り替えるには、[Current VDOM] メニューで、ドロップダウン リストから切り替え先の VDOM を選択します。Web ベース マネージャ内のその VDOM に自動的にリダイレクトされます。

VDOM のリソース制限の設定

スーパー管理者は、各 VDOM が使用できるリソースの量を制御するための、VDOM のリソース制限を設定できます。つまり、異なる VDOM に階層型のサービスを提供できます。また、リソース制限を使用して VDOM 間で均等にリソースを共有することにより、ある VDOM が他の VDOM のパフォーマンスに影響を与えないようにすることもできます。

動的リソースおよび一部の静的リソースの制限を設定できます。動的リソースとは、FortiGate の設定によって制御されないリソースのことです。動的リソースを制限すると、VDOM が処理するトラフィックの量を制限でき、それによって VDOM が使用できる FortiGate の処理リソースの量を制限できます。動的リソースの数を制限しない場合は、FortiGate ユニットの容量が制約要因になるまで、各 VDOM が可能な限り多くのリソースを使用します。次の動的リソースの制限を設定できます。

- VDOM で開始できる通信 *セッション*の総数。この制限に達すると、追加のセッションは破棄されます。
- VDOM で開始できる IPSec VPN *ダイヤルアップ トンネル*の数。この制限に達すると、追加のトンネルは破棄されます。
- VDOM で開始できる *SSL VPN* ユーザ セッションの数。この制限に達すると、ユーザが SSL VPN セッションを開始するためにログインしようとしたときに、VDOM はログイン ページの代わりにシステム ビジー メッセージを表示します。

静的リソースは、FortiGate の設定内の制限によって制御されます。これらの制限はモデルによって異なり、『*FortiGate 最大値マトリックス*』に記載されています。静的リソースを制限しても、VDOM が処理するトラフィックの量は制限されません。代わりに、静的リソースを制限すると、VDOM に追加できる設定要素の数が制御されます。次の静的リソースの制限を設定できます。

- VDOM の設定に追加できる *VPN IPSec フェーズ 1* および *フェーズ 2* トンネルの数。トンネルの数は、FortiGate モデルの最大値によって制限されます。
- VDOM の設定に追加できる *ファイアウォール ポリシー*、*プロテクション プロファイル*、*ファイアウォール アドレス*、*ファイアウォール アドレス グループ*、*ファイアウォール カスタム サービス*、*ファイアウォール サービス グループ*、*ファイアウォールのワンタイム スケジュール*、および *ファイアウォールの反復スケジュール*の数。
- VDOM の設定に追加できる *ローカル ユーザとユーザ グループ*の数。

VDOM のグローバル リソース制限の設定

グローバル リソース制限は、すべての VDOM に適用されるリソース制限を設定するために使用します。グローバル リソース制限を設定すると、どの VDOM でもそのリソース制限を超えることはできません。

たとえば、すべての VDOM を 100 個の VPN IPSec フェーズ 1 トンネルに制限する場合は、*[System]*、*[VDOM]*、*[Global Resources]* の順に選択し、*[VPN IPsec Phase1 Tunnels]* のリソース制限を編集して、このグローバル リソース制限を 100 に設定します。このグローバル制限が設定されていると、どのVDOMにも最大100個のVPN IPSecフェーズ1トンネルを追加できます。

また、個々の VDOM のリソース制限を編集して、個々の VDOM に追加できるリソースの数をさらに制限することもできます。86 ページの「個々の VDOM のリソース使用量の設定」を参照してください。

0 のリソース制限は、制限がないことを示します。制限がないということは、リソースがリソース制限の設定によって制限されていないことを示します。代わりに、リソースは他の要因によって制限されています。FortiGate ユニットは、その FortiGate ユニットの容量によって動的リソースを制限しており、システムのビジー状態に応じて変動することがあります。静的リソースの制限は、『*FortiGate 最大値マトリックス*』のドキュメントに記載されている FortiGate の設定の制限によって設定されます。

個々の VDOM のリソース使用量の設定

個々の VDOM のリソース使用量を設定することにより、グローバル制限を置き換えたり、その VDOM の保証された使用量を指定したりすることができます。

新しい VDOM を追加する場合は、その VDOM に名前を付けて *[OK]* を選択した後、その VDOM のリソース使用量を設定できます。また、*[System]*、*[VDOM]* の順に選択し、VDOM の [編集] アイコンを選択することによって、VDOM のリソース使用量をいつでも設定できます。

VDOM のリソース使用量を設定するときは、各リソースの *[Maximum]* および *[Guaranteed]* 値を設定できます。

- *[Maximum]* 値は、VDOM が使用できるリソースの量を制限します。VDOM を追加したときは、最大リソース使用量のすべての設定が 0 になります。これは、この VDOM のリソース制限がグローバル リソース制限によって制御されることを示します。グローバル制限を置き換えて、この VDOM に使用できるリソースをさらに制限する必要がない限り、この最大の設定を置き換える必要はありません。VDOM の最大リソース使用量を、グローバル リソース制限に対応する値より高く設定することはできません。グローバル リソース制限を設定するには、*[System]*、*[VDOM]*、*[Global Resources]* の順に選択します。86 ページの「VDOM のグローバル リソース制限の設定」を参照してください。
- *[Guaranteed]* 値は、その VDOM に使用できるリソースの最小の量を表します。保証された値を設定すると、他の VDOM ですべてのリソースが使用されることがないように保証されます。保証された値が 0 のときは、このリソースの量がこの VDOM に対して保証されないことを示します。保証された値の設定を変更する必要があるのは、FortiGate のリソースが不足する可能性があり、この VDOM で最小のレベルを使用できるように保証したい場合だけです。

[Edit Virtual Domain] ページ上の [Resource Usage] セクション

[Resource] このリソースの名前。動的リソースと静的リソースが含まれます。

[Maximum]	この VDOM に使用できる各リソースの量を削減するために、グローバル制限を置き換えます。この最大値は、グローバル制限以下である必要があります。デフォルト値は 0 です。これは、最大値がグローバル制限と同じであることを示します。 **注記 :** VDOM の最大リソース使用量を設定した場合、すべての VDOM のデフォルトの最大グローバル制限をこの最大値未満に削減することはできません。
[Guaranteed]	他の VDOM による使用量には関係なく、この VDOM で使用できるリソースの最小の量を入力します。デフォルト値は 0 です。これは、このリソースの量がこの VDOM に対して保証されないことを示します。
[Current]	この VDOM が現在使用しているリソースの量。

システム - ネットワーク

この項では、FortiGate ユニットをネットワークで動作するように設定する方法について説明します。基本的なネットワーク設定として、FortiGate のインタフェースと DNS オプションの設定があります。さらに高度な設定として、FortiGate のネットワーク設定へのゾーンや VLAN サブインタフェースの追加があります。また、オプションの設定として、DNS サーバや Explicit Web プロキシ サーバとしての FortiGate ユニットの設定もあります。

FortiGateユニット上でバーチャル ドメイン (VDOM) を有効にした場合、インタフェースとネットワーク オプションは FortiGate ユニット全体に対してグローバルに設定されます。すべてのインタフェース設定 (VDOM へのインタフェースの追加を含む) がグローバル設定の一部になります。ゾーン、モデム インタフェース、DNS データベース、Explicit Web プロキシ、およびトランスペアレント モードのルーティング テーブルは、VDOM ごとに別々に設定します。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には、以下のトピックが含まれています。

注記： 特に断りのない限り、*インタフェース*という用語は、物理的な FortiGate インタフェースまたは仮想的な FortiGateVLAN サブインタフェースのどちらかを指します。

同じフィールド内に IP アドレスとネットマスクの両方を入力できる場合は、短い形式のネットマスクを使用できます。たとえば、「192.168.1.100/255.255.255.0」は「192.168.1.100/24」とも入力できます。

インタフェースの設定

FortiGate インタフェースを設定するには、*[System]*、*[Network]*、*[Interface]* の順に選択します。多くのインタフェース オプションを使用できます。NAT/ ルート モードとトランスペアレント モードでは、使用可能なオプションが異なります。

使用可能なオプションの一部として、次のものがあります。

- 物理インタフェースの設定変更
- VLAN サブインタフェースの追加
- 複数の物理インタフェースの IEEE 802.3ad アグリゲート インタフェースへのアグリゲート (一部のモデル)
- 複数の物理インタフェースの冗長インタフェースへの追加 (一部のモデル)
- ループバック インタフェースの追加
- 無線インタフェース (FortiWiFi モデル) および SSID (Service Set Identifier) の追加
- 複数の VDOM が有効になっている FortiGate ユニット上での VDOM リンクの追加
- sFlow をサポートするための sFlow サンプラの追加 (CLI のみ)
- モデム インタフェースの設定 (一部のモデル)
- ゲートウェイ負荷分散のためのインタフェース ステータスの検出

- インタフェースに関して表示される情報の変更
- 仮想無線アクセス ポイント (VAP) インタフェースの設定

[Interface] ページ

デフォルトのインタフェースと、作成したインタフェースをすべて表示します。このページでは、各インタフェースのステータスの表示、新しいインタフェースの作成、既存のインタフェースの編集、またはインタフェースの削除を行うことができます。

[Create New]

新しいインタフェースを追加するには、*[Create New]* を選択します。[Create New] を選択すると、[New Interface] ページに自動的にリダイレクトされます。
モデルに応じて、VLAN インタフェース、ループバック インタフェース、IEEE 802.3ad アグリゲート インタフェース、または冗長インタフェースを追加できます。
- 95 ページの「VLAN インタフェースの追加」
- 95 ページの「ループバック インタフェースの追加」
- 96 ページの「802.3ad アグリゲート インタフェースの追加」
- 97 ページの「冗長インタフェースの追加」

VDOM が有効になっている場合は、*[Create New]* を選択して VDOM 間リンクを追加することもできます。詳細については、82 ページの「VDOM 間リンク」を参照してください。

[Switch Mode]

[Switch Mode] は、サポートされているモデルでスイッチ モードとインタフェース モードを切り替える場合に選択します。スイッチ モードは、いくつかの FortiGate インタフェースを、1 つの IP アドレスを持つ 1 つのスイッチに結合します。インタフェース モードを使用すると、各インタフェースを個別のインタフェースとして設定できます。
一部の FortiGate モデルでは、*[Hub Mode]* も選択できます。ハブ モードはスイッチ モードに似ていますが、ハブ モードでは、インタフェースが接続先のネットワーク上のデバイスの MAC アドレスを学習せず、ネットワークの変更にもよりすばやく対応できる点が異なります。通常、*[Hub Mode]* を選択するのは、スイッチ モードでの動作時にネットワーク パフォーマンスの問題が発生している場合だけです。FortiGate ユニットの設定は、スイッチ モードとハブ モードのどちらでも同じです。
モードを切り替える前に、変更によって影響を受けるインタフェースのすべての設定がデフォルトに設定されている必要があります。*[Switch Mode]* を選択した場合、Web ベース マネージャには、影響を受けるインタフェースのリストが表示されます。
92 ページの「スイッチ モード」を参照してください。

[Show backplane interfaces]

FortiGate-5000 シリーズのバックプレーン インタフェースを表示する場合に選択します。表示した後は、これらのインタフェースを通常の物理インタフェースとして設定できます。

[Column Settings]

インタフェース リストに表示される情報のカラムを変更する場合に選択します。詳細については、34 ページの「表示されるカラムのカラム設定を使用した制御」を参照してください。

[Description]

インタフェースの説明を表示します (追加されている場合)。詳細については、92 ページの「インタフェースの設定」を参照してください。

[Name]

FortiGate ユニット上の物理インタフェースの名前。これには、設定されている任意のエイリアス名が含まれます。

物理インタフェースの名前は、モデルによって異なります。*internal*、*external*、wan1 (ワイド エリア ネットワーク)、*wlan* (無線 LAN)、*dmz* などの一部の名前は、そのインタフェースのデフォルトの機能を示しています。その他の名前は、*port1* や *port20* などの、より一般的な名前です
一部の FortiGate モデルにはまた、*modem* という名前のモデム インタフェースも含まれています。107 ページの「モデム インタフェースの設定」を参照してください。

複数のインタフェースをアグリゲート インタフェースまたは冗長インタフェースに含めた場合は、コンポーネント インタフェースではなく、アグリゲート インタフェースまたは冗長インタフェースだけが表示されます。96 ページの「802.3ad アグリゲート インタフェースの追加」または 97 ページの「冗長インタフェースの追加」を参照してください。

スイッチ モードをサポートする FortiGate モデルの場合、スイッチ モードにあるときは、スイッチ内の個々のインタフェースは表示されません。詳細については、92 ページの「スイッチ モード」を参照してください。
VLAN インタフェースを追加した場合、これらのインタフェースも、[Name] リスト内の追加先の物理インタフェースまたはアグリゲート インタフェースの下に表示されます。『*FortiGate VLAN および VDOM ガイド*』を参照してください。

ループバック インタフェースを追加した場合、これらのインタフェースも、[Interface] リスト内の追加先の物理インタフェースの下にも表示されます。
ソフトウェア スイッチ インタフェースが設定されている場合は、それらのインタフェースを表示できます。詳細については、105 ページの「ソフトウェア スイッチ インタフェースの追加」を参照してください。

	スイッチ インタフェースを備えたFortiGateモデル上でインタフェース モードを有効にしている場合は、複数の Internal インタフェースが表示されます。スイッチ モードが有効になっている場合は、1 つの Internal インタフェースのみが表示されます。詳細については、92 ページの「スイッチ モード」を参照してください。 FortiGate ユニットで AMC モジュールがサポートされ、かつインタフェースを含む AMC モジュール (たとえば、ASM-FB4 には 4 つのインタフェースが含まれています) をインストールしている場合は、これらのインタフェースがインタフェースのステータス表示に追加されます。これらのインタフェースには、amc-sw1/1、amc-dw1/2 などの名前が付けられます。sw1 は、スロット 1 内のシングル幅 (ダブル幅の場合は dw1) のカードであることを示します。最後の数字 "/1" は、そのカード上のインタフェース番号 (ASM-FB4 カードの場合は "/1" ～ "/4") を示します。
[IP/Netmask]	インタフェースの現在の IP アドレス / ネットマスク。 VDOM モードで、すべての VDOM が NAT モードまたはトランスペアレント モードになっていない場合は、一部の値が表示されず、代わりに "-" と表示されます。 Web ベース マネージャで IPv6 サポートが有効になっている場合は、IPv6 アドレスがこのカラムに表示されます。
[Access]	このインタフェースの管理アクセスの設定。 詳細については、101 ページの「インタフェースへの管理アクセスの設定」を参照してください。
[Administrative Status]	このインタフェースの管理ステータス。 管理ステータスが緑色の矢印である場合、このインタフェースはアップしており、ネットワーク トラフィックを受け付けることができます。管理ステータスが赤色の矢印である場合、このインタフェースは管理上ダウンしており、トラフィックを受け付けることができません。インタフェースの管理ステータスを変更するには、*[編集]* アイコンを選択してこのインタフェースを編集し、インタフェースの *[Administrative Status]* 設定を変更します。
[Link Status]	このインタフェースの物理的な接続のステータス。リンク ステータスは、アップまたはダウンのどちらかです。リンク ステータスがアップの場合は、物理インタフェースとネットワーク スイッチの間にアクティブな物理的な接続が存在します。リンク ステータスがダウンの場合は、このインタフェースがネットワークに接続されていないか、または接続に関する問題が発生しています。Web ベース マネージャからリンク ステータスを変更することはできません。 リンク ステータスは、物理インタフェースに関して表示されるだけです。
[MAC]	このインタフェースの MAC アドレス。
[Mode]	このインタフェースのアドレッシング モードを示します。アドレッシング モードは、手動、DHCP、または PPPoE のいずれかです。
[MTU]	このインタフェースの転送単位あたりの最大バイト数 (MTU)。102 ページの「インタフェースの MTU パケット サイズの変更」を参照してください。
[Secondary IP]	このインタフェースに追加されたセカンダリ IP アドレスを表示します。103 ページの「インタフェースへのセカンダリ IP アドレスの追加」を参照してください。
[Type]	このインタフェースの種類。有効な種類には次のものがあります。 ・ [Physical] - 物理的なネットワーク インタフェース (モデム インタフェースを含む) ・ [VLAN] - VLAN インタフェース ・ [Aggregate] - 802.3ad アグリゲート インタフェースのグループ ・ [Redundant] - 冗長インタフェースのグループ ・ [VDOM Link] - 2 つの VDOM をリンクする仮想インタフェースのペア ・ [Pair] - 一緒に結合された1組の2つのインタフェース (2つのVDOMリンクなど) ・ [Switch] - ソフトウェア スイッチ インタフェースを作成するために一緒に含められた 2 つ以上のインタフェース ・ [Tunnel] - 仮想 IPSec VPN インタフェース ・ [VAP] - 無線コントローラ仮想アクセス ポイント (VAP または仮想 AP) インタフェース
[Virtual Domain]	このインタフェースが属するバーチャル ドメイン。このカラムは、VDOM の設定が有効になっている場合に表示されます。
[VLAN ID]	VLAN サブインタフェースのために設定されている VLAN ID。
[Delete]	このインタフェースを削除します。*[Create New]* を選択することによって追加されたインタフェースに使用できます。たとえば、VLAN インタフェース、ループバック インタフェース、アグリゲート インタフェース、および冗長インタフェースを削除できます。インタフェースは、別の設定で使用されていない場合のみ削除できます。
[Edit]	このインタフェースの設定を変更します。
[View]	このインタフェースの設定を表示します。

次の項も参照してください。

- スイッチ モード

スイッチ モード

スイッチ モードを使用すると、関連する FortiGate インタフェースのグループを、1 つの IP アドレスを持つマルチポート スイッチとして動作するように切り替えることができます。スイッチ モードは、スイッチ ハードウェアを備えた FortiGate モデルで使用できます。

スイッチ モード機能には、スイッチ モードとインタフェース モードの 2 つの状態があります。スイッチ モードは、内部スイッチ全体に対して 1 つのインタフェースと 1 つのアドレスだけが存在する、デフォルトのモードです。インタフェース モードを使用すると、内部スイッチの各物理インタフェース接続を別々に設定できます。これにより、内部の各物理インタフェース接続に異なるサブネットとネットマスクを割り当てることができます。

スイッチ モードとインタフェース モードを切り替えるには、影響を受けるインタフェースのすべての設定がデフォルトに設定されている必要があります。これには、ファイアウォール ポリシー、ルーティング、DNS 転送、DHCP サービス、VDOM インタフェースの割り当て、およびルーティングが含まれます。これらが削除されていない場合は、モードを切り替えることができず、エラー メッセージが表示されます。Web ベース マネージャには、影響を受けるインタフェースのリストが表示されます。

[System]、*[Network]*、*[Interface]* の順に選択して表示されるページで [Switch Mode] を選択すると、[Switch Mode Management] 画面が表示されます。FortiGate の CLI からは、ソフトウェア スイッチ インタフェースを追加することもできます。詳細については、105 ページの「ソフトウェア スイッチ インタフェースの追加」を参照してください。

[Interface] ページ (FortiWiFi モデルのみ)

関連する FortiGate インタフェースのグループを、1 つの IP アドレスを持つマルチポート スイッチとして動作するように切り替えるための設定を提供します。

[Switch Mode]	スイッチ モードを選択します。1 つの Internal インタフェースだけが表示されます。これがデフォルトのモードです。
[Interface Mode]	インタフェース モードを選択します。スイッチ上のすべての Internal インタフェースが、個別に設定可能なインタフェースとして表示されます。
[Hub Mode]	一部の FortiGate モデルでは、*[Hub Mode]* を選択できます。ハブ モードはスイッチ モードに似ていますが、ハブ モードでは、インタフェースが接続先のネットワーク上のデバイスの MAC アドレスを学習せず、一部の環境ではネットワークの変更にもよりすばやく対応できる点が異なります。[Hub Mode] を選択する必要があるのは、スイッチ モードでの動作時にネットワーク パフォーマンスの問題が発生している場合だけです。FortiGate ユニットの設定は、スイッチ モードとハブ モードのどちらでも同じです。

次の項も参照してください。

- インタフェースの設定

インタフェースの設定

VLAN インタフェース、ループバック インタフェース、IEEE 802.3ad アグリゲート インタフェース、または冗長インタフェースを追加したり設定したりするには、*[System]*、*[Network]*、*[Interface]* の順に選択し、*[Create New]* を選択します。また、既存のインタフェースを編集して、インタフェースの設定を変更することもできます。

[New Interface] ページ

新しいインタフェースを設定するための各設定を提供します。[Interface] ページで [Create New] を選択すると、このページに自動的にリダイレクトされます。既存のインタフェースを編集する場合は、[Edit Interface] ページに自動的にリダイレクトされます。

[Name] このインタフェースの名前。VLAN インタフェース、ループバック インタフェース、IEEE 802.3ad アグリゲート インタフェース、および冗長インタフェースの名前を指定したり、変更したりすることができます。
既存のインタフェースの名前を変更することはできません。
インタフェースの表示には、物理インタフェースの MAC アドレスも含まれます。

[Alias] このインタフェースを別のインタフェースから容易に区別できる、インタフェースの別の名前を入力します。このフィールドは、名前を設定できない物理インタフェースに対してのみ使用できます。このエイリアスは最大 15 文字です。
エイリアス名はインタフェース名には含まれませんが、インタフェース名の横のかっこ内に表示されます。ログには表示されません。

[Link Status] このインタフェースがネットワークに接続されているか (リンク ステータスは *[Up]*)、または接続されていないか (リンク ステータスは *[Down]*) を示します。

[Type] 新しいインタフェースを追加する場合は、*[Type]* を、追加するインタフェースの種類に設定します。

- VLAN インタフェースを追加するには、*[Type]* を *[VLAN]* に設定します。95 ページの「VLAN インタフェースの追加」を参照してください。
- ループバック インタフェースを追加するには、*[Type]* を *[Loopback Interface]* に設定します。95 ページの「ループバック インタフェースの追加」を参照してください。
- 一部のモデルでは、アグリゲート インタフェースを追加するために、*[Type]* を *[802.3ad Aggregate]* に設定できます。96 ページの「802.3ad アグリゲート インタフェースの追加」を参照してください。
- 一部のモデルでは、冗長インタフェースを追加するために、*[Type]* を *[Redundant Interface]* に設定できます。97 ページの「冗長インタフェースの追加」を参照してください。

その他の種類には次のものがあります。

- [Software Switch] - ソフトウェア スイッチ インタフェース。105 ページの「ソフトウェア スイッチ インタフェースの追加」を参照してください。
- [Tunnel] - 仮想 IPSec VPN インタフェース。100 ページの「仮想 IPSec インタフェースの設定」を参照してください。
- [VAP Interface] - 無線コントローラ仮想アクセス ポイント (VAPまたは仮想AP) インタフェース。480 ページの「仮想無線アクセス ポイントの設定」を参照してください。

新しいインタフェースを追加する場合を除き、*[Type]* を変更することはできません。

[Interface] VLAN インタフェースの追加先の物理インタフェースの名前を選択します。作成されると、VLAN インタフェースは、[Interface] リスト内の対応する物理インタフェースの下に表示されます。
新しい VLAN インタフェースを追加する場合を除き、VLAN インタフェースの物理インタフェースを変更することはできません。
[Type] が *[VLAN]* に設定されている場合に表示されます。

[VLAN ID] この VLAN サブインタフェースで受信されるパケットの VLAN ID に一致する VLAN ID を入力します。新しい VLAN インタフェースを追加する場合を除き、*[VLAN ID]* を変更することはできません。
VLAN ID は 1 ～ 4094 の任意の数値にすることができ、また、この VLAN サブインタフェースに接続された IEEE 802.1Q 準拠のルータまたはスイッチによって追加される VLAN ID に一致している必要があります。詳細については、95 ページの「VLAN インタフェースの追加」を参照してください。
[Type] が *[VLAN]* に設定されている場合に表示されます。

[Virtual Domain] このインタフェースの追加先のバーチャル ドメインを選択します。
super_adminプロファイルを持つ管理者アカウントが *[Virtual Domain]* を変更できます。

[Physical Interface Members] この項には、インタフェースの種類に応じて次の 2 種類の形式があります。

- **[Software switch interface]** - この項は、ソフトウェア スイッチの仮想インタフェースに属するインタフェースを示す表示専用のフィールドです。105 ページの「ソフトウェア スイッチ インタフェースの追加」を参照してください。
- **[802.3ad aggregate or Redundant interface]** - この項には、各インタフェースへの追加または削除を可能にする、使用可能なインタフェースと選択されたインタフェースのリストが含まれています。96 ページの「802.3ad アグリゲート インタフェースの追加」および 97 ページの「冗長インタフェースの追加」を参照してください。

[Available Interfaces] このリストからインタフェースを選択して、グループ化されたインタフェース (冗長インタフェースまたはアグリゲート インタフェースのどちらか) に含めます。グループ化されたインタフェースにインタフェースを追加するには、右矢印を選択します。

[Selected Interfaces]	これらのインタフェースは、アグリゲート インタフェースまたは冗長インタフェースに含まれています。 グループ化されたインタフェースからインタフェースを削除するには、左矢印を選択します。 冗長インタフェースの場合、これらのインタフェースはフェールオーバー中に、このリストの一番上から一番下への順番にアクティブ化されます。
[Addressing Mode]	このインタフェースのアドレッシング モードを選択します。 ・ *[Manual]* を選択し、このインタフェースの *[IP/Netmask]* を追加します。IPv6 設定が有効になっている場合は、IPv4 と IPv6 の両方の IP アドレスを追加できます。 ・ インタフェース IP アドレスやその他のネットワーク設定を DHCP サーバから取得するには、*[DHCP]* を選択します。98 ページの「インタフェース上での DHCP の設定」を参照してください。 ・ インタフェース IP アドレスやその他のネットワーク設定を PPPoE サーバから取得するには、*[PPPoE]* を選択します。99 ページの「インタフェース上での PPPoE の設定」を参照してください。
[IP/Netmask]	*[Addressing Mode]* が *[Manual]* に設定されている場合は、このインタフェースの IPv4 アドレス / サブネット マスクを入力します。 2 つの FortiGate インタフェースに、同じサブネット上の IP アドレスを設定することはできません。
[IPv6 Address]	*[Addressing Mode]* が *[Manual]* に設定され、Web ベース マネージャで IPv6 サポートが有効になっている場合は、このインタフェースの IPv6 アドレス / サブネット マスクを入力します。1 つのインタフェースに IPv4 アドレスと IPv6 アドレスの両方、またはそのどちらかだけを設定できます。
[Enable one-arm sniffer]	実際にパケットを受信したり、それ以外の方法で処理したりすることなく、攻撃のパケットをスニッフィングすることによって FortiGate ユニットを IDS アプライアンスとして動作するように設定する一環として、このインタフェースをワンアームド スニッファとして動作するように設定する場合に選択します。スニッフィング用に有効になった後は、このインタフェースをその他のトラフィックのために使用することはできません。実際にパケットをスニッフィングするには、このインタフェースのスニッファ ポリシーを追加する必要があります。 ワンアームド IPS の詳細については、281 ページの「ファイアウォール ポリシーネットワーク攻撃を検出するワンアーム スニファ ポリシーの使用 」を参照してください。
[Enable explicit Web Proxy]	このインタフェース上で Explicit Web プロキシを有効にする場合に選択します。有効になっている場合、このインタフェースは、*[System]*、*[Network]*、*[Web Proxy]* の順に選択して表示されるページの *[Listen on Interfaces]* に表示されます。また、このインタフェース上の Web トラフィックは、Web プロキシ設定に従ってプロキシ処理されます。詳細については、117 ページの「Explicit Web プロキシの設定」を参照してください。
[Enable DDNS]	このインタフェースのダイナミック DNS サービスを設定するには、[Enable DDNS] を選択します。詳細については、100 ページの「インタフェース上でのダイナミック DNS の設定」を参照してください。
[Override default MTU value]	MTU を変更するには、[Override default MTU value (1500)] をオンにし、このインタフェースのアドレッシング モードに基づいた MTU サイズを入力します。 ・ 静的モードの場合は、68 ～ 1,500 バイト ・ DHCP モードの場合は、576 ～ 1,500 バイト ・ PPPoE モードの場合は、576 ～ 1,492 バイト ・ FortiGate モデルでサポートされている場合は、さらに大きなフレーム サイズ 物理インタフェース上でのみ使用できます。物理インタフェースに関連付けられている仮想インタフェースは、その物理インタフェースの MTU サイズを継承します。 MTU サイズの詳細については、102 ページの「インタフェースの MTU パケット サイズの変更」を参照してください。 **注記**：トランスペアレント モードでは、インタフェースの MTU を変更した場合、その新しい MTU に一致するようにすべてのインタフェースの MTU を変更する必要があります。
[Enable DNS Query]	DNS クエリを受け付けるようにこのインタフェースを設定する場合に選択します。[Recursive] または [Non-Recursive] を選択します。詳細については、113 ページの「FortiGate DNS サービスの設定」を参照してください。
[Recursive]	FortiGate DNS データベースでドメイン名を検索します。エントリが見つからない場合は、*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで設定された DNS サーバに要求を中継します。
[Non-Recursive]	FortiGate DNS データベースでドメイン名を検索します。*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで設定された DNS サーバに要求を中継しません。
[Administrative Access]	このインタフェースへの IPv4 接続に許可される管理アクセスの種類を選択します。

[Ipv6 Administrative Access]	このインタフェースへの IPv6 接続に許可される管理アクセスの種類を選択します。
[HTTPS]	このインタフェースを介した Web ベース マネージャへのセキュアな HTTPS 接続を許可します。
[PING]	ping に応答するインタフェース。この設定は、インストールの確認やテストに使用します。
[HTTP]	このインタフェースを介した Web ベース マネージャへの HTTP 接続を許可します。HTTP 接続はセキュリティ保護されていないため、第三者によって傍受される可能性があります。
[SSH]	このインタフェースを介した CLI への SSH 接続を許可します。
[SNMP]	リモートの SNMP マネージャがこのインタフェースに接続することによって SNMP 情報を要求できるようにします。143 ページの「SNMP の設定」を参照してください。
[TELNET]	このインタフェースを介した CLI への Telnet 接続を許可します。Telnet 接続はセキュリティ保護されていないため、第三者によって傍受される可能性があります。
[Detect Interface Status for Gateway Load Balancing]	メインのインタフェース IP アドレスのインタフェース ステータス検出を設定します。101 ページの「ゲートウェイ負荷分散のためのインタフェース ステータス検出の設定」を参照してください。
[Secondary IP Address]	このインタフェースに IPv4 アドレスを追加します。このセクションを展開したり非表示にしたりするには、青色の矢印を選択します。103 ページの「インタフェースへのセカンダリ IP アドレスの追加」を参照してください。
[Description]	このインタフェースを説明するための最大 63 文字の説明を入力します。
[Administrative Status]	このインタフェースのステータスとして *[Up]*（緑色の矢印）または *[Down]*（赤色の矢印）のどちらかを選択します。 *[Up]* は、このインタフェースがアクティブであり、ネットワーク トラフィックを受け付けることができることを示します。 *[Down]* は、このインタフェースがアクティブでなく、トラフィックを受け付けることができないことを示します。

VLAN インタフェースの追加

VLAN インタフェース（VLAN または VLAN サブインタフェースとも呼ばれる）は、物理インタフェース上の仮想インタフェースであり、その物理インタフェースを使用して VLAN タグ付きパケットを受け付けます。

VLAN インタフェースを追加するには

1 *[System]*、*[Network]*、*[Interface]* の順に選択します。

2 *[Create New]* を選択し、*[Type]* を *[VLAN]* に設定します。

3 VLAN サブインタフェースを設定します。

VLAN サブインタフェースの *[Name]*、親の物理インタフェースの *[Interface]*、および *[VLAN ID]* が設定されている必要があります。92 ページの「インタフェースの設定」を参照してください。

4 [OK] を選択します。

新しい VLAN サブインタフェースを表示するには、*[System]*、*[Network]*、*[Interface]* の順に選択し、その VLAN インタフェースの親の物理インタフェースの横にある展開の矢印を選択します。これにより表示が展開されて、この物理インタフェース上のすべての VLAN サブインタフェースが表示されます。展開の矢印が表示されていない場合は、その物理インタフェース上にサブインタフェースは設定されていません。

詳細については、『*FortiGate VLAN および VDOM ガイド*』を参照してください。

ループバック インタフェースの追加

ループバック インタフェースは、他のどのインタフェースにも接続されていない「常時アップ」の仮想インタフェースです。ループバック インタフェースは、特定の外部ポートに依存することなく、FortiGate ユニットのインタフェース IP アドレスに接続されます。

ループバック インタフェースは、特定のネットワーク アドレスに送信されたパケットを破棄するブラックホール ルーティングを支援するために追加されました。

ループバック インタフェースはハードウェアに接続されていないため、ハードウェアの問題の影響を受けません。FortiGate ユニットが機能している限り、ループバック インタフェースはアクティブです。この「常時アップ」機能は、FortiGate リモート ルータと依存するダイナミック ルーティング環境と、ループバック インタフェースへのアクセスのためのローカル ファイアウォール ポリシーなどにおいて有用です。

ループバック インタフェースを追加するには - Web ベース マネージャ

1 *[System]*、*[Network]*、*[Interface]* の順に選択します。

2 *[Create New]* を選択し、*[Type]* を *[Loopback Interface]* に設定してループバック インタフェースを追加します。

3 ループバック インタフェースを設定します。

ループバック インタフェースの *[Name]* が設定されている必要があります。また、管理アクセスを設定したり、説明を追加したりすることもできます。詳細については、92 ページの「インタフェースの設定」を参照してください。

4 [OK] を選択します。

ループバック インタフェースを追加するには - CLI

10.0.0.10 の IP アドレスを持つ `loop1` という名前のループバック インタフェースを設定するための CLI コマンドは次のとおりです。

```
config system interface
  edit loop1
    set type loopback
    set ip 10.0.0.10 255.255.255.0
  end
```

詳細については、『*FortiGate CLI リファレンス*』にある `config system interface` セクションを参照してください。

802.3ad アグリゲート インタフェースの追加

一部の FortiGate モデルでは、2 つ以上の物理インタフェースを IEEE 標準の 802.3ad リンク アグリゲート インタフェースにアグリゲートする（束ねる）ことによって、帯域幅を増やすと同時に、ある程度のリンクの冗長性を実現できます。アグリゲート インタフェースは、冗長インタフェースに似ています。アグリゲート インタフェースでは、冗長インタフェースに比べてネットワークへの接続のために提供される帯域幅は増えますが、障害ポイントも多く作成されます。アグリゲート インタフェースはすべて、同じネクストホップ ルーティング宛先に接続する必要があります。

インタフェースをアグリゲート インタフェースとして使用できるのは、そのインタフェースが次の条件を満たしている場合です。

- VLAN インタフェースではなく、物理インタフェースである。
- まだアグリゲート インタフェースまたは冗長インタフェースの一部になっていない。
- アグリゲート インタフェースと同じ VDOM に含まれている。
- IP アドレスが定義されておらず、DHCP や PPPoE も設定されていない。
- DHCP サーバまたはリレーが設定されていない。
- VLAN サブインタフェースが存在しない。
- どのファイアウォール ポリシー、VIP、マルチキャスト ポリシーでも参照されていない。
- HA ハートビート インタフェースではない。
- FortiGate-5000 シリーズのバックプレーン インタフェースのいずれでもない。

アグリゲート インタフェースに含まれているインタフェースは、*[System]*、*[Network]*、*[Interface]* の順に選択して表示されるリストには表示されません。このインタフェースを個別に設定することはできず、ファイアウォール ポリシー、ファイアウォール仮想 IP、またはルーティングに含めることもできません。

注記： 高速化インタフェース（FA2 インタフェース）をアグリゲート リンクに追加することはできますが、FA2 アクセラレーションは失われます。たとえば、2 つの高速化インタフェースをアグリゲートすると、これらの 2 つのインタフェースが分離されている場合に比べてスループットは低下します。

802.3ad アグリゲート インタフェースを作成するには

1 *[System]*、*[Network]*、*[Interface]* の順に選択します。
2 *[Create New]* を選択します。
3 *[Name]* フィールドに、このアグリゲート インタフェースの名前を入力します。
このインタフェース名は、他のどのインタフェース、ゾーン、VDOM とも異なっている必要があります。
4 *[Type]* リストから、*[802.3ad Aggregate]* を選択します。
5 *[Available Interfaces]* リストで、アグリゲート インタフェースに含める 2 つ以上のインタフェースを *[Selected Interfaces]* リストに移動します。
6 必要に応じて、その他のインタフェース オプションを設定します。92 ページの「インタフェースの設定」を参照してください。
7 *[OK]* を選択します

冗長インタフェースの追加

一部の FortiGate モデルでは、2 つ以上の物理インタフェースを結合することによってリンクの冗長性を実現できます。この機能を使用すると、2 つ以上のスイッチに接続して、1 つの物理インタフェースまたはそのインタフェース上の装置に障害が発生した場合でも接続を保証することができます。

冗長インタフェースでは、トラフィックが、常に 1 つのインタフェースしか通過しません。この点は、帯域幅を増やすためにトラフィックがすべてのインタフェースを通過するアグリゲート インタフェースとは異なります。この違いは、冗長インタフェースの方が、発生し得る障害ポイントの少ない、より安定した構成を実現できることを示します。フルメッシュ HA 構成では、この点が重要です。

インタフェースを冗長インタフェースに含めることができるのは、そのインタフェースが次の条件を満たしている場合です。

- VLAN インタフェースではなく、物理インタフェースである。
- まだアグリゲート インタフェースまたは冗長インタフェースの一部になっていない。
- 冗長インタフェースと同じ VDOM に含まれている。
- IP アドレスが定義されておらず、DHCP や PPPoE も設定されていない。
- DHCP サーバまたはリレーが設定されていない。
- VLAN サブインタフェースが存在しない。
- どのファイアウォール ポリシー、VIP、マルチキャスト ポリシーでも参照されていない。
- HA によって監視されていない。
- FortiGate-5000 シリーズのバックプレーン インタフェースのいずれでもない。

インタフェースが冗長インタフェースに含まれている場合、そのインタフェースは *[System]*、*[Network]*、*[Interface]* の順に選択して表示されるページには表示されません。このインタフェースを個別に設定することはできず、ファイアウォール ポリシー、VIP、またはルーティングに含めることもできません。

冗長インタフェースを作成するには

1 *[System]*、*[Network]*、*[Interface]* の順に選択します。

2 *[Create New]* を選択します。

3 *[Name]* フィールドに、この冗長インタフェースの名前を入力します。

このインタフェース名は、他のどのインタフェース、ゾーン、VDOM とも異なっている必要があります。

4 *[Type]* リストから、*[Redundant Interface]* を選択します。

5 *[Available Interfaces]* リストで、冗長インタフェースに含める各インタフェースを選択し、それを *[Selected Interfaces]* リストに移動します。

フェールオーバーの状況では、*[Selected Interfaces]* リスト内の次にあるインタフェースが、アクティブ化されるインタフェースになります。

6 必要に応じて、その他のインタフェース オプションを設定します。92 ページの「インタフェースの設定」を参照してください。

7 *[OK]* を選択します

インタフェース上での DHCP の設定

DHCP を使用するようにインタフェースを設定した場合、FortiGate ユニットは、そのインタフェースから DHCP 要求を自動的にブロードキャストします。このインタフェースには、IP アドレスと任意の DNS サーバ アドレス、および DHCP サーバによって提供されるデフォルト ゲートウェイ アドレスが設定されます。

デフォルトでは、ローエンド モデルは *[Override internal DNS]* と *[Retrieve default Gateway from DHCP server]* の両方を有効にして、DHCP アドレッシング モードに設定されます。これらの設定により、簡単な標準設定が可能になります。

インタフェースに DHCP を設定するには、*[System]*、*[Network]*、*[Interface]* の順に選択し、*[Create New]* を選択して、[Addressing Mode] セクションの *[DHCP]* を選択します。

[New Interface] ページの [Addressing Mode] セクション

[Status] このインタフェースが DHCP サーバに接続し、アドレッシング情報を取得するときの DHCP の状態メッセージを表示します。アドレッシング モードの状態メッセージを更新するには、*[Status]* を選択します。
[Status] には、次のいずれかが表示されます。
- **[initializing]** - 動作していません。
- **[connecting]** - インタフェースは、DHCP サーバに接続しようとしています。
- **[connected]** - インタフェースは、DHCP サーバから IP アドレス、ネットマスク、その他の設定を取得しました。
- **[failed]** - インタフェースは、DHCP サーバから IP アドレスやその他の設定を取得できませんでした。

[Obtained IP/Netmask] DHCP サーバからリースされた IP アドレスとネットマスク。
[Status] が [connected] の場合にのみ表示されます。

[Renew] このインタフェースの DHCP ライセンスを更新する場合に選択します。
[Status] が [connected] の場合にのみ表示されます。

[Expiry Date] リースされた IP アドレスとネットマスクが有効でなくなる時刻と日付。
[Status] が [connected] の場合にのみ表示されます。

[Default Gateway] DHCP サーバで定義されたゲートウェイの IP アドレス。
[Status] が [connected] であり、かつ *[Retrieve default gateway from server]* がオンになっている場合にのみ表示されます。

[Distance] DHCP サーバから取得されたデフォルト ゲートウェイのディスタンスを入力します。ディスタンス (1 ～ 255 の整数) は、同じ宛先へのルートが複数存在する場合の、ルートの相対的なプライオリティを指定します。ディスタンスが小さいほど、プライオリティが高いルートであることを示します。デフォルト ゲートウェイのデフォルトのディスタンスは 5 です。

[Retrieve default gateway from server]	DHCP サーバからデフォルト ゲートウェイの IP アドレスを取得する場合にオンにします。このデフォルト ゲートウェイは、スタティック ルーティング テーブルに追加されます。 ローエンド モデルでは、デフォルトで有効になっています。
[Override internal DNS]	[DNS] ページ上の DNS サーバ IP アドレスの代わりに、DHCP サーバから取得された DNS アドレスを使用する場合にオンにします。 ローエンド モデルでは、デフォルトで有効になっています。 VDOM が有効になっている場合、内部の DNS は管理 VDOM 上でのみ置き換えることができます。

インタフェース上での PPPoE の設定

PPPoE を使用するようにインタフェースを設定したした場合、FortiGate ユニットは、そのインタフェースから PPPoE 要求を自動的にブロードキャストします。

FortiGate ユニットは、Unnumbered IP、初期検出タイムアウト、PADT (PPPoE Active Discovery Terminate) などの、多くの PPPoE RFC 機能 (RFC 2516) をサポートしています。

インタフェースに PPPoE を設定するには、*[System]*、*[Network]*、*[Interface]* の順に選択し、*[Create New]* を選択して、[Addressing Mode] セクションの *[PPPoE]* を選択します。

[New Interface] ページの [Addressing Mode] セクション

[Status]	FortiGate ユニットが PPPoE サーバに接続し、アドレッシング情報を取得するときの PPPoE の状態メッセージを表示します。アドレッシング モードの状態メッセージを更新するには、[Status] を選択します。 *[Edit]* を選択した場合にのみ表示されます。 [Status] には、次の 4 つのメッセージのいずれかが表示されます。
[initializing]	動作していません。
[connecting]	インタフェースは、PPPoE サーバに接続しようとしています。
[connected]	インタフェースは、PPPoE サーバから IP アドレス、ネットマスク、その他の設定を取得しました。 [Status] が [connected] の場合は、PPPoE の接続情報が表示されます。
[failed]	インタフェースは、PPPoE サーバから IP アドレスやその他の情報を取得できませんでした。
[Reconnect]	PPPoE サーバに再接続する場合に選択します。 [Status] が [connected] の場合にのみ表示されます。
[User Name]	PPPoE アカウントのユーザ名。
[Password]	PPPoE アカウントのパスワード。
[Unnumbered IP]	このインタフェースの IP アドレスを指定します。ISP から IP アドレスのブロックが割り当てられている場合は、そのうちの 1 つを使用します。それ以外の場合、この IP アドレスは別のインタフェースの IP アドレスと同じでも、その他の任意の IP アドレスでもかまいません。
[Initial Disc Timeout]	初期検出タイムアウトを入力します。PPPoE 検出の再試行を開始するまでに待つ時間を入力します。
[Initial PADT timeout]	初期の PADT (PPPoE Active Discovery Terminate) タイムアウト (秒単位) を入力します。このタイムアウトは、この秒数の間アイドルになっている PPPoE セッションをシャットダウンするために使用します。ISP で PADT がサポートされている必要があります。無効にするには、[Initial PADT timeout] を 0 に設定します。
[Distance]	PPPoE サーバから取得されたデフォルト ゲートウェイのディスタンスを入力します。ディスタンス (1 ～ 255 の整数) は、同じ宛先へのルートが複数存在する場合の、ルートの相対的なプライオリティを指定します。ディスタンスが小さいほど、プライオリティが高いルートであることを示します。デフォルト ゲートウェイのデフォルトのディスタンスは 1 です。
[Retrieve default gateway from server]	PPPoE サーバからデフォルト ゲートウェイの IP アドレスを取得する場合にオンにします。このデフォルト ゲートウェイは、スタティック ルーティング テーブルに追加されます。
[Override internal DNS]	[System DNS] ページ上の DNS サーバ IP アドレスを、PPPoE サーバから取得された DNS アドレスで置き換える場合にオンにします。 VDOM が有効になっている場合、内部の DNS は管理 VDOM 上でのみ置き換えることができます。

インタフェース上でのダイナミック DNS の設定

FortiGate ユニットに静的なドメイン名と動的なパブリック IP アドレスが設定されている場合は、ダイナミック DNS (DDNS) サービスを使用して、ドメインの IP アドレスの変更時にインターネット DNS サーバを更新できます。

DDNS は、NAT/ ルート モードでのみ使用できます。

インタフェース上で DDNS を設定するには

1 DDNS サービスから DDNS 設定情報を取得します。

2 *[System]*、*[Network]*、*[Interface]* の順に選択します。

3 *[Create New]* を選択します。

4 *[DDNS]* を有効にします。

5 DDNS 設定情報を入力します。

FortiGate ユニットは、DDNS サーバに接続できない場合は常に、1 分間隔で 3 回の再試行を行った後、3 分間隔での再試行に移行します。これは、DDNS サーバのフラッディングを防ぐためです。

[Enable DDNS] を選択すると、次の画面が表示されます。

[Server]	使用する DDNS サーバを選択します。これらのサービスのクライアント ソフトウェアは、FortiGate ファームウェアに組み込まれています。FortiGate ユニットは、これらのサービスのいずれかにのみ接続できます。
[Domain]	DDNS サービスの完全修飾ドメイン名を入力します。
[Username]	DDNS サーバに接続するときに使用するユーザ名を入力します。
[Password]	DDNS サーバに接続するときに使用するパスワードを入力します。

仮想 IPSec インタフェースの設定

仮想 IPSec インタフェースは、IPSec VPN フェーズ 1 の *[Advanced]* オプションを設定するときに *[Enable IPSec Interface Mode]* を選択することによって作成します。

IPSec VPN フェーズ 1 を設定するには、*[VPN]*、*[IPSec]*、*[Auto Key (IKE)]* の順に選択し、*[Create Phase 1]* を選択します。また、IPSec VPN 手動キーの設定を設定するときに [IPsec Interface Mode] を選択することもできます。IPSec VPN 手動キーを設定するには、*[VPN]*、*[IPSec]*、*[Manual Key]* の順に選択し、*[Create New]* を選択します。

どちらの場合も、IPSec VPN 設定で選択した物理インタフェースに IPSec VPN 仮想インタフェースが追加されます。

仮想 IPSec インタフェースは、*[System]*、*[Network]*、*[Interface]* の順に選択して表示されるリストに示されます。IPSec VPN の設定の詳細については、413 ページの「自動キー (IKE)」および 419 ページの「手動キー」を参照してください。

IPSec VPN インタフェースでは、次の操作を行うことができます。

- IPSec インタフェースのローカルおよびリモート エンドポイントの IP アドレスを設定することにより、そのインタフェースを介してダイナミック ルーティングを実行したり、ping を使用してトンネルをテストしたりできるようにする。
- IPSec インタフェースを介した管理アクセスを有効にする。
- インタフェースの説明を入力する。

[Name]	この IPSec インタフェースの名前。
[Virtual Domain]	この IPSec インタフェースの VDOM を選択します。
[IP] **[Remote IP]**	トンネルでダイナミック ルーティングを使用する場合や、トンネル インタフェースに ping を発行できるようにする場合は、トンネルのローカルおよびリモート エンドポイントの IP アドレスを入力します。この 2 つのアドレスは、ネットワーク内の他のどの場所でも使用されていないアドレスにする必要があります。

[Administrative Access]	このインタフェースで許可されている管理アクセスの種類を選択します。
[HTTPS]	このインタフェースを介した Web ベース マネージャへのセキュアな HTTPS 接続を許可します。
[PING]	このインタフェースによる ping への応答を許可します。この設定は、インストールの確認やテストに使用します。
[HTTP]	このインタフェースを介した Web ベース マネージャへの HTTP 接続を許可します。HTTP 接続はセキュリティ保護されていないため、第三者によって傍受される可能性があります。
[SSH]	このインタフェースを介した CLI への SSH 接続を許可します。
[SNMP]	リモートの SNMP マネージャがこのインタフェースに接続することによって SNMP 情報を要求できるようにします。143 ページの「SNMP の設定」を参照してください。
[TELNET]	このインタフェースを介した CLI への Telnet 接続を許可します。Telnet 接続はセキュリティ保護されていないため、第三者によって傍受される可能性があります。
[Description]	このインタフェースの説明を入力します。最大 63 文字まで入力できます。

インタフェースへの管理アクセスの設定

管理アクセスは、管理者が FortiGate ユニットに接続して設定を表示したり変更したりするための方法です

NAT/ ルート モードで動作している FortiGate ユニットのリモート管理を許可できますが、インターネットからのリモート管理を許可すると、FortiGate ユニットのセキュリティが危険にさらされる可能性があります。設定にとって必須でない限り、この危険性を避けるようにしてください。

インターネットからのリモート管理を許可する FortiGate ユニットのセキュリティを向上させるための方法は次のとおりです。

- セキュアな管理ユーザ パスワードを使用します。
- これらのパスワードを定期的に変更します。
- HTTPS または SSH のみを使用して、このインタフェースへのセキュアな管理アクセスを有効にします。
- システムのアイドル タイムアウトをデフォルト値の 5 分から変更しないでください（184 ページの「設定」を参照）。

トランスペアレント モードで管理アクセスを設定する方法の詳細については、165 ページの「動作モードおよび VDOM 管理アクセス」を参照してください。

インタフェースへの管理アクセスを制御するには

1 *[System]*、*[Network]*、*[Interface]* の順に選択します。
2 管理アクセスを制御するインタフェースを編集します。
3 このインタフェースの *[Administrative Access]* の方法を選択します。
4 *[OK]* を選択します

ゲートウェイ負荷分散のためのインタフェース ステータス検出の設定

インタフェース ステータス検出は、あるインタフェースから送信されたパケットに対してサーバから応答が返ることを確認する FortiGate ユニットで構成されます。最大 3 種類のプロトコルを使用して、インタフェースがそのサーバに接続できることを確認できます。通常、このサーバは、外部ネットワークまたはインターネットにつながるネクストホップ ルータです。インタフェース ステータス検出では、設定されているプロトコルを使用してパケットを送信します。サーバから応答が受信された場合、FortiGate ユニットは、このインタフェースがネットワークに接続できると見なします。応答が受信されない場合、FortiGate ユニットは、このインタフェースがネットワークに接続できないと見なします。

インタフェース ステータス検出は、ECMP ルート フェールオーバーや負荷分散に使用されます。237 ページの「ECMP ルートのフェールオーバーと負荷分散」*を参照してください。*

サーバやネットワークが正常に動作していたとしても応答が受信されない可能性があるため、停止ゲートウェイ検出の設定では、サーバへの接続をテストする時間間隔と、FortiGate ユニットによってインタフェースがサーバに接続できないと判断されるまでにテストが失敗できる回数を制御します。停止ゲートウェイ検出の設定については、112 ページの「ネットワーク オプションの設定」を参照してください。

インタフェースのゲートウェイ フェールオーバーの検出を設定するには、Web ベース マネージャから *[System]*、*[Network]*、*[Interface]* の順に選択し、インタフェースを編集します。*[Detect Interface Status for Gateway Load Balancing]* を選択し、接続をテストするサーバの IP アドレスを入力して、そのサーバへの接続をテストするために使用する 1 つ以上のプロトコルを選択します。インタフェースにセカンダリ IP アドレスを追加した場合は、セカンダリ IP アドレスごとに別々にインタフェース ステータス検出を設定することもできます。

注記：FortiGate ユニットが、選択したプロトコルのうちの少なくとも 1 つに対する応答を受信している限り、FortiGate ユニットはそのサーバが動作しており、パケットを転送できると見なします。複数のプロトコルに対して応答を受信してもサーバまたはインタフェースのステータスが強化されることはなく、応答を受信したプロトコルの数が少なくてもサーバまたはインタフェースのステータスが低下することはありません。

[New Interface] ページの [Detect Interface Status for Gateway Load Balancing] セクション

[Detect Server]	接続をテストするサーバの IP アドレス。
[Ping]	サーバが応答していることを確認するために、標準の ICMP ping を使用します。ping によって、サーバが ICMP ping 要求に応答できることが確認されます。
[TCP Echo]	サーバが応答していることを確認するために、TCP エコーを使用します。このオプションは、サーバが TCP エコー サービスを提供するように設定されている場合に選択します。場合によっては、サーバが TCP エコー要求には応答するが、ICMP ping に応答しないように設定されていることがあります。 TCP エコーは、ポート番号 7 上の TCP パケットを使用してテキスト文字列をサーバに送信し、そのサーバからのエコー応答の戻りを期待します。エコー応答は、単にその同じテキストをエコーバックして、サーバが TCP 要求に応答できることを確認します。 FortiGate ユニットは、TCP エコー サーバからの RST（リセット）パケットを通常の TCP エコー応答として認識しません。FortiGate が TCP エコー要求に対する RST 応答を受信した場合、その FortiGate ユニットはサーバが到達不可であると見なします。
[UDP Echo]	サーバを検出するために、UDP エコーを使用します。このオプションは、サーバが UDP エコー サービスを提供するように設定されている場合に選択します。場合によっては、サーバが UDP エコー要求には応答するが、ICMP ping に応答しないように設定されていることがあります。 UDP エコーは、ポート番号 7 上の UDP パケットを使用してテキスト文字列をサーバに送信し、そのサーバからのエコー応答を期待します。エコー応答は、単にその同じテキストをエコーバックして、サーバが UDP 要求に応答できることを確認します。
[Spillover Threshold]	このインタフェースで処理される帯域幅の量を制限するには、スピルオーバーしきい値を設定します。*[Spillover Thresholds]* の範囲は 0 ～ 2097000 KBps です。 このインタフェースで処理される帯域幅がスピルオーバーしきい値に達するまで、FortiGate ユニットは、ECMP によってルーティングされるすべてのセッションを最も小さい番号のインタフェースに送信します。その後、FortiGate ユニットは、以降のセッションをその次に小さい番号のインタフェースに送信します。 各インタフェースが選択される順序を含む詳細については、237 ページの「ECMP ルートのフェールオーバーと負荷分散」を参照してください。

注記：TCP エコーと UDP エコーの詳細については、RFC 862 を参照してください。

インタフェースの MTU パケット サイズの変更

ネットワーク パフォーマンスを向上させるために、FortiGate ユニットが転送するパケットの最大転送単位（MTU）を変更できます。MTU は、FortiGate ユニットとパケットの宛先との間のすべてのネットワークの最小の MTU と同じであることが理想です。FortiGate ユニットが送信するパケットが最小の MTU より大きい場合は、パケットが分割（または断片化）され、それによって転送速度が低下します。MTU を小さくしてみることにより、最適なネットワーク パフォーマンスが得られる MTU サイズを簡単に見つけることができます。

一部のFortiGateモデルでは、従来の1,500バイトを超えるフレームをサポートするインタフェースを選択します。FortiGate ユニットがサポートしている最大フレーム サイズについては、フォーティネット カスタマ サポートにお問い合わせください。

あるルートを介してより大きなフレームを送信できるようにするには、そのルート上のすべてのイーサネット デバイスがその大きなフレーム サイズをサポートしている必要があります。そうしないと、その大きなフレームが認識されずに破棄されます。

同じインタフェース上に標準のサイズとより大きなフレーム サイズのトラフィックが存在する場合、ルーティングの仕組みだけでは、フレーム サイズのみに基づいて各トラフィックを異なるルートにルーティングすることができません。ただし、VLAN を使用すると、より大きなフレーム トラフィックが、そのより大きなサイズをサポートするネットワーク デバイスを介してルーティングされることを保証できます。VLAN は、MTU サイズを親インタフェースから継承します。VLAN を、そのルートの両端だけでなく、そのルートに沿ったすべてのスイッチおよびルータに設定する必要があります。VLAN 設定の詳細については、『*FortiGate VLAN および VDOM ガイド*』を参照してください。

インタフェースから送信されるパケットの MTU サイズを変更するには

1 *[System]*、*[Network]*、*[Interface]* の順に選択します。
2 物理インタフェースを選択し、*[Edit]* を選択します。
3 *[Administrative Access]* で、*[Override default MTU value (1500)]* を選択します。
4 MTU サイズを設定します。

FortiGate ユニットでサポートされているサイズより大きい MTU サイズを選択すると、エラー メッセージが表示されます。この場合は、値がサポートされるサイズになるまで MTU サイズを小さくしてみてください。

注記: MTU を変更した場合は、変更されたインタフェース上の VLAN サブインタフェースの MTU 値を更新するために、FortiGate ユニットを再起動する必要があります。

トランスペアレント モードでは、インタフェースの MTU を変更した場合、その新しい MTU に一致するように FortiGate ユニット上のすべてのインタフェースの MTU を変更する必要があります。

インタフェースへのセカンダリ IP アドレスの追加

インタフェースに手動またはスタティック IP アドレスが設定されている場合は、そのインタフェースにセカンダリ スタティック IP アドレスを追加することもできます。セカンダリ IP アドレスの追加によって、そのインタフェースに実質的に複数の IP アドレスが追加されます。FortiGate ユニット、スタティック ルーティングやダイナミック ルーティング、およびネットワークは、セカンダリ IP アドレスを、そのインタフェースで終了する追加の IP アドレスとして認識します。DCHP または PPPoE を使用してセカンダリ IP アドレスを割り当てることはできません。

インタフェースに追加されたすべての IP アドレスが、物理インタフェースの 1 つの MAC アドレスに関連付けられます。また、すべてのセカンダリ IP アドレスが、追加先のインタフェースと同じ VDOM 内に存在します。ゲートウェイ負荷分散のためのインタフェース ステータス検出は、セカンダリ IP アドレスごとに別々に設定します。他のすべてのインタフェース IP アドレスと同様に、別の VDOM に含まれていない限り、セカンダリ IP アドレスは、FortiGate インタフェースに割り当てられた他のプライマリまたはセカンダリ IP アドレスと同じサブネット上に存在できません。

インタフェースにセカンダリ IP アドレスを追加するには

1 *[System]*、*[Network]*、*[Interface]* の順に選択します。
2 セカンダリ IP アドレスの追加先の物理インタフェースを編集します。
3 インタフェースの *[Addressing Mode]* が *[Manual]* に設定され、そのインタフェースに *[IP/Netmask]* を追加していることを確認します。
4 青色の矢印を選択して *[Secondary IP Address]* セクションを展開します。

5 セカンダリ IP アドレスを設定し、*[OK]* を選択して、アドレスとその設定をインタフェースに追加します。

6 さらに多くのセカンダリ IP アドレスを追加するには、この手順を繰り返します。

7 *[Edit Interface]* ダイアログの一番下にある *[OK]* または *[Apply]* を選択して、インタフェースにセカンダリ IP アドレスを追加します。

ヒント： セカンダリ IP アドレスを追加し、*[OK]* を選択して *[Edit Interface]* ダイアログへの変更を保存したら、セカンダリ IP アドレスが予期したとおりに追加されていることを確認するために、再度インタフェースを表示してください。

[New Interface] ページの [Secondary IP Address] セクション

作成されたセカンダリ IP アドレスを表示します。

[Add]	新しいセカンダリ IP アドレスを作成する場合に選択します。[Add] を選択すると、[Edit Interface] ページに自動的にリダイレクトされます。
[IP/Netmask]	このセカンダリ IP の IP アドレスとネットマスク。
[Detect Server Enable]	このセカンダリ IP アドレスに対してインタフェース ステータス検出が有効になっているかどうかを示します。
[Detect Server]	このセカンダリ IP アドレスの検出サーバの IP アドレス。複数のセカンダリ IP アドレスで同じ検出サーバを共有できます。
[Detect Protocol]	このセカンダリ IP アドレスに対して設定されている検出プロトコル。
[Administrative Access]	このアドレスの管理アクセス方法。プライマリ IP アドレスとは異なる方法を選択できます。
[Delete]	このセカンダリ IP アドレスを削除する場合に選択します。
[Edit]	選択されたセカンダリ IP アドレスを編集します。*[編集]* アイコンを選択すると、編集するセカンダリ IP アドレスの設定が、セカンダリ IP アドレス テーブルの上にあるフィールドに表示されます。これらの設定を編集し、*[OK]* を選択して、セカンダリ IP アドレスへの変更を保存できます。 **注記：**[編集] アイコンを選択してセカンダリ IP アドレスを編集し、*[IP/Netmask]* を変更した場合は、[OK] を選択したときに新しいセカンダリ IP アドレスが追加されます。変更するのが *[IP/Netmask]* だけであり、新しいセカンダリ IP アドレスを追加したくない場合は、[編集] アイコンを選択した時点のセカンダリ IP アドレスを削除する必要があります。

[Edit Interface] ページ

IP アドレスを設定するための各設定を提供します。[Add] を選択すると、このページに自動的にリダイレクトされます。

[IP/Netmask]	このセカンダリ IP アドレスの IP アドレス / サブネット マスクを入力します。セカンダリ IP アドレスは、プライマリ IP アドレスとは別のサブネット上に存在する必要があります。[To]
[Detect Interface Status for Gateway Load Balancing]	このセカンダリ IP アドレスのインタフェース ステータス検出を設定します。101 ページの「ゲートウェイ負荷分散のためのインタフェース ステータス検出の設定」を参照してください。
[Detect Server]	使用されるサーバを入力します。
[Detect Protocol]	このセカンダリ IP アドレスのプロトコルを入力します。ping、udp-echo、および tcp-echo から選択できます。
[Administrative Access]	このセカンダリ IP で許可される管理アクセスの種類を選択します。
[HTTPS]	このセカンダリ IP を介した Web ベース マネージャへのセキュアな HTTPS 接続を許可します。
[PING]	セカンダリ IP による ping への応答を許可します。この設定は、インストールの確認やテストに使用します。
[HTTP]	このセカンダリ IP を介した Web ベース マネージャへの HTTP 接続を許可します。HTTP 接続はセキュリティ保護されていないため、第三者によって傍受される可能性があります。
[SSH]	このセカンダリ IP を介した CLI への SSH 接続を許可します。

[SNMP]	リモートの SNMP マネージャがこのセカンダリ IP に接続することによって SNMP 情報を要求できるようにします。143 ページの「SNMP の設定」を参照してください。
[TELNET]	このセカンダリ IP を介した CLI への Telnet 接続を許可します。 Telnet 接続はセキュリティ保護されていないため、 第三者によって傍受される可能性があります。

ソフトウェア スイッチ インタフェースの追加

FortiGate の CLI からソフトウェア スイッチ インタフェース (ソフト スイッチ インタフェースとも呼ばれる) を追加できます。ソフトウェア スイッチ インタフェースによって、2 つ以上の物理または無線FortiGate インタフェース間の単純なブリッジが形成されます。ソフトウェア スイッチ インタフェースに追加されたインタフェースは、物理インタフェース メンバと呼ばれます。ソフトウェア スイッチ インタフェースに追加した後、ソフトウェア スイッチ インタフェースのメンバに個別々のインタフェースとしてアクセスすることはできません。これらのインタフェースは、システムのインタフェース テーブルから削除されます。

アグリゲート インタフェースと同様に、ソフトウェア スイッチ インタフェースは通常のインタフェースのように機能します。ソフトウェア スイッチ インタフェースには 1 つの IP アドレスがあります。ソフトウェア スイッチ インタフェースとの間のファイアウォール ポリシーを作成したり、ソフトウェア スイッチ インタフェースをゾーンに追加したりできます。制限もいくつかあります。ソフトウェア スイッチ インタフェースを HA によって監視したり、HA ハートビート インタフェースとして使用したりすることはできません。

ソフトウェア スイッチ インタフェースにインタフェースを追加した場合は、どの設定からもこれらのインタフェースを参照できません。これには、デフォルト ルート、VLAN、VDOM 間リンク、およびポリシーが含まれます。

port1、external、および dmz 物理インタフェースを含む soft_switch という名前のソフトウェア スイッチ インタフェースを追加するには、次の CLI コマンドを使用します。

```
config system switch-interface
  edit soft_switch
    set members port1 external dmz
end
```

FortiGate インタフェースへの sFlow エージェントの追加

sFlow は、RFC 3176 で定義され、http://www.sflow.org で説明されているネットワーク監視プロトコルです。1 つ以上の FortiGate インタフェースを、ネットワーク トラフィックを監視し、トラフィック フローに関する情報を含むsFlowデータグラムをsFlowコレクタに送信するsFlowエージェントとして設定できます。sFlow エージェントは、物理インタフェース、VLAN インタフェース、およびアグリゲート インタフェースを含む任意の FortiGate インタフェースに追加できます。

sFlow は通常、ネットワークのトラフィック フローの全体像を提供するために使用されます。通常は、ネットワーク上のスイッチ、ルータ、およびファイアウォール上で sFlow エージェントを動作させ、それらのすべてからトラフィック データを収集し、コレクタを使用してトラフィック フローやパターンを表示します。

このデータを使用すると、ネットワークの正常なトラフィック フロー パターンを特定し、その後でトラフィック フローの問題を監視できます。これらの問題が見つかったら、それらの修正を試みた後、引き続き sFlow エージェントと sFlow コレクタを使用してその修正結果を表示できます。

FortiGate の sFlow エージェントは任意の sFlow エージェントのように機能して、インタフェース カウンタやフロー サンプルを sFlow データグラムに結合し、それが直ちに sFlow コレクタに送信されます。sFlow データグラムは、データを処理したり、大量のデータを収集したりすることなく直ちに送信されるため、sFlow エージェントを実行してもシステム パフォーマンスへの影響はほとんどありません。

sFlow データグラムを sFlow コレクタに送信するように FortiGate ユニットを設定するには

sFlow は、CLI からのみ設定できます。sFlow の使用を開始するには、sFlow コレクタの IP アドレスを FortiGate の設定に追加した後、FortiGate インタフェース上で sFlow エージェントを設定する必要があります。

1 sFlow コレクタの IP アドレスを 172.20.120.11 に設定するには、次のコマンドを入力します。

```
config system sflow
  set collector-ip 172.20.120.11
end
```

2 必要に応じて、sFlow エージェントが使用する UDP ポート番号を変更することもできます。このポートは、ネットワーク構成や sFlow コレクタで必要になった場合にのみ変更してください。デフォルトの sFlow ポートは 6343 です。次のコマンドは、sFlow エージェントのポートを 6345 に変更します。

```
config system sflow
  set collector-port 6345
end
```

3 port1 インタフェースの sFlow を有効にするには、次のコマンドを使用します。

```
  config system interface
    edit port1
      set sflow-sample enable
    end
```

4 sFlow エージェントを FortiGate インタフェースに追加するには、この手順を繰り返します。

5 また、各 sFlow エージェントのサンプリング レート、ポーリング間隔、およびサンプル方向を変更することもできます。

```
  config system interface
    edit port1
      set sample-rate <rate_number>
      set polling-interval <frequency>
      set sample-direction {both | rx | tx}
    end
```

複数の VDOM での sFlow

複数の VDOM で動作している FortiGate ユニットでは、管理 VDOM 以外の各 VDOM に、sFlow コレクタの異なる IP アドレスとポート番号を追加できます。VDOM_1 という名前の VDOM の sFlow 設定をカスタマイズするには、次のコマンドを使用します。

```
config vdom
  edit VDOM_1
    config system vdom-sflow
      set vdom-sflow enable
      set collector-ip 172.20.120.11
    end
```

管理 VDOM と、VDOM 固有の設定が設定されていないすべての VDOM は、グローバルな sFlow 設定を使用します。

ゾーンの設定

インタフェースをゾーンにグループ化すると、ポリシーの作成が簡略化されます。インタフェースをゾーンにグループ化することにより、各インタフェースの個別のポリシーを追加する代わりに、そのゾーンの 1 組のファイアウォール ポリシーを追加できます。インタフェースをゾーンに追加した後は、各インタフェースのポリシーは設定できなくなり、ゾーンのポリシーのみを設定できます。

ゾーンにはすべての種類のインタフェース (物理、VLAN、スイッチなど) を追加できるほか、ゾーンをインタフェースの種類の任意の組み合わせで構成できます。ゾーンの追加、ゾーンの名前変更や編集、ゾーン リストからのゾーンの削除を行うことができます。ゾーンを追加する場合は、ゾーンに追加するインタフェースの名前を選択します。

ゾーンは、バーチャル ドメインから設定されます。FortiGate の設定に複数のバーチャル ドメインを追加している場合は、ゾーンを追加または編集する前に、正しいバーチャル ドメインを設定していることを確認してください。

[Zone] ページ

作成したすべてのゾーンを表示します。このページでは、新しいゾーンを編集、削除、および作成することができます。

[Create New]	新しいゾーンを作成する場合に選択します。
[Name]	このゾーンの名前。
[Block intra-zone traffic]	同じゾーン内のインタフェース間のトラフィックがブロックされている場合は [Yes]、同じゾーン内のインタフェース間のトラフィックがブロックされていない場合は [No] を表示します。
[Interface Members]	このゾーンに追加されたインタフェースの名前。インタフェース名は、FortiGate モデルによって異なります。
[Edit]	ゾーンを編集または表示します。
[Delete]	ゾーンを削除します。

[Edit Zone] ページ

ゾーンを設定するための各設定を提供します。既存のゾーンを編集する場合は、このページに自動的にリダイレクトされます。

[Zone Name]	このゾーンの名前を入力します。
[Block intra-zone traffic]	ゾーン内のトラフィックのブロッキングを有効にします。
[Interface members]	このゾーンに関連付けられる (1 つまたは複数の) インタフェースを選択します。表示されるインタフェースは、特定のモデル上に存在するインタフェースを反映しています。たとえば、FortiGate-50B 上では、internal、wan1、および wan2 インタフェースをゾーンに使用できます。

モデム インタフェースの設定

次のいずれかの方法でモデムを接続する場合は、FortiGate ユニットにモデム インタフェースを含めることができます。

- サポートされている USB モデムを、USB インタフェースを備えた任意の FortiGate モデルに接続できます。
- サポートされているシリアル モデムを、シリアル モデム ポートを備えた任意の FortiGate モデルに接続できます。
- サポートされている PCMCIA モデムを、PCMCIA スロットを備えた任意の FortiGate モデルに挿入できます。PCMCIA モデムを挿入する前に、FortiGate ユニットの電源を切ってください。モデムを挿入した後に FortiGate ユニットに電源を入れると、そのモデムが自動的に検出され、モデム インタフェースが作成されます。

NAT/ ルート モードでは、モデムは次の 2 つのモードのいずれかで動作できます。

- 冗長 (バックアップ) モードでは、選択されたイーサネット インタフェースが使用できなくなると、そのイーサネット インタフェースからモデム インタフェースが自動的に処理を引き継ぎます。
- スタンドアロン モードでは、モデム インタフェースが、FortiGate ユニットからインターネットへの接続になります。

冗長モードまたはスタンドアロン モードでは、ISP に接続する場合、モデムが ISP に接続されるまで自動的に最大 3 つのダイヤルアップ アカウントをダイヤルするように FortiGate ユニットを設定できます。

その他のモデムは、USB シリアル コンバータを介して外付けモデムに接続できます。これらのモデムの場合は、CLI を使用してモデムの動作を設定する必要があります。

モデム インタフェースは最初、無効になっているため、Web ベース マネージャに表示するには CLI で有効にする必要があります。『*FortiGate CLI リファレンス*』にある `system modem` コマンドを参照してください。

注記：モデム インタフェースは AUX ポートではありません。モデムと AUX ポートは同じように見えるかもしれませんが、AUX ポートは関連付けられたインタフェースがなく、リモート コンソール接続に使用されます。AUX ポートは、FortiGate モデル 1000A、1000AFA2、および 3000A でのみ使用できます。詳細については、『*FortiGate CLI リファレンス*』にある `config system aux` コマンドを参照してください。

このトピックには、以下の内容が含まれています。

モデム設定の設定

FortiGate ユニットがモデムを使用して ISP のダイヤルアップ アカウントに接続するように、モデム設定を設定します。最大 3 つのダイヤルアップ アカウントを設定したり、スタンドアロンまたは冗長の動作を選択したり、モデムのダイヤルや接続解除の方法を設定したりすることができます。

モデムを備えた FortiGate-60B および FortiWifi-60B モデルの場合は、モデムを管理インタフェースにすることができます。有効になっている場合、ユーザはユニットのモデムにダイヤルし、いずれかの標準インタフェースを介してログインしているかのように管理アクションを実行できます。この機能は、CLI で `config system dialinsvr` コマンド構文を使用して有効にします。

VDOM が有効になっている場合は、他のインタフェースと同様に、モデムをいずれかの VDOM に割り当てることができます。

モデムは、無効になっているとインタフェース リストに表示されないため、CLI から次のコマンド構文を使用して有効にする必要があります。

```
config system modem
  set status enable
end
```

CLI で有効にした後、*[System]*、*[Network]*、*[Modem]* の順に選択して、Web ベース マネージャでモデムを設定することができます。

注記：モデムをトランスペアレント モードで設定したり、 使用したりすることはできません。

[Modem] ページ

モデムとダイヤルアップ アカウントを設定するための各設定を提供します。

[Enable Modem]	FortiGate のモデムを有効にする場合に選択します。
[Modem status]	モデム状態は [not active]、[connecting]、[connected]、[disconnecting]、[hung up] のいずれかです。
[Dial Now]/[Hang Up]	（スタンドアロン モードのみ）ダイヤルアップ アカウントに手動で接続するには、*[Dial Now]* を選択します。モデムが接続されている場合は、*[Hang Up]* を選択して手動でモデムを接続解除できます。
[Mode]	*[Standalone]* または *[Redundant]* モードを選択します。

[Auto-dial]（スタンドアロン モード）	接続が失われるか、または FortiGate ユニットが再起動されたら自動的にモデムをダイヤルする場合に選択します。*[Dial on demand]* がオンになっている場合は、*[Auto- dial]* をオンにできません。
[Dial on demand]（スタンドアロン モード）	パケットがモデム インタフェースにルーティングされたらモデムをダイヤルする場合に選択します。ネットワークが動作していない場合、モデムはアイドル タイムアウト期間の後に接続解除します。*[Auto-dial]* がオンになっている場合は、*[Dial on demand]* をオンにできません。
[Idle timeout]（スタンドアロン モード）	タイムアウト期間（分単位）を入力します。動作していない状態がこの期間続くと、モデムは接続解除します。
[Redundant for]（冗長モード）	モデムがバックアップ サービスを提供する対象のイーサネット インタフェースを選択します。
[Holddown Timer]（冗長モード）	（冗長モードのみ）プライマリ インタフェースが復旧した後、モデム インタフェースから元のプライマリ インタフェースに切り替えるまでに FortiGate ユニットが待つ時間（1 ～ 60 秒）を入力します。デフォルト値は 1 秒です。プライマリ インタフェースとモデム インタフェースの間で FortiGate ユニットの切り替えが繰り返し発生する場合は、設定する値を大きくします。
[Redial Limit]	接続に障害が発生した場合に、FortiGate ユニットのモデムが ISP への再接続を試行する最大回数（1 ～ 10）。デフォルトの再ダイヤル制限は 1 回です。再ダイヤルの試行回数を制限しないようにするには、*[None]* を選択します。
[Wireless Modem]	接続されている無線モデムを表示します（使用可能な場合）。
[Supported Modems]	サポートされているモデムのリストを表示する場合に選択します。
[Usage History]	モデム インタフェース上で作成された接続を表示します。接続に関する次の情報が表示されます。 ・ 日付と時刻 ・ 接続時間（時間、分、秒） ・ 接続先の IP アドレス ・ トラフィック統計（受信、送信、合計を含む） ・ 接続の現在のステータス
[Dialup Account]	最大 3 つのダイヤルアップ アカウントを設定します。FortiGate ユニットは、接続を確立できるまで、順番に各アカウントへの接続を試みます。アクティブなダイヤルアップ アカウントは緑色のチェックマークで示されます。
[Phone Number]	ダイヤルアップ アカウントに接続するために必要な電話番号。電話番号にはスペースを追加しないでください。ダイヤルアップ アカウントに接続するためにモデムに必要な一時停止、国番号、その他の機能に対する標準の特殊文字を間違いなく含めるようにしてください。
[User Name]	ISP に送信されるユーザ名（最大 63 文字）。
[Password]	ISP に送信されるパスワード。
[Extra Initialization String]	追加の初期化文字列。

冗長モードでモデムを設定するには、110 ページの「冗長モードの設定」を参照してください。

スタンドアロン モードでモデムを設定するには、110 ページの「スタンドアロン モードの設定」を参照してください。

次の項も参照してください。

- モデム インタフェースの設定
- モデム接続のためのファイアウォール ポリシーの追加
- モデムの接続と接続解除
- モデム状態の確認

冗長モードの設定

冗長モードでは、モデム インタフェースは選択されたイーサネット インタフェースをバックアップします。そのイーサネット インタフェースがネットワークから接続解除した場合、モデムは、設定済みのダイヤルアップ アカウントに自動的にダイヤルします。モデムがダイヤルアップ アカウントに接続すると、FortiGate ユニットは、通常は選択されたイーサネット インタフェースに宛てられる IP パケットをモデム インタフェースにルーティングします。

イーサネット インタフェースがネットワークに接続できるようになると、FortiGate ユニットはモデム インタフェースを接続解除して、イーサネット インタフェースに戻します。トラフィックを切り替える前にインタフェースが安定し、完全にアクティブな状態であることを保証するために、元のイーサネット インタフェースへの切り替えを遅延させるホールドダウンタイマを設定できます。

モデムは、アイドル タイムアウトの値で設定された、ネットワークが動作していない期間の後に接続解除します。これにより、ダイヤルアップ接続料金が節約されます。

FortiGate ユニットでのイーサネット インタフェースからモデムへの切り替えを可能にするには、モデム設定でインタフェースの名前を選択し、そのインタフェースのための ping サーバを設定する必要があります。また、モデム インタフェースとその他の FortiGate インタフェースの間の接続のためのファイアウォール ポリシーも設定する必要があります。

注記： モデム インタフェースと、モデムがバックアップしているイーサネット インタフェースの間の接続のためのポリシーは追加しないでください。

冗長モードを設定するには

1 *[System]*、*[Network]*、*[Modem]* の順に選択します。
2 *[Redundant]* モードを選択します。
3 次の情報を入力します。

[Redundant for]	リストから、バックアップするインタフェースを選択します。
[Holddown timer]	ネットワーク接続が復旧した後もモデムを使用し続ける秒数を入力します。
[Redial Limit]	ISP が応答しない場合の再試行の最大回数を入力します。
[Dialup Account 1] **[Dialup Account 2]** **[Dialup Account 3]**	最大 3 つのダイヤルアップ アカウントに対する ISP の電話番号、ユーザ名、およびパスワードを入力します。

4 *[Apply]* を選択します。
5 モデムがバックアップするイーサネット インタフェースのインタフェース ステータス検出を設定します。
101 ページの「ゲートウェイ負荷分散のためのインタフェース ステータス検出の設定」を参照してください。
6 モデム インタフェースを介したネットワーク接続のためのファイアウォール ポリシーを設定します。
111 ページの「モデム接続のためのファイアウォール ポリシーの追加」を参照してください。

スタンドアロン モードの設定

スタンドアロン モードでは、モデムは、インターネットへの接続を提供するためにダイヤルアップ アカウントに接続します。FortiGate ユニットが再起動した場合や、ルーティングされていないパケットが存在する場合にダイヤルするようにモデムを設定できます。また、手動でモデムを接続解除したり、再ダイヤルしたりすることもできます。

ダイヤルアップ アカウントへの接続が切断した場合、FortiGate ユニットはモデムを再ダイヤルします。モデムは、再ダイヤル制限で指定された回数に達するか、またはダイヤルアップ アカウントに接続するまで再ダイヤルします。

モデムは、アイドル タイムアウトの値で設定された、ネットワークが動作していない期間の後に接続解除します。これにより、ダイヤルアップ接続料金が節約されます。

モデム インタフェースとその他の FortiGate インタフェースの間の接続のためのファイアウォール ポリシーを設定する必要があります。

また、*[Router]*、*[Static]* の順に選択して、トラフィックをモデム インタフェースにルーティングするためのスタティック ルートを設定することも必要です。たとえば、モデム インタフェースが FortiGate ユニットの外部インタフェースとして機能している場合は、モデムへの FortiGate ユニットのデフォルト ルートのデバイス設定を設定する必要があります。

スタンドアロン モードを設定するには

1 *[System]*、*[Network]*、*[Modem]* の順に選択します。
2 *[Standalone]* モードを選択します。
3 次の情報を入力します。

[Auto-dial]	FortiGateユニットが再起動したらモデムがダイヤルするようにする場合に選択します。
[Dial on demand]	ルーティングされていないパケットが存在したら常にモデムが ISP に接続するようにしたい場合に選択します。
[Idle timeout]	タイムアウト期間（分単位）を入力します。動作していない状態がこの期間続くと、モデムは接続解除します。
[Redial Limit]	ISP が応答しない場合の再試行の最大回数を入力します。
[Dialup Account 1] **[Dialup Account 2]** **[Dialup Account 3]**	最大 3 つのダイヤルアップ アカウントに対する ISP の電話番号、ユーザ名、およびパスワードを入力します。

4 *[Apply]* を選択します。
5 モデム インタフェースを介したネットワーク接続のためのファイアウォール ポリシーを設定します。
111 ページの「モデム接続のためのファイアウォール ポリシーの追加」を参照してください。
6 *[Router]*、*[Static]* の順に選択し、モデムへのデバイスを設定して、トラフィックをモデム インタフェースにルーティングするためのスタティック ルートを設定します。
236 ページの「ルーティング テーブルへのスタティック ルートの追加」を参照してください。

モデム接続のためのファイアウォール ポリシーの追加

モデム インタフェースには、ファイアウォール アドレスとファイアウォール ポリシーが必要です。モデム インタフェースに 1 つ以上のアドレスを追加できます。アドレスの追加については、297 ページの「アドレスの設定」を参照してください。

ファイアウォール ポリシーを設定することにより、モデム インタフェースと、FortiGate ユニット上のその他のインタフェースの間のパケットのフローを制御できます。ファイアウォール ポリシーの設定については、268 ページの「ファイアウォール ポリシーの設定」を参照してください。

モデムの接続と接続解除

次の手順は、ダイヤルアップ アカウントに接続する方法と、ダイヤルアップ アカウントから接続解除する方法を示しています。モデムはスタンドアロン モードにある必要があるため、ダイヤルアップ アカウントへの接続または接続解除の前に、モデムがスタンドアロン モードにあることを確認する必要があります。

ダイヤルアップ アカウントに接続するには

1 *[System]*、*[Network]*、*[Modem]* の順に選択します。
2 *[Enable USB Modem]* を選択します。

3 ダイヤルアップ アカウントの情報を確認します。
4 *[Apply]* を選択します。
5 *[Dial Now]* を選択します。
FortiGate ユニットは、モデムが ISP に接続するまで、順番に各ダイヤルアップ アカウントにダイヤルします。

ダイヤルアップ アカウントから接続解除するには

1 *[System]*、*[Network]*、*[Modem]* の順に選択します。
2 *[Hang Up]* を選択して、モデムを接続解除します。

モデム状態の確認

モデムの接続状態や、現在どのダイヤルアップ アカウントがアクティブになっているかを確認できます。モデムが ISP に接続されている場合は、IP アドレスとネットマスクを表示できます。

モデム状態を確認するには、*[System]*、*[Network]*、*[Modem]* の順に選択します。

モデム状態は次のいずれかです。

[not active]	このモデムは、ISP に接続されていません。
[connecting]	このモデムは、ISP に接続しようとしています。
[connected]	このモデムは、ISP に接続されています。
[disconnecting]	このモデムは、ISP から接続解除しています。
[hung up]	このモデムは、ISP から接続解除しました。（スタンドアロン モードのみ） [Dial Now] を選択しない限り、モデムは再ダイヤルしません。

緑色のチェックマークは、アクティブなダイヤルアップ アカウントを示します。

モデム インタフェースに割り当てられた IP アドレスとネットマスクは、Web ベース マネージャの *[System]*、*[Network]*、*[Interface]* の順に選択して表示される画面に表示されます。

ネットワーク オプションの設定

ネットワーク オプションには、DNS サーバや停止ゲートウェイ検出の設定が含まれます。停止ゲートウェイ検出の設定によって、インタフェース ステータス検出の動作が制御されます。DNS やその他のネットワーク オプションの設定は、*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページから設定できます。

***[Networking Options]* ページ**

DNS 設定のほか、停止ゲートウェイ検出の設定を設定するための各設定を提供します。また、このページから DNS サーバの設定や停止ゲートウェイ検出の設定を表示することもできます。

[DNS Settings]

[Primary DNS Server]	プライマリ DNS サーバの IP アドレスを入力します。
[Secondary DNS Server]	セカンダリ DNS サーバの IP アドレスを入力します。
[Local Domain Name]	DNS参照の実行時にドメイン部分のないアドレスに追加するドメイン名を入力します。

[IPv6 DNS Settings]

[Primary DNS Server]	プライマリ IPv6 DNS サーバの IP アドレスを入力します。
[Secondary DNS Server]	セカンダリ IPv6 DNS サーバの IP アドレスを入力します。
[Dead Gateway Detection]	1 つ以上の FortiGate インタフェースのインタフェース ステータス検出を設定し、停止ゲートウェイ検出の設定を使用してインタフェース ステータス検出の動作を設定します。詳細については、101 ページの「ゲートウェイ負荷分散のためのインタフェース ステータス検出の設定」を参照してください。

[Detection Interval]	FortiGate ユニットがインタフェース ステータスを検出する間隔を示す秒数を入力します。
[Fail-over Detection]	FortiGate ユニットがこのインタフェースを機能していないと見なすまでのインタフェース ステータス テストの失敗回数を入力します。

DNS サーバ

アラート メールや URL ブロッキングなど、FortiGate 機能の一部は DNS を使用しています。FortiGate ユニットの接続先の DNS サーバの IP アドレスを指定することができます。DNS サーバ IP アドレスは通常、ISP によって指定されます。

100 以下の番号の FortiGate モデルは、DNS サーバ アドレスを自動的に取得するように設定できます。これらのアドレスを自動的に取得するには、少なくとも 1 つの FortiGate ユニット インタフェースが DHCP または PPPoE アドレッシング モードを使用する必要があります。98 ページの「インタフェース上での DHCP の設定」または 99 ページの「インタフェース上での PPPoE の設定」を参照してください。

100 以下の FortiGate モデルは、そのインタフェース上で DNS 転送を実行できます。接続されたネットワーク上のホストは、このインタフェースの IP アドレスを DNS サーバとして使用します。このインタフェースに送信された DNS 要求は、ユーザによって設定されたか、または FortiGate ユニットによって自動的に取得された DNS サーバ アドレスに転送されます。

FortiGate DNS サービスの設定

FortiGate ユニットを、FortiGate インタフェースと通信できる任意のネットワークの DNS サーバになるように設定できます。各インタフェースの DNS 設定を、次のいずれかの方法で設定します。

- インタフェースは、*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで FortiGate ユニット用に設定された DNS サーバに DNS 要求を中継します。115 ページの「DNS 要求を外部の DNS サーバに中継するように FortiGate インタフェースを設定するには」を参照してください。
- インタフェースは、FortiGate DNS データベースを使用して DNS 要求を解決します。FortiGate DNS データベース内に存在しないホスト名への DNS 要求は破棄されます。115 ページの「FortiGate DNS データベースのみを使用して DNS 要求を解決するように FortiGate インタフェースを設定するには」を参照してください。
- インタフェースは、FortiGate DNS データベースを使用して DNS 要求を解決し、FortiGate DNS データベース内に存在しないホスト名への DNS 要求を、*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで FortiGate ユニット用に設定された DNS サーバに中継します。これは、分割 DNS 設定と呼ばれます。116 ページの「分割 DNS 設定を設定するには」を参照してください。

バーチャル ドメインが有効になっていない場合は、すべての FortiGate インタフェースで共有できる 1 つの DNS データベースを作成できます。

バーチャル ドメインが有効になっている場合は、各 VDOM で DNS データベースを作成します。VDOM 内のすべてのインタフェースが、その VDOM 内の DNS データベースを共有します。

この項には、以下のトピックが含まれています。

分割 DNS について

分割 DNS 設定では、FortiGate ユニット上で、通常は内部ネットワーク上のホスト名、またはローカル ドメインのための DNS データベースを作成します。内部ネットワーク上のユーザがこれらのホスト名に接続しようとした場合、IP アドレスは、FortiGate ユニットの DNS データベースによって提供されます。FortiGate ユニットの DNS データベース内に存在しないホスト名は、DNS 参照を外部の DNS サーバに中継することによって解決されます。

分割 DNS 設定を使用すると、内部ユーザが、インターネットからもアクセスできるプライベート ネットワーク上のリソースにアクセスできるようになります。たとえば、NAT/ ルート モードで動作している FortiGate ユニットの背後にパブリック Web サーバを配置できます。インターネット上のユーザは、ポート フォワーディング仮想 IP を使用して、この Web サーバにアクセスします。そのため、この Web サーバには、インターネット ユーザのためのパブリック IP アドレスが存在します。しかし、内部ユーザからのトラフィックをインターネットから遮断するために、内部ネットワーク上のユーザがプライベート IP アドレスを使用してサーバにアクセスするようにしたい場合があります。これを行うには、FortiGate ユニット上で分割 DNS 設定を作成し、サーバのホスト名を FortiGate DNS データベースに追加します。ただし、外部 IP アドレスの代わりに、サーバの内部 IP アドレスを含めます。FortiGate ユニットは最初に FortiGate DNS データベースをチェックするため、サーバのホスト名へのすべての DNS 参照がサーバの内部 IP アドレスを返します。

分割 DNS を設定する方法の例については、116 ページの「分割 DNS 設定を設定するには」を参照してください。

FortiGate DNS サービスの設定

この項では、FortiGate DNS を設定するための一般的な手順のほか、さまざまな方法で DNS サービスを提供するように FortiGate インタフェースを設定するための特定の手順について説明します。

一般的な FortiGate DNS サーバ設定

1 *[System]*、*[Network]*、*[Options]* の順に選択し、プライマリおよびセカンダリ DNS サーバの IP アドレスを追加します。

これらのサーバは、ISP によって提供される DNS サーバまたはその他のパブリック DNS サーバである必要があります。FortiGate ユニットが、これらの DNS サーバを独自の DNS 参照に使用するほか、内部ネットワークの DNS 参照を提供するためにも使用できます。112 ページの「ネットワーク オプションの設定」を参照してください。

2 *[System]*、*[Network]*、*[Interface]* の順に選択し、FortiGate ユニットを DNS サーバにする対象のネットワークに接続されるインタフェースを編集します。

3 *[Enable DNS Query]* を選択します。

[Enable DNS Query] を選択した場合、FortiGate ユニットは、このインタフェースで受信されたすべての DNS クエリを、*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで設定された DNS サーバに中継します。この動作を制御するには、*[Recursive]* または *[Non-Recursive]* を選択します。

[Recursive]	FortiGate DNS データベースでドメイン名を検索します。エントリが見つからない場合は、*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで設定された DNS サーバに要求を中継します。分割 DNS 設定に使用できます。
[Non-Recursive]	FortiGate DNS データベースでドメイン名を検索します。*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで設定された DNS サーバに要求を中継しません。

4 *[System]*、*[Network]*、*[DNS Database]* の順に選択し、FortiGate DNS データベースを設定します。

必要に応じてゾーンとエントリを追加します。116 ページの「FortiGate DNS データベースの設定」を参照してください。

5 FortiGate インタフェースを DNS サーバとして使用する内部ネットワーク上のホストを設定します。

また、FortiGate DHCP サーバを使用してこのネットワーク上のホストを設定している場合は、DNS サーバ IP アドレス リストに FortiGate インタフェースの IP アドレスを追加します。

DNS 要求を外部の DNS サーバに中継するように FortiGate インタフェースを設定するには

FortiGate インタフェースを、*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで FortiGate ユニット用に設定された DNS サーバに DNS 要求を中継するように設定します。

1 *[System]*、*[Network]*、*[Options]* の順に選択し、プライマリおよびセカンダリ DNS サーバの IP アドレスを追加します。

これらのサーバは、ISP によって提供される DNS サーバまたはその他のパブリック DNS サーバである必要があります。FortiGate ユニットが、これらの DNS サーバを独自の DNS 参照に使用するほか、内部ネットワークの DNS 参照を提供するためにも使用できます。112 ページの「ネットワーク オプションの設定」を参照してください。

2 *[System]*、*[Network]*、*[Interface]* の順に選択し、FortiGate ユニットを DNS サーバにする対象のネットワークに接続されるインタフェースを編集します。

3 *[Enable DNS Query]* を選択し、*[Recursive]* を選択します。

インタフェースは、FortiGate DNS データベース内でドメイン名を検索し、FortiGate DNS データベース内に存在しない名前への要求を、*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで設定された DNS サーバに中継するように設定されます。FortiGate DNS データベースにエントリを追加しない場合は、すべての DNS 要求が、*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで設定された DNS サーバに中継されます。

4 FortiGate インタフェースを DNS サーバとして使用する内部ネットワーク上のホストを設定します。

また、FortiGate DHCP サーバを使用してこのネットワーク上のホストを設定している場合は、DNS サーバ IP アドレス リストに FortiGate インタフェースの IP アドレスを追加します。

FortiGate DNS データベースのみを使用して DNS 要求を解決するように FortiGate インタフェースを設定するには

FortiGate インタフェースを、FortiGate DNS データベースを使用して DNS 要求を解決し、FortiGate DNS データベース内に存在しないホスト名への要求を破棄するように設定します。

1 *[System]*、*[Network]*、*[Options]* の順に選択し、プライマリおよびセカンダリ DNS サーバの IP アドレスを追加します。

これらのサーバは、ISP によって提供される DNS サーバまたはその他のパブリック DNS サーバである必要があります。FortiGate ユニットが、これらの DNS サーバを独自の DNS 参照に使用するほか、内部ネットワークの DNS 参照を提供するためにも使用できます。112 ページの「ネットワーク オプションの設定」を参照してください。

2 *[System]*、*[Network]*、*[Interface]* の順に選択し、FortiGate ユニットを DNS サーバにする対象のネットワークに接続されるインタフェースを編集します。

3 *[Enable DNS Query]* を選択し、*[Non-Recursive]* を選択します。

[Non-Recursive] 選択した場合は、FortiGate DNS データベース内のエントリのみが使用されます。

4 *[System]*、*[Network]*、*[DNS Database]* の順に選択し、FortiGate DNS データベースを設定します。

必要に応じてゾーンとエントリを追加します。116 ページの「FortiGate DNS データベースの設定」を参照してください。

5 FortiGate インタフェースを DNS サーバとして使用する内部ネットワーク上のホストを設定します。

また、FortiGate DHCP サーバを使用してこのネットワーク上のホストを設定している場合は、DNS サーバ IP アドレス リストに FortiGate インタフェースの IP アドレスを追加します。

分割 DNS 設定を設定するには

インタフェースを、FortiGate DNS データベースを使用して DNS 要求を解決し、FortiGate DNS データベース内に存在しないホスト名への DNS 要求を、*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで設定された DNS サーバに中継するように設定します。これは、分割 DNS 設定と呼ばれます。113 ページの「分割 DNS について」を参照してください。

1 *[System]*、*[Network]*、*[Options]* の順に選択し、プライマリおよびセカンダリ DNS サーバの IP アドレスを追加します。

これらのサーバは、ISP によって提供される DNS サーバまたはその他のパブリック DNS サーバである必要があります。FortiGate ユニットが、これらの DNS サーバを独自の DNS 参照に使用するほか、内部ネットワークの DNS 参照を提供するためにも使用できます。112 ページの「ネットワーク オプションの設定」を参照してください。

2 *[System]*、*[Network]*、*[Interface]* の順に選択し、FortiGate ユニットを DNS サーバにする対象のネットワークに接続されるインタフェースを編集します。

3 *[Enable DNS Query]* を選択し、*[Recursive]* を選択します。

インタフェースは、FortiGate DNS データベース内でドメイン名を検索し、FortiGate DNS データベース内に存在しない名前への要求を、*[System]*、*[Network]*、*[Options]* の順に選択して表示されるページで設定された DNS サーバに中継するように設定されます。内部ネットワーク上のユーザのために、FortiGate DNS データベースにエントリを追加できます。

4 *[System]*、*[Network]*、*[DNS Database]* の順に選択し、FortiGate DNS データベースを設定します。

内部ネットワーク上のユーザのために、必要に応じてゾーンとエントリを追加します。116 ページの「FortiGate DNS データベースの設定」を参照してください。

5 FortiGate インタフェースを DNS サーバとして使用する内部ネットワーク上のホストを設定します。

また、FortiGate DHCP サーバを使用してこのネットワーク上のホストを設定している場合は、DNS サーバ IP アドレス リストに FortiGate インタフェースの IP アドレスを追加します。

FortiGate DNS データベースの設定

内部ネットワークからの DNS 参照が FortiGate DNS データベースによって解決されるように FortiGate DNS データベースを設定します。DNS データベースを設定するには、ゾーンを追加します。各ゾーンには独自のドメイン名があります。

次に、各ゾーンにエントリを追加します。各エントリは、ホスト名と、そのホスト名が解決される IP アドレスで構成されます。また、そのエントリが IPv4 アドレス (A)、IPv6 アドレス (AAAA)、ネーム サーバ (NS)、正規名 (CNAME)、Mail Exchange (MX) 名のいずれであるかを指定することもできます。

FortiGate DNS データベースを設定するには、*[System]*、*[Network]*、*[DNS Server]* の順に選択します。

[DNS Server] ページ

作成した DNS サーバを表示します。このページでは、新しい DNS サーバを編集、削除、または作成することができます。

[Create New]	DNS データベース リストに新しい DNS ゾーンを追加します。[Create New] を選択すると、[New DNS Zone] ページに自動的にリダイレクトされます。
[DNS Zone]	DNS データベース リストに追加された DNS ゾーンの名前。
[Domain Name]	各ゾーンのドメイン名。
[TTL]	パケットの TTL (Time to Live) を示す、ドメイン名の TTL 値 (秒単位)。範囲は 0 ～ 2,147,483,647 です。
[# of Entries]	ゾーン内のエントリの数。
[Delete]	DNS データベースからゾーンを削除します。
[Edit]	既存のゾーンを変更するには、その横にある *[Edit]* を選択します。

[New DNS Zone] ページ

DNS サーバを構成する DNS ゾーンを設定するための各設定を提供します。

[DNS Zone] DNS ゾーンを入力します。

[Domain Name] ドメイン名を入力します。

[TTL (seconds)] TTL 値を入力します。ゾーンの TTL 値を使用するには、0 を入力します。

Explicit Web プロキシの設定

FortiGate の Explicit Web プロキシを使用すると、1 つ以上の FortiGate インタフェース上の明示的な HTTP と HTTPS のプロキシ処理を有効にすることができます。Explicit Web プロキシはまた、Web ブラウザから送信された FTP セッションのプロキシ処理や、Explicit Web プロキシのユーザの自動プロキシ設定を可能にするプロキシ自動設定 (PAC) もサポートしています。また、CLI からは、Web ブラウザから送信された SOCKS セッションをサポートするように Explicit Web プロキシを設定することもできます。

注記：VDOM が有効になっている場合、Web プロキシは各 VDOM に対して設定されます。

Web プロキシは、FortiGate のルーティングを使用して、セッションを FortiGate ユニット経由で宛先インタフェースにルーティングします。セッションが終了インタフェースから送信される前に、Explicit Web プロキシは、そのセッション パケットの発信元アドレスを終了インタフェースの IP アドレスに変更します。FortiGate ユニットがトランスペアレント モードで動作している場合、Explicit Web プロキシは、発信元アドレスを管理 IP アドレスに変更します。

通常、ネットワーク上のユーザのために Web プロキシ サーバを設定する場合は、そのネットワークに接続された FortiGate インタフェース上で Explicit Web プロキシを有効にします。ネットワーク上のユーザは、HTTP と HTTPS、FTP、または SOCKS に対してプロキシ サーバを使用するように Web ブラウザを設定し、プロキシ サーバの IP アドレスをそのネットワークに接続された FortiGate インタフェースの IP アドレスに設定します。ユーザはまた、FortiGate ユニット上に格納された PAC ファイルを使用して Web プロキシ設定を自動化するために、Web ブラウザに PAC URL を入力することもできます。

WAN 最適化をサポートする FortiGate ユニットでは、明示的なプロキシの Web キャッシュを有効にすることもできます。

Explicit Web プロキシを有効にするには

1 *[System]*、*[Network]*、*[Interface]* の順に選択し、1 つ以上の FortiGate インタフェースの Explicit Web プロキシを有効にします。

注意：インターネットに接続されたインタフェース上で Explicit Web プロキシを有効にすると、そのプロキシを見つけたインターネット上の任意のユーザがそれを使用して自分の発信元アドレスを隠すことができるため、セキュリティ上のリスクが発生します。

2 *[System]*、*[Network]*、*[Web Proxy]* の順に選択します。*[Enable Explicit Web Proxy]* を選択して、Explicit Web プロキシを有効にします。

3 *[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、[Create New] を選択して、*[Source Interface/Zone]* を *[web-proxy]* に設定します。

4 Explicit Web プロキシで処理されるようにしたいトラフィックを受け付けるために必要なファイアウォール ポリシーを設定します。

このポリシーの発信元アドレスは、クライアントの発信元 IP アドレスに一致している必要があります。このポリシーの宛先アドレスは、クライアントの接続先の Web サイトの IP アドレスに一致している必要があります。

Explicit Web プロキシに送信されたが、Web プロキシのファイアウォール ポリシーによって受け付けられないトラフィックは破棄されます。

5 必要に応じて、その他のファイアウォール ポリシー オプションを選択できます。

たとえば、Web プロキシ セッションに UTM 保護を適用したり、許可された Web プロキシ トラフィックをログに記録したりできます。

6 また、Explicit Web プロキシ セッションに認証を適用するために *[Enable Identity Based Policy]* を選択することもできます。

次のいくつかの認証オプションが使用できます。

- *[IP Based]* 認証では、発信元 IP アドレスによる認証が適用されます。ユーザが認証された後は、その認証がタイムアウトするまで、その IP アドレスから Explicit Web プロキシへのすべてのセッションが受け付けられます。
- *[IP Based]* を選択しない場合は、FortiGate ユニットによってセッション単位の HTTP 認証が適用されます。この認証はブラウザ ベースです。クライアントが、Web プロキシで認証されるためにブラウザにユーザ名とパスワードを入力すると、これらの情報はそのブラウザによって格納されます。同じ Web ブラウザによって開始される新しい各セッションも認証する必要がありますが、これはブラウザによって自動的に行われます。

  この認証はブラウザ ベースであるため、同じ IP アドレスを持つ複数のクライアントを独自の資格情報を使用してプロキシで認証できます。HTTP 認証では、同じ発信元 IP アドレスからの複数のユーザ セッションの認証が可能です。この状況は、各ユーザと FortiGate ユニットの間に NAT デバイスが存在する場合に発生することがあります。HTTP 認証はまた、複数のユーザの間で 1 つの IP アドレスを共有する他の構成での認証もサポートしています。これらには、Citrix 製品や Windows ターミナル サーバ、その他の同様の仮想化ソリューションが含まれます。

7 ユーザ グループごとに異なる認証を適用したり、さらにはまたユーザ グループごとに異なる UTM やロギングの設定を適用したりするために、複数の ID ベースのポリシーを追加できます。

Explicit Web プロキシ設定の設定

Explicit Web プロキシを設定するには、*[System]*、*[Network]*、*[Web Proxy]* の順に選択します。

[Web Proxy] ページ

Explicit Web プロキシとトランスペアレント Web キャッシュを設定するための各設定を提供します。

[Explicit Web Proxy Options] セクション

[Enable Explicit Web Proxy]	HTTP/HTTPS、FTP、およびプロキシ自動設定 PAC セッションに対する Explicit Web プロキシ サーバを有効にします。Explicit Web プロキシでパケットを受け付けたり、転送したりできるようにするには、このオプションを選択する必要があります。FTP と PAC は Web ブラウザからのみサポートされ、スタンドアロンのクライアントからはサポートされません（たとえば、スタンドアロンの FTP クライアントは Explicit Web プロキシ サーバを使用できません）。
[Listen on Interfaces]	Explicit Web プロキシによって監視されているインタフェースを表示します。VDOM が有効になっている場合は、現在の VDOM に属し、かつ Explicit Web プロキシが有効になっているインタフェースのみが表示されます。VLAN が設定されているインタフェース上で Web プロキシを有効にした場合、それらの VLAN は、手動で有効にした場合にのみ Web プロキシに対して有効になります。
[HTTP Port]	クライアントの Web ブラウザからの HTTP トラフィックが明示的なプロキシに接続するために使用するポート番号を入力します。デフォルトのポート番号は 8080 です。範囲は 0 ～ 65535 です。明示的なプロキシのユーザは、このポートを使用するように Web ブラウザの HTTP プロキシの設定を設定する必要があります。
[HTTPS Port]	クライアントの Web ブラウザからの HTTPS トラフィックが明示的なプロキシに接続するために使用するポート番号を入力します。範囲は 0 ～ 65535 です。明示的なプロキシのユーザは、このポートを使用するように Web ブラウザの HTTPS プロキシの設定を設定する必要があります。 0 のデフォルト値は、HTTP と同じポートを使用することを示します。
[FTP Port]	クライアントの Web ブラウザからの FTP トラフィックが明示的なプロキシに接続するために使用するポート番号を入力します。範囲は 0 ～ 65535 です。明示的なプロキシのユーザは、このポートを使用するように Web ブラウザの FTP プロキシの設定を設定する必要があります。 0 のデフォルト値は、HTTP と同じポートを使用することを示します。

[PAC Port]	クライアントの Web ブラウザからの PAC トラフィックが明示的なプロキシに接続するために使用するポートを選択します。範囲は 0 ～ 65535 です。明示的なプロキシのユーザは、このポートを使用するように Web ブラウザの PAC プロキシの設定を設定する必要があります。 0 のデフォルト値は、HTTP と同じポートを使用することを示します。

[PAC File Content]	PAC ファイル内の内容を変更するには、このオプションの横にある [編集] アイコンを選択します。また、このオプションを使用して PAC ファイルをインポートすることもできます。
	PAC ファイルの最大サイズは 8192 バイトです。
	ユーザのブラウザでサポートされている任意の PAC ファイル構文を使用できます。FortiGate ユニットは PAC ファイルを解析しません。
	PAC を使用するには、ユーザは、Web ブラウザのプロキシ設定に自動プロキシ設定 URL (または PAC URL) を追加する必要があります。デフォルトの PAC ファイルの URL は次のとおりです。
	`http://<interface_ip>:<PAC_port_int>/<pac_file_str>`
	たとえば、Explicit Web プロキシが設定されたインタフェースの IP アドレスが 172.20.120.122 で、PAC ポートが明示的なプロキシのデフォルトの HTTP ポート (8080) と同じであり、PAC ファイル名が proxy.pac の場合、PAC ファイルの URL は次のようになります。
	`http://172.20.120.122:8080/proxy.pac`
	CLI から、次のコマンドを使用して PAC ファイルの URL を表示できます。
	`get web-proxy explicit`

[Unknown HTTP version]	プロキシ サーバが不明な HTTP バージョンの要求またはメッセージを処理する必要がある場合に実行されるアクションを選択します。[Reject] または [Best Effort] から選択します。 [Best Effort] を指定すると、HTTP トラフィックを可能な限り処理しようとします。[Reject] を指定すると、既知の HTTP トラフィックを不正な形式として扱い、破棄します。[Reject] オプションの方が安全です。
[Realm]	Explicit Web プロキシを識別するための認証領域を入力します。この領域には、最大 63 文字の任意のテキスト文字列を指定できます。領域にスペースが含まれている場合は、引用符で囲みます。 ユーザが明示的なプロキシで認証される場合は、そのユーザの Web プロキシを領域で明示的に識別できるように、 HTTP 認証のダイアログにこの領域が含まれます。
[Default Firewall Policy Action]	Explicit Web プロキシのためのファイアウォール ポリシーが追加されていない場合にセッションをブロック (拒否) するか、または受け付けるように Explicit Web プロキシを設定します。Explicit Web プロキシのためのファイアウォール ポリシーを追加するには、ファイアウォール ポリシーを追加し、発信元インタフェースを *[web-proxy]* に設定します。 デフォルト設定または [Deny] を指定すると、ファイアウォール ポリシーを追加する前の Explicit Web プロキシへのアクセスがブロックされます。このオプションを *[Accept]* に設定すると、ファイアウォール ポリシーを定義していない場合でも、Explicit Web プロキシ サーバはセッションを受け付けます。

[General Options] (Explicit Web プロキシおよびトランスペアレント Web キャッシュ) セクション

[Proxy FQDN]	プロキシ サーバの完全修飾ドメイン名 (FQDN) を入力します。これは、このプロキシ サーバにアクセスするときにブラウザに入力するドメイン名です。
[Max HTTP request length]	HTTP 要求の最大の長さを入力します。これより長い要求は拒否されます。
[Max HTTP message length]	HTTP メッセージの最大の長さを入力します。これより長いメッセージは拒否されます。
[Add headers to Forwarded Requests]	Web プロキシ サーバは、HTTP 要求を内部ネットワークに転送します。これらの要求に含まれている次のヘッダを含めることができます。
[Client IP Header]	元の HTTP 要求の Client IP ヘッダを含める場合にオンにします。
[Via Header]	元の HTTP 要求の Via ヘッダを含める場合にオンにします。
[X-forwarded-for Header]	X-Forwarded-For (XFF) HTTP ヘッダを含める場合にオンにします。 XFF HTTP ヘッダは、HTTP プロキシを介して接続している Web クライアントまたはブラウザの発信元の IP アドレスと、このポイントに到達するまでに通過したリモート アドレスを識別します。
[Front-end HTTPS Header]	元の HTTPS 要求の Front-end HTTP ヘッダを含める場合にオンにします。

.

WCCP の設定

WCCP の設定はすべて、CLI で設定されます。WCCP (Web Cache Communication Protocol) バージョン 2 の設定は、Web トラフィックを最適化し、それによって転送コストとダウンロード時間を削減するために設定します。

コンピュータ上の Web クライアントが Web コンテンツに対する要求を発行した場合、WCCP は、ローカル ネットワーク上のルータが、その Web コンテンツ要求をローカル ネットワーク上の適切な Web キャッシュ サーバにリダイレクトできるようにします。Web キャッシュ サーバに Web コンテンツ要求内の情報が含まれている場合、Web キャッシュ サーバはそのコンテンツをローカル クライアントに直接送信します。Web キャッシュに要求された情報が含まれていない場合、Web キャッシュ サーバは HTTP 情報をダウンロードしてキャッシュし、それをローカル クライアントに送信します。ローカル クライアントは、このキャッシュが実行されていることを認識していません。

Web キャッシュが機能するには、HTTP 要求を Web キャッシュ サーバに転送できる 1 つ以上のルータを介してローカル ネットワーク トラフィックを転送する必要があります。FortiGate ユニットは、WCCP バージョン 2 が有効なルータとして機能し、Web コンテンツ要求を設定されている Web キャッシュ サーバに転送することができます。

Web キャッシュを使用すると、HTTP 要求のたびにリモートの Web サイトにアクセスすることがなくなるため、ダウンロード速度が向上します。また、企業ネットワークがインターネット経由で送受信するデータ量が削減されるため、コストも削減されます。

WCCP を設定するために使用される変数とコマンドを次に示します。

WCCP クライアントの場合 :

```
config system setting
  set wccp-cache-engine {enable | disable}
end
```

WCCP サービスの場合 :

```
config system wccp
  edit <service_id>
    set cache-id <ip_address>
    set group-address <ip_multicast_address>
    set router-list <ip_router_address>
    set authentication {enable | disable}
    set service-type {auto | standard | dynamic}
    set assignment-weight <weight_number>
    set assignment-bucket-form {cisco-implementation | wccp-v2}
end
```

ルーティング テーブル (トランスペアレント モード)

FortiGate ユニットがトランスペアレント モードで動作している場合は、*[System]*、*[Network]*、*[Routing Table]* の順に選択して、FortiGate ユニットを通過するトラフィックのフローを制御するためのスタティック ルートを追加できます。

注記 : NAT/ ルート モードでは、スタティック ルーティング テーブルは *[System]*、*[Routing]*、*[Static]* の順に選択して表示されるページにあります。

[Routing Table] ページ

作成したすべてのスタティック ルートを表示します。このページでは、新しいルートを編集、削除、または作成することができます。

[Create New] トランスペアレント モードの新しいスタティック ルートを追加します。

[IP/Mask]	このルートの宛先 IP アドレスとネットマスク。
[Gateway]	このルートがトラフィックを転送する先のネクストホップ ルータの IP アドレス。インターネット接続の場合は、ネクストホップ ルーティング ゲートウェイがトラフィックをインターネットにルーティングします。
[Delete]	ルートを削除します。
[Edit]	ルートを編集または表示します。既存のスタティック ルートを編集する場合は、[Edit Static Route] ページに自動的にリダイレクトされます。
[Destination IP /Mask]	宛先 IP アドレス。

[New Static Route] ページ

スタティック ルートを設定するための各設定を提供します。既存のスタティック ルートを編集する場合は、[Edit Static Route] ページに自動的にリダイレクトされます。

[Destination IP/Netmask]	新しいスタティック ルートの IP アドレスとネットマスクを入力します。デフォルト ルートを作成するには、IP とネットマスクを「0.0.0.0」に設定します。
[Gateway]	ゲートウェイの IP アドレスを入力します。
[Priority]	このスタティック ルートのプライオリティの数値を入力します。

システム - 無線

この項では、FortiWiFi ユニットで無線 LAN インタフェースを設定する方法について説明します。この項のほとんどの部分は、すべての FortiWiFi ユニットに適用できます。

FortiGate ユニット上でバーチャル ドメイン (VDOM) を有効にした場合、MAC フィルタと無線モニタはバーチャル ドメインごとに別々に設定されます。システム無線の設定はグローバルに設定されます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には、以下のトピックが含まれています。

FortiWiFi の無線インタフェース

FortiWiFi ユニットは、最大 4 つの無線インタフェースと 4 種類の SSID をサポートしています。各無線インタフェースの SSID は異なっている必要があり、各無線インタフェースには異なるセキュリティ設定を割り当てることができます。無線インタフェースの追加の詳細については、127 ページの「無線インタフェースの追加」を参照してください。

次の動作を行うように FortiWiFi ユニットを設定できます。

- 無線ネットワーク カードを備えたクライアントが接続できるアクセス ポイントを提供する。これはアクセス ポイント モードと呼ばれ、デフォルトのモードです。すべての FortiWiFi ユニットに、最大 4 つの無線インタフェースを割り当てることができます。

または

- FortiWiFi ユニットを別の無線ネットワークに接続する。これはクライアント モードと呼ばれます。クライアント モードで動作している FortiWiFi ユニットにも、無線インタフェースを 1 つだけ割り当てることができます。

または

- 無線の範囲内にあるアクセス ポイントを監視する。これは監視モードと呼ばれます。追跡のために、検出されたアクセス ポイントを [Accepted] または [Rogue] として指定できます。このモードでは、アクセス ポイントまたはクライアントの動作はできません。ただし、ユニットがアクセス ポイント モードにあるときに、バックグラウンド動作として監視を有効にすることができます。

FortiWiFi ユニットは、次の無線ネットワーク標準をサポートしています。

- IEEE 802.11a (5 GHz 帯)
- IEEE 802.11b (2.4 GHz 帯)
- IEEE 802.11g (2.4 GHz 帯)
- WEP64 および WEP128 WEP (Wired Equivalent Privacy)
- 事前共有キーまたは RADIUS サーバを使用した Wi-Fi WPA (Wi-Fi Protected Access)、WPA2、および WPA2 Auto

チャネル割り当て

選択された無線プロトコルと、世界のどの地域にいるかに応じて、特定のチャネルを使用できます。*[System]*、*[Wireless]*、*[Settings]* の順に選択することによって、無線ネットワークのチャネルを設定します。詳細については、126 ページの「無線の設定」を参照してください。

次の表は、サポートされている無線プロトコルごとの無線ネットワークのチャネル割り当てを示しています。

IEEE 802.11a のチャネル番号

表 10は、IEEE 802.11a無線標準をサポートするFortiWiFi製品でサポートされているIEEE 802.11aチャネルを示しています。802.11a は、FortiWiFi-60B ユニットでのみ使用できます。

アメリカを除き、すべてのチャネルが屋内使用に制限されています。アメリカの場合、米国ではチャネル 52 ～ 64 について屋内使用と屋外使用の両方が許可されています。

表 10: IEEE 802.11a（5 GHz 帯）のチャネル番号

チャネル番号	周波数 (MHz)	規制地域				
		アメリカ	ヨーロッパ	台湾	シンガポール	日本
34	5170		·			·
36	5180	·	·		·	
38	5190		·			·
40	5200	·	·		·	
42	5210		·			·
44	5220	·	·		·	
46	5230		·			·
48	5240	·	·		·	
52	5260	·	·	·		
56	5280	·	·	·		
60	5300	·	·	·		
64	5320	·	·	·		
149	5745					
153	5765					
157	5785					
161	5805					

IEEE 802.11b のチャネル番号

表 11 は、IEEE 802.11b チャネルを示しています。すべての FortiWiFi ユニットが 802.11b をサポートしています。

メキシコは、アメリカ規制ドメインに含まれています。チャネル 1 ～ 8 は、屋内使用のみ可能です。チャネル 9 ～ 11 は、屋内および屋外で使用できます。チャネル番号がメキシコの規制標準に準拠していることを確認する必要があります。

表 11: IEEE 802.11b（2.4 GHz 帯）のチャネル番号

チャネル番号	周波数 (MHz)	規制地域			
		アメリカ	EMEA	イスラエル	日本
1	2412	·	·		·
2	2417	·	·		·
3	2422	·	·		·
4	2427	·	·	·	·
5	2432	·	·	·	·
6	2437	·	·	·	·
7	2442	·	·	·	·
8	2447	·	·	·	·
9	2452	·	·	·	·
10	2457	·	·	·	·
11	2462	·	·		·
12	2467		·		·
13	2472		·		·
14	2484				·

IEEE 802.11g のチャネル番号

表 12 は、IEEE 802.11b チャネルを示しています。すべての FortiWiFi 製品が 802.11g をサポートしています。

表 12: IEEE 802.11g（2.4 GHz 帯）のチャネル番号

チャネル番号	周波数 (MHz)	規制地域							
		アメリカ		EMEA		イスラエル		日本	
		CCK	ODFM	CCK	ODFM	CCK	ODFM	CCK	ODFM
1	2412	·	·	·	·			·	·
2	2417	·	·	·	·			·	·
3	2422	·	·	·	·			·	·
4	2427	·	·	·	·			·	·
5	2432	·	·	·	·	·	·	·	·
6	2437	·	·	·	·	·	·	·	·
7	2442	·	·	·	·	·	·	·	·
8	2447	·	·	·	·	·	·	·	·
9	2452	·	·	·	·			·	·
10	2457	·	·	·	·			·	·
11	2462	·	·	·	·			·	·
12	2467			·	·			·	·
13	2472			·	·			·	·
14	2484							·	

無線の設定

FortiWiFi ユニットには、デフォルトで、wlan という名前の 1 つの無線インタフェースが含まれています。FortiWiFi ユニットをアクセス ポイント モードで動作させている場合は、最大 3 つの仮想無線インタフェースを追加できます。すべての無線インタフェースが同じ無線パラメータを使用します。つまり、無線の設定を 1 回設定すると、すべての無線インタフェースがこれらの設定を使用します。無線インタフェースの追加の詳細については、127 ページの「無線インタフェースの追加」を参照してください。

FortiWiFi ユニットをクライアント モードで動作させている場合、 無線の設定は設定できません。

無線の設定を設定するには、*[System]*、*[Wireless]*、*[Settings]* の順に選択します。

[Wireless Parameters] ページ

無線パラメータを設定するための各設定を提供します。このページではまた、動作モードを変更することもできます。モードを変更すると、一部の設定が非表示になります。たとえば、クライアント モードでは、アクセス ポイントでは使用できた設定 ([Band] など) を表示できません。監視モードにある場合は、[Operation Mode] のみが使用できます。

[Operation Mode] 動作モードを切り替えるには、[Change] を選択します。[Change] を選択すると、[Change operation mode for wireless] ページに自動的にリダイレクトされます。

[Access Point] — FortiWiFi ユニットは、無線ネットワークに接続して情報を送受信する無線ユーザのためのアクセス ポイントとして機能します。複数の無線ネットワーク ユーザが、物理的に接続することなくネットワークにアクセスできるようにします。FortiWiFi ユニットは内部ネットワークに接続したり、インターネットに対するファイアウォールとして機能したりすることができます。

[Client] — FortiWiFi ユニットは、別のアクセス ポイントから転送を受信するように設定されます。これにより、無線プロトコルを使用して、リモート ユーザを既存のネットワークに接続できます。

[Monitoring] — 他のアクセス ポイントをスキャンします。これらのアクセス ポイントは [Rogue AP] リストに表示されます。130 ページの「悪意のある AP の検出」を参照してください。

注記 *:* 仮想無線インタフェースを追加している場合は、クライアント モードまたは監視モードに切り替えることができません。これらのモードでは、1 つの無線インタフェース (wlan) しか存在できません。

[Band] 無線周波数帯を選択します。無線ネットワークの使用が制限されることがあるため、ユーザがどのような無線カードまたはデバイスを用意しているかに注意してください。たとえば、FortiWiFi ユニットで 802.11g を設定したときに、ユーザのデバイスが 802.11b である場合、そのユーザは無線ネットワークを使用できない可能性があります。

[Geography] 国または地域を選択します。これにより、使用可能なチャネルが決定されます。チャネルの情報については、 124 ページの「チャネル割り当て」を参照してください。

[Channel] 無線ネットワークのチャネルを選択するか、または [Auto] を選択します。選択できるチャネルは、[Geography] の設定によって異なります。チャネルの情報については、124 ページの「チャネル割り当て」を参照してください。

[Tx Power] 送信機の出力レベルを設定します。この数値が大きいほど、FortiWiFi がブロードキャストする領域が広くなります。無線信号を小さな領域に保持したい場合は、小さな数値を入力します。

[Beacon Interval] ビーコン パケット間の間隔を設定します。アクセス ポイントは、無線ネットワークの同期をとるために、ビーコンまたは TIM (Traffic Indication Messages) をブロードキャストします。
大きな値を指定すると、 送信されるビーコンの数が減ります。 ただし、ビーコン パケットを受け取れない一部の無線クライアントの接続が遅れることがあります。
この値を小さくすると、送信されるビーコンの数が増えます。これによって、無線ネットワークをよりすばやく見つけて接続できるようになりますが、必要なオーバーヘッドが増えるため、スループットが低下します。

[Background Rogue AP Scan] ユニットがアクセス ポイント モードにあるときに、監視モードのスキャン機能を実行します。スキャンは、アクセス ポイントがアイドル状態のときに実行されます。このスキャンは、すべての無線チャネルを対象にしています。アクセス ポイントがビジー状態の場合は、バックグラウンド スキャンによってパフォーマンスが低下することがあります。130 ページの「悪意のある AP の検出」を参照してください。

[Interface] この無線インタフェースの名前。無線インタフェースの設定を変更するには、インタフェース名を選択します。アクセス ポイント モードで無線インタフェースを追加するには、127 ページの「無線インタフェースの追加」を参照してください。

[MAC Address] この無線インタフェースの MAC アドレス。

[SSID] この無線インタフェースの無線 SSID (Service Set Identifier) またはネットワーク名。通信するには、アクセス ポイントとクライアントは同じ SSID を使用する必要があります。

[SSID Broadcast] 緑色のチェックマーク アイコンは、この無線インタフェースが固有の SSID をブロードキャストすることを示します。SSID をブロードキャストすると、クライアントは、最初に SSID がわからなくても無線ネットワークに接続できるようになります。
この列は、アクセス ポイント モードでのみ表示されます。

[Security Mode] この無線インタフェースのセキュリティ モード。これらのモードについては、127 ページの「無線インタフェースの追加」の「Security Mode」を参照してください。
アクセス ポイント モード : [WEP64]、[WEP128]、[WPA]、[WPA2]、[WPA2 Auto]、または [None]。
クライアント モード : [WEP64]、[WEP128]、[WPA]、または [None]。
注記 : クライアント モードの [WPA] セキュリティでは、FortiWiFi ユニットは [WPA2] セキュリティを使用して接続しようとします。これが失敗すると、[WPA] セキュリティを使用して再試行します。

無線インタフェースの追加

アクセス ポイントには、最大 3 つの仮想無線インタフェースを追加できます。これらの追加のインタフェースは、WLAN インタフェースの [Band]、[Geography]、[Channel]、[Tx Power]、および [Beacon Interval] に対して設定された同じ無線パラメータを共有します。各無線インタフェースに固有の SSID が割り当てられていることを確認してください。

注記 : FortiWiFi ユニットがクライアント モードまたは監視モードにあるときは、無線インタフェースを追加できません。

[New Interface] ページの [Wireless Settings] セクション

[SSID] この無線インタフェースの無線 SSID (Service Set Identifier) またはネットワーク名を入力します。無線ネットワークを使用するユーザは、自分のコンピュータにこのネットワーク名を設定する必要があります。

[SSID Broadcast] SSID をブロードキャストする場合に選択します。SSID をブロードキャストすると、クライアントは、最初に SSID がわからなくても無線ネットワークに接続できるようになります。セキュリティを向上させるには、SSID をブロードキャストしないでください。インタフェースがブロードキャストしない場合、不審なユーザがこの無線ネットワークに接続する可能性は低くなります。SSID をブロードキャストしないことを選択した場合は、ユーザが無線デバイスを設定できるように、各ユーザに SSID を通知する必要があります。

[Security Mode] この無線インタフェースのセキュリティ モードを選択します。この無線インタフェースに接続するには、無線ユーザは同じセキュリティ モードを使用する必要があります。
[None] — セキュリティが設定されません。すべての無線ユーザがこの無線ネットワークに接続できます。
[WEP64] — 64 ビット WEP (Web Equivalent Privacy)。WEP64 を使用するには、10 個の 16 進数 (0 ～ 9、a ～ f) を含むキーを入力し、そのキーを無線ユーザに通知する必要があります。
[WEP128] — 128 ビット WEP。WEP128 を使用するには、26 個の 16 進数 (0 ～ 9、a ～ f) を含むキーを入力し、そのキーを無線ユーザに通知する必要があります。
[WPA] — Wi-Fi WPA (Wi-Fi Protected Access) セキュリティ。WPA を使用するには、データ暗号化の方法を選択する必要があります。また、少なくとも 8 文字を含む事前共有キーを入力するか、または RADIUS サーバを選択することも必要です。RADIUS サーバを選択した場合は、その RADIUS サーバ上に無線クライアントのアカウントが存在する必要があります。
[WPA2] — セキュリティ機能が向上した WPA。WPA2 を使用するには、データ暗号化の方法を選択した後、少なくとも 8 文字を含む事前共有キーを入力するか、または RADIUS サーバを選択する必要があります。RADIUS サーバを選択した場合は、その RADIUS サーバ上に無線クライアントのアカウントが存在する必要があります。
[WPA2 Auto] — セキュリティ機能は WPA2 と同じですが、[WPA] セキュリティを使用している無線クライアントも受け付けます。WPA2 Auto を使用するには、データ暗号化の方法を選択する必要があります。また、少なくとも 8 文字を含む事前共有キーを入力するか、または RADIUS サーバを選択することも必要です。RADIUS サーバを選択した場合は、その RADIUS サーバ上に無線クライアントのアカウントが存在する必要があります。

[Key] セキュリティ キーを入力します。このフィールドは、[WEP64] または [WEP128] セキュリティを選択した場合に表示されます。

[Data Encryption]	WPA、WPA2、または WPA2 Auto で使用されるデータ暗号化の方法を選択します。TKIP (Temporal Key Integrity Protocol) を使用するには、*[TKIP]* を選択します。AES (Advanced Encryption Standard) 暗号化を使用するには、*[AES]* を選択します。AES は、TKIP より安全と見なされています。WPA の一部の実装では、AES がサポートされていない可能性があります。
[Pre-shared Key]	事前共有キーを入力します。このフィールドは、[WPA]、[WPA2]、または [WPA2 Auto] セキュリティを選択した場合に表示されます。
[RADIUS Server]	[WPA] または [WPA2] セキュリティの選択時に RADIUS サーバを使用する場合に選択します。WPA Radius または WPA2 Radius セキュリティを使用すると、無線ネットワーク構成を RADIUS サーバまたは Windows AD サーバと統合できます。リストから RADIUS サーバ名を選択します。*[User]*、*[RADIUS]* の順に選択することによって、RADIUS サーバを設定する必要があります。詳細については、449 ページの「RADIUS」を参照してください。
[RTS Threshold]	RTS (Request to Send) のしきい値を設定します。 RTS のしきい値は、FortiWiFi が送信側の無線デバイスに RTS/CTS パケットを送信することなく受け付けるパケットの最大サイズ (バイト単位) です。場合によっては、大きなパケットの送信によって衝突が発生し、データの転送が遅延することがあります。この値をデフォルトの 2346 から変更することによって、事実上、送信側の無線デバイスが大きな転送を送信する前にクリアを求めるように FortiWiFi ユニットを設定できます。引き続き小さなパケットが衝突するリスクは存在しますが、この確率は低くなります。 2346 バイトを設定すると、事実上このオプションは無効になります。
[Fragmentation Threshold]	小さなパケットに分割されないデータ パケットの最大サイズを設定することにより、パケット衝突の可能性を減らします。パケットがこのしきい値より大きいと、FortiWiFi ユニットは転送を断片化します。パケット サイズがこのしきい値より小さいと、FortiWiFi ユニットは転送を断片化しません。 2346 バイトを設定すると、事実上このオプションは無効になります。

無線インタフェースを追加するには

1 *[System]*、*[Network]*、*[Interface]* の順に選択します。

2 *[Create New]* を選択します。

3 以下の設定を行います。

[Name]	この無線インタフェースの名前を入力します。この名前を既存のインタフェース、ゾーン、または VDOM と同じにすることはできません。
[Type]	*[Wireless]* を選択します。
[Address Mode]	この無線インタフェースは、手動のアドレスとしてのみ設定できます。有効な IP アドレスとネットマスクを入力します。 FortiWiFi がトランスペアレント モードで動作している場合、このフィールドは表示されません。このインタフェースは、他のインタフェースと同じサブネット上に配置されます。
[Administrative Access]	このインタフェースの管理アクセスを設定します。

4 *[Wireless Settings]* セクションで、必要な情報を入力して *[OK]* を選択します。

無線 MAC フィルタ

無線ネットワークのセキュリティを向上させるために、FortiWiFi ユニット上で MAC アドレス フィルタリングを有効にすることができます。MAC アドレス フィルタリングを有効にすることにより、システムの MAC アドレスに基づいてネットワークにアクセスできる無線デバイスが定義されます。あるユーザが無線ネットワークにアクセスしようとすると、FortiWiFi ユニットは、そのユーザの MAC アドレスを作成されているリストと照合します。MAC アドレスが承認されたリストに記載されていると、そのユーザはネットワークへのアクセスを取得します。ユーザがそのリストに記載されていない場合、そのユーザは拒否されます。

必要に応じて、 拒否リストを作成できます。 許可リストと同様に、 MAC アドレス リストに記載されている接続を除く、 すべての接続を許可するように無線インタフェースを設定できます。

MAC アドレス フィルタリングを使用すると、ランダムな MAC アドレスを使用するか、または MAC アドレスをスプーフィングしているハッカーがネットワークへのアクセスを取得することは困難になります。WLAN インタフェースあたり 1 つのリストしか設定できないことに注意してください。

無線クライアントへの無線アクセスを、そのクライアントの無線カードの MAC アドレスに基づいて許可または拒否するには、*[System]*、*[Wireless]*、*[MAC Filter]* の順に選択します。

MAC フィルタ リストの管理

MAC フィルタ リストを使用すると、無線インタフェースに追加した MAC アドレスとそのステータス (許可または拒否のどちらか) を表示できます。また、MAC フィルタ リストを編集したり、管理したりすることもできます。

変更対象の既存の MAC アドレスを変更するには、[MAC Filter Settings] ページにある設定を使用します。

[MAC Filter] ページ

無線インタフェースに追加した MAC アドレス (そのステータスを含む) を表示します。MAC アドレスを編集する場合は、[MAC Filter Settings] ページに自動的にリダイレクトされます。

[Interface]	この無線インタフェースの名前。
[MAC address]	この無線インタフェースの MAC フィルタ リスト内の MAC アドレスのリスト。
[List Access]	この無線インタフェースのリストされている MAC アドレスへのアクセスを許可または拒否します。
[Enable]	この無線インタフェースに対する MAC フィルタリングを有効にする場合に選択します。
[Edit]	インタフェースの MAC アドレス リストを編集します。[Edit] を選択すると、[MAC Filter Settings] ページに自動的にリダイレクトされます。

[MAC Filter Settings] ページ

無線インタフェースに追加した既存の MAC アドレスを変更するための設定を提供します。

[List Access]	MAC アドレス リスト内のアドレスからのこの無線ネットワークへのアクセスを許可または拒否する場合に選択します。
[MAC Address]	リストに追加する MAC アドレスを入力します。
[Add]	入力した MAC アドレスをリストに追加します。
[Remove]	リスト内の 1 つ以上の MAC アドレスを選択し、[Remove] を選択して、それらの MAC アドレスをリストから削除します。

無線モニタ

無線ネットワークに関する情報を表示するには、*[System]*、*[Wireless]*、*[Monitor]* の順に選択します。アクセス ポイント モードでは、無線 LAN に接続しているユーザを表示できます。クライアント モードでは、無線の範囲内に存在するアクセス ポイントを表示できます。

[Monitor] ページ

無線インタフェースと、現在アクティブなクライアントまたは隣接機器を表示します。これらの情報はグループ化され、このページ内の独自のセクションに配置されています。

[Statistics] セクション

各無線インタフェースの無線のパフォーマンスに関する統計情報。

[AP Name / Name]	この無線インタフェースの名前。
[Frequency]	この無線インタフェースが動作している周波数。802.11a インタフェースの場合は約 5 GHz、802.11b および 802.11g ネットワークの場合は約 2.4 GHz です。
[Signal Strength (dBm)]	クライアントからの信号の強度。
[Noise (dBm)]	受信されたノイズ レベル。
[S/N (dB)]	信号強度とノイズ レベルから計算された信号対雑音比 (デシベル値)。

[Rx (KBytes)]	このセッションで受信されたデータ量 (KB 単位)。
[Tx (KBytes)]	このセッションで送信されたデータ量 (KB 単位)。

[Clients list] セクション (AP モード)

この FortiWiFi ユニット アクセス ポイントに到達できるクライアント無線デバイスに関するリアルタイムの詳細。同じ無線帯域にあるデバイスのみが表示されます。

[MAC Address]	接続された無線クライアントの MAC アドレス。
[IP Address]	接続された無線クライアントに割り当てられた IP アドレス。
[AP Name]	このクライアントが接続されている無線インタフェースの名前。

[Neighbor AP list] セクション (クライアント モード)

このクライアントが受信できるアクセス ポイントに関するリアルタイムの詳細。

[MAC Address]	接続された無線クライアントの MAC アドレス。
[SSID]	このアクセス ポイントがブロードキャストする無線 SSID (Service Set Identifier)。
[Channel]	このアクセス ポイントが使用している無線チャネル。
[Rate (M)]	このアクセス ポイントのデータ レート (M ビット / 秒単位)。
[RSSI]	受信された信号強度の表示。0 (最小) ～ 255 (最大) の相対的な値です。

悪意のある AP の検出

悪意のあるアクセス ポイントの検出をサポートしているモデルでは、使用可能な無線アクセス ポイントをスキャンするために監視モードを選択できます。また、ユニットがアクセス ポイント モードにあるときに、バックグラウンドでのスキャンを有効にすることもできます。

監視モードを有効にするには

1 *[System]*、*[Wireless]*、*[Settings]* の順に選択します。
2 現在の動作モードの横にある *[Change]* を選択します。
3 *[Monitoring]* を選択し、*[OK]* を選択します
4 *[OK]* を選択して、モードの変更を確認します。
5 *[Apply]* を選択します。

バックグラウンド スキャンを有効にするには

1 アクセス ポイント モードにあるときに、*[System]*、*[Wireless]*、*[Settings]* の順に選択します。
2 *[Background Rogue AP Scan]* を有効にして、*[Apply]* を選択します。

無線アクセス ポイントの表示

アクセス ポイントは、[Accepted] または [Rogue] のどちらかのアクセス ポイントとしてマークするまで *[Unknown Access Points]* リストに表示されます。この指定は、アクセス ポイントの追跡に役立ちます。ただし、他のユーザがこれらのアクセス ポイントを使用できるかどうかには影響を与えません。

検出されたアクセス ポイントを表示するには、*[System]*、*[Wireless]*、*[Rogue AP]* の順に選択します。この機能は、監視モード、または *[Background Rogue AP Scan]* が有効になったアクセス ポイント モードで使用できます。

[Rogue AP] ページ

アクティブな状態にある検出されたアクセス ポイントを表示します。

[Refresh Interval]	情報更新の間隔を設定します。*[none]* は、更新しないことを示します。
[Refresh]	現在表示されている情報を更新します。

[Inactive Access Points]	アクティブでないどのアクセス ポイントを表示するかを、すべて、なし、過去 1 時間以内に検出されたアクセス ポイント、過去 1 日以内に検出されたアクセス ポイントから選択します。
[Online]	緑色のチェックマークは、アクティブなアクセス ポイントを示します。灰色の X は、このアクセス ポイントがアクティブでないことを示します。
[SSID]	この無線インタフェースの無線SSID (Service Set Identifier) またはネットワーク名。
[MAC Address]	この無線インタフェースの MAC アドレス。
[Signal Strength /Noise]	信号強度とノイズ レベル。
[Channel]	このアクセス ポイントが使用している無線チャネル。
[Rate]	このアクセス ポイントのデータ レート。
[First Seen]	FortiWiFi ユニットがこのアクセス ポイントを最初に検出した日付と時刻。
[Last Seen]	FortiWiFi ユニットがこのアクセス ポイントを最後に検出した日付と時刻。
[Mark as ´Accepted AP´]	このエントリを *[Accepted Access Points]* リストに移動するには、このアイコンを選択します。
[Mark as ´Rogue AP´]	このエントリを *[Rogue Access Points]* リストに移動するには、このアイコンを選択します。
[Forget AP]	項目を *[Accepted Access Points]* リストまたは *[Rogue Access Points]* リストから *[Unknown Access Points]* リストに戻します。

また、最初に各 AP を検出することなく、受け付ける AP と悪意のある AP に関する情報を CLI で入力することもできます。『*FortiGate CLI リファレンス*』にある `system wireless ap-status` コマンドを参照してください。

システム - DHCP サーバ

この項では、DHCP を使用して、クライアントのネットワーク構成を自動で容易に行う方法について説明します。

DHCP は、トランスペアレント モードでは使用できません。DHCP 要求は、トランスペアレント モードにある FortiGate ユニットを通過します。

FortiGate ユニット上でバーチャル ドメイン (VDOM) を有効にした場合、DHCP はバーチャル ドメインごとに別々に設定されます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には、以下のトピックが含まれています。

FortiGate DHCP サーバおよびリレー

DHCP は、ホストが IP アドレスを DHCP サーバから自動的に取得できるようにするプロトコルです。必要に応じて、デフォルト ゲートウェイと DNS サーバの設定を取得することも可能です。FortiGate インタフェースまたは VLAN サブインタフェースでは、次の DHCP サービスを提供できます。

- IPSec 以外の IP ネットワークのための基本的な DHCP サーバ
- IPSec (VPN) 接続のための IPSec DHCP サーバ
- 標準的なイーサネットまたは IPSec (VPN) 接続のための DHCP リレー

同じタイプの接続 (標準またはIPSec) にインタフェースでサーバとリレーの両方を提供することはできません。ただし、インタフェースがスタティック IP アドレスが設定された物理インタフェースである場合にのみ、そのインタフェース上で標準 DHCP サーバを設定できます。スタティックまたはダイナミックIPアドレスのいずれかが設定されたインタフェース上のIPSec DHCP サーバを設定することは可能です。

任意の FortiGate インタフェースに 1 つ以上の DHCP サーバを設定できます。 DHCP サーバは、インタフェースに接続されたネットワーク上のホストに動的に IP アドレスを割り当てます。DHCP を使用して IP アドレスを取得するには、 ホスト コンピュータを設定する必要があります。

インタフェースがルータを介して複数のネットワークに接続されている場合、それぞれのネットワークに DHCP を追加できます。各 DHCP の IP の範囲は、ネットワーク アドレスの範囲と一致する必要があります。ルータは、DHCP リレー用に設定しなければなりません。

DHCP サーバを設定するには、134 ページの「DHCP サーバの設定」を参照してください。

FortiGate インタフェースは、DHCP リレーとして設定できます。インタフェースにより、DHCP 要求は DHCP クライアントから外部の DHCP サーバに転送され、DHCP クライアントには応答が返されます。DHCP クライアントへの応答パケットが FortiGate ユニットに到達するよう、DHCP サーバは適切なルーティングを行う必要があります。

DHCP リレーを設定するには、134 ページの「DHCP リレー エージェントとしてのインタフェースの設定」を参照してください。

DHCP サービスは、コマンドライン インタフェース (CLI) で設定することもできます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

DHCP サービスの設定

DHCP サービスを設定するには、*[System]*、*[DHCP Server]*、*[Service]* の順に選択します。各 FortiGate インタフェースでは、必要に応じて DHCP リレーを設定したり、DHCP サーバを追加したりすることができます。

FortiGate50 および 60 シリーズ ユニットでは、DHCP サーバはデフォルトで、次のように内部インタフェースで設定されています。

[IP Range]	192.168.1.110 ～ 192.168.1.210
[Netmask]	255.255.255.0
[Default gateway]	192.168.1.99
[Lease time]	7 日
[DNS Server 1]	192.168.1.99

このデフォルトの DHCP サーバ設定は、無効にしたり変更したりすることができます。ただし、トランスペアレント モードで DHCP を設定することはできません。トランスペアレント モードでは、DHCP 要求が FortiGate ユニットを通過します。

DHCP サーバを設定する前に、インタフェースにスタティック IP アドレスが設定されている必要があります。

これらの設定は、内部インタフェースのデフォルト IP アドレス 192.168.1.99 に適しています。このアドレスを異なるネットワークに変更する場合、DHCP サーバ設定を変更して一致させる必要があります。

DHCP リレー エージェントとしてのインタフェースの設定

インタフェースの DHCP リレー設定を編集するには、*[System]*、*[DHCP Server]*、*[Service]* の順に選択します。

***[Edit DHCP Service]* ページ**

[New DHCP Service] ページで以前に設定された DHCP リレーの既存の設定を提供します。

[Interface Name]	このインタフェースの名前。
[DHCP Relay Agent]	このインタフェース上で DHCP リレー エージェントを有効にする場合に選択します。
[Type]	必要な DHCP サービスのタイプを *[Regular]* または *[IPSEC]* のどちらかとして選択します。
[DHCP Server IP]	インタフェースに接続されているネットワーク上のコンピュータからの DHCP 要求に応答する DHCP サーバの IP アドレスを入力します。

DHCP サーバの設定

[System]、*[DHCP Server]*、*[Service]* の順に選択して表示される画面では、既存の DHCP サーバにアクセスできます。この画面ではまた、新しい DHCP サーバの設定も行います。

DHCP サーバを設定するには

1 *[System]*、*[DHCP Server]*、*[Service]* の順に選択します。

2 このインタフェースの青色の矢印を選択します。

3 *[Add DHCP Server]* アイコンを選択して新しい DHCP サーバを作成するか、または既存の DHCP サーバの横にある *[編集]* アイコンを選択してその設定を変更します。

4 DHCP サーバを設定します。

5 *[OK]* を選択します

[New DHCP Service] ページ

DHCP リレー エージェントまたは DHCP サーバを設定するための各設定を提供します。

[Name] この DHCP サーバの名前を入力します。

[Mode] DHCP リレー エージェントを設定するには、[Relay] を選択します。DHCP サーバを設定するには、[Server] を選択します。

[Enable] この DHCP サーバを有効にします。

[Type] [Regular] または [IPSEC] の DHCP サーバを選択します。
ダイナミック IP アドレスを持つインタフェース上の標準 DHCP サーバは設定できません。

[IP Range] この DHCP サーバが DHCP クライアントに割り当てる IP アドレスの範囲の始めと終わりを入力します。
[IP Assignment Mode] が *[User-group defined method]* に設定されている場合、これらのフィールドは灰色で表示されます。

[Network Mask] この DHCP サーバが割り当てるアドレスのネットマスクを入力します。

[Default Gateway] この DHCP サーバが DHCP クライアントに割り当てるデフォルト ゲートウェイの IP アドレスを入力します。

[DNS Service] 特定の DNS サーバまたはシステムの DNS 設定のどちらかを使用する場合に選択します。[DNS Server 1] の横にあるプラス記号 (+) を選択することによって、複数の DNS サーバを追加できます。

[DNS Server 0] DNS サーバを入力します。

[DNS Server 1] 2 番目の DNS サーバを入力します。さらに DNS サーバを追加する必要がある場合は、プラス記号 (+) を選択します。

[New DHCP Service] ページの [Advanced] セクション

詳細設定オプションを設定する場合に選択します。

[Domain] この DHCP サーバが DHCP クライアントに割り当てるドメインを入力します。

[Lease Time] [Unlimited] を選択してリース期間を無期限とするか、または日、時間、および分で期間を入力します。その期間を過ぎると、DHCP クライアントは DHCP サーバに新しい設定を照会しなければなりません。リース期間は、5 分から 100 日までの範囲を設定できます。

[IP Assignment Mode] ダイヤルアップ IPSec VPN ユーザに IPSec DHCP サーバの IP アドレスを割り当てる方法を設定します。次の中から選択します。

- [Server IP Range] - IPSec DHCP サーバは、*[IP Range]* と *[Exclude Ranges]* の指定に従って IP アドレスを割り当てます。
- [User-group defined method] - IP アドレスは、ユーザを認証するために使用されるユーザ グループによって割り当てられます。このユーザ グループは、XAUTH ユーザを認証するために使用されます。461 ページの「ユーザ グループからの動的な VPN クライアント IP アドレス割り当て」を参照してください。

[User-group defined method] が選択されている場合は、*[IP Range]* フィールドが灰色で表示され、*[Exclude Ranges]* テーブルおよびコントロールは表示されません。

[WINS Server 1]
[WINS Server 2] この DHCP サーバが DHCP クライアントに割り当てる 1 つまたは 2 つの WINS サーバの IP アドレスを追加します。

[Options] DHCP リレーまたはサーバのオプションを追加する場合に選択します。このオプションを有効にすると、[Code] フィールドと [Options] フィールドが表示されます。[Options] フィールドの横にあるプラス記号を選択することによって、複数のオプションを追加できます ([Code] フィールドと [Options] フィールドの両方が表示されます)。

[Exclude Ranges]

[Add] 除外する IP アドレスの範囲を追加します。
この DHCP サーバが DHCP クライアントに割り当てることのできない最大 16 の IP アドレスの範囲を追加できます。どの範囲も 65536 の IP アドレスを超えることはできません。

[Starting IP] 除外範囲の最初の IP アドレスを入力します。

[End IP] 除外範囲の最後の IP アドレスを入力します。

[Delete]
(マイナス記号) 除外範囲を削除します。

アドレス リースの表示

この DHCP サーバが割り当てた IP アドレスと、それに対応するクライアント MAC アドレスを表示するには、*[System]*、*[DHCP Server]*、*[Address Leases]* の順に選択します。

[Address Leases] ページ

このDHCPサーバが割り当てたIPアドレスと、それに対応するクライアントMACアドレスを表示します。

[Interface]	リースを表示するインタフェースを選択します。
[Refresh]	アドレス リースのリストを更新するには、[Refresh] を選択します。
[IP]	割り当てられた IP アドレス。
[MAC]	IP アドレスが割り当てられたデバイスの MAC アドレス。
[Expire]	DHCP リースの期限が切れる日付と時刻。
[Status]	DHCP サーバの IP アドレスのステータスを示します。

特定のクライアントに対する IP アドレスの予約

クライアント デバイスの MAC アドレスと標準イーサネットまたは IPSec の接続タイプで識別される特定のクライアントに対して IP アドレスを予約することができます。DHCP サーバは、そのクライアントに常に予約済みのアドレスを割り当てます。予約として最大 200 の IP アドレスを割り当てることができます。詳細については、『*FortiGate 最大値マトリックス*』を参照してください。

CLI の `config system dhcp reserved-address` コマンドを使用します。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

システム - 設定

この項では、HA、SNMP、カスタム差し替えメッセージ、動作モードなどの、ネットワーク以外のいくつかの機能を設定する方法について説明します。

FortiGate ユニット上でバーチャル ドメイン (VDOM) を有効にした場合、HA、SNMP、および差し替えメッセージは FortiGate ユニット全体に対してグローバルに設定されます。動作モードの変更は、個々の VDOM に対して設定されます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には、以下のトピックが含まれています。

HA

FortiGate 高可用性 (HA) は、信頼性の向上とパフォーマンスの増強という 2 つの重要なエンタープライズ ネットワーキング要件を満たすソリューションを提供します。この項では、HA Web ベース マネージャの設定オプション、HA クラスタ メンバ リスト、HA 統計、およびクラスタ メンバの切断について簡潔に説明します。

FortiGate ユニット上でバーチャル ドメイン (VDOM) を有効にした場合、HA は FortiGate ユニット全体に対してグローバルに設定されます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

FortiGate HA クラスタの設定および操作方法の詳細については、『*FortiGate HA 概要*』および『*FortiGate HA ガイド*』を参照してください。

- このトピックには、以下の内容が含まれています。HA オプション
- クラスタ メンバ リスト
- HA 統計の表示
- 副系ユニットのホスト名およびデバイス プライオリティの変更
- クラスタ ユニットのクラスタからの切断

HA オプション

FortiGate ユニットがクラスタに参加できるようにしたり、動作中のクラスタまたはクラスタ メンバの設定を変更したりするには、HA オプションを設定します。

FortiGateユニットがHAクラスタに参加できるようにHAオプションを設定するには、*[System]*、*[Config]*、*[HA]* の順に選択します。

注記：FortiGate HA は、PPPoE などの PPP プロトコルとの互換性がありません。FortiGate HA はまた、DHCP との互換性もありません。1 つ以上の FortiGate ユニット インタフェースが DHCP または PPPoE を使用して動的に設定された場合は、HA モードで動作するように切り替えることができません。また、1 つ以上の FortiGate ユニット インタフェースが PPTP または L2TP クライアントとして設定されている場合や、FortiGate ユニットでスタンドアロン セッション同期が設定された場合も、HA モードで動作するように切り替えることができません。

HA がすでに有効になっている場合にクラスタ メンバ リストを表示するには、*[System]*、*[Config]*、*[HA]* の順に選択します。マスタのロール (プライマリ ユニットとも呼ばれる) を持つ FortiGate ユニットの *[Edit]* を選択します。プライマリ ユニットの HA 設定を編集すると、すべての変更がクラスタ内の他のユニットに同期されます。

グローバル admin 管理者として Web ベース マネージャにログインし、*[System]*、*[Config]*、*[HA]* の順に選択することによって、バーチャル ドメイン (VDOM) が有効になっている FortiGate ユニットの HA オプションを設定できます。HA が有効になっている場合、クラスタ ユニットの仮想クラスタ設定画面を表示するには、そのクラスタ メンバの [Edit] を選択する必要があります。詳細については、139 ページの「クラスタ メンバ リスト」を参照してください。

注記 : FortiGate クラスタでバーチャル ドメインを使用している場合は、HA 仮想クラスタリングを設定します。仮想クラスタのほとんどの HA オプションは、通常の HA オプションと同じです。ただし、仮想クラスタには VDOM パーティショニング オプションが含まれています。通常の HA と仮想クラスタリング HA の設定オプションのその他の違いについては、以下の説明や、『*FortiGate HA 概要*』および『*FortiGate HA ガイド*』を参照してください。

[High Availability] ページ

設定されている HA クラスタの既存の設定を表示するだけでなく、まだ設定されていない場合は HA クラスタを設定することもできます。このページからはまた、ほとんどの既存の設定も変更できます。

[Mode]
クラスタに HA モードを選択するか、またはクラスタ内の FortiGate ユニットをスタンドアロン モードに戻します。クラスタを設定する場合は、HA クラスタのすべてのメンバを同じ HA モードに設定する必要があります。*[Standalone]* (HA を無効化)、*[Active-Passive]*、または *[Active-Active]* を選択できます。
バーチャル ドメインが有効になっている場合は、*[Active-Passive]* または *[Standalone]* を選択できます。

[Device Priority]
必要に応じて、クラスタ ユニットのデバイス プライオリティを設定します。クラスタ内の各ユニットには、異なるデバイス プライオリティを設定できます。HA ネゴシエーション中、通常は、デバイス プライオリティの最も高いユニットがプライマリ ユニットになります。
仮想クラスタ設定では、各クラスタ ユニットに (各仮想クラスタに 1 つの) 2 つの異なるデバイス プライオリティを設定できます。HA ネゴシエーション中、仮想クラスタ内でデバイス プライオリティの最も高いユニットが、その仮想クラスタのプライマリ ユニットとなります。
デバイス プライオリティへの変更は同期されません。最初にクラスタを設定するときに、デフォルトのデバイス プライオリティを使用できます。クラスタが動作している場合は、必要に応じて別のクラスタ ユニットのデバイス プライオリティを変更できます。

[Group Name]
クラスタを識別するための名前を入力します。グループ名の最大の長さは 32 文字です。クラスタ ユニットでクラスタを形成するには、すべてのクラスタ ユニットのグループ名が同じになっている必要があります。グループ名は、クラスタが動作した後に変更できます。グループ名の変更は、すべてのクラスタ ユニットに対して同期されます。
デフォルトのグループ名は *FGT-HA* です。最初にクラスタを設定するときにデフォルトのグループ名を使用できますが、同じネットワーク上の 2 つのクラスタに同じグループ名を設定することはできません。クラスタが動作している場合は、必要に応じてグループ名を変更できます。

[Password]
クラスタを識別するためのパスワードを入力します。パスワードの最大の長さは 15 文字です。クラスタ ユニットでクラスタを形成するには、すべてのクラスタ ユニットのパスワードが同じになっている必要があります。
デフォルトでは、パスワードは設定されていません。最初にクラスタを設定するときに、デフォルトのパスワードを使用できます。クラスタが動作している場合は、必要に応じてパスワードを追加できます。同じネットワーク上の 2 つのクラスタには、異なるパスワードを設定する必要があります。

[Enable Session pickup]
プライマリ ユニットに障害が発生した場合に、新しいプライマリ ユニットになったクラスタ ユニットにセッションが引き継がれるようにセッション ピックアップを有効にする場合に選択します。
セッション フェールオーバー保護のためには、セッション ピックアップを有効にする必要があります。セッション フェールオーバー保護が必要ない場合は、セッション ピックアップを無効のままにすると、HA の CPU 使用率や HA ハートビート ネットワークの帯域幅使用率が削減されることがあります。
セッション ピックアップは、デフォルトで無効に設定されています。セッション ピックアップのデフォルト設定を使用し、後でクラスタが動作した後にセッション ピックアップを有効にすることを選択できます。

[Port Monitor]	監視対象インタフェースが正しく機能し、かつネットワークに接続されていることを確認するために FortiGate インタフェースの監視を有効または無効にする場合に選択します。 監視対象インタフェースに障害が発生するか、またはネットワークから切断された場合、そのインタフェースはクラスタから切り離され、リンク フェールオーバーが発生します。リンク フェールオーバーが発生すると、クラスタはそのインタフェースによって処理されているトラフィックを、引き続きネットワークに接続されている別のクラスタ ユニットの同じインタフェースにルーティングし直します。この別のクラスタ ユニットが新しいプライマリ ユニットになります。 ポート監視（インタフェース監視とも呼ばれる）は、デフォルトで無効に設定されています。クラスタが作動するまでポート監視を無効にしておき、接続されているインタフェースに対してのみポート監視を有効にします。 最大 16 のインタフェースを監視できます。この制限は、16 を超える物理インタフェースを備えた FortiGate ユニットにのみ適用されます。
[Heartbeat Interface]	クラスタ内の各インタフェースの HA ハートビート通信を有効または無効にしたり、ハートビート インタフェースのプライオリティを設定したりする場合に選択します。最もプライオリティの高いハートビート インタフェースが、すべてのハートビート トラフィックを処理します。2 つ以上のハートビート インタフェースのプライオリティが同じである場合は、ハッシュ マップの順序の値が最も小さいハートビート インタフェースが、すべてのハートビート トラフィックを処理します。Web ベース マネージャでは、インタフェースが英数字の順に表示されます。 ・ port1 ・ port2 ～ 9 ・ port10 ハッシュ マップの順序では、インタフェースが次の順序に並べ替えられます。 ・ port1 ・ port10 ・ port2 ～ port9 デフォルトのハートビート インタフェース設定は、FortiGate ユニットごとに異なります。このデフォルト設定では通常、2 つのハートビート インタフェースのプライオリティが 50 に設定されます。デフォルトのハートビート インタフェース設定を使用するか、または必要に応じてその設定を変更することができます。 ハートビート インタフェースのプライオリティの範囲は 0 ～ 512 です。新しいハートビート インタフェースを選択したときのデフォルトのプライオリティは 0 です。 ハートビート インタフェースは少なくとも 1 つ選択する必要があります。ハートビート通信が中断された場合、クラスタはトラフィックの処理を停止します。ハートビート インタフェースの設定の詳細については、『*FortiGate HA 概要*』を参照してください。 最大 8 つのハートビート インタフェースを選択できます。この制限は、8 以上の物理インタフェースを備えた FortiGate ユニットにのみ適用されます。
[VDOM partitioning]	仮想クラスタリングを設定する場合は、仮想クラスタ 1 に含まれるバーチャル ドメインと、仮想クラスタ 2 に含まれるバーチャル ドメインを設定できます。ルート バーチャル ドメインは、常に仮想クラスタ 1 に含まれている必要があります。 VDOM パーティショニングの設定の詳細については、『*FortiGate HA 概要*』を参照してください。

クラスタ メンバ リスト

クラスタ メンバ リストを表示すると、動作中のクラスタのステータスや、クラスタ内の FortiGate ユニットのステータスを確認できます。クラスタ メンバ リストにはクラスタ内の FortiGate ユニットが表示され、さらに FortiGate ユニットごとに、インタフェース接続、クラスタ ユニット、そのクラスタ ユニットのデバイス プライオリティが表示ます。クラスタ メンバ リストからは、クラスタからユニットを切断したり、プライマリ ユニットの HA 設定を編集したり、副系ユニットのデバイス プライオリティやホスト名を変更したり、任意のクラスタ ユニットのデバッグ ログをダウンロードしたりすることができます。また、クラスタの HA 統計を表示することもできます。

クラスタ メンバ リストを表示するには、動作中のクラスタにログインし、*[System]*、*[Config]*、*[HA]* の順に選択します。

バーチャル ドメインが有効になっている場合は、クラスタ メンバ リストを表示して、動作中の仮想クラスタのステータスを確認できます。仮想クラスタ メンバ リストには、各仮想クラスタに追加されたバーチャル ドメインを含む、両方の仮想クラスタのステータスが表示されます。

動作中のクラスタの仮想クラスタ メンバ リストを表示するには、グローバル admin 管理者としてログインし、*[System]*、*[Config]*、*[HA]* の順に選択します。

[View HA Statistics]	各クラスタ ユニットのシリアル番号、ステータス、および監視情報を表示します。140 ページの「HA 統計の表示」を参照してください。
上下矢印	リスト内のクラスタ メンバの順序を変更します。クラスタまたはクラスタ内のユニットの動作には影響ありません。変更されるのは、クラスタ メンバ リスト上のユニットの順序だけです。
[Cluster member]	クラスタ ユニットのフロント パネルの図です。インタフェースのネットワーク ジャックが緑色で表示されている場合、そのインタフェースは接続されています。各図の上にマウス ポインタを置くと、クラスタ ユニットのホスト名、シリアル番号、そのユニットが動作している時間 (アップ タイム)、およびポート監視が設定されているインタフェースを表示できます。
[Hostname]	FortiGate ユニットのホスト名。FortiGate ユニットのデフォルトのホスト名は、FortiGate ユニットのシリアル番号です。 ・ プライマリ ユニットのホスト名を変更するには、*[System]*、*[Status]* の順に選択し、現在のホスト名の横にある *[Change]* を選択します。 ・ 副系ユニットのホスト名を変更するには、クラスタ メンバ リストから副系ユニットの *[編集]* アイコンを選択します。
[Role]	クラスタ内のクラスタ ユニットのステータスまたはロール。 ・ プライマリ (またはマスタ) ユニットのロールは *[MASTER]* です。 ・ すべての副系 (またはバックアップ) クラスタ ユニットのロールは *[SLAVE]* です。
[Priority]	クラスタ ユニットのデバイス プライオリティ。各クラスタ ユニットには、異なるデバイス プライオリティを設定できます。HA ネゴシエーション中、デバイス プライオリティの最も高いユニットがプライマリ ユニットになります。デバイス プライオリティの範囲は 0 ～ 255 です。
[Disconnect from cluster]	選択したクラスタ ユニットをクラスタから切断する場合に選択します。141 ページの「クラスタ ユニットのクラスタからの切断」を参照してください。
[Edit]	クラスタ ユニットの HA 設定を変更する場合に選択します。 ・ プライマリ ユニットの場合は、*[Edit]* を選択して、そのプライマリ ユニットのクラスタの HA 設定 (デバイス プライオリティを含む) を変更します。 ・ 仮想クラスタ内のプライマリ ユニットの場合は、[Edit] を選択して、その仮想クラスタの HA 設定 (このクラスタ ユニットの仮想クラスタ 1 および仮想クラスタ 2 のデバイス プライオリティを含む) を変更します。 ・ 副系ユニットの場合は、*[Edit]* を選択して、その副系ユニットのホスト名とデバイス プライオリティを変更します。141 ページの「副系ユニットのホスト名およびデバイス プライオリティの変更」を参照してください。 ・ 仮想クラスタ内の副系ユニットの場合は、*[Edit]* を選択して、選択した仮想クラスタの副系ユニットのホスト名とデバイス プライオリティを変更します。141 ページの「副系ユニットのホスト名およびデバイス プライオリティの変更」を参照してください。
[Download debug log]	暗号化されたデバッグ ログをファイルにダウンロードする場合に選択します。このデバッグ ログ ファイルをフォーティネット テクニカル サポート (http://support.fortinet.com) に送信することで、クラスタまたは個々のクラスタ ユニットでの問題の診断に役立てることができます。

HA 統計の表示

クラスタ メンバ リストから *[View HA Statistics]* を選択して、各クラスタ ユニットのシリアル番号、ステータス、および監視情報を表示できます。HA 統計を表示するには、*[System]*、*[Config]*、*[HA]* の順に選択し、*[View HA Statistics]* を選択します。

[Refresh every]	Web ベース マネージャが HA 統計の表示を更新する頻度を制御する場合に選択します。
[Back to HA monitor]	HA 統計リストを閉じて、クラスタ メンバ リストに戻る場合に選択します。
[Unit]	このクラスタ ユニットのホスト名とシリアル番号。
[Status]	各クラスタ ユニットのステータスを示します。 緑色のチェックマークは、このクラスタ ユニットが正常に動作していることを示します。 赤色の X は、このクラスタ ユニットがプライマリ ユニットと通信できないことを示します。
[Up Time]	このクラスタ ユニットが最後に起動されてからの日数、時間、分、秒。
[Monitor]	各クラスタ ユニットのシステム ステータス情報を表示します。

[CPU Usage]	各クラスタ ユニットの現在の CPU ステータス。Web ベース マネージャは、コア プロセスの CPU 使用率のみを表示します。管理プロセス (たとえば、Web ベース マネージャへの HTTPS 接続) のための CPU 使用率は除外されます。CPU 使用率の詳細については、46 ページの「[System Resources]」を参照してください。
[Memory Usage]	各クラスタ ユニットの現在のメモリ ステータス。Web ベース マネージャは、コア プロセスのメモリ使用率のみを表示します。管理プロセス (たとえば、Web ベース マネージャへの HTTPS 接続) のためのメモリ使用率は除外されます。メモリ使用率の詳細については、46 ページの「[System Resources]」を参照してください。
[Active Sessions]	このクラスタ ユニットによって処理されている通信セッションの数。
[Total Packets]	このクラスタ ユニットが最後に起動されてから処理したパケットの数。
[Virus Detected]	このクラスタ ユニットによって検出されたウイルスの数。
[Network Utilization]	すべてのクラスタ ユニット インタフェースで使用されているネットワークの総帯域幅。
[Total Bytes]	このクラスタ ユニットが最後に起動されてから処理したバイト数。
[Intrusion Detected]	このクラスタ ユニット上で実行されている不正侵入防御機能によって検出された侵入または攻撃の数。

副系ユニットのホスト名およびデバイス プライオリティの変更

動作中のクラスタ内の副系ユニットのホスト名とデバイス プライオリティを変更するには、*[System]*、*[Config]*、*[HA]* の順に選択してクラスタ メンバ リストを表示します。クラスタ メンバ リスト内のいずれかのスレーブ (副系) ユニットの *[Edit]* を選択します。

バーチャル ドメインが有効な動作中のクラスタ内の副系ユニットのホスト名とデバイス プライオリティを変更するには、グローバル admin 管理者としてログインし、*[System]*、*[Config]*、*[HA]* の順に選択してクラスタ メンバ リストを表示します。クラスタ メンバ リスト内のいずれかのスレーブ (副系) ユニットの *[Edit]* を選択します。

この副系ユニットのホスト名 ([Peer]) およびデバイス プライオリティ ([Priority]) を変更できます。これらの変更は、副系ユニットの設定にのみ影響します。

[Peer]	副系ユニットのホスト名を表示し、必要に応じて変更します。
[Priority]	副系ユニットのデバイス プライオリティを表示し、必要に応じて変更します。 デバイス プライオリティは、クラスタ メンバ間では同期されません。動作中のクラスタで、デバイス プライオリティを変更して、クラスタ内の任意のユニットのプライオリティを変更できます。次回クラスタがネゴシエートするときに、デバイス プライオリティの最も高いクラスタ ユニットがプライマリ ユニットになります。 デバイス プライオリティの範囲は 0 ～ 255 です。デフォルトのデバイス プライオリティは 128 です。

クラスタ ユニットのクラスタからの切断

FortiGate ユニットを切断して、たとえばスタンドアロン ファイアウォールとして動作させるなどの別の目的に使用する必要がある場合は、そのクラスタ ユニットを切断できます。*[System]*、*[Config]*、*[HA]* の順に選択し、*[クラスタから切断]* アイコンを選択すると、クラスタの動作を中断させることなく、動作中のクラスタからクラスタ ユニットを切断できます。

[Serial Number]	クラスタから切断されるクラスタ ユニットのシリアル番号を表示します。
[Interface]	設定するインタフェースを選択します。また、このインタフェースの IP アドレスとネットマスクも指定します。FortiGate ユニットが切断されると、このインタフェースに対する管理アクセスのすべてのオプションが有効になります。
[IP/Netmask]	このインタフェースの IP アドレスとネットマスクを指定します。この IP アドレスを使用してこのインタフェースに接続し、切断されたFortiGateユニットを設定できます。

SNMP

SNMP (Simple Network Management Protocol) により、ネットワーク上のハードウェアを監視できます。ハードウェア、つまり FortiGate SNMP エージェントを設定して、SNMP マネージャにシステム情報を報告したり、トラップ (アラームやイベント メッセージ) を送信したりできます。SNMP マネージャ、またはホストとは、エージェントからの受信トラップを読み取ったり情報を追跡できるアプリケーションが動作しているコンピュータです。FortiManager ユニットは、1 つ以上の FortiGate ユニットに対する SNMP マネージャ (または、ホスト) として機能できます。

SNMPマネージャを使用すると、SNMP管理アクセスが設定された任意のFortiGateインタフェースまたは VLAN サブインタフェースから、SNMP トラップやデータにアクセスできます。SNMP マネージャの設定の 1 つとして、監視対象となる FortiGate ユニット上のコミュニティのホストとして自身をリストに加える作業があります。これを行わないと、SNMP モニタは FortiGate ユニットからのトラップを一切受信せず、クエリも行えません。

FortiGate SNMP 実装は読み取り専用です。SNMP v1、v2c、および v3 に準拠した SNMP マネージャは、クエリによる FortiGate システム情報への読み取り専用アクセス権があり、また FortiGate ユニットからトラップ メッセージを受信できます。

FortiGate システム情報を監視したり、FortiGate トラップを受信したりするには、最初にフォーティネット独自 MIB および FortiGate MIB (Management Information Base) ファイルをコンパイルする必要があります。MIB は、SNMP マネージャで使用される SNMP データ オブジェクトのリストが記述されたテキスト ファイルです。これらの MIB は、SNMP マネージャが、FortiGate ユニットの SNMP エージェントによって送信された SNMP トラップ、イベント、およびクエリ メッセージを解釈するために必要な情報を提供します。MIB ファイルをダウンロードする方法については、Fortinet Knowledge Base を参照してください。

SNMP のフォーティネットによる実装には、大部分の RFC 2665 (Ethernet-like MIB) と、大部分の RFC 1213 (MIB II) のサポートが含まれています。詳細については、145 ページの「フォーティネット MIB」を参照してください。

SNMP v3 の RFC サポートには、SNMP フレームワークのアーキテクチャ (RFC 3411) のほか、ユーザ ベースのセキュリティ モデル (RFC 3414) の部分的なサポートが含まれています。

SNMP トラップは、いっぱいになったログ ディスクや、検出されたウイルスといった発生したイベントについての警告を通知します。SNMPトラップの詳細については、146ページの「フォーティネットおよび FortiGate トラップ」を参照してください。

SNMP フィールドには、CPU 使用率 (%) やセッションの数などの、FortiGate ユニットに関する情報が含まれています。これらの情報は、継続的に、またはトラップ発生時に詳細情報を提供するために、ユニットの状態を監視する場合に有効です。SNMP フィールドの詳細については、149 ページの「フォーティネットおよび FortiGate MIB フィールド」を参照してください。

FortiGate SNMP v3 の実装には、クエリ、トラップ、認証、およびプライバシーのサポートが含まれています。認証と暗号化は、CLI で設定されます。『*FortiGate CLI リファレンス*』にある `system snmp user` コマンドを参照してください。

注記: FortiOS v3.0 と v4.0 の間で、MIB ファイルへの大きな変更がありました。FortiOS v4.0 では、新しい MIB を使用する必要があります。そうしないと、間違ったトラップやフィールドにアクセスする可能性があります。

このトピックには、以下の内容が含まれています。

SNMP の設定

SNMP エージェントを設定するには、*[System]*、*[Config]*、*[SNMP v1/v2c]* の順に選択します。

[SNMP v1/v2c] ページ

SNMP エージェントを設定するための各設定を提供します。

[SNMP Agent]	FortiGate SNMP エージェントを有効にします。
[Description]	FortiGate ユニットについての説明情報を入力します。説明は最大 35 文字です。
[Location]	FortiGate ユニットの物理的な場所を入力します。システムの場所の説明は最大 35 文字です。
[Contact]	この FortiGate ユニットの担当者の連絡先情報を入力します。連絡先情報は最大 35 文字です。
[Apply]	説明、場所、および連絡先情報への変更を保存します。
[Create New]	新しい SNMP コミュニティを追加するには、[Create New] を選択します。 143 ページの「SNMP コミュニティの設定」を参照してください。
[Communities]	FortiGate の設定に追加された SNMP コミュニティのリスト。最大 3 つのコミュニティを追加できます。
[Name]	この SNMP コミュニティの名前。
[Queries]	各 SNMP コミュニティの SNMP クエリのステータス。クエリ ステータスは、有効または無効にすることができます。
[Traps]	各 SNMP コミュニティの SNMP トラップのステータス。トラップ ステータスは、有効または無効にすることができます。
[Enable]	SNMP コミュニティをアクティブにするには、[Enable] を選択します。
[Delete]	SNMP コミュニティを削除するには、[Delete] を選択します。
[Edit]	SNMP コミュニティを表示または変更する場合に選択します。

SNMP コミュニティの設定

SNMP コミュニティとは、ネットワークの管理を目的としたデバイスのグループ化です。その SNMP コミュニティ内で、各デバイスは、トラップやその他の情報を送受信することによって通信できます。1 つの管理者端末でファイアウォール SNMP コミュニティとプリンタ SNMP コミュニティの両方を監視する場合のように、1 つのデバイスは複数のコミュニティに属することができます。

FortiGate ユニットに SNMP コミュニティを追加すると、SNMP マネージャが接続してシステム情報を表示したり、SNMP トラップを受信したりできます。

最大 3 つの SNMP コミュニティを追加できます。各コミュニティには、SNMP クエリとトラップに対する異なる設定を割り当てることができます。各コミュニティは、FortiGate ユニットの一連の異なるイベントを監視するように設定できます。また、各コミュニティに、最大 8 つの SNMP マネージャの IP アドレスを追加することもできます。

注記：FortiGate ユニットがバーチャル ドメイン モードにある場合、SNMP トラップは、管理バーチャル ドメイン内のインタフェース上でのみ送信できます。その他のインタフェースを介してトラップを送信することはできません。

[New SNMP Community] ページ

SNMP コミュニティを設定するための各設定を提供します。

[Community Name] SNMP コミュニティを識別するための名前を入力します。

[Hosts] セクション

IP アドレスを入力し、この SNMP コミュニティ内の設定を使用して FortiGate ユニットを監視できる SNMP マネージャを識別します。

[IP Address] このSNMPコミュニティ内の設定を使用してFortiGateユニットを監視できるSNMP マネージャの IP アドレス。また、任意の SNMP マネージャがこの SNMP コミュニティを使用できるように、IP アドレスを 0.0.0.0 に設定することもできます。

[Interface] 必要に応じて、この SNMP マネージャが FortiGate ユニットに接続するために使用するインタフェースの名前を選択します。インタフェースを選択する必要があるのは、SNMP マネージャが FortiGate ユニットと同じサブネット上に存在しない場合だけです。この状況は、SNMP マネージャがインターネット上か、またはルータの背後に存在する場合に発生することがあります。
バーチャル ドメイン モードの場合、SNMP トラップを通過させるには、インタフェースが管理 VDOM に属している必要があります。

[削除] SNMP マネージャを削除するには、[削除] アイコンを選択します。

[Add] ホスト リストに空白行を追加します。1 つのコミュニティに最大 8 つの SNMP マネージャを追加できます。

[Queries] セクション

FortiGate ユニットから設定情報を受信するために、このコミュニティ内の SNMP マネージャが SNMP v1 および SNMP v2c クエリのために使用するポート番号 (デフォルトでは 161) を入力します。各 SNMP バージョンのクエリをアクティブにするには、[Enable] チェック ボックスをオンにします。
注記 : SNMP クライアント ソフトウェアと FortiGate ユニットは、クエリのために同じポートを使用する必要があります。

[Protocol] SNMP プロトコル。

[Port] このプロトコルが使用するポート。必要に応じて、ポートを変更できます。

[Enable] この SNMP プロトコルを有効にする場合に選択します。

[Traps] セクション

FortiGate ユニットがこのコミュニティ内の SNMP マネージャに SNMP v1 および SNMP v2c トラップを送信するために使用する [Local] と [Remote] のポート番号 (デフォルトでは、それぞれポート 162) を入力します。各 SNMP バージョンのトラップをアクティブにするには、[Enable] チェック ボックスをオンにします。
注記 : SNMP クライアント ソフトウェアと FortiGate ユニットは、トラップのために同じポートを使用する必要があります。

[SNMP Event] FortiGate ユニットがこのコミュニティ内の SNMP マネージャにトラップを送信する必要のある各 SNMP イベントを有効にします。
[CPU 過剰使用] トラップの感度は 8 ポーリングサイクル以上の値から計算されるので、いくぶん低く抑えられます。これはポリシーの変更といった CPU を短期間に大きく使用するイベントによる急激な上昇を防止します。
[電源障害] イベント トラップは、一部の FortiGate モデルでのみ使用できます。
[AMC インタフェースのバイパス モードへの切り替え] イベント トラップは、AMC モジュールをサポートする FortiGate モデルでのみ使用できます。

[Enable] この SNMP イベントを有効にする場合に選択します。

SNMP アクセスを設定するには (NAT/ ルート モード)

リモートの SNMP マネージャが FortiGate エージェントに接続できるようにするには、SNMP 接続を受け付けるように 1 つ以上の FortiGate インタフェースを設定する必要があります。

1 *[System]*、*[Network]*、*[Interface]* の順に選択します。
2 SNMP マネージャが接続するインタフェースを選択し、[Edit] を選択します。
3 [Administrative Access] で、[SNMP] を選択します。
4 [OK] を選択します。

SNMP アクセスを設定するには (トランスペアレント モード)

1 *[System]*、*[Config]*、*[Operation]* の順に選択します。
2 [Management IP/Netmask] フィールドに、管理アクセスのために使用する IP アドレスとネットマスクを入力します。
3 *[Apply]* を選択します。

フォーティネット MIB

FortiGate SNMP エージェントは、標準の RFC 1213 および RFC 2665 MIB だけでなく、フォーティネット独自 MIB をサポートします。RFC のサポートには、RFC 2665 (Ethernet-like MIB) の一部と、FortiGate ユニットの設定に適用される RFC 1213 (MIB II) の一部のサポートが含まれています。

FortiGate ユニットの MIB ファイルには、フォーティネット MIB と FortiGate MIB の 2 つが存在します。フォーティネット MIB には、すべてのフォーティネット製品に共通のトラップ、フィールド、および情報が含まれています。FortiGate MIB には、FortiGate ユニットに固有のトラップ、フィールド、および情報が含まれています。各フォーティネット製品には、独自の MIB があります。他のフォーティネット製品を使用する場合は、その製品の MIB ファイルもダウンロードする必要があります。

この項の表には、フォーティネット MIB と FortiGate MIB が、2 つの RFC MIB とともに示されています。2 つの FortiGate MIB ファイルをフォーティネット カスタマ サポートからダウンロードできます。MIB ファイルをダウンロードする方法については、Fortinet Knowledge Base を参照してください。

SNMP マネージャが、すぐに使用できるコンパイル済みのデータベースに、標準 MIB とプライベート MIB をすでに追加している場合があります。フォーティネット固有の情報にアクセスするには、このデータベースにフォーティネット独自 MIB を追加する必要があります。このリリース用の 2 つの MIB を取得してコンパイルする必要があります。

フォーティネット MIB とトラップの詳細については、『*FortiGate 管理ガイド*』を参照してください。

注記: FortiOS v3.0 と v4.0 の間で、MIB ファイルへの大きな変更がありました。FortiOS v4.0 では、新しい MIB を使用する必要があります。そうしないと、間違ったトラップやフィールドに誤ってアクセスする可能性があります。

表 13: フォーティネット MIB

MIB ファイル名または RFC	説明
FORTINET-CORE-MIB.mib	フォーティネット独自 MIB には、すべてのフォーティネット製品に共通の、すべてのシステム設定情報とトラップ情報が含まれています。 SNMP マネージャが FortiGate ユニットの設定を監視したり、FortiGate SNMP エージェントからトラップを受信したりするには、これらの情報が必要です。詳細については、146 ページの「フォーティネットおよび FortiGate トラップ」および 149 ページの「フォーティネットおよび FortiGate MIB フィールド」を参照してください。
FORTINET-FORTIGATE-MIB.mib	独自 FortiGate MIB には、FortiGate ユニットに固有の、すべてのシステム設定情報とトラップ情報が含まれています。 SNMP マネージャが FortiGate の設定を監視したり、FortiGate SNMP エージェントからトラップを受信したりするには、これらの情報が必要です。FortiManager システムが FortiGate ユニットを監視するには、この MIB が必要です。 詳細については、146 ページの「フォーティネットおよび FortiGate トラップ」および 149 ページの「フォーティネットおよび FortiGate MIB フィールド」を参照してください。
RFC-1213 (MIB II)	FortiGate SNMP エージェントは、以下を例外として、MIB II グループをサポートします。 ・ MIB II からの EGP グループはサポートされません (RFC 1213、項 3.11 および 6.10)。 ・ MIB II グループ (IP/ICMP/TCP/UDP など) に返されるプロトコル統計では、FortiGate のトラフィック活動がすべて正確にキャプチャされるわけではありません。より正確な情報は、フォーティネット MIB によって報告される情報から取得できます。
RFC-2665 (Ethernet-like MIB)	FortiGate SNMP エージェントは、以下を例外として、Ethernet-like MIB の情報をサポートします。
	dot3Tests および dot3Errors グループはサポートされません。

フォーティネットおよび FortiGate トラップ

SNMP マネージャは、フォーティネット デバイスの SNMP エージェントに情報を要求できます。または、イベントが発生したときに、そのエージェントがトラップを送信できます。トラップとは、フォーティネット デバイス上で何かが発生したか、または変更されたことを SNMP マネージャに通知するために使用される方法です。

FortiGate デバイスの SNMP トラップを受信するには、FORTINET-CORE-MIB と FORTINET-FORTIGATE-MIB を SNMP マネージャにロードしてコンパイルする必要があります。送信されるトラップには、トラップ メッセージの他に、FortiGate ユニットのシリアル番号 (fnSysSerial) とホスト名 (sysName) が含まれます。

この項の表には、SNMP トラップおよび変数に関する情報が含まれています。これらの表は、必要なフォーティネット トラップまたは変数のオブジェクト識別子番号 (OID)、トラップ メッセージ、およびトラップの説明を見つけるのに役立つように掲載されています。

表の名前は、そのトラップが、フォーティネット MIB または FortiGate MIB のどちらで見つかるかを示しています。「トラップ メッセージ」カラムには、トラップに含まれるメッセージのほか、そのトラップに関する情報を見つけるのに役立つ SNMP MIB フィールド名が含まれています。fn で始まるトラップ (fnTrapCpuThreshold Ç»Ç«) は、フォーティネット MIB で定義されています。fg で始まるトラップ (fgTrapAvVirus など) は、FortiGate MIB で定義されています。

オブジェクト識別子 (OID) は、表の一番上にある番号の最後にインデックスを追加して構成されます。たとえば、OID が 1.3.6.1.4.1.12356.1.3.0 で、インデックスが 4 の場合、完全な OID は 1.3.6.1.4.1.12356.1.3.0.4 になります。OID とオブジェクトの名前は、SNMP マネージャが、フォーティネットおよび FortiGate MIB のフィールドとトラップをどのように参照するかを示しています。

インデントされた行は、直前の行に関連するメッセージまたは表に含まれるフィールドです。

以下の表には、次の内容が含まれています。

- 一般的なフォーティネット トラップ (OID 1.3.6.1.4.1.12356.1.3.0)
- システム トラップ (OID1.3.6.1.4.1.12356.1.3.0)
- FortiGate VPN トラップ (OID1.3.6.1.4.1.12356.1.3.0)
- FortiGate IPS トラップ (OID1.3.6.1.4.1.12356.1.3.0)
- FortiGate アンチウイルス トラップ (OID1.3.6.1.4.1.12356.1.3.0)
- FortiGate HA トラップ (OID1.3.6.1.4.1.12356.1.3.0)

表 14: 一般的なフォーティネット トラップ (OID 1.3.6.1.4.1.12356.1.3.0)

インデックス	トラップ メッセージ	説明
.1 .2 .3 .4	ColdStart WarmStart LinkUp LinkDown	RFC 1215 に記述されている標準的なトラップ。

表 15: システム トラップ (OID1.3.6.1.4.1.12356.1.3.0)

インデックス	トラップ メッセージ	説明
.101	CPU 使用率が高い (fnTrapCpuThreshold)	CPU 使用率が 80% を超えています。このしきい値は、CLI で `config system snmp sysinfo, set trap-high-cpu-threshold` を使用して設定できます。
.102	メモリの残量が少ない (fnTrapMemThreshold)	メモリ使用率が 90% を超えています。このしきい値は、CLI で `config system snmp sysinfo, set trap-low-memory-threshold` を使用して設定できます。
.103	ログ ディスクがいっぱい (fnTrapLogDiskThreshold)	ログ ディスクの使用率が設定されたしきい値を超えています。ログ ディスクを備えたデバイスでのみ使用できます。このしきい値は、CLI で `config system snmp sysinfo, set trap-log-full-threshold` を使用して設定できます。
.104	温度が高過ぎる (fnTrapTempHigh)	デバイス上の温度センサーがしきい値を超えています。すべてのデバイスに温度センサーがあるわけではありません。仕様については、マニュアルを参照してください。
.105	電圧が許容範囲外 (fnTrapVoltageOutOfRange)	出力レベルが正常なレベルの範囲外に変動しています。すべてのデバイスに電圧監視計器があるわけではありません。
.106	電源障害 (fnTrapPowerSupplyFailure)	電源障害が検出されました。すべてのモデルで使用できるわけではありません。冗長電源をサポートしている一部のデバイスで使用できます。
.201	インタフェース IP の変更 (fnTrapIpChange)	インタフェースの IP アドレスが変更されました。 このトラップ メッセージには、インタフェースの名前、新しい IP アドレス、および Fortinet ユニットのシリアル番号が含まれます。このトラップを使用すると、DHCP または PPPoE を使用してダイナミック IP アドレスが設定されたインタフェースのインタフェース IP アドレスの変更を追跡できます。
.999	診断トラップ (fnTrapTest)	このトラップは、診断の目的で送信されます。 `.999` の OID インデックスを持っています。

表 16: FortiGate VPN トラップ (OID1.3.6.1.4.1.12356.1.3.0)

インデックス	トラップ メッセージ		説明
.301	VPN トンネルが起動 (fgTrapVpnTunUp)		IPSec VPN トンネルが起動しました。
.302	VPN トンネルが停止 (fgTrapVpnTunDown)		IPSec VPN トンネルが停止しました。
		ローカル ゲートウェイ アドレス (fgVpnTrapLocalGateway)	VPN トンネルのローカル側のアドレス。 この情報は、両方の VPN トンネル トラップに関連付けられています。 (OID1.3.6.1.4.1.12356.101.12.3.2)
		リモート ゲートウェイ アドレス (fgVpnTrapRemoteGateway)	VPN トンネルのリモート側のアドレス。 この情報は、両方の VPN トンネル トラップに関連付けられています。 (OID1.3.6.1.4.1.12356.101.12.3.2)

表 17: FortiGate IPS トラップ (OID1.3.6.1.4.1.12356.1.3.0)

インデックス	トラップ メッセージ	説明
.503	IPS シグネチャ (fgTrapIpsSignature)	IPS シグネチャが検出されました。
.504	IPS アノマリ (fgTrapIpsAnomaly)	IPS アノマリが検出されました。
.505	IPS パッケージの更新 (fgTrapIpsPkgUpdate)	IPS シグネチャのデータベースが更新されました。
	(fgIpsTrapSigId)	トラップ内で識別された IPS シグネチャの ID。 (OID 1.3.6.1.4.1.12356.101.9.3.1)
	(fgIpsTrapSrcIp)	IPS シグネチャ トリガの IP アドレス。 (OID 1.3.6.1.4.1.12356.101.9.3.2)
	(fgIpsTrapSigMsg)	IPS イベントに関連付けられたメッセージ。 (OID 1.3.6.1.4.1.12356.101.9.3.3)

表 18: FortiGate アンチウイルス トラップ (OID1.3.6.1.4.1.12356.1.3.0)

インデックス	トラップ メッセージ	説明
.601	ウイルスを検出 (fgTrapAvVirus)	アンチウイルス エンジンが、HTTP または FTP ダウンロード、あるいは電子メール メッセージからの感染ファイル内にウイルスを検出しました。
.602	サイズ超過のファイル/電子メールを検出 (fgTrapAvOversize)	アンチウイルス スキャナが、サイズ超過のファイルを検出しました。
.603	ファイル名のブロックを検出 (fgTrapAvPattern)	アンチウイルス スキャナが、既知のウイルス パターンに一致するファイルをブロックしました。
.604	断片化されたファイルを検出 (fgTrapAvFragmented)	アンチウイルス スキャナが、断片化されたファイルまたは添付ファイルを検出しました。
.605	(fgTrapAvEnterConserve)	メモリが不足しているため、AV エンジンが資源保護モードに入りました。
.606	(fgTrapAvBypass)	資源保護モードのために AV スキャナがバイパスされました。
.607	(fgTrapAvOversizePass)	サイズ超過のファイルが検出されましたが、設定によってパスされました。
.608	(fgTrapAvOversizeBlock)	サイズ超過のファイルが検出され、ブロックされました。
	(fgAvTrapVirName)	このイベントをトリガしたウイルス名。 (OID1.3.6.1.4.1.12356.101.8.3.1)

表 19: FortiGate HA トラップ (OID1.3.6.1.4.1.12356.1.3.0)

インデックス	トラップ メッセージ	説明
.401	HA の切り替え (fgTrapHaSwitch)	指定されたクラスタ メンバが、スレーブからマスタに移行しました。
.402	HA 状態の変更 (fgTrapHaStateChange)	HA クラスタ メンバが状態を変更したときに送信されるトラップ。 .
.403	HA ハートビートの障害 (fgTrapHaHBFail)	ハートビートの障害の回数が設定されたしきい値を超えています。
.404	HA メンバが使用不可 (fgTrapHaMemberDown)	HA メンバがクラスタから使用できなくなりました。
.405	HA メンバが使用可能 (fgTrapHaMemberUp)	HA メンバがクラスタから使用できるようになりました。
	(fgHaTrapMemberSerial)	HA クラスタ メンバのシリアル番号。クラスタが設定されている場合、トラップの発生源を識別するために使用されます。 (OID1.3.6.1.4.1.12356.101.13.3.1)

フォーティネットおよび FortiGate MIB フィールド

FortiGate MIB には、FortiGate ユニットの現在のステータス情報を報告するフィールドが含まれています。以下の表は、MIB フィールドの名前の一覧であり、各フィールドで使用できるステータス情報を説明しています。FORTINET-CORE-MIB.mib ファイルと FORTINET-FORTIGATE-MIB.mib ファイルを SNMP マネージャでコンパイルし、コンピュータ上で MIB フィールドを参照することによって、すべてのフォーティネットおよび FortiGate MIB フィールドから使用可能な情報に関する詳細を表示できます。

フィールドが見つけやすくなるように、フィールドの各表のオブジェクト識別子 (OID) 番号が含まれています。フィールドの OID 番号は、表内のそのフィールドの (0 から始まる) 位置を示します。たとえば、fnSysVersion は、1.3.6.1.4.1.12356.2 の OID を持っています。

以下の表には、次の内容が含まれています。

- FortiGate HA MIB の情報フィールド (OID 1.3.6.1.4.1.12356.101.13.1)
- FortiGate HA ユニットのステータス フィールド (OID 1.3.6.1.4.1.12356.101.13.2)
- FortiGate 管理者アカウント (OID 1.3.6.1.4.1.12356.101)
- FortiGate バーチャル ドメイン (OID 1.3.6.1.4.1.12356.101.3.1)
- FortiGate バーチャル ドメインのテーブル エントリ (OID 1.3.6.1.4.1.12356.101.3.2.1.1)
- FortiGate のアクティブな IP セッションのテーブル (OID 1.3.6.1.4.1.12356.101.11.2.1.1)
- FortiGate ファイアウォール ポリシーの統計テーブル (OID 1.3.6.1.4.1.12356.101.5.1.2.1.1)
- FortiGate のダイヤルアップ VPN ピア (OID 1.3.6.1.4.1.12356.101.12.2.1.1)
- VPN トンネル テーブル (OID 1.3.6.1.4.1.12356.101.12.2.2.1)

表 20: FortiGate HA MIB の情報フィールド (OID 1.3.6.1.4.1.12356.101.13.1)

MIB フィールド	説明	インデックス
fgHaSystemMode	高可用性モード (スタンドアロン、A-A、または A-P)。	.1
fgHaGroupId	HA クラスタのグループ ID。	.2
fgHaPriority	HA クラスタのプライオリティ (デフォルトは 127)。	.3
fgHaOverride	マスタ置き換えフラグのステータス。	.4
fgHaAutoSync	自動設定同期のステータス。	.5
fgHaSchedule	アクティブ - アクティブ モードでのクラスタの負荷分散スケジュール。	.6
fgHaGroupName	HA クラスタのグループ名。	.7
fgHaTrapMemberSerial	HA クラスタ メンバのシリアル番号。	.8

表 21: FortiGate HA ユニットのステータス フィールド (OID 1.3.6.1.4.1.12356.101.13.2)

MIB フィールド		説明	インデックス
fgHaStatsTable	HA クラスタ内の個々の FortiGate ユニットの統計。		
	fgHaStatsIndex	クラスタ内のユニットのインデックス番号。	.1
	fgHaStatsSerial	FortiGate ユニットのシリアル番号。	.2
	fgHaStatsCpuUsage	FortiGate ユニットの現在の CPU 使用率 (%)。	.3
	fgHaStatsMemUsage	ユニットの現在のメモリ使用率 (%)。	.4
	fgHaStatsNetUsage	ユニットの現在のネットワーク使用量 (Kbps)。	.5
	fgHaStatsSesCount	アクティブなセッションの数。	.6
	fgHaStatsPktCount	処理されたパケットの数。	.7
	fgHaStatsByteCount	FortiGate ユニットによって処理されたバイト数。	.8
	fgHaStatsIdsCount	起動してから IPS が検出した攻撃の数。	.9
	fgHaStatsAvCount	起動してからアンチウイルス システムが検出したウイルスの数。	.10
	fgHaStatsHostname	HA クラスタのユニットのホスト名。	.11

表 22: FortiGate 管理者アカウント (OID 1.3.6.1.4.1.12356.101)

MIB フィールド		説明	インデックス
fgAdminIdleTimeout	管理者がシステムから自動的にログアウトされるまでのアイドル期間。		.1
fgAdminLcdProtection	LCD 保護のステータスであり、有効または無効のどちらになっているかを示します。		.2
fgAdminTable	この FortiGate ユニット上の管理者のテーブル。		
	fgAdminVdom	この管理者が属するバーチャル ドメイン。 (OID 1.3.6.1.4.1.12356.101.6.1.2.1.1.1)	

表 23: FortiGate バーチャル ドメイン (OID 1.3.6.1.4.1.12356.101.3.1)

MIB フィールド	説明		インデックス
fgVdInfo	FortiGate ユニットのバーチャル ドメイン関連情報。		
	fgVdNumber	この FortiGate ユニット上に設定されているバーチャル ドメインの数。	.1
	fgVdMaxVdoms	ハードウェアまたはライセンスによって許可された、FortiGate ユニット上で許可されているバーチャル ドメインの最大数。	.2
	fgVdEnabled	この FortiGate ユニット上でバーチャル ドメインが有効になっているかどうか。	.3

表 24: FortiGate バーチャル ドメインのテーブル エントリ (OID 1.3.6.1.4.1.12356.101.3.2.1.1)

MIB フィールド	説明		インデックス
fgVdTable.fgVdEntry	各バーチャル ドメインに関する情報のテーブル。各バーチャル ドメインに *fgVdEntry* があります。各エントリには次のフィールドがあります。		
	fgVdEntIndex	このテーブル内のエントリを一意に識別するために使用される内部のバーチャル ドメイン インデックス。このインデックスは、バーチャル ドメインを参照している他のテーブルでも使用されます。	.1
	fgVdEntName	このバーチャル ドメインの名前。	.2
	fgVdEntOpMode	このバーチャル ドメインの動作モード ([NAT] または [Transparent])。	.3

表 25: FortiGate のアクティブな IP セッションのテーブル (OID 1.3.6.1.4.1.12356.101.11.2.1.1)

MIB フィールド	説明		インデックス
fgIpSessIndex	`fgIpSessTable` テーブル内の IP セッションのインデックス番号。		.1
fgIpSessProto	このセッションが使用している IP プロトコル (IP、TCP、UDP など)。		.2
fgIpSessFromAddr	アクティブな IP セッションの発信元 IPv4 アドレス。		.3
fgIpSessFromPort	アクティブな IP セッションの発信元ポート (UDP と TCP のみ)。		.4
fgIpSessToAddr	アクティブな IP セッションの宛先 IPv4 アドレス。		.5
fgIpSessToPort	アクティブな IP セッションの宛先ポート (UDP と TCP のみ)。		.6
fgIpSessExp	このセッションの期限が切れるまでの残り秒数(アイドル状態の場合)。		.7
fgIpSessVdom	このセッションが含まれているバーチャル ドメイン。*fgVdTable* 内のインデックスに対応します。		.8
fgIpSessStatsTable	バーチャル ドメインの IP セッション統計テーブル。		
	fgIpSessStatsEntry.fgIpSessNumber	このバーチャル ドメイン上の合計セッション数。(OID 1.3.6.1.4.1.12356.101.11.2.1.2.1.1)	

表 26: FortiGate ファイアウォール ポリシーの統計テーブル（OID 1.3.6.1.4.1.12356.101.5.1.2.1.1）

MIB フィールド	説明	インデックス
fgFwPolicyStatsTable.fgFwPolicyStatsEntry	バーチャル ドメイン上のファイアウォール ポリシー統計テーブル内のエントリ。	
fgFwPolicyID	ファイアウォール ポリシー ID。 クエリに使用できるのは、有効になっているポリシーだけです。 **ポリシー ID は、バーチャル ドメイン内でのみ一意です。**	.1
fgFwPolicyPktCount	ポリシーに一致した（ポリシー アクションに応じて、パスまたはブロックされた）パケットの数。カウントは、そのポリシーがアクティブになった時点から始まります。	.2
fgFwPolicyByteCount	ポリシーに一致した（ポリシー アクションに応じて、パスまたはブロックされた ）バイト数。カウントは、そのポリシーがアクティブになった時点から始まります。	.3

表 27: FortiGate のダイヤルアップ VPN ピア（OID 1.3.6.1.4.1.12356.101.12.2.1.1）

MIB フィールド	説明	インデックス
fgVpnDialupIndex	このテーブル内のVPNダイヤルアップ ピアを一意に識別するインデックス値。	.1
fgVpnDialupGateway	トンネル上のリモート ゲートウェイの IP アドレス。	.2
fgVpnDialupLifetime	VPN トンネル存続期間（秒単位）。	.3
fgVpnDialupTimeout	このトンネルの次のキー交換までの残り時間（秒）。	.4
fgVpnDialupSrcBegin	トンネルのリモート サブネット アドレス。	.5
fgVpnDialupSrcEnd	トンネルのリモート サブネット マスク。	.6
fgVpnDialupDstAddr	トンネルのローカル サブネット アドレス。	.7
fgVpnDialupVdom	このトンネルが含まれているバーチャル ドメイン。このインデックスは、*fgVdTable* 内のインデックスに対応します。	.8
fgVpnDialUpInOctets	トンネルを介して受信されたバイト数。	.9
fgVpnDialUpOutOctets	トンネルを介して送信されたバイト数。	.10

表 28: VPN トンネル テーブル (OID 1.3.6.1.4.1.12356.101.12.2.2.1)

MIB フィールド	説明	インデックス
fgVpnTunEntIndex	VPN トンネル テーブル内の VPN トンネルを一意に識別するインデックス値。	.1
fgVpnTunEntPhase1Name	このトンネルのフェーズ 1 設定のわかりやすい名前。	.2
fgVpnTunEntPhase2Name	このトンネルのフェーズ 2 設定のわかりやすい名前。	.3
fgVpnTunEntRemGwyIp	このトンネルで使用されるリモート ゲートウェイの IP。	.4
fgVpnTunEntRemGwyPort	このトンネルで使用されるリモート ゲートウェイのポート (UDP の場合)。	.5
fgVpnTunEntLocGwyIp	このトンネルで使用されるローカル ゲートウェイの IP。	.6
fgVpnTunEntLocGwyPort	このトンネルで使用されるローカル ゲートウェイのポート (UDP の場合)。	.7
fgVpnTunEntSelectorSrcBeginIp	送信元セレクタのアドレス範囲の始まり。	.8
fgVpnTunEntSelectorSrcEndIp	送信元セレクタのアドレス範囲の終わり。	.9
fgVpnTunEntSelectorSrcPort	送信元セレクタ ポート。	.10
fgVpnTunEntSelectorDstBeginIp	送信先セレクタのアドレス範囲の始まり。	.11
fgVpnTunEntSelectorDstEndIp	送信先セレクタのアドレス範囲の終わり。	.12
fgVpnTunEntSelectorDstPort	送信先セレクタ ポート。	.13
fgVpnTunEntSelectorProto	セレクタのプロトコル番号。	.14
fgVpnTunEntLifeSecs	時間ベースの存続期間が使用されている場合の、このトンネルの存続期間 (秒単位)。	.15
fgVpnTunEntLifeBytes	バイト転送ベースの存続期間が使用されている場合の、このトンネルの存続期間 (バイト単位)。	.16
fgVpnTunEntTimeout	このトンネルのタイムアウト (秒単位)。	.17
fgVpnTunEntInOctets	このトンネル上で受信されたバイト数。	.18
fgVpnTunEntOutOctets	このトンネル上で送信されたバイト数。	.19
fgVpnTunEntStatus	このトンネルの現在のステータス (起動または停止)。	.20
fgVpnTunEntVdom	このトンネルが属するバーチャル ドメイン。このインデックスは、*fgVdTable* で使用されているインデックスに対応します。	.21

差し替えメッセージ

FortiGate ユニットは、さまざまなコンテンツ ストリームに差し替えメッセージを追加します。たとえば、電子メール メッセージの添付ファイルにウイルスが検出された場合、そのファイルは電子メールから削除され、差し替えメッセージに置き換えられます。Web フィルタリングでブロックされたページや、電子メール フィルタリングでブロックされた電子メールにも同じ処理が適用されます。

差し替えメッセージを変更したり、FortiGate ユニットが電子メール メッセージ、Web ページ、FTP セッションなどのコンテンツ ストリームに追加するアラート メールや情報をカスタマイズしたりするには、*[System]*、*[Config]*、*[Replacement Message]* の順に選択します。

注記: フォーティネットが用意した免責の差し替えメッセージは、例にすぎません。

VDOM とグローバル差し替えメッセージ

FortiGate ユニットには、すべての VDOM で使用されるグローバル差し替えメッセージが含まれています。グローバル レベルで、差し替えメッセージをカスタマイズしたり、変更したメッセージを工場出荷のデフォルト値にリセットしたりすることができます。カスタマイズしたメッセージをデフォルト メッセージに戻すことにした場合は、差し替えメッセージ リストにカスタマイズしたメッセージを表示し、*[リセット]* アイコンを選択してメッセージをデフォルト バージョンに戻すことができます。

各 VDOM では、必要に応じてその VDOM の差し替えメッセージをカスタマイズすることにより、グローバル メッセージを置き換えることができます。カスタマイズしたメッセージをグローバル メッセージに戻すことにした場合は、差し替えメッセージ リストにカスタマイズしたメッセージを表示し、*[リセット]* アイコンを選択してメッセージをこのメッセージのグローバル バージョンを使用するように戻すことができます。

差し替えメッセージ リストの表示

差し替えメッセージ リストを表示するには、*[System]*、*[Config]*、*[Replacement Message]* の順に選択します。差し替えメッセージ リストは、差し替えメッセージを表示したり、要件に応じてカスタマイズしたりするために使用します。このリストでは、差し替えメッセージがいくつかの種類 (メール、HTTP など) に整理されます。各種類の横にある展開の矢印を使用すると、そのカテゴリの差し替えメッセージが表示されます。各差し替えメッセージを要件に応じてカスタマイズするには、そのメッセージの横にある [編集] アイコンを選択します。

VDOM で差し替えメッセージ リストを表示している場合、その VDOM のカスタマイズされたメッセージの横には、その差し替えメッセージをグローバル バージョンにリセットするために使用できる [リセット] アイコンが表示されます。

[Replacement Messages] ページ

差し替えメッセージを、関連する FortiOS 機能によってグループ化された状態で表示します。たとえば、ウイルス メッセージは [Mail] グループに配置されます。

[Name]	差し替えメッセージのカテゴリ。このカテゴリを展開または縮小するには、展開の矢印を選択します。各カテゴリには、FortiGate の異なる機能で使用されるいくつかの差し替えメッセージが含まれています。これらの差し替えメッセージについては以下で説明します。
[Description]	この差し替えメッセージの説明。
[Edit]	差し替えメッセージを変更または表示する場合に選択します。
[Reset]	VDOM の差し替えメッセージ リストでのみ表示されます。この差し替えメッセージのグローバル バージョンに戻す場合に選択します。

注記 : FortiOS は、ファイアウォール ポリシーが有効になる前に、ユーザが承認する認証免責ページを HTTP を使用して送信します。したがって、認証免責ページを表示させるには、ユーザはまず HTTP トラフィックを開始する必要があります。免責事項が承認されると、ユーザはファイアウォール ポリシーで許可されたトラフィックをすべて送信できます。

差し替えメッセージの変更

差し替えメッセージ リストを変更するには、*[System]*、*[Config]*、*[Replacement Message]* の順に選択します。展開の矢印を使用して、変更する差し替えメッセージを表示します。テキストや HTML コードを編集したり、差し替えメッセージ タグを操作したりすることによって、差し替えメッセージのコンテンツを変更できます。差し替えメッセージ タグの説明については、164 ページの表 39 を参照してください。

差し替えメッセージは、テキストまたは HTML メッセージにすることができます。HTML メッセージには HTML コードを追加できます。差し替えメッセージで使用する形式は、[Allowed Formats] に表示されます。各差し替えメッセージについて、8192 文字の制限があります。差し替えメッセージを編集する場合は、次のフィールドとオプションが使用できます。差し替えメッセージごとに、異なる種類のフィールドとオプションがあります。

差し替えメッセージの差し替えメッセージ ページ	
[Message Setup]	この差し替えメッセージの名前。
[Allowed Formats]	差し替えメッセージに含めることのできるコンテンツの種類。許可される形式は [Text] または [HTML] のどちらかです。テキスト メッセージには HTML コードを使用できません。テキストや HTML メッセージには、差し替えメッセージ タグを含めることができます。
[Size]	この差し替えメッセージで許可される文字数。通常、サイズは 8192 文字です。
[Message Text]	差し替えメッセージの編集可能なテキスト。メッセージ テキストには、テキスト、HTML コード (許可される形式が [HTML] の場合)、および差し替えメッセージ タグを含めることができます。

次のカテゴリの差し替えメッセージをカスタマイズできます。

メール差し替えメッセージ

電子メールに添付されたウイルスを含むファイルのアンチウイルスによるブロックなどのイベントが発生した場合、FortiGate ユニットは IMAP、POP3、または SMTP を使用して、表 29 に表示されているメール差し替えメッセージを電子メール クライアントおよびサーバに送信します。電子メール差し替えメッセージはテキスト メッセージです。

FortiGate ユニットが SSL コンテンツのスキャンと検査をサポートしている場合は、これらの差し替えメッセージを IMAPS、POP3S、および SMTPS 電子メール メッセージに追加することもできます。詳細については、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。

表 29: メール差し替えメッセージ

メッセージ名	説明
ウイルス メッセージ	プロテクション プロファイルで電子メール プロトコルに対して有効になっているアンチウイルスの *[Virus Scan]* が電子メール メッセージからの感染ファイルを削除し、そのファイルをこのメッセージに置き換えます。
ファイル ブロック メッセージ	プロテクション プロファイルで電子メール プロトコルに対して有効になっているアンチウイルスの *[File Filter]* が、選択されたファイル フィルタ リスト内のエントリに一致するファイルを削除した場合は、そのファイルがブロックされ、その電子メールがこのメッセージに置き換えられます。
サイズ超過のファイル メッセージ	アンチウイルスの *[Oversized File/Email]* がプロテクション プロファイルで電子メール プロトコルに対して *[Block]* に設定され、かつ電子メール メッセージからのサイズ超過のファイルを削除した場合は、そのファイルがこのメッセージに置き換えられます。
断片化された電子メール	プロテクション プロファイルでは、アンチウイルスの *[Pass Fragmented Emails]* が有効になっていないため、断片化された電子メールはブロックされます。このメッセージは、断片化された電子メールの最初の部分を置き換えます。
情報漏洩防止メッセージ	DLP センサーでは、アクションが *[Block]* に設定されたルールが、ブロックされた電子メール メッセージをこのメッセージに置き換えます。
情報漏洩防止メッセージの件名	このメッセージは、DLP センサーの *[Block]*、*[Ban]*、*[Ban Sender]*、*[Quarantine IP address]*、および *[Quarantine interface]* アクションによって置き換えられたすべての電子メール メッセージの件名フィールドに追加されます。
情報漏洩防止メッセージによって禁止	DLP センサーでは、アクションが *[Ban]* に設定されたルールが、ブロックされた電子メール メッセージをこのメッセージに置き換えます。このメッセージはまた、禁止ユーザが禁止ユーザ リストから削除されるまで、それらのユーザから送信された追加の電子メール メッセージもすべて置き換えます。
情報漏洩防止メッセージによって禁止された送信者	DLP センサーでは、アクションが *[Ban Sender]* に設定されたルールが、ブロックされた電子メール メッセージをこのメッセージに置き換えます。このメッセージはまた、禁止ユーザが禁止ユーザ リストから削除されるまで、それらのユーザから送信された追加の電子メール メッセージもすべて置き換えます。
ウイルス メッセージ（スプライス モード）	スプライス モードが有効になっているとき、アンチウイルス システムが SMTP 電子メール メッセージ内のウイルスを検出します。FortiGate ユニットは SMTP セッションを中止し、この差し替えメッセージを含む 554 SMTP エラー メッセージを送信者に返します。
ファイル ブロック メッセージ（スプライス モード）	スプライス モードが有効になっているとき、アンチウイルス ファイル フィルタが SMTP 電子メール メッセージからファイルを削除しました。FortiGate ユニットは SMTP セッションを中止し、この差し替えメッセージを含む 554 SMTP エラー メッセージを送信者に返します。
サイズ超過のファイル メッセージ（スプライス モード）	スプライス モードが有効で、アンチウイルスの *[Oversized File/Email]* が *[Block]* に設定されているとき、FortiGate ユニットがサイズ超過の SMTP 電子メール メッセージをブロックします。FortiGate ユニットは SMTP セッションを中止し、この差し替えメッセージを含む 554 SMTP エラー メッセージを送信者に返します。

HTTP 差し替えメッセージ

HTTP セッションでウイルスを含むファイルのアンチウイルスによるブロックなどのイベントが発生した場合、FortiGate ユニットは HTTP プロトコルを使用して、表 30 に表示されている HTTP 差し替えメッセージを Web ブラウザに送信します。HTTP 差し替えメッセージは HTML ページです。

FortiGate ユニットが SSL コンテンツのスキャンと検査をサポートしており、かつ *[Protocol Recognition]* の *[HTTPS Content Filtering Mode]* がプロテクション プロファイルで [Deep Scan] に設定されている場合は、これらの差し替えメッセージで、HTTPS プロトコルを使用してダウンロードされた Web ページを置き換えることもできます。SSL コンテンツのスキャンと検査の詳細については、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。

表 30: HTTP 差し替えメッセージ

メッセージ名	説明
ウイルス メッセージ	プロテクション プロファイルで HTTP または HTTPS に対して有効になっているアンチウイルスの *[Virus Scan]* が、HTTP GET を使用してダウンロードされている感染ファイルを削除し、そのファイルをクライアント ブラウザによって表示されるこの Web ページに置き換えます。
感染キャッシュ メッセージ	プロテクション プロファイルでクライアント コンフォーティングが有効になっているとき、FortiGate ユニットがクライアント コンフォーティング URL キャッシュに追加されたURLをブロックし、ブロックされたURLをこのWebページに置き換えます。
ファイル ブロック メッセージ	プロテクション プロファイルで HTTP または HTTPS に対して有効になっているアンチウイルスの *[File Filter]* が、選択されたファイル フィルタ リスト内のエントリに一致する、HTTP GET を使用してダウンロードされているファイルをブロックし、そのファイルをクライアント ブラウザによって表示されるこの Web ページに置き換えます。
サイズ超過のファイル メッセージ	プロテクション プロファイルで HTTP または HTTPS に対して *[Block]* に設定されたアンチウイルスの *[Oversized File/Email]* が、HTTP GET を使用してダウンロードされているサイズ超過のファイルをブロックし、そのファイルをクライアント ブラウザによって表示されるこの Web ページに置き換えます。
情報漏洩防止 メッセージ	DLP センサーでは、アクションが *[Block]* に設定されたルールが、ブロックされた Web ページまたはファイルをこの Web ページに置き換えます。
情報漏洩防止 メッセージによって禁止	DLP センサーでは、アクションが *[Ban]* に設定されたルールが、ブロックされた Web ページまたはファイルをこの Web ページに置き換えます。この Web ページはまた、禁止ユーザが禁止ユーザ リストから削除されるまで、それらのユーザがアクセスしようとする追加の Web ページまたはファイルもすべて置き換えます。
禁止単語メッセージ	プロテクション プロファイルで有効になっている Web コンテンツ フィルタリングが、選択された Web コンテンツ フィルタ リスト内のエントリに一致するコンテンツを含む、HTTP GET を使用してダウンロードされている Web ページをブロックします。ブロックされたページがこの Web ページに置き換えられます。
コンテンツの種類ブロック メッセージ	電子メール ヘッダには、画像に対する image などの、コンテンツの種類に関する情報が含まれています。特定のコンテンツの種類がブロックされた場合は、ブロックされたメッセージがこの Web ページに置き換えられます。
URL ブロック メッセージ	プロテクション プロファイルで有効になっている Web URL フィルタが、選択された URL フィルタ リスト内のエントリに一致する URL を含む Web ページをブロックします。ブロックされたページがこの Web ページに置き換えられます。
クライアント ブロック	プロテクション プロファイルで HTTP または HTTPS に対して有効になっているアンチウイルスの *[File Filter]* が、選択されたファイル フィルタ リスト内のエントリに一致する、HTTP POST を使用してアップロードされているファイルをブロックし、そのファイルをクライアント ブラウザによって表示されるこの Web ページに置き換えます。
クライアント アンチウイルス	プロテクション プロファイルで HTTP または HTTPS に対して有効になっているアンチウイルスの *[Virus Scan]* が、HTTP PUT を使用してアップロードされている感染ファイルを削除し、そのファイルをクライアント ブラウザによって表示されるこの Web ページに置き換えます。
クライアント ファイル サイズ	プロテクション プロファイルで HTTP または HTTPS に対して *[Block]* に設定されたアンチウイルスの *[Oversized File/Email]* が、HTTP PUT を使用してアップロードされているサイズ超過のファイルをブロックし、そのファイルをこの Web ページに置き換えます。
クライアント禁止単語	プロテクション プロファイルで有効になっている Web コンテンツ フィルタリングが、選択された Web コンテンツ フィルタ リスト内のエントリに一致するコンテンツを含む、HTTP PUT を使用してアップロードされている Web ページをブロックします。クライアント ブラウザには、この Web ページが表示されます。
POST ブロック	プロテクション プロファイルで *[HTTP POST Action]* が *[Block]* に設定されているとき、FortiGate ユニットが HTTP POST をブロックし、この Web ページを表示します。

FTP 差し替えメッセージ

FTP セッションでウイルスを含むファイルのブロックなどのイベントが発生した場合、FortiGate ユニットは、表 31 に表示されている FTP 差し替えメッセージを FTP クライアントに送信します。FTP 差し替えメッセージはテキスト メッセージです。

表 31: FTP 差し替えメッセージ

メッセージ名	説明
ウイルス メッセージ	プロテクション プロファイルで FTP に対して有効になっているアンチウイルスの *[Virus Scan]* が、FTP を使用してダウンロードされている感染ファイルを削除し、このメッセージを FTP クライアントに送信します。
ブロックされたメッセージ	プロテクション プロファイルで FTP に対して有効になっているアンチウイルスの *[File Filter]* が、選択されたファイル フィルタ リスト内のエントリに一致する、FTP を使用してダウンロードされているファイルをブロックし、このメッセージを FTP クライアントに送信します。
サイズ超過のメッセージ	プロテクション プロファイルで FTP に対して *[Block]* に設定されたアンチウイルスの *[Oversized File/Email]* が、サイズ超過のファイルが FTP を使用してダウンロードされるのをブロックし、このメッセージを FTP クライアントに送信します。
DLP メッセージ	DLP センサーでは、アクションが *[Block]* に設定されたルールが、ブロックされた FTP ダウンロードをこのメッセージに置き換えます。
DLP 禁止メッセージ	DLP センサーでは、アクションが *[Ban]* に設定されたルールが FTP セッションをブロックし、このメッセージを表示します。このメッセージは、禁止ユーザが禁止ユーザ リストから削除されるまで、それらのユーザがアクセスしようとした場合は常に表示されます。

NNTP 差し替えメッセージ

NNTP メッセージに添付されたウイルスを含むファイルのブロックなどのイベントが発生した場合、FortiGate ユニットは、表 32 に表示されている NNTP 差し替えメッセージを NNTP クライアントに送信します。NNTP 差し替えメッセージはテキスト メッセージです。

表 32: NNTP 差し替えメッセージ

メッセージ名	説明
ウイルス メッセージ	プロテクション プロファイルで NNTP に対して有効になっているアンチウイルスの *[Virus Scan]* が、NNTP メッセージに添付された感染ファイルを削除し、このメッセージを NNTP クライアントに送信します。
ブロックされたメッセージ	プロテクション プロファイルで NNTP に対して有効になっているアンチウイルスの *[File Filter]* が、選択されたファイル フィルタ リスト内のエントリに一致する、NNTP メッセージに添付されたファイルをブロックし、このメッセージを NNTP クライアントに送信します。
サイズ超過のメッセージ	プロテクション プロファイルで NNTP に対して *[Block]* に設定されたアンチウイルスの *[Oversized File/Email]* が、NNTP メッセージからのサイズ超過のファイルを削除し、そのファイルをこのメッセージに置き換えます。
情報漏洩防止メッセージ	DLP センサーでは、アクションが *[Block]* に設定されたルールが、ブロックされた NNTP メッセージをこのメッセージに置き換えます。
情報漏洩防止メッセージの件名	このメッセージは、DLP センサーの *[Block]*、*[Ban]*、*[Quarantine IP address]*、および *[Quarantine interface]* アクションによって置き換えられたすべての NNTP メッセージの件名フィールドに追加されます。
情報漏洩防止メッセージによって禁止	DLP センサーでは、アクションが *[Ban]* に設定されたルールが、ブロックされた NNTP メッセージをこのメッセージに置き換えます。このメッセージはまた、禁止ユーザが禁止ユーザ リストから削除されるまで、それらのユーザから送信された追加の NNTP メッセージもすべて置き換えます。

アラート メール差し替えメッセージ

FortiGate ユニットは、管理者に送信されたアラート メール メッセージに、表 33 に表示されているアラート メール差し替えメッセージを追加します。アラート メールの詳細については、495 ページの「アラート メール」を参照してください。アラート メール差し替えメッセージはテキスト メッセージです。

表 33: アラート メール差し替えメッセージ

メッセージ名	説明
ウイルス メッセージ	アラート メールに対して *[Virus detected]* が有効になっている必要があります。プロテクション プロファイルでアンチウイルスの *[Virus Scan]* が有効になっていて、ウイルスを検出する必要があります。
ブロック メッセージ	アラート メールに対して *[Virus detected]* が有効になっている必要があります。プロテクション プロファイルでアンチウイルスの *[File Filter]* が有効になっていて、選択されたファイル フィルタ リスト内のエントリに一致するファイルをブロックする必要があります。
侵入メッセージ	アラート メールに対して *[Intrusion detected]* が有効になっています。IPS センサーまたは DoS センサーが攻撃を検出します。
重大なイベント メッセージ	*[Send alert email for logs based on severity]* を有効にするようにアラート メールを設定し、かつ *[Minimum log level]* を *[Alert]* または *[Emergency]* に設定していない限り、重大なレベルのイベント ログ メッセージが生成された場合は常に、この差し替えメッセージが送信されます。
ディスク フル メッセージ	*[Disk usage]* が有効になっていて、ディスク使用率がアラート メールに対して設定されている割合に達しました。
アラート メールに対して *[Send alert email for logs based on severity]* を有効にした場合、アラート メールによって差し替えメッセージが送信されるかどうかは、アラート メールの *[Minimum log level]* の設定方法によって異なります。	

スパム差し替えメッセージ

電子メール メッセージがスパムとして識別され、スパム アクションが破棄された場合、FortiGate ユニットは、SMTP サーバの応答に表 34 に表示されているスパム差し替えメッセージを追加します。FortiGate ユニットが SSL コンテンツのスキャンと検査をサポートしている場合は、これらの差し替えメッセージを SMTPS サーバの応答に追加することもできます。SSL コンテンツのスキャンと検査の詳細については、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。

表 34: スパム差し替えメッセージ

メッセージ名	説明
電子メール IP	プロテクション プロファイルで電子メール プロトコルに対して有効になっている *[IP address BWL check]* が電子メール メッセージをスパムとして識別し、この差し替えメッセージを追加します。
DNSBL/ORDBL	CLI から、プロテクション プロファイルで電子メール プロトコルに対して有効になっている `spamrbl` が電子メール メッセージをスパムとして識別し、この差し替えメッセージを追加します。
HELO/EHLO ドメイン	プロテクション プロファイルでSMTPに対して有効になっている *[HELO DNS lookup]* が電子メール メッセージをスパムとして識別し、この差し替えメッセージを追加します。*[HELO DNS lookup]* は、SMTPS には使用できません。
電子メール アドレス	プロテクション プロファイルで電子メール プロトコルに対して有効になっている *[E-mail address BWL check]* が電子メール メッセージをスパムとして識別し、この差し替えメッセージを追加します。
MIME ヘッダ	CLI から、プロテクション プロファイルで電子メール プロトコルに対して有効になっている `spamhdrcheck` が電子メール メッセージをスパムとして識別し、この差し替えメッセージを追加します。
返された電子メール ドメイン	プロテクション プロファイルで電子メール プロトコルに対して有効になっている *[Return e-mail DNS check]* が電子メール メッセージをスパムとして識別し、この差し替えメッセージを追加します。
禁止単語	プロテクション プロファイルで電子メール プロトコルに対して有効になっている *[Banned word check]* が電子メール メッセージをスパムとして識別し、この差し替えメッセージを追加します。
スパム送信メッセージ	プロテクション プロファイルで電子メール プロトコルに対して有効になっている [Any Email Filtering] オプションが電子メール メッセージをスパムとして識別し、この差し替えメッセージを追加します。[Email Filtering] が、このメッセージをスパムのタグが付いているすべての電子メールに追加します。このメッセージでは、電子メールに誤ってスパムのタグが付けられた (誤検知) 場合に、メッセージの受信者が FortiGuard アンチスパム サービスに電子メール シグネチャを送信するために選択できるボタンについて説明しています。

管理差し替えメッセージ

次の CLI コマンドを入力すると、管理者が FortiGate ユニットの Web ベース マネージャまたは CLI にログインした場合は常に、FortiGate ユニットに管理ログイン免責事項が表示されます。

```
config system global
  set access-banner enable
end
```

Web ベース マネージャの管理者ログイン免責事項には、ログイン免責事項差し替えメッセージのテキストのほか、[Accept] および [Decline] ボタンが含まれています。ログインするには、管理者は [Accept] を選択する必要があります。

ユーザ認証差し替えメッセージ

FortiGate ユニットは、ファイアウォール ポリシーにファイアウォール ユーザの認証が必要な少なくとも 1 つの ID ベースのポリシーが含まれていて、ユーザの認証が必要な場合に表示されるさまざまなユーザ認証の HTML ページに、表 35 に表示されている認証差し替えメッセージのテキストを使用します。ID ベースのポリシーの詳細については、273 ページの「ID ベースのファイアウォール ポリシーの設定」および 275 ページの「SSL VPN の ID ベース ファイアウォール ポリシーの設定」を参照してください。

これらの差し替えメッセージ ページは、HTTP と HTTPS を使用した認証を目的にしています。認証差し替えメッセージは HTML メッセージです。FTP や Telnet 用にファイアウォール認証メッセージをカスタマイズすることはできません。

認証ログイン ページと認証免責ページには、他の差し替えメッセージにはない差し替えタグとコントロールが含まれています。

ユーザが認証を必要とする VPN またはファイアウォール ポリシーを使用する場合は、認証ログイン ページが表示されます。このページは、他の差し替えメッセージを変更する場合と同じようにカスタマイズできます。

これらの差し替えメッセージに固有のいくつかの要件を次に示します。

- ログイン ページは、ACTION="/" および METHOD="POST" のフォームを含む HTML ページである必要があります。
- フォームには、次の非表示コントロールが含まれている必要があります。
  - `<INPUT TYPE="hidden" NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%STATEID%%" VALUE="%%STATEVAL%%">`
  - `<INPUT TYPE="hidden" NAME="%%REDIRID%%" VALUE="%%PROTURI%%">`
- フォームには、次の表示コントロールが含まれている必要があります。
  - `<INPUT TYPE="text" NAME="%%USERNAMEID%%" size=25>`
  - `<INPUT TYPE="password" NAME="%%PASSWORDID%%" size=25>`

例

上に示した要件を満たす単純な認証ページの例を次に示します。

```
<HTML><HEAD><TITLE> ファイアウォール認証 </TITLE></HEAD>
<BODY><H4> このサービスを利用するには、認証を行わなければなりません。</H4>

<FORM ACTION="/" method="post">
<INPUT NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%" TYPE="hidden">

<TABLE ALIGN="center" BGCOLOR="#00cccc" BORDER="0"
CELLPADDING="15" CELLSPACING="0" WIDTH="320"><TBODY>

<TR><TH> ユーザ名 :</TH>
<TD><INPUT NAME="%%USERNAMEID%%" SIZE="25" TYPE="text"> </TD></TR>
```

```
<TR><TH> パスワード :</TH>
<TD><INPUT NAME="%%PASSWORDID%%" SIZE="25" TYPE="password">
</TD></TR>

<TR><TD COLSPAN="2" ALIGN="center" BGCOLOR="#00cccc">
<INPUT NAME="%%STATEID%%" VALUE="%%STATEVAL%%" TYPE="hidden">
<INPUT NAME="%%REDIRID%%" VALUE="%%PROTURI%%" TYPE="hidden">
<INPUT VALUE="Continue" TYPE="submit"> </TD></TR>

</TBODY></TABLE></FORM></BODY></HTML>
```

表 35: 認証差し替えメッセージ

メッセージ名	説明
免責ページ	ID ベースのポリシーを含むファイアウォール ポリシーで選択された *[Enable Disclaimer and Redirect URL to]*。ファイアウォール ユーザが HTTP または HTTPS を使用して FortiGate ユニットで認証された後、この免責ページが表示されます。 CLI には、認証免責ページの差し替えメッセージのサイズを増やすために使用できる auth-disclaimer-page-1、auth-disclaimer-page-2、および auth-disclaimer-page-3 が含まれています。詳細については、『*FortiGateCLI リファレンス*』を参照してください。
辞退された免責ページ	ファイアウォール ユーザが、FortiGate ユニットを介したアクセスを辞退するための免責ページ上のボタンを選択すると、*[Declined disclaimer page]* が表示されます。
ログイン ページ	FortiGate ユニットを介して接続する前に、HTTP または HTTPS を使用して認証を行う必要があるファイアウォール ユーザのために表示される HTML ページ。
ログイン失敗ページ	ファイアウォール ユーザが正しくないユーザ名とパスワードの組み合わせを入力した場合に表示される HTML ページ。
ログイン チャレンジ ページ	ファイアウォール ユーザが認証を完了するために質問に答える必要がある場合に表示される HTML ページ。このページには質問が表示され、その答えを入力するためのフィールドが含まれています。この機能は RADIUS でサポートされており、一般的な RADIUS チャレンジ アクセス認証応答を使用しています。通常、チャレンジ アクセス応答には、ユーザのためのメッセージ (たとえば、「新しい PIN を入力してください」) を含む Reply-Message 属性が含まれています。このメッセージがログイン チャレンジ ページに表示されます。ユーザが応答を入力すると、それが RADIUS サーバに送り返されて、確認されます。 ログイン チャレンジ ページは、RSA SecurID 認証のために RSA RADIUS サーバで最もよく使用されます。ログイン チャレンジ ページは、サーバでユーザが新しい PIN を入力する必要がある場合に表示されます。この差し替えメッセージをカスタマイズして、ユーザに SecurID PIN の入力を求めることができます。

キープアライブ ページ	次のコマンドでファイアウォール認証キープアライブが有効になっている場合に表示される HTML ページ。
	`config system global`
	`set auth-keepalive enable`
	`end`
	認証キープアライブは、認証タイムアウトが終了しても、認証されたファイアウォール セッションが終了されないようにします。*[Authentication Timeout]* を設定するには、*[User]*、*[Options]* の順に選択します。

FortiGuard Web フィルタリング差し替えメッセージ

FortiGuard Web フィルタリングが URL をブロックした場合、FortiGate ユニットは HTTP プロトコルを使用して、表 36 に表示されている FortiGuard Web フィルタリング差し替えメッセージを Web ブラウザに送信し、ブロックされた HTTP 4xx および 5xx のエラーや、FortiGuard の上書きに関する詳細を提供します。FortiGuard Web フィルタリング差し替えメッセージは HTTP ページです。

FortiGate ユニットが SSL コンテンツのスキャンと検査をサポートしており、かつ *[Protocol Recognition]* の *[HTTPS Content Filtering Mode]* がプロテクション プロファイルで [Deep Scan] に設定されている場合は、これらの差し替えメッセージで、HTTPS プロトコルを使用してダウンロードされた Web ページを置き換えることもできます。SSL コンテンツのスキャンと検査の詳細については、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。

表 36: FortiGuard Web フィルタリング差し替えメッセージ

メッセージ名	説明
URL ブロック メッセージ	プロテクション プロファイルで HTTP または HTTPS に対して有効になっている *[Enable FortiGuard Web Filtering]* がWebページをブロックします。ブロックされたページがこの Web ページに置き換えられます。
HTTP エラー メッセージ	プロテクション プロファイルで HTTP または HTTPS に対して有効になっている *[Provide details for blocked HTTP 4xx and 5xx errors]* が Web ページをブロックします。ブロックされたページがこの Web ページに置き換えられます。
FortiGuard Web フィルタリング 上書きフォーム	FortiGuard Web フィルタリング カテゴリに対して [Override] が選択されているとき、FortiGuard Web フィルタリングがこのカテゴリ内の Web ページをブロックし、この Web ページを表示します。ユーザは、この Web ページを使用して、このページへのアクセスを取得するための認証を行うことができます。上書きルールを追加するには、*[UTM]*、*[Web Filter]*、*[Override]* の順に選択します。 %%OVRD_FORM%% タグは、FortiGuard Web フィルタリングで Web ページへのアクセスがブロックされた場合に、上書きの処理を開始するために使用されるフォームです。差し替えメッセージからこのタグを削除しないでください。

IM および P2P 差し替えメッセージ

電子メールに添付されたウイルスを含むファイルのブロックなどのイベントが発生した場合、FortiGate ユニットは AIM、ICQ、MSN、または Yahoo! Messenger を使用して、表 37 に表示されている IM および P2P 差し替えメッセージを IM および P2P クライアントに送信します。IM および P2P 差し替えメッセージはテキスト メッセージです。

表 37: IM および P2P 差し替えメッセージ

メッセージ名	説明
ファイル ブロック メッセージ	プロテクション プロファイルでIMに対して有効になっているアンチウイルスの *[File Filter]* が、選択されたファイル フィルタ リスト内のエントリに一致するファイルを削除し、そのファイルをこのメッセージに置き換えます。
ファイル名ブロック メッセージ	プロテクション プロファイルでIMに対して有効になっているアンチウイルスの *[File Filter]* が、選択されたファイル フィルタ リスト内のエントリに一致する名前を持つファイルを削除し、そのファイルをこのメッセージに置き換えます。
ウイルス メッセージ	プロテクション プロファイルで IM に対して有効になっているアンチウイルスの *[Virus Scan]* が感染ファイルを削除し、そのファイルをこのメッセージに置き換えます。
サイズ超過のファイル メッセージ	プロテクション プロファイルで IM に対して *[Block]* に設定されたアンチウイルスの *[Oversized File/Email]* がサイズ超過のファイルを削除し、そのファイルをこのメッセージに置き換えます。
情報漏洩防止 メッセージ	DLP センサーでは、アクションが *[Block]* に設定されたルールが、ブロックされた IM または P2P メッセージをこのメッセージに置き換えます。
情報漏洩防止 メッセージによって禁止	DLP センサーでは、アクションが *[Ban]* に設定されたルールが、ブロックされた IM または P2P メッセージをこのメッセージに置き換えます。このメッセージはまた、禁止ユーザが禁止ユーザ リストから削除されるまで、それらのユーザから送信された追加のメッセージもすべて置き換えます。
音声チャット ブロック メッセージ	アプリケーション制御リストで、AIM、ICQ、MSN、または Yahoo! に対して *[Block Audio]* オプションが選択されていると、そのアプリケーション制御リストがプロテクション プロファイルに追加されます。
写真共有ブロック メッセージ	アプリケーション制御リストで、MSN または Yahoo に対して `block-photo` CLI キーワードが有効になっていると、そのアプリケーション制御リストがプロテクション プロファイルに追加されます。写真のブロッキングは、CLI から有効にします。

エンドポイント NAC 差し替えメッセージ

FortiGate ユニットは、エンドポイント NAC が有効になっているファイアウォール ポリシーを使用しようとする非準拠ユーザに次のいずれかのページを送信します。

- *[Endpoint NAC Download Portal]* — FortiGate ユニットは、エンドポイント NAC プロファイルで *[Quarantine Hosts to User Portal (Enforce compliance)]* オプションが選択されている場合にこのページを送信します。ユーザは、FortiClient Endpoint Security アプリケーション インストーラをダウンロードできます。この差し替えメッセージを変更する場合は、FortiClient インストーラのダウンロード URL を提供する %%LINK%% タグを保持するようにしてください。
- *[Endpoint NAC Recommendation Portal]* — FortiGate ユニットは、エンドポイント NAC プロファイルで *[Notify Hosts to Install FortiClient (Warn only)]* オプションが選択されている場合にこのページを送信します。ユーザは、FortiClient Endpoint Security アプリケーション インストーラをダウンロードするか、または *[Continue to]* リンクを選択して目的の宛先にアクセスすることができます。この差し替えメッセージを変更する場合は、FortiClient インストーラのダウンロード URL を提供する %%LINK%% タグと、ユーザが要求した URL を含む %%DST_ADDR%% リンクの両方を保持するようにしてください。

これらのメッセージを変更するには、*[System]*、*[Config]*、*[Replacement Message]* の順に選択します。*[Endpoint NAC]* を展開し、変更するメッセージの *[編集]* アイコンを選択します。

エンドポイント NAC の詳細については、469 ページの「エンドポイント」を参照してください。

NAC 隔離差し替えメッセージ

アクションが [Quarantine IP address] または [Quarantine interface] に設定された NAC 隔離または DLP センサーでブロックされたユーザが、TCP ポート 80 を使用して FortiGate ユニット経由で HTTP セッションを開始しようとすると、FortiGate ユニットは、表 38 に表示されている 4 つの NAC 隔離 HTML ページのいずれかにそのユーザを接続します。

このユーザのために表示されるページは、そのユーザが NAC 隔離によってブロックされた理由が、ウイルスが検出された、DoS センサーが攻撃を検出した、IPS センサーが攻撃を検出した、アクションが *[Quarantine IP address]* または *[Quarantine interface]* に設定された DLP ルールがそのユーザからのセッションに一致した、のいずれであるかによって異なります。

デフォルト メッセージは、このページが表示されている理由をユーザに通知し、システム管理者に問い合わせることを推奨します。このページは必要に応じて、たとえば電子メール アドレスまたはその他の連絡先情報、あるいは該当する場合は、ユーザがブロックされる予測期間に関するメモを含めるようにカスタマイズできます。

NAC 隔離の詳細については、466 ページの「NAC 隔離および禁止ユーザ リスト」を参照してください。

表 38: NAC 隔離差し替えメッセージ

メッセージ名	説明
ウイルス メッセージ	プロテクション プロファイルで有効になっているアンチウイルスの *[Quarantine Virus Sender]* が、発信元 IP アドレスまたは FortiGate インタフェースを禁止ユーザ リストに追加します。ブロックされたユーザがポート 80 上で HTTP を使用して FortiGate ユニット経由で接続しようとするか、または任意のユーザがポート 80 上で HTTP を使用して禁止ユーザ リストに追加された FortiGate インタフェースを介して接続しようとすると、FortiGate ユニットは、この差し替えメッセージを Web ページとして表示します。
DoS メッセージ	DoS センサーでは、`attacker` または `interface` に設定された CLI `quarantine` オプション、および DoS ファイアウォール ポリシーに追加された DoS センサーが、発信元 IP、宛先 IP、または FortiGate インタフェースを禁止ユーザ リストに追加します。ブロックされたユーザがポート 80 上で HTTP を使用して FortiGate ユニット経由で接続しようとするか、または任意のユーザがポート 80 上で HTTP を使用して禁止ユーザ リストに追加された FortiGate インタフェースを介して接続しようとすると、FortiGate ユニットは、この差し替えメッセージを Web ページとして表示します。この差し替えメッセージは、`quarantine` が `both` に設定されている場合は表示されません。

表 38: NAC 隔離差し替えメッセージ （続き）

メッセージ名	説明
IPS メッセージ	IPSセンサー フィルタまたは上書きで *[Quarantine Attackers]* が有効になっていてプロテクション プロファイルに追加されたその IPS センサーが、発信元 IP アドレス、宛先 IP アドレス、または FortiGate インタフェースを禁止ユーザ リストに追加します。ブロックされたユーザがポート 80 上で HTTP を使用して FortiGate ユニット経由で接続しようとするか、または任意のユーザがポート 80 上で HTTP を使用して禁止ユーザ リストに追加された FortiGate インタフェースを介して接続しようとすると、FortiGate ユニットは、この差し替えメッセージを Web ページとして表示します。この差し替えメッセージは、*[method]* が *[Attacker and Victim IP Address]* に設定されている場合は表示されません。
DLP メッセージ	DLP センサーで、[Action] が *[Quarantine IP address]* または *[Quarantine interface]* に設定されプロテクション プロファイルに追加されたその DLP センサーが、発信元 IP アドレスまたは FortiGate インタフェースを禁止ユーザ リストに追加します。ブロックされたユーザがポート 80 上で HTTP を使用して FortiGate ユニット経由で接続しようとするか、または任意のユーザがポート 80 上で HTTP を使用して禁止ユーザ リストに追加された FortiGate インタフェースを介して接続しようとすると、FortiGate ユニットは、この差し替えメッセージを Web ページとして表示します。

トラフィック クォータ制御差し替えメッセージ

FortiGate ユニットを通過するユーザ トラフィックがトラフィック シェーピング クォータ制御でブロックされた場合、ユーザが HTTP を使用して FortiGate ユニット経由で接続しようとすると、*[Traffic shaper block message]* または *[Per IP traffic shaper block message]* が表示されます。

このトラフィック クォータ HTTP ページには、このユーザをブロックしているトラフィック シェーピング クォータ設定に関する情報を表示するための %%QUOTA_INFO%% タグが含まれています。

SSL VPN 差し替えメッセージ

SSL VPN ログイン差し替えメッセージは、FortiGate SSL VPN ポータル ログイン ページをフォーマットする HTML 差し替えメッセージです。この差し替えメッセージは、組織のニーズに従ってカスタマイズできます。このページは FortiGate の機能にリンクされています。その動作を保証するために、次のガイドラインに従って構築する必要があります。

- ログイン ページは、`ACTION="%%SSL_ACT%%"` と `METHOD="%%SSL_METHOD%%"` が含まれる HTML ページでなければなりません。
- フォームには、ログイン フォームを提供する `%%SSL_LOGIN%%` タグが含まれている必要があります。
- フォームには、`%%SSL_HIDDEN%%` タグが含まれている必要があります。

差し替えメッセージ タグ

差し替えメッセージには、差し替えメッセージ タグを含めることができます。ユーザが差し替えメッセージを受信すると、差し替えメッセージ タグはそのメッセージに関連したコンテンツに置き換えられます。表 39 は、追加できる差し替えメッセージ タグの一覧です。

表 39: 差し替えメッセージ タグ

タグ	説明
`%%AUTH_LOGOUT%%`	現在のポリシーを直ちに削除し、セッションを終了する URL。auth-keepalive ページで使用されます。
`%%AUTH_REDIR_URL%%`	auth-keepalive ページで、このタグにリンクした新しいウィンドウを開くようユーザに促すことができます。
`%%CATEGORY%%`	Web サイトのコンテンツ カテゴリの名前。
`%%DEST_IP%%`	ウイルスが送信された要求宛先の IP アドレス。電子メールの場合、これはウイルスを含む電子メールを送信した電子メール サーバの IP アドレスです。HTTP の場合、これはウイルスを送信した Web ページの IP アドレスです。
`%%EMAIL_FROM%%`	ファイルが削除されたメッセージの送信者の電子メール アドレス。

表 39: 差し替えメッセージ タグ （続き）

タグ	説明
%%EMAIL_TO%%	ファイルが削除されたメッセージの目的の受信者の電子メール アドレス。
%%FAILED_MESSAGE%%	auth-login-failed ページに表示されるログイン失敗メッセージ。
%%FILE%%	コンテンツ ストリームから削除されたファイルの名前。これは、ウイルスを含んだファイルか、またはアンチウイルスのファイル ブロッキングでブロックされたファイルの可能性があります。%%FILE%% は、ウイルスおよびファイル ブロック メッセージで使用できます。
%%FORTIGUARD_WF%%	FortiGuard – Web フィルタリングのロゴ。
%%FORTINET%%	フォーティネットのロゴ。
%%LINK%%	エンドポイント制御機能のための FortiClient Host Security インストール ダウンロードへのリンク。
%%HTTP_ERR_CODE%%	HTTP エラー コード。たとえば "404"。
%%HTTP_ERR_DESC%%	HTTP エラー コードの説明。
%%NIDSEVENT%%	IPS 攻撃メッセージ。%%NIDSEVENT%% は、侵入警告メッセージに追加されます。
%%OVERRIDE%%	FortiGuard Web フィルタリング上書きフォームへのリンク。これは、FortiGuard Web フィルタリング上書きの作成が許可されたグループにユーザが属する場合にのみ表示されます。
%%OVRD_FORM%%	FortiGuard Web フィルタ ブロック上書きフォーム。このタグは、FortiGuard Web フィルタリング上書きフォームに存在する必要があります。他の差し替えメッセージでは使用しないでください。
%%PROTOCOL%%	ウイルスが検出されたプロトコル (http、ftp、pop3、imap、または smtp)。%%PROTOCOL%% は、ウィルス警告メッセージに追加されます。
%%QUARFILENAME%%	コンテンツ ストリームから削除され、隔離場所に追加されたファイルの名前。これは、ウイルスを含んだファイルか、またはアンチウイルスのファイル ブロッキングでブロックされたファイルの可能性があります。%%QUARFILENAME%% は、ウイルスおよびファイル ブロック メッセージで使用できます。隔離は、ローカル ディスクを備えた FortiGate ユニットでのみ使用できます。
%%QUOTA_INFO%%	ユーザをブロックしているトラフィック シェーピング クォータ設定に関する情報を表示します。トラフィック クォータ制御差し替えメッセージで使用されます。
%%QUESTION%%	auth-challenge ページの認証チャレンジの質問。 auth-login ページでユーザ名とパスワードの入力が求められます。
%%SERVICE%%	Web フィルタリング サービスの名前。
%%SOURCE_IP%%	ブロックされたファイルを受信する要求発信元の IP アドレス。電子メールでは、これは、ファイルが削除されたメッセージをダウンロードしようとしたユーザのコンピュータの IP アドレスです。
%%TIMEOUT%%	認証キープアライブ接続間の設定された秒数。auth-keepalive ページで使用されます。
%%URL%%	Web ページの URL。これは、Web フィルタ コンテンツまたは URL ブロッキングでブロックされた Web ページの可能性があります。%%URL%% はまた、ユーザがブロックされているファイルをダウンロードしようとした Web ページの URL にするために、http ウイルスおよびファイル ブロック メッセージでも使用できます。
%%VIRUS%%	アンチウイルス システムでファイル内に検出されたウイルスの名前。%%VIRUS%% は、ウイルス メッセージで使用できます。

動作モードおよび VDOM 管理アクセス

各 VDOM の動作モードは、他の VDOM とは独立に変更できます。これにより、FortiGate ユニットの VDOM 上で、NAT/ ルートとトランスペアレントの動作モードを任意に組み合わせることができます。

VDOM への管理アクセスは、FortiGate ユニットへの接続に使用可能なインタフェースおよびプロトコルに基づいて制限できます。

動作モードの変更

VDOM の動作モードを設定し、ネットワーク設定を十分に行うことで、新しいモードで確実に Web ベース マネージャに接続できます。

FortiGate ユニットには、NAT/ ルートとトランスペアレントの 2 つの動作モードがあります。各モードは、それぞれ異なる状況に適しています。

NAT/ ルート モードからトランスペアレント モードに切り替えるには

1 *[System]*、*[Config]*、*[Operation]* の順に選択するか、またはバーチャル ドメインの [System Status] ページの [Operation Mode] の横にある [Change] を選択します。
2 [Operation Mode] リストから、[Transparent] を選択します。
3 次の情報を入力し、[Apply] を選択します。

[Management IP/Netmask]	管理 IP アドレスとネットマスクを入力します。これは、FortiGate ユニットの管理に使用するネットワークの有効な IP アドレスである必要があります。
[Default Gateway]	FortiGate ユニットから他のネットワークに到達するために必要なデフォルト ゲートウェイを入力します。

トランスペアレント モードから NAT/ ルート モードに切り替えるには

1 *[System]*、*[Config]*、*[Operation]* の順に選択するか、またはバーチャル ドメインの [System Status] ページの [Operation Mode] の横にある [Change] を選択します。
2 [Operation Mode] リストから、[NAT] を選択します。
3 次の情報を入力し、[Apply] を選択します。

[Interface IP/Netmask]	FortiGate ユニットの管理に使用するネットワークの有効な IP アドレスとネットマスクを入力します。
[Device]	[Interface IP/Netmask] の設定を適用するインタフェースを選択します。
[Default Gateway]	FortiGate ユニットから他のネットワークに到達するために必要なデフォルト ゲートウェイを入力します。
[Gateway Device]	デフォルト ゲートウェイが接続されるインタフェースを選択します。

管理アクセス

管理アクセスによって、管理者が設定やメンテナンスなどの管理タスクを実行するために FortiGate ユニットにログオンできる方法が定義されます。アクセスの方法には、コンソール接続を介したローカル アクセスのほか、Telnet や HTTPS を含むさまざまなプロトコルを使用したネットワークまたはモデム インタフェースを介したリモート アクセスが含まれる場合があります。

管理アクセスは、VDOM 内の任意のインタフェース上で設定できます。101 ページの「インタフェースへの管理アクセスの設定」を参照してください。NAT/ ルート モードでは、管理アクセスにインタフェース IP アドレスが使用されます。トランスペアレント モードでは、管理アクセスが可能な VDOM 内のすべてのインタフェースに適用される単一の管理 IP アドレスを設定します。また、FortiGate はこの IP アドレスを使用して FDN に接続し、ウイルスおよび攻撃の更新も行います (205 ページの「FortiGate ユニットでの FDN および FortiGuard サブスクリプション サービスの設定」を参照)。

システム管理者 (admin) は、すべての VDOM にアクセスし、標準管理者アカウントを作成することができます。標準管理者アカウントでは、自身が属する VDOM にのみアクセスできます。管理コンピュータは、その VDOM 内のインタフェースに接続する必要があります。インタフェースがどの VDOM に属しているのかは関係ありません。どちらの場合も、管理コンピュータは管理アクセスが可能なインタフェースに接続する必要があり、その IP アドレスは同じネットワーク上に存在する必要があります。インタフェース上で HTTP、HTTPS、telnet、または SSH のサービスが有効になっている場合は、それらのセッションを管理アクセスに使用できます。HTTPS と SSH は安全性が高いことから、それらの使用が望まれます。

FortiGate ユニットのリモート管理を許可することができます。ただし、インターネットからのリモート管理を許可すると、FortiGate ユニットのセキュリティが危険にさらされる可能性があります。設定にとって必須でない限り、この危険性を避けるようにしてください。インターネットからの リモート管理を許可する FortiGate ユニットのセキュリティを向上させるための方法は次のとおりです。

- セキュアな管理ユーザ パスワードを使用します。
- これらのパスワードを定期的に変更します。
- HTTPS または SSH のみを使用して、このインタフェースへのセキュアな管理アクセスを有効にします。
- 信頼できるホストを使用して、リモート アクセスの発信元を制限します。
- システムのアイドル タイムアウトをデフォルト値の 5 分から変更しないでください（184 ページの「設定」を参照）。

システム - 管理者

この項では、FortiGate ユニット上で管理者アカウントを設定する方法について説明します。管理者は、FortiGate ユニットにアクセスしてその動作を設定します。工場出荷のデフォルト設定では、admin という 1 つの管理者アカウントが設定されています。Web ベース マネージャまたは CLI に接続した後、FortiGate ユニットの設定の各部分へのさまざまなレベルのアクセス権を持つ追加の管理者を設定できます。

FortiGate ユニット上でバーチャル ドメイン (VDOM) を有効にした場合、システム管理者は FortiGate ユニット全体に対してグローバルに設定されます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には、以下のトピックが含まれています。

注記： FortiGate セッションは、常に CLI または Web ベース マネージャでログアウトすることによって終了してください。そうしないと、そのセッションが開いたままになります。

管理者

管理者アカウントには、次の 2 つのレベルがあります。

標準管理者	super_admin 以外の任意の管理者プロファイルを持つ管理者。標準管理者アカウントでは、その管理者プロファイルで決定される設定オプションにアクセスできます。バーチャル ドメインが有効になっている場合、標準管理者は 1 つの VDOM に割り当てられ、グローバル設定オプションまたは他の VDOM の設定にはアクセスできません。グローバル オプションと VDOM ごとのオプションについては、74 ページの「VDOM の設定」および 76 ページの「グローバル設定」を参照してください。
システム管理者	工場出荷のデフォルト値のシステム管理者である *admin*、super_admin プロファイルに割り当てられたその他の任意の管理者、および super_admin_readonly プロファイルに割り当てられた任意の管理者が含まれます。super_admin 管理者プロファイルに割り当てられた任意の管理者（デフォルトの管理者アカウントである *admin* を含む）は、FortiGate ユニットの設定と、次の機能を含む一般的なシステム設定に完全にアクセスできます。 ・ VDOM の設定の有効化 ・ VDOM の作成 ・ VDOM の設定 ・ 標準管理者の VDOM への割り当て ・ グローバル オプションの設定 ・ FortiGate Web ベース マネージャのカスタマイズ *super_admin* 管理者プロファイルは変更できません。このプロファイルは、*[System]*、*[Admin]*、*[Admin Profile]* の順に選択して表示される画面にあるプロファイルのリストには表示されませんが、*[System]*、*[Admin]* の順に選択して表示される *[New/Edit Administrator]* ダイアログ ボックスの [Admin Profile] ドロップダウン リストにある選択項目の 1 つです。

super_admin プロファイルに割り当てられたユーザには、次の特性があります。

- 同じく super_admin プロファイルに割り当てられている、ログインしているユーザを削除することはできません。

- 該当するユーザがログインしていない場合にのみ、super_admin プロファイルに割り当てられている他のユーザを削除したり、設定されている認証方法、パスワード、または管理者プロファイルを変更したりできます。
- デフォルトの *admin* ユーザがログインしていない場合にのみ、デフォルトの "admin" アカウントを削除できます。

デフォルトでは、*admin* にパスワードは設定されていません。このパスワードは、32 文字以下にする必要があります。super_admin 管理者プロファイルを持つユーザのパスワードは、CLI でリセットできます。ログインしているユーザのパスワードが変更された場合、そのユーザはログアウトされ、新しいパスワードで再認証を受けるよう求められます。

例 : 管理者プロファイル super_admin を持つユーザ `ITAdmin` のパスワードを 123456 に設定するには、次のコマンドを使用します。

```
config sys admin
edit ITAdmin
    set password 123456
end
```

例: 管理者プロファイル super_admin を持つユーザ `ITAdmin` のパスワードを 123456 からデフォルトの「空」にリセットするには、次のコマンドを使用します。

```
config sys admin
    edit ITAdmin
        unset password 123456
end
```

super_admin_readonly と呼ばれる、読み取り専用のスーパー管理者特権を許可する管理者プロファイルも存在します。このプロファイルは、super_admin プロファイルと同様に、削除したり変更したりすることはできません。読み取り専用の super_admin プロファイルは、システム管理者が、変更を行えない状態で顧客の設定をトラブルシューティングする必要がある場合に適しています。読み取り専用であることを除き、super_admin_readonly プロファイルでは、FortiGate のすべての設定ツールを表示できます。

管理者の認証は、FortiGate ユニットやリモート認証サーバ (LDAP、RADIUS、TACACS+ など) に格納されているパスワードを使用して、または PKI 証明書ベース認証を使用して行うことができます。LDAP または TACACS+ サーバを使用して管理者を認証するには、そのサーバを認証リストに追加し、そのサーバをユーザ グループに含め、さらに管理者をそのユーザ グループに関連付ける必要があります。RADIUS サーバはユーザを認証し、そのユーザの管理者プロファイルに基づいて内部ネットワーク リソースへのアクセスを承認します。PKI ベースの証明書を使用して認証されたユーザは、自身が属するユーザ グループおよび関連付けられている管理者プロファイルに基づいて内部ネットワーク リソースへのアクセスを許可されます。

VDOM/ 管理者プロファイルの置き換え機能は、RADIUS を介した管理者の認証をサポートしています。管理者ユーザには、そのユーザが制限されている対象の VDOM および関連付けられている管理者プロファイルに応じたアクセス権が与えられます。この機能はワイルドカード管理者に対してのみ使用可能であり、また FortiGate の CLI でのみ設定できます。VDOM 置き換えユーザは、システムごとに 1 人しか存在できません。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

このトピックには、以下の内容が含まれています。

管理者リストの表示

新しい管理者アカウントを追加したり、そのアクセス権のレベルを制御したりするには、デフォルトの "admin" アカウント、super_admin 管理者プロファイルを持つアカウント、または読み取り / 書き込みアクセス制御が許可されている管理者を使用する必要があります。super_admin 管理者プロファイルを持っていない管理者アカウントを使用してログインした場合、管理者リストには現在のバーチャル ドメインの管理者のみが表示されます。

管理者のリストを表示するには、*[System]*、*[Admin]*、*[Administrators]* の順に選択します。

[Administrators] ページ

デフォルトの super_admin 管理者アカウント、および作成したすべての管理者アカウントを表示します。

[Create New] 管理者アカウントを追加します。

[Name] 管理者アカウントのログイン名。

[Trusted Hosts] この管理者がログインできる信頼できるホストの IP アドレスとネットマスク。詳細については、179 ページの「信頼できるホストの使用」を参照してください。

[Profile] この管理者の管理者プロファイル。

[Type] この管理者の認証のタイプで、次のいずれかです。

- **[Local]** FortiGate ユニット上にローカル パスワードが格納されているアカウントの認証。
- **[Remote]** RADIUS、LDAP、または TACACS+ サーバ上の特定のアカウントの認証。
- **[Remote+ Wildcard]** LDAP、RADIUS、または TACACS+ サーバ上の任意のアカウントの認証。
- **[PKI]** アカウントの PKI ベースの証明書認証。

[Delete] この管理者アカウントを削除します。
元の "admin" アカウントは、super_admin プロファイルを持つ別のユーザを作成し、"admin" アカウントからログアウトして、super_admin プロファイルを持つ代わりのユーザを使用してログインするまで削除できません。

[Edit] この管理者アカウントを編集または表示します。

[Change Password] この管理者アカウントのパスワードを変更します。172 ページの「管理者アカウントのパスワードの変更」を参照してください。

管理者アカウントの設定

新しい管理者を作成するには、デフォルトの "admin" アカウント、super_admin 管理者プロファイルを持つアカウント、または読み取り / 書き込みアクセス制御が許可されている管理者を使用する必要があります。

新しい管理者を作成するには、*[System]*、*[Admin]*、*[Administrators]* の順に選択し、*[Create New]* を選択します。

[New Administrator] ページ

管理者アカウントを設定するための各設定を提供します。

[Administrator] この管理者アカウントのログイン名を入力します。
管理者の名前に、<>()#"' の文字を含めることはできません。管理者アカウントの名前にこれらの文字を使用すると、クロスサイト スクリプティング (XSS) の脆弱性が生じる場合があります。

[Type] 管理者アカウントの種類を選択します。

- **[Regular]** ローカル管理者アカウントを作成する場合に選択します。詳細については、172 ページの「管理者に対する通常の (パスワード) 認証の設定」を参照してください。
- **[Remote]** RADIUS、LDAP、または TACACS+ サーバを使用して管理者を認証する場合に選択します。まず、管理者に対するサーバ認証を設定する必要があります。詳細については、173 ページの「管理者に対するリモート認証の設定」を参照してください。

[PKI]	管理者に対する証明書ベースの認証を有効にする場合に選択します。PKI 認証が有効になっているときにログインできるのは 1 人の管理者だけです。詳細については、178 ページの「管理者に対する PKI 証明書認証の設定」を参照してください。
[User Group]	*[User Group]* のメンバとしてリモート サーバ/PKI(ピア)ユーザを含む管理者ユーザ グループを選択します。管理者ユーザ グループが認証のために選択された後、このグループを削除することはできません。 これは、*[Type]* が *[Remote]* または *[PKI]* の場合にのみ使用できます。
[Wildcard]	RADIUS、LDAP、または TACACS+ サーバ上のすべてのアカウントを管理者にできるようにする場合に選択します。 これは、*[Type]* が *[Remote]* の場合にのみ使用できます。VDOM ごとに許可されるワイルドカード ユーザは 1 人だけです。
[Password]	この管理者アカウントのパスワードを入力します。セキュリティを強化するために、パスワードは 6 文字以上にする必要があります。 これは、*[Wildcard]* が選択されているか、または *[Type]* が *[PKI]* の場合は使用できません。 管理者アカウントのパスワードを忘れたか、または失うかして FortiGate ユニットにログインできない場合は、詳細について Fortinet Knowledge Base の記事「*失われた管理者アカウントのパスワードの復旧*」を参照してください。
[Confirm Password]	この管理者アカウントのパスワードをもう一度入力して、パスワードを正しく入力したことを確認します。 これは、*[Wildcard]* が選択されているか、または PKI 認証が選択されている場合は使用できません。
[Trusted Host #1] [Trusted Host #2] [Trusted Host #3]	FortiGate ユニット上でこの管理者ログインが制限されている対象の信頼できるホストの IP アドレスとネットマスクを入力します。最大 3 つの信頼できるホストを指定できます。これらのアドレスはすべて、デフォルトで 0.0.0.0/0 または 0.0.0.0/0.0.0.0 に設定されています。 詳細については、179 ページの「信頼できるホストの使用」を参照してください。
[IPv6 Trusted Host #1] [IPv6 Trusted Host #2] [IPv6 Trusted Host #3]	FortiGate ユニット上でこの管理者ログインが制限されている対象の信頼できるホストの IPv6 アドレスとネットマスクを入力します。最大 3 つの信頼できるホストを指定できます。これらのアドレスはすべて、デフォルトで ::/0 に設定されています。 詳細については、179 ページの「信頼できるホストの使用」を参照してください。
[Admin Profile]	この管理者の管理者プロファイルを選択します。また、*[Create New]* を選択して新しい管理者プロファイルを作成することもできます。管理者プロファイルの詳細については、183 ページの「管理者プロファイルの設定」を参照してください。

管理者アカウントのパスワードの変更

管理者パスワードを変更するには、*[System]*、*[Admin]*、*[Administrators]* の順に選択し、パスワードを変更する管理者アカウントの横にある *[パスワードの変更]* アイコンを選択します。新しいパスワードを入力して確認し、*[OK]* を選択して変更を保存します。

管理者に対する通常の (パスワード) 認証の設定

ローカルの FortiGate ユニット上に格納されているパスワードを使用して管理者を認証できます。

FortiGate ユニット上に格納されているパスワードを使用して認証されるように管理者を設定するには

1 *[System]*、*[Admin]*、*[Administrators]* の順に選択します。

2 *[Create New]* を選択するか、または既存の管理者の横にある *[編集]* アイコンを選択します。

3 次の情報を入力します。

[Administrator]	この管理者の名前。
[Type]	*[Regular]*。
[Password]	この管理者が認証に使用するパスワード。
[Confirm Password]	*[Password]* に入力したパスワード。
[Admin Profile]	この管理者に適用される管理者プロファイル。

4 必要に応じて、追加機能を設定します。詳細については、171 ページの「管理者アカウントの設定」を参照してください。

5 *[OK]* を選択します

[Type] に *[Regular]* を選択した場合は、管理者のリストを表示したときに、*[Type]* カラム内のエントリとして *[Local]* が表示されます。詳細については、171 ページの「管理者リストの表示」を参照してください。

注記：管理者アカウントのパスワードを忘れたか、または失うかして FortiGate ユニットにログインできない場合は、Fortinet Knowledge Base の記事「失われた FortiGate 管理者アカウントのパスワードの復旧」を参照してください。

管理者に対するリモート認証の設定

RADIUS、LDAP、または TACACS+ サーバを使用して管理者を認証できます。これを行うには、サーバを設定し、そのサーバをユーザとしてユーザ グループに含めた後、そのユーザ グループに含める管理者アカウントを作成する必要があります。

管理者に対する RADIUS 認証の設定

RADIUS (Remote Authentication and Dial-in User Service) サーバは、認証、承認、およびアカウンティング機能を提供します。FortiGate ユニットは、RADIUS サーバの認証と承認の機能を使用します。RADIUS サーバを認証に使用するには、サーバを設定してから、そのサーバを必要とする FortiGate ユーザまたはユーザ グループを設定する必要があります。

RADIUS のサポートが設定されており、RADIUS サーバを使用してユーザを認証する必要がある場合、FortiGate ユニットは認証のためにそのユーザの資格情報を RADIUS サーバに送信します。RADIUS サーバがそのユーザを認証できる場合、そのユーザは FortiGate ユニットで正常に認証されます。RADIUS サーバがそのユーザを認証できない場合、FortiGate ユニットはその接続を拒否します。

RADIUS サーバを使用して VDOM 内の管理者を認証する場合は、その管理者アカウントを作成する前に認証を設定する必要があります。それには、次のことを行う必要があります。

- RADIUS サーバにアクセスするように FortiGate ユニットを設定するには
- ユーザ グループを作成するには (RADIUS)
- RADIUS サーバを使用して認証されるように管理者を設定するには

次の手順では、管理者の名前とパスワードが設定された RADIUS サーバがネットワーク上に存在することを前提にしています。RADIUS サーバを設定する方法については、使用している RADIUS サーバのドキュメントを参照してください。

RADIUS サーバのリストを表示するには、*[User]*、*[Remote]*、*[RADIUS]* の順に選択します。

[RADIUS] ページ

設定されているすべての RADIUS サーバを表示します。このページでは、新しい RADIUS サーバを編集、削除、および作成することができます。

[Create New]	新しい RADIUS サーバを追加します。
[Name]	FortiGate ユニット上の RADIUS サーバを識別する名前。
[Server Name/IP]	この RADIUS サーバのドメイン名または IP アドレス。
[Delete]	この RADIUS サーバの設定を削除します。 ユーザ グループに追加されている RADIUS サーバを削除することはできません。
[Edit]	この RADIUS サーバの設定を編集します。

注記：FortiGate ユニットへのアクセスは、管理者アカウントに関連付けられている VDOM によって異なります。

RADIUS サーバにアクセスするように FortiGate ユニットを設定するには

1 *[User]*、*[Remote]*、*[RADIUS]* の順に選択します。

2 *[Create New]* を選択するか、または既存の RADIUS サーバの横にある *[編集]* アイコンを選択します。

3 次の情報を入力します。

[Name]	この RADIUS サーバを識別する名前。
[Primary Server Name/IP]	この RADIUS サーバのドメイン名または IP アドレスを入力します。
[Primary Server Secret]	RADIUS サーバ シークレットを入力します。RADIUS サーバ管理者がこの情報を提供できます。
[Secondary Server Name/IP]	2番目のRADIUSサーバのドメイン名またはIPアドレスを入力します (オプション)。
[Secondary Server Secret]	2 番目の RADIUS サーバ シークレットを入力します (オプション)。
[Authentication Scheme]	*[Use Default Authentication Scheme]* または *[Specify Authentication Protocol]* のどちらかを選択します。方式を指定することを選択した場合は、ドロップダウン メニューからいずれかの方式を選択します。
[NAS IP/Called Station ID]	NAS (Network Attached Storage) の IP アドレスを入力します。
[Include in every User Group]	この RADIUS サーバを、この VDOM 内のすべてのユーザ グループに追加する場合に選択します (オプション)。

4 *[OK]* を選択します

RADIUS 認証の詳細については、450 ページの「RADIUS サーバの設定」を参照してください。

ユーザ グループを作成するには (RADIUS)

1 *[User]*、*[User Group]*、*[User Group]* の順に選択します。
2 *[Create New]* を選択するか、または既存の RADIUS グループの横にある *[編集]* アイコンを選択します。
3 このユーザ グループを識別する名前を入力します。
4 *[Type]* には *[Firewall]* を入力します。
5 *[Available Users/Groups]* リストで RADIUS サーバ名を選択し、それを *[Members]* リストに移動します。
6 *[OK]* を選択します

RADIUS サーバを使用して認証されるように管理者を設定するには

1 *[System]*、*[Admin]*、*[Administrators]* の順に選択します。
2 *[Create New]* を選択するか、または既存の管理者の横にある *[編集]* アイコンを選択します。
3 次の情報を入力します。

[Name]	この管理者を識別する名前。
[Type]	*[Remote]*。
[User Group]	この RADIUS サーバをメンバとして含むユーザ グループ。
[Password]	この管理者が認証に使用するパスワード。
[Confirm Password]	*[Password]* への元の入力を確認するための再入力されたパスワード。
[Admin Profile]	この管理者に適用される管理者プロファイル。

4 必要に応じて、追加機能を設定します。詳細については、171 ページの「管理者アカウントの設定」を参照してください。
5 *[OK]* を選択します

RADIUS サーバを使用してシステム管理者を認証する方法の詳細については、Fortinet Knowledge Base の記事「RADIUS を使用した管理者のアクセス権および認証」を参照してください。

管理者に対する LDAP 認証の設定

LDAP (Lightweight Directory Access Protocol) は、認証データを保守するために使用されるインターネット プロトコルです。これらのデータには、部門、ユーザ、ユーザのグループ、パスワード、電子メール アドレス、プリンタなどが含まれる可能性があります。

LDAP のサポートが設定されており、LDAP サーバを使用して管理者を認証する必要がある場合、FortiGate ユニットは認証のために LDAP サーバに接続します。LDAP サーバがその管理者を認証できない場合、FortiGate ユニットはその接続を拒否します。

LDAP サーバを使用して VDOM 内の管理者を認証する場合は、その管理者アカウントを作成する前に認証を設定する必要があります。それには、次のことを行う必要があります。

- LDAP サーバを設定するには
- ユーザ グループを作成するには (LDAP)
- LDAP サーバを使用して認証されるように管理者を設定するには

LDAP サーバのリストを表示するには、*[User]*、*[Remote]*、*[LDAP]* の順に選択します。

[LDAP] ページ

作成したすべての LDAP サーバを表示します。このページでは、新しい LDAP ページを編集、削除、または作成することができます。

[Create New]	新しい LDAP サーバを追加します。
[Name]	FortiGate ユニット上の LDAP サーバを識別する名前。
[Server Name/IP]	この LDAP サーバのドメイン名または IP アドレス。
[Port]	この LDAP サーバとの通信に使用される TCP ポート。
[Common Name Identifier]	この LDAP サーバの共通名識別子。
[Distinguished Name]	この LDAP サーバ上のエントリの検索に使用される識別名。
[Delete]	この LDAP サーバの設定を削除します。
[Edit]	この LDAP サーバの設定を編集します。

LDAP サーバを設定するには

1 *[User]*、*[Remote]*、*[LDAP]* の順に選択します。

2 *[Create New]* を選択するか、または既存の LDAP サーバの横にある *[編集]* アイコンを選択します。

3 次の情報を入力または選択し、*[OK]* を選択します。

[Name]	FortiGate ユニット上の LDAP サーバを識別する名前。
[Server Name/IP]	この LDAP サーバのドメイン名または IP アドレス。
[Server Port]	この LDAP サーバとの通信に使用される TCP ポート。
[Common Name Identifier]	この LDAP サーバの共通名識別子。
[Distinguished Name]	正しい X.500 または LDAP 形式での、このサーバの基本識別名。
[Query]	設定している LDAP サーバの LDAP サーバ *[Distinguished Name Query]* ツリーを表示して、*[Distinguished Name]* と相互参照できるようにします。詳細については、453 ページの「クエリの使用」を参照してください。
[Bind Type]	LDAP 認証のバインドの種類。
[Anonymous]	匿名ユーザ検索を使用してバインドします。
[Regular]	ユーザ名 / パスワードを使用してバインドしてから検索します。
[Simple]	検索せずに、単純なパスワード認証を使用してバインドします。
[Filter]	グループ検索に使用されるフィルタ。*[Bind Type]* が *[Anonymous]* または *[Regular]* の場合にのみ使用できます。
[User DN]	認証されるユーザの識別名。*[Bind Type]* が *[Regular]* の場合にのみ使用できます。
[Password]	認証されるユーザのパスワード。*[Bind Type]* が *[Regular]* の場合にのみ使用できます。

[Secure Connection]	認証のためのセキュアな LDAP サーバ接続を有効にするチェック ボックス。
[Protocol]	認証に使用するセキュアな LDAP プロトコル。*[Secure Connection]* が選択されている場合にのみ使用できます。
[Certificate]	認証に使用する証明書。*[Secure Connection]* が選択されている場合にのみ使用できます。

LDAP 認証の詳細については、452 ページの「LDAP サーバの設定」を参照してください。

ユーザ グループを作成するには (LDAP)

1 *[User]*、*[User Group]*、*[User Group]* の順に選択します。
2 *[Create New]* を選択するか、または既存のユーザ グループの横にある *[編集]* アイコンを選択します。
3 この LDAP ユーザ グループを識別する *[Name]* を入力します。
4 *[Type]* には *[Firewall]* を入力します。
5 *[Available Users/Groups]* リストで LDAP サーバ名を選択し、それを *[Members]* リストに移動します。
6 *[OK]* を選択します

LDAP サーバを使用して認証されるように管理者を設定するには

1 *[System]*、*[Admin]*、*[Administrators]* の順に選択します。
2 *[Create New]* を選択するか、または既存の管理者アカウントの横にある *[編集]* アイコンを選択します。
3 次の情報を入力または選択します。

[Administrator]	この管理者を識別する名前。
[Type]	*[Remote]*。
[User Group]	この LDAP サーバをメンバとして含むユーザ グループ。
[Wildcard]	LDAP サーバ上のすべてのアカウントを管理者にできるようにするためのチェック ボックス。
[Password]	この管理者が認証に使用するパスワード。*[Wildcard]* が有効になっている場合は使用できません。
[Confirm Password]	*[Password]* への元の入力を確認するための再入力されたパスワード。*[Wildcard]* が有効になっている場合は使用できません。
[Admin Profile]	この管理者に適用される管理者プロファイル。

4 必要に応じて、追加機能を設定します。詳細については、171 ページの「管理者アカウントの設定」を参照してください。
5 *[OK]* を選択します

管理者に対する TACACS+ 認証の設定

TACACS+ (Terminal Access Controller Access-Control System) は、1 台以上の集中管理サーバを介したルータ、ネットワーク アクセス サーバ、その他のネットワーク接続されたコンピューティング デバイスに対するアクセス制御を提供するリモート認証プロトコルです。

TACACS+ のサポートが設定されており、TACACS+ サーバを使用して管理者を認証する必要がある場合、FortiGate ユニットは認証のために TACACS+ サーバに接続します。TACACS+ サーバがその管理者を認証できない場合、その接続は FortiGate ユニットによって拒否されます。

TACACS+ サーバを使用して VDOM 内の管理者を認証する場合は、その管理者アカウントを作成する前に認証を設定する必要があります。それには、次のことを行う必要があります。

- TACACS+ サーバにアクセスするように FortiGate ユニットを設定するには
- ユーザ グループを作成するには (TACACS+)
- TACACS+ サーバを使用して認証されるように管理者を設定するには

TACACS+ サーバのリストを表示するには、*[User]*、*[Remote]*、*[TACACS+]* の順に選択します。

[TACACS+] ページ

作成したすべての TACACS+ サーバを表示します。このページでは、新しい TACACS+ サーバを編集、削除、または作成することができます。

[Create New]	新しい TACACS+ サーバを追加します。
[Server]	この TACACS+ サーバのサーバ ドメイン名または IP アドレス。
[Authentication Type]	サポートされている認証方法。TACACS+ の認証方法には、[Auto]、[ASCII]、[PAP]、[CHAP]、および [MSCHAP] があります。
[Delete]	この TACACS+ サーバを削除します。
[Edit]	この TACACS+ サーバを編集します。

TACACS+ サーバにアクセスするように FortiGate ユニットを設定するには

1 *[User]*、*[Remote]*、*[TACACS+]* の順に選択します。
2 *[Create New]* を選択するか、または既存の TACACS+ サーバの横にある *[編集]* アイコンを選択します。
3 次の情報を入力または選択します。

[Name]	この TACACS+ サーバを識別する名前を入力します。
[Server Name/IP]	この TACACS+ サーバのサーバ ドメイン名または IP アドレスを入力します。
[Server Key]	この TACACS+ サーバにアクセスするためのキーを入力します。最大数は 16 です。
[Authentication Type]	[Auto]、[ASCII]、[PAP]、[CHAP]、[MSCHAP] のいずれかを入力します。[Auto] は、PAP、MSCHAP、および CHAP を (その順序で) 使用して認証します。

4 *[OK]* を選択します

TACACS+ 認証の詳細については、454 ページの「TACACS+ サーバの設定」を参照してください。

ユーザ グループを作成するには (TACACS+)

1 *[User]*、*[User Group]* の順に選択します。
2 *[Create New]* を選択するか、または既存のユーザ グループの横にある *[編集]* アイコンを選択します。
3 この TACAS+ ユーザ グループを識別する *[Name]* を入力します。
4 *[Type]* には *[Firewall]* を選択します。
5 *[Available Users/Groups]* リストで TACACS+ サーバ名を選択し、それを *[Members]* リストに移動します。
6 *[OK]* を選択します

TACACS+ サーバを使用して認証されるように管理者を設定するには

1 *[System]*、*[Admin]*、*[Administrators]* の順に選択します。
2 *[Create New]* を選択するか、または既存の管理者の横にある *[編集]* アイコンを選択します。
3 次の情報を入力または選択します。

[Administrator]	この管理者を識別する名前。
[Type]	*[Remote]*。
[User Group]	この TACACS+ サーバをメンバとして含むユーザ グループ。
[Wildcard]	TACACS+ サーバ上のすべてのアカウントを管理者にできるようにする場合に選択します。
[Password]	この管理者が認証に使用するパスワード。*[Wildcard]* が有効になっている場合は使用できません。
[Confirm Password]	*[Password]* への元の入力を確認するための再入力されたパスワード。*[Wildcard]* が有効になっている場合は使用できません。
[Admin Profile]	この管理者に適用される管理者プロファイル。

4 必要に応じて、追加機能を設定します。詳細については、171 ページの「管理者アカウントの設定」を参照してください。

5 *[OK]* を選択します

管理者に対する PKI 証明書認証の設定

PKI (Public Key Infrastructure) 認証は、ピア、ピア グループ、およびユーザ グループのリストを取得し、認証の成功または拒否の通知を返す証明書認証ライブラリを使用します。ユーザに必要なのは認証が成功するための有効な証明書だけであり、ユーザ名やパスワードは必要ありません。

管理者に対する PKI 認証を使用するには、管理者アカウントを作成する前に認証を設定する必要があります。それには、次のことを行う必要があります。

- PKI ユーザを設定するには
- ユーザ グループを作成するには (PKI)
- PKI 証明書を使用して認証されるように管理者を設定するには

PKI ユーザ リストを表示するには、*[User]*、*[PKI]*、*[PKI]* の順に選択します。

[PKI] ページ

作成したすべての PKI ユーザ リストを表示します。このページでは、新しい PKI ユーザ リストを編集、削除、または作成することができます。

[Create New]	新しい PKI ユーザを追加します。
[Name]	この PKI ユーザの名前。
[Subject]	認証しているユーザの証明書の件名フィールドに表示されるテキスト文字列。
[CA]	このユーザの認証に使用される CA 証明書。
[Delete]	この PKI ユーザを削除します。
[Edit]	この PKI ユーザを編集します。

PKI ユーザを設定するには

1 *[User]*、*[PKI]*、*[PKI]* の順に選択します。

2 *[Create New]* を選択するか、または既存の PKI ユーザの横にある *[編集]* アイコンを選択します。

3 この PKI ユーザの *[Name]* を入力します。

4 *[Subject]* には、認証しているユーザの証明書の件名フィールドに表示されるテキスト文字列を入力します。

5 このユーザの認証に使用される *[CA]* 証明書を選択します。

6 *[OK]* を選択します

ユーザ グループを作成するには (PKI)

1 *[User]*、*[User Group]*、*[User Group]* の順に選択します。

2 *[Create New]* を選択するか、または既存のユーザ グループの横にある *[編集]* アイコンを選択します。

3 次の情報を入力または選択します。

[Name]	この PKI ユーザ グループを識別する名前。
[Type]	[Firewall]。
[Available Users/Groups]	PKI ユーザの名前を選択し、それを [Members] リストに移動します。

4 *[OK]* を選択します

PKI 証明書を使用して認証されるように管理者を設定するには

1 *[System]*、*[Admin]*、*[Administrators]* の順に選択します。

2 *[Create New]*を選択するか、または既存の管理者の横にある *[編集]* アイコンを選択します。
3 次の情報を入力または選択します。

[Administrator]	この管理者を識別する名前。
[Type]	*[PKI]*。
[User Group]	この PKI ユーザをメンバとして含むユーザ グループ。
[Admin Profile]	この管理者に適用される管理者プロファイル。

4 必要に応じて、追加機能を設定します。詳細については、171 ページの「管理者アカウントの設定」を参照してください。
5 *[OK]* を選択します

信頼できるホストの使用

信頼できるホストをすべての管理者に対して設定すると、管理アクセスがさらに制限されることになるため、ネットワークのセキュリティが向上します。管理者はパスワードを知っていることに加えて、指定された (1 つまたは複数の) サブネットだけを介して接続する必要があります。さらに、ネットマスクが 255.255.255.255 の信頼できるホスト IP アドレスを 1 つだけ設定すれば、管理者を 1 つの IP アドレスに制限することもできます。

信頼できるホストをすべての管理者に対して設定した場合、FortiGate ユニットは、他のどのホストからの管理アクセスの試行にも応答しません。これにより、最高のセキュリティが実現します。管理者が 1 人でも制限されない状態のままになっていると、ユニットは管理アクセスが有効になっている任意のインタフェース上の管理アクセスの試行を受け付けてしまうため、ユニットが不正なアクセスを取得しようとする試みにさらされる恐れがあります。

定義した信頼できるホストは、Telnet または SSH を介してアクセスされたときに、Web ベース マネージャと CLI の両方に適用されます。コンソール コネクタを介した CLI アクセスには影響ありません。

信頼できるホストのアドレスはすべて、IPv4 の場合は 0.0.0.0/0.0.0.0 に、IPv6 の場合は ::/0 にデフォルトで設定されています。いずれかの 0 のアドレスを 0 以外のアドレスに設定すると、その他の 0 のアドレスは無視されます。ワイルドカードのエントリを使用するには、信頼できるホストを 0.0.0.0/0.0.0.0 または ::0 のままにしておくしかありません。ただし、この設定では安全性が低くなります。

管理者プロファイル

各管理者アカウントは、1 つの管理者プロファイルに属します。管理者プロファイルによって FortiGate の機能が、読み取り / 書き込みアクセス権なし (拒否)、読み取り専用、または読み取り / 書き込みアクセスを有効にできるアクセス制御カテゴリに分離されます。

次の表は、各カテゴリによってアクセスが提供される Web ベース マネージャ ページを示しています。

表 40: Web ベース マネージャ ページへのアクセスの管理者プロファイル制御

アクセス制御	影響を受ける Web ベース マネージャ ページ
管理者ユーザ	[System]、[Admin]、[Administrators] [System]、[Admin]、[Admin Profile]
アンチウイルス設定	[UTM]、[AntiVirus]
アプリケーション制御	[UTM]、[Application Control]
ユーザ認証	[User]
情報漏洩防止 (DLP)	[UTM]、[Data Leak Prevention]
電子メール フィルタ	[UTM]、[Email Filter]
ファイアウォール設定	[Firewall]
FortiGuard 更新	[System]、[Maintenance]、[FortiGuard]

表 40: Web ベース マネージャ ページへのアクセスの管理者プロファイル制御（続き）

IM、P2P、および VoIP 設定	[IM, P2P & VoIP]、[Statistics] [IM, P2P & VoIP]、[User]、[Current Users] [IM, P2P & VoIP]、[User]、[User List] [IM, P2P & VoIP]、[User]、[Config]
IPS 設定	[UTM]、[Intrusion Protection]
ログとレポート	[Log&Report]
メンテナンス	[System]、[Maintenance]
ネットワーク設定	[System]、[Network]、[Interface] [System]、[Network]、[Zone] [System]、[Network]、[Web Proxy] [System]、[DHCP]
ルータ設定	[Router]
スパムフィルタ設定	[UTM]、[AntiSpam]
システム設定	[System]、[Status]（セッション情報を含む） [System]、[Config] [System]、[Hostname] [System]、[Network]、[Options] [System]、[Admin]、[Central Management] [System]、[Admin]、[Settings] [System]、[Status]、[System Time] [Wireless Controller]
VPN 設定	[VPN]
Web フィルタ設定	[UTM]、[Web Filter]

Web ベース マネージャ ページに対する読み取り専用アクセスにより、管理者はそのページを表示できます。ただし、管理者がそのページ上の設定を変更するには、書き込みアクセスが必要です。

ファイアウォール設定のアクセス制御を拡張して、ファイアウォール機能へのよりきめ細かなアクセス制御を有効にすることができます。ポリシー、アドレス、サービス、スケジュール、プロファイル、その他の仮想 IP（VIP）設定への管理アクセスを制御できます。

注記：*[Virtual Domain Configuration]* が有効になっている場合（184 ページの「設定」を参照）、グローバル設定にアクセスできるのは管理者プロファイル super_admin を持つ管理者だけです。その他の管理者アカウントは 1 つの VDOM に割り当てられ、グローバル設定オプションまたは他の VDOM の設定にはアクセスできません。
グローバル設定については、74 ページの「VDOM の設定」を参照してください。

管理者プロファイルは、CLI コマンドへの管理アクセスにも同様の影響を与えます。次の表は、各 *[Access Control]* カテゴリでどのコマンドの種類が使用できるかを示しています。*[Read Only]* アクセスでは、"get" および "show" コマンドにアクセスできます。"config" コマンドへのアクセスには、*[Read-Write]* アクセスが必要です。

表 41: CLI コマンドへのアクセスの管理者プロファイル制御

アクセス制御	使用可能な CLI コマンド
管理者ユーザ (admingrp)	`system admin` `system accprofile`
アンチウイルス設定 (avgrp)	`antivirus`
アプリケーション制御	`application`
ユーザ認証 (authgrp)	`user`
情報漏洩防止 (DLP)	`dlp`
電子メール フィルタ	`spamfilter`

表 41: CLI コマンドへのアクセスの管理者プロファイル制御（続き）

アクセス制御	使用可能な CLI コマンド
ファイアウォール設定 (fwgrp)	`firewall` いくつかのファイアウォール権限を個別に設定するには、`set fwgrp custom` および `config fwgrp-permission` コマンドを使用します。ポリシー、アドレス、サービス、スケジュール、プロファイル、その他の (VIP) 設定の選択を行うことができます。詳細については、『FortiGate CLI リファレンス』を参照してください。

FortiGuard 更新 (updategrp)	`system autoupdate`
	`execute update-av`
	`execute update-ips`
	`execute update-now`

IPS 設定 (ipsgrp)	`ips`

ログとレポート (loggrp)	`system alertemail`
	`log`
	`system fortianalyzer`
	`execute log`

メンテナンス (mntgrp)	`execute formatlogdisk`
	`execute restore`
	`execute backup`
	`execute batch`
	`execute usb-disk`

ネットワーク設定 (netgrp)	`system arp-table`
	`system dhcp`
	`system interface`
	`system zone`
	`execute dhcp lease-clear`
	`execute dhcp lease-list`
	`execute clear system arp table`
	`execute interface`

表 41: CLI コマンドへのアクセスの管理者プロファイル制御（続き）

アクセス制御	使用可能な CLI コマンド
ルータ設定 (routegrp)	router execute router execute mrouter
スパムフィルタ設定 (spamgrp)	spamfilter
システム設定 (sysgrp)	system（admingrp、loggrp、および netgrp コマンドを除く） gui wireless-controller execute cfg execute cli execute date execute disconnect-admin-session execute enter execute factoryreset execute fortiguard-log execute ha execute ping execute ping-options execute ping6 execute ping6-options execute reboot execute send-fds-statistics execute set-next-reboot execute shutdown execute ssh execute telnet execute time execute traceroute execute usb-disk
VPN 設定 (vpngrp)	vpn execute vpn
Web フィルタ設定 (webgrp)	webfilter

FortiGate 管理者の管理者プロファイルを追加するには、*[System]*、*[Admin]*、*[Admin Profile]* の順に選択します。各管理者アカウントは、1 つの管理者プロファイルに属します。読み取り / 書き込みアクセス権を持つ管理者は、FortiGate 機能へのアクセスを拒否する管理者プロファイル、読み取り専用アクセスを許可する管理者プロファイル、または読み取りと書き込みの両方のアクセスを許可する管理者プロファイルを作成できます。

ある機能への読み取り専用アクセス権を持っている管理者は、その機能の Web ベース マネージャ ページにアクセスできますが、その設定を変更することはできません。*[Create]* または *[Apply]* ボタンは存在せず、リストには *[編集]*、*[削除]*、またはその他の変更コマンドのアイコンの代わりに *[表示]*（  ）アイコンのみが表示されます。

管理者プロファイル リストの表示

管理者プロファイルを作成または編集するには、*[Admin Users]* の読み取り / 書き込みアクセス権を持つ管理者アカウントまたはアカウントを使用する必要があります。管理者プロファイル リストを表示するには、*[System]*、*[Admin]*、*[Admin Profile]* の順に選択します。

[Admin Profile] ページ

デフォルトの管理者プロファイルだけでなく、作成したすべての管理者プロファイルを表示します。このページでは、新しい管理者プロファイルを編集、削除、または作成することができます。既存の管理者プロファイル（デフォルトの管理者プロファイルまたは作成した管理者プロファイル）を編集できます。

[Create New] 新しい管理者プロファイルを追加します。

[Profile Name]	この管理者プロファイルの名前。
[Delete]	この管理者プロファイルを削除する場合に選択します。 管理者が割り当てられている管理者プロファイルを削除することはできません。
[Edit]	この管理者プロファイルを変更する場合に選択します。[Edit] を選択すると、[Edit Admin Profile] ページに自動的にリダイレクトされます。

管理者プロファイルの設定

管理者プロファイルを編集するには、[Admin Users] の読み取り / 書き込みアクセス権を持つ管理者アカウントまたはアカウントを使用する必要があります。

[New Admin Profile] ページ

管理者プロファイルを設定するための各設定を提供します。既存の管理者プロファイルを編集する場合は、[Edit Admin Profile] ページに自動的にリダイレクトされます。

[Profile Name]	この管理者プロファイルの名前を入力します。
[Access Control]	アクセス制御の設定をカスタマイズできる項目のリスト（設定されている場合）。
[None]	すべての *[Access Control]* カテゴリへのアクセスを拒否します。
[Read Only]	すべての *[Access Control]* カテゴリ内の *[Read]* アクセスを有効にします。
[Read-Write]	すべての *[Access Control]* カテゴリ内の読み取り / 書き込みアクセスを許可する場合に選択します。
[Access Control (categories)]	必要に応じて、特定の制御を選択します。*[Access Control]* カテゴリの詳細については、179 ページの「管理者プロファイル」を参照してください。

管理者プロファイルを設定するには

1 *[System]*、*[Admin]*、*[Admin Profile]* の順に選択します。
2 *[Create New]* を選択するか、または既存のプロファイルの横にある *[編集]* アイコンを選択します。
3 目的のプロファイル オプションを入力または選択し、*[OK]* を選択します。

集中管理

[Central Management] タブは、FortiManager ユニットまたは FortiGuard Analysis and Management Service のどちらかによって FortiGate ユニットをリモートで管理するためのオプションを提供します。

[System]、*[Admin]*、*[Central Management]* の順に選択して表示される画面から、設定を指定した集中管理サーバに自動的にバックアップまたは復元するように FortiGate ユニットを設定できます。集中管理サーバは、有効にするサービスの種類であり、FortiManager ユニットまたは FortiGuard Analysis and Management Service のどちらかです。FortiGuard Analysis and Management Service のサブスクリプションを持っている場合は、FortiGate ユニット上のファームウェアをリモートでアップグレードすることもできます。

集中管理の設定時に、自己発信トラフィックの発信元 IP アドレスを指定することもできます。ただし、これは CLI でのみ使用できます（`set fmg-source-ip`）。

[Central Management] ページ

集中管理オプションの設定のほか、FortiGate ユニット上のサービスの有効化または無効化のための各設定を提供します。

[Enable Central Management]	FortiGate ユニット上の集中管理機能を有効にします。
[Type]	この FortiGate ユニットに対する集中管理の種類を選択します。FortiManager または FortiGuard Management Service を選択できます。

[FortiManager]	FortiGate ユニットに対する集中管理サービスとして FortiManager を使用する場合に選択します。 *[IP/Name]* フィールドに、FortiManager ユニットの IP アドレスまたは名前を入力します。 組織で FortiManager クラスタを動作させている場合は、*[IP/Name]* フィールドにプライマリ FortiManager ユニットの IP アドレスまたは名前を追加し、*[Trusted FortiManager]* リストにバックアップ FortiManager ユニットの IP アドレスまたは名前を追加します。 *[Status]* は、FortiGate ユニットが、[IP/Name] フィールドに追加された FortiManager ユニットと通信できるかどうかを示します。 [Trusted FortiManager] リストにこの FortiManager ユニットを含めるには、[Register] を選択します。 赤色の下矢印は、接続が有効になっていないことを示します。 緑色の上矢印は、接続されていることを示します。 FortiGate ユニットが FortiManager ユニットに未登録デバイスと認識されている場合は、黄色の注意記号が表示されます。
[FortiGuard Management Service]	FortiGate ユニットに対する集中管理サービスとして FortiGuard Management Service を使用する場合に選択します。 [Account ID] フィールドに、アカウント ID を入力します。アカウント ID がない場合は、FortiGuard Management Service の Web サイトで FortiGuard Management Service に登録します。 *[Change]* を選択すると、*[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択して表示される画面に直接移動します。*[Analysis & Management Service]* オプションで、*[Account ID]* フィールドにアカウント ID を入力します。

FortiManager ユニットに接続し、このユニットと通信するように FortiGate ユニットを設定する場合は、次の 2 種類の展開シナリオのために、次の各手順を実行する必要があります。

- FortiManager から FortiGate に直接到達できるようにする場合
  - FortiManager の GUI で、Device Manager モジュール内の FortiManager データベースに FortiGate ユニットを追加します。
  - FortiManager の IP アドレスを変更します。
  - FortiGate の IP アドレスを変更します。
- FortiGate が NAT の背後に存在する場合
  - *[System]*、*[Admin]*、*[Central Management]* の順に選択し、[FortiManager] を選択します。
  - FortiManager ユニットを *[Trusted FortiManager]* リストに追加します (該当する場合)。
  - FortiManager の IP アドレスを変更します。
  - FortiGate の IP アドレスを変更します。
  - FortiManager 管理者に問い合わせて、FortiGate ユニットが Device Manager モジュール内の [Device] リストに表示されていることを確認します。

設定リビジョン

[System]、*[Maintenance]*、*[Configuration Revision]* の順に選択して表示される画面にある [Configuration Revision] メニューには、バックアップされた設定ファイルのリストが表示されます。リビジョン制御には、設定された集中管理サーバ、またはローカルのハード ドライブのどちらかが必要です。集中管理サーバは、FortiManager ユニットまたは FortiGuard Analysis and Management Service のどちらにすることもできます。詳細については、200 ページの「[Configuration Revision]」を参照してください。

設定

[Settings] タブには、設定可能な次の機能が含まれています。

- HTTP/HTTPS 管理アクセスおよび SSL VPN ログインのためのポート
- 管理者および IPSec 事前共有キーのためのパスワード ポリシー
- アイドル タイムアウトの設定
- Web ベース マネージャの言語、および生成されたレポートに表示される行数の設定
- LCD および制御ボタンの PIN 保護 (LCD 装備モデルのみ)

- SSH を介してログインしているユーザのための SCP 機能
- 無線コントローラ機能
- Web ベース マネージャ上の IPv6 サポート

これらの設定を行うには、*[System]*、*[Admin]*、*[Settings]* の順に選択し、次の情報を入力または選択して *[OK]* を選択します。

[Administrators Settings] ページ

Web ベース マネージャ上の IPv6 の有効化などの、各種のシステム オプションを設定するための各設定を提供します。

[Web Administration Ports]

[HTTP]	管理 HTTP アクセスに使用される TCP ポート。デフォルト値は 80 です。
[HTTPS]	管理 HTTPS アクセスに使用される TCP ポート。デフォルト値は 443 です。
[SSLVPN Login Port]	リモート クライアントの Web ブラウザが FortiGate ユニットに接続するための代わりの HTTPS ポート番号。デフォルトのポート番号は 10443 です。
[Telnet Port]	管理 Telnet アクセスに使用される TCP ポート。デフォルト値は 23 です。
[SSH Port]	管理 SSH アクセスに使用される TCP ポート。デフォルト値は 22 です。
[Enable SSH v1 compatibility]	SSH v2 に加え、SSH v1 との互換性を有効にします。(オプション)

[Password Policy]

[Enable]	このパスワード ポリシーを有効にする場合に選択します。
[Minimum Length]	パスワードの許容可能な最小の長さを設定します。
[Must contain]	次のいずれかの特殊文字の種類を選択します。選択された各種類が、パスワード内に少なくとも 1 回出現する必要があります。 [Upper Case Letters] — A、B、C、... Z [Lower Case Letters] — a、b、c、... z [Numerical digits] — 0、1、2、3、4、5、6、7 8、9 [Non-alphanumeric Letters] — 句読点、@,#、... %
[Apply Password Policy to]	パスワード ポリシーの適用対象を選択します。 **[Admin Password]** — 管理者パスワードに適用されます。いずれかのパスワードがこのポリシーに従っていない場合は、次回のログイン時に、その管理者にパスワードの変更を求めます。 **[IPSEC Preshared Key]** — IPSec VPN の事前共有キーに適用されます。このポリシーは、新しい事前共有キーにのみ適用されます。既存の事前共有キーを変更する必要はありません。
[Admin Password Expires after *n* days]	指定された日数が経過したら、管理者にパスワードの変更を求めます。定期的なパスワード変更の必要性をなくすには、0 を指定します。

[Timeout Settings]

[Idle Timeout]	管理者が再度ログインしなければならなくなるまでに管理接続がアイドルになっている必要のある分数。最大値は 480 分 (8 時間) です。 セキュリティを強化するために、アイドル タイムアウトを 5 分のデフォルト値のままにしてください。

[Display Settings]

[Language]	Web ベース マネージャが使用する言語。[English]、[Simplified Chinese]、[Japanese]、[Korean]、[Spanish]、[Traditional Chinese]、[French] から選択します。 管理コンピュータのオペレーティング システムが使用している言語を選択する必要があります。
[Lines per Page]	テーブル リストに表示するページあたりの行数。デフォルト値は 50 です。範囲は 20 ～ 1000 です。

[IPv6 Support on GUI]	GUI から IPv6 オプションを設定する場合にオンにします（ファイアウォール ポリシー、ルート、アドレス、およびアドレス グループ）。デフォルトでは、CLI からの設定のみが許可されます。IPv6 の詳細については、IPv6 に関連するフィールドを含むセクションを参照するか、または 186 ページの「FortiGate の IPv6 サポート」を参照してください。

[LCD Panel]（LCD 装備モデルのみ）

[PIN Protection]	6 桁の PIN を選択および入力します。 制御ボタンおよび LCD を使用するには、管理者は PIN を入力する必要があります。
[Enable SCP]	SSH を介してログインしているユーザが、Secure Copy（SCP）を使用して設定ファイルをコピーできるようにします。
[Enable Wireless Controller]	無線コントローラ機能を有効にします。これにより、Web ベース マネージャの [Wireless Controller] メニュー、および対応する CLI コマンドにアクセスできるようになります。詳細については、479 ページの「無線コントローラ」を参照してください。

注記： HTTP、HTTPS、Telnet、または SSH のデフォルトのポート番号を変更する場合は、そのポート番号が一意であることを確認してください。

管理者の監視

ログインしている管理者の数を表示するには、*[System]*、*[Dashboard]*、*[Status]* の順に選択します。*[System Information]* の下に *[Current Administrators]* が表示されます。現在 FortiGate ユニットにログインしている管理者に関する情報を表示するには、*[Details]* を選択します。

[Current Administrators] 情報ページ（[System Information] ウィジェット）

現在 Web ベース マネージャおよび CLI にログインしている管理者を表示します。このページから管理者を接続解除したり、このページの情報を更新したりすることができます。

[Disconnect]	選択された管理者を接続解除する場合に選択します。これは、管理者プロファイルによって *[System Configuration]* への書き込み権限が許可されている場合にのみ使用できます。
[Refresh]	このリストを更新する場合に選択します。
[Close]	このウィンドウを閉じる場合に選択します。 管理者セッションを選択し、*[Disconnect]* を選択して、この管理者をログオフさせます。これは、管理者プロファイルによって *[System Configuration]* への書き込みアクセスが許可されている場合にのみ使用できます。 デフォルトの "admin" ユーザをログオフさせることはできません。
[User Name]	この管理者アカウントの名前。
[Type]	アクセスのタイプであり、[http]、[https]、[jsconsole]、[sshv2] のいずれかです。
[From]	*[Type]* が *[jsconsole]* である場合、*[From]* の値は *[N/A]* です。 それ以外の場合、*[Type]* には、この管理者の IP アドレスが含まれています。
[Time]	この管理者がログオンした日付と時刻。

FortiGate の IPv6 サポート

IPv6 は、TCP/IP プロトコル スイートの一部であるインターネット プロトコルのバージョン 6 です。以前の標準である IPv4 に比べて、一意の IP アドレスを数 10 億個多く提供できます。インターネットは現在、IPv4 から IPv6 のアドレッシングに移行しています。IPv6 のホストとルータは、既存の IPv4 インフラストラクチャとの相互運用性を次の 2 つの方法で維持します。

- IPv6 と IPv4 の両方をサポートするデュアル IP レイヤの実装
- IPv4 ヘッダ内の IPv6 パケットの、IPv6 over IPv4 トンネリングを使用したカプセル化

FortiGate ユニットはデュアル IP レイヤの IPv6/IPv4 ノードであり、NAT/ ルートとトランスペアレントの両方の動作モードで IPv6 をサポートします。また、IPv6 のルーティング、ファイアウォール ポリシー、IPSec VPN だけでなく、IPv6 over IPv4 トンネリングもサポートします。FortiGate ユニット上の任意のインタフェースに、IPv4 アドレスと IPv6 アドレスの両方を割り当てることができます。このインタフェースは、IPv4 アドレス指定パケット用と IPv6 アドレス指定パケット用の、2 つのインタフェースとして機能します。

詳細については、『*FortiGate IPv6 サポート テクニカル ノート*』を参照してください。

FortiGate ユニット上の IPv6 の設定

FortiGate の設定は、その多くの部分で IPv6 アドレッシングをサポートしています。Web ベース マネージャで IPv6 を操作するには、事前に IPv6 サポートを有効にする必要があります。

IPv6 サポートを有効にするには、*[System]*、*[Admin]*、*[Settings]* の順に選択し、*[Display Settings]* で *[IPv6 Support on GUI]* を選択します。

Web ベース マネージャで IPv6 サポートを有効にした後、次の操作を行うことができます。

- IPv6 インタフェースを設定する (システム – ネットワークを参照)
- IPv6 DNS サービスを設定する (システム – ネットワークを参照)
- IPv6 管理アクセスを設定する (システム – 管理者を参照)
- IPv6 スタティック ルートを作成する (ルータ – スタティックを参照)
- IPv6 ルートを監視する (ルータ – モニタを参照)
- IPv6 ファイアウォール アドレスを作成する (ファイアウォール アドレスを参照)
- IPv6 ファイアウォール アドレス グループを作成する (ファイアウォール アドレスを参照)
- DoSなどのIPv6ファイアウォール ポリシーを作成する (ファイアウォール ポリシーを参照)
- IPv6 トラフィックに対してアンチウイルス スキャンを実行する
- IPv6 トラフィックに対して Web サイト フィルタリングを実行する
- IPv6 アドレッシングを使用する VPN を作成する (IPsec VPN を参照)

IPv6 サポートを有効にしたら、Web ベース マネージャまたは CLI を使用して IPv6 オプションを設定できます。一部の IPv6 設定は CLI でのみ使用できることに注意してください。

CLI を使用した IPv6 サポートの設定の詳細については、『*FortiGate CLI リファレンス*』を参照してください。

IP バージョン 6 アドレス

32 ビットのアドレス (つまり、50 億個弱のアドレス) は多いように見えますが、実際にはすぐに使い果たされます。IP アドレス空間の大部分は、数千のコンピュータを保有する大企業や政府にインターネットのバックボーン通信を提供するサーバやルータの間で予約されるか、または使い果たされてしまいました。

1998 年には、主に提供されるアドレスを増やすために IP バージョン 6 が設計されましたが、IP バージョン 4 (IPv4) についてもいくつかの改善が行われました。IP バージョン 6 (IPv6) は、RFC 2460 で定義されています。

4 バイトのアドレスの場合は、合計で 50 億個弱のアドレスが存在します。IPv6 アドレスは 32 バイトの長さがあるため、不足するという問題はありません。また、この非常に大きなアドレス空間によってアドレスのより論理的な構成も可能になるため、ネットワークのより効率的な管理やルーティングが促進されます。

IPv6 アドレスの表記

IPv6 アドレッシングの標準は、RFC 3513 で詳細に規定されています。次にその概要を示します。

IPv6 アドレスは通常、それぞれが 4 桁の 16 進数で構成された 8 つのグループとして記述されます。たとえば、

```
3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234
```

は有効な IPv6 アドレスです。

4 桁のグループが 0000 の場合は、そのグループを省略できます。たとえば、

```
3f2e:6a8b:78a3:0000:1725:6a2f:0370:6234
```

は、次と同じ IPv6 アドレスです。

```
3f2e:6a8b:78a3::1725:6a2f:0370:6234
```

"::" の表記を使用して、複数の省略された 0 のグループの連続を示すことができます。1 つのアドレス内での複数の "::" の使用は、あいまいになるため許可されません。また、グループ内の先行する 0 を省略することもできます。そのため、

```
19a4:0478:0000:0000:0000:0000:1a57:ac9e
19a4:0478:0000:0000:0000::1a57:ac9e
19a4:478:0:0:0:0:1a57:ac9e
19a4:478:0::0:1a57:ac9e
19a4:478::1a57:ac9e
```

はすべて有効であり、同じアドレスを示します。

IPv4 互換または IPv4 射影 IPv6 アドレスの場合は、IPv4 の部分を 16 進数またはドット区切り 10 進数のどちらかを使用して入力できますが、FortiGate の CLI には常に、IPv4 の部分がドット区切り 10 進数の形式で表示されます。その他のすべての IPv6 アドレスの場合、CLI は 16 進数のみを受け付けて表示します。

IPv6 ネットマスク

IP アドレスと同様に、IPv4 のドット区切り 10 進数表記が 16 進数表記で置き換えられます。また、CIDR 表記も使用できます。この表記では、IP アドレスにスラッシュ ("/") と、そのアドレスのネットワーク部分のビット数が付加されます。

表 42: IPv6 ネットマスク

IP アドレス	3ffe:ffff:1011:f101:0210:a4ff:fee3:9566
ネットマスク	ffff:ffff:ffff:ffff:0000:0000:0000:0000
ネットワーク	3ffe:ffff:1011:f101:0000:0000:0000:0000
CIDR IP/ ネットマスク	3ffe:ffff:1011:f101:0210:a4ff:fee3:9566/64

IPv6 アドレスの種類

IPv6 アドレスには、IPv4 アドレスより多くの種類があります。これらの種類は、そのプレフィックス値によって識別できます。

表 43: IPv6 アドレスの種類

アドレスの種類	プレフィックス / プレフィックスの長さ	コメント
指定なし	::/128	IPv4 の 0.0.0.0 に相当します。
ループバック	::1/128	IPv4 の 127.0.0.1 に相当します。
IPv4 互換	::/96	最下位の 32 ビットを、IPv6 の 16 進数または IPv4 のドット区切り 10 進数の形式にすることができます。
IPv4 射影	::FFFF/96	最下位の 32 ビットを、IPv6 の 16 進数または IPv4 のドット区切り 10 進数の形式にすることができます。
マルチキャスト	::FF00/8	
エニーキャスト	上に示されているものを除く、すべてのプレフィックス	トラフィックの負荷を分散させるために使用されるルーティングで、複数のサーバに同じアドレスを割り当てることができます。 IPv4 とは異なり、IPv6 のエニーキャスト アドレスは他のユニキャスト アドレスと区別できません。
リンクローカル	FE80::/10	リンクローカル アドレスは、自動アドレス設定のための単一リンク上でのアドレス指定や、隣接機器の検出に、またはルータが存在しない場合に使用されます。 ルータは、リンクローカル発信元または宛先アドレスを含むパケットを転送できません。
サイトローカル	FEC0::/10	サイトローカル アドレスは、グローバル プレフィックスを必要とすることなく、サイト内部のアドレス指定に使用されます。 ルータは、サイトローカル発信元または宛先アドレスを含むパケットをサイトの外部に転送できません。
グローバル	その他のすべて	

IPv4 から IPv6 への移行

インターネットは、IPv4 から IPv6 のアドレッシングに移行しています。IPv6 のホストとルータは、既存の IPv4 インフラストラクチャとの相互運用性を次の 2 つの方法で維持します。

- IPv6 と IPv4 の両方をサポートするデュアル IP レイヤの実装
- IPv4 ヘッダ内の IPv6 パケットの、IPv6 over IPv4 トンネリングを使用したカプセル化による IPv4 インフラストラクチャを介した転送

FortiGate ユニットはデュアル IP レイヤの IPv6/IPv4 ノードであり、IPv4 と IPv6 の両方をサポートしています。FortiGate ユニットはまた、IPv6 over IPv4 トンネリングもサポートしています。

IPv6 形式での IPv4 アドレス

IPv4 アドレスを IPv6 形式で表す方法には 2 つあります。これらの方法は、アドレスの IPv4 の部分の前にある 16 ビットで区別できます。

表 44: IPv4 互換および IPv4 射影 IPv6 アドレスの例

IPv4 互換 IPv6 アドレス	0000:0000:0000:0000:0000: または ::	0000:	874B:2B34 または 135.75.43.52
IPv4 射影 IPv6 アドレス	0000:0000:0000:0000:0000: または ::	FFFF:	874B:2B34 または 135.75.43.52

IPv4 互換アドレスは、ホストやルータが、IPv4 ルーティング インフラストラクチャを介して IPv6 パケットを動的にトンネリングするために使用されます。IPv4 射影アドレスは、IPv6 をサポートしていないノードのために使用されます。

IPv6 トンネリング

IPv6 アドレッシングを使用してているネットワークは、いくつかのトンネリング テクニックを使用して、IPv4 アドレス指定インフラストラクチャを介してリンクできます。

表 45: トンネリング テクニック

IPv6 over IPv4	IPv4 ルーティング インフラストラクチャを介して転送できるように、IPv6 パケットを IPv4 内にカプセル化します。
設定済み	エンドポイント アドレスは、カプセル化ノード上の設定情報によって決定されます。
自動	IPv4 トンネルのエンドポイント アドレスは、トンネリングされている IPv6 パケットの IPv4 互換宛先アドレスに埋め込まれた IPv4 アドレスから決定されます。
IPv4 マルチキャスト	IPv4 トンネルのエンドポイント アドレスは、 隣接機器の検出を使用して決定されます。 アドレス設定は必要ありませんが、IPv4 インフラストラクチャが IPv4 マルチキャストをサポートしている必要があります。

FortiGate ユニットは、IPv6 over IPv4 トンネリングをサポートしています。

システム - 証明書

この項では、 FortiGate Web ベース マネージャを使用して X.509 セキュリティ証明書を管理する方法について説明します。 証明書認証を使用すると、 管理者は証明書要求を生成したり、 署名済み証明書をインストールしたり、 CA ルート証明書や証明書失効リストをインポートしたり、 インストールされた証明書や秘密鍵をバックアップおよび復元したりすることができます。

認証とは、ネットワーク リソースへのアクセスに関して、リモート ホストを信頼できるかどうかを判断するプロセスです。リモート ホストは、自身の信頼性を確立するために、証明機関 (CA) から証明書を取得することによって受け付け可能な認証証明書を提供する必要があります。FortiGate ユニットは次に、証明書認証を使用して、HTTPS を介した管理アクセスを拒否または許可したり、IPSec VPN ピアまたはクライアントや、SSL VPN ユーザ グループまたはクライアントを認証したりすることができます。

FortiGate ユニット上でバーチャル ドメイン (VDOM) を有効にした場合、システム証明書は FortiGate ユニット全体に対してグローバルに設定されます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

FortiGate ユニット上には、自動的に生成された証明書がいくつかあります。

表 46: 自動的に生成された FortiGate 証明書

Fortinet_Firmware	ファームウェア内に組み込まれています。Fortinet_CA によって署名されます。すべての FortiGate ユニット上で同じです。Fortinet_Factory2 証明書がない FortiGate ユニットに、FortiGate CA によって署名された組み込みの証明書が割り当てられるようにするために使用されます。 *[Certificates]*、*[Local]* の順に選択するか、FortiGate の CLI で `vpn certificate local` を実行することによって表示されます。
Fortinet_Factory	BIOS 内に組み込まれています。Fortinet_CA によって署名されます。各 FortiGate ユニットに固有です。Fortinet_Factory2 が使用できない場合、FortiGate/FortiManager トンネル、HTTPS 管理アクセスに使用されます。 *[Certificates]*、*[Local]* の順に選択するか、FortiGate の CLI で `vpn certificate local` を実行することによって表示されます。
Fortinet_Factory2	BIOS 内に組み込まれています。Fortinet_CA2 によって署名されます。各 FortiGate ユニットに固有です。FortiGate/FortiManager トンネルおよび HTTPS 管理アクセスに使用されます。 *[Certificates]*、*[Local]* の順に選択するか、FortiGate の CLI で `vpn certificate local` を実行することによって表示されます。2008 年末以降に出荷されたユニット上にのみ存在します。
Fortinet_CA	ファームウェアおよび BIOS 内に組み込まれています。フォーティネットの CA 証明書です。たとえば、FortiGate/FortiManager トンネルまたは FortiGuard サーバへの SSL 接続を使用して、フォーティネットによって署名されたと主張している証明書を確認するために使用されます。 *[Certificates]*、*[CA]* の順に選択するか、FortiGate の CLI で `vpn certificate ca` または `vpn certificate ocsp` を実行することによって表示されます。
Fortinet_CA2	BIOS 内に組み込まれています。フォーティネットの CA 証明書です。2020 年に Fortinet_CA の期限が切れたら、最終的には Fortinet_CA に代わって使用されます。 *[Certificates]*、*[CA]* の順に選択するか、FortiGate の CLI で `vpn certificate ca` または `vpn certificate ocsp` を実行することによって表示されます。2008 年末以降に出荷されたユニット上にのみ存在します。

システム管理者は、たとえば、SSL VPN、IPSec、LDAP、PKI などで要求された場合は常に、これらの証明書を使用できます。

証明書に関する背景の詳細については、『*FortiGate 証明書管理ユーザ ガイド*』を参照してください。

この項には、以下のトピックが含まれています。

- リモート証明書
- CA 証明書
- CRL

注記：クライアント証明書を使用する SSL セッションは現在、SSL 検査をバイパスできます。これが正しく機能するには、クライアント側の証明書を要求する SSL サーバを設定する必要があります。それにより、これらの証明書がクライアントにアップロードされ、FortiGate ユニット上で有効になった SSL 検査機能を使用して、FortiGate ユニットを介した接続が作成されます。

ローカル証明書

[Local Certificates] リストには、証明書要求とインストールされたサーバ証明書が表示されます。CA に要求を送信すると、CA は情報を検証し、シリアル番号、有効期限、および CA の公開鍵が含まれたデジタル証明書に連絡先情報を登録します。CA は次に、その証明書に署名し、FortiGate ユニット上にインストールできるように証明書を送り返してきます。

ローカル証明書は、期限が切れる前にオンラインで自動的に更新できます。これは、CLI で設定する必要があります。『*FortiGate CLI リファレンス*』にある `vpn certificate local` コマンドを参照してください。

証明書要求を表示したり、署名済みサーバ証明書をインポートしたりするには、*[System]*、*[Certificates]*、*[Local Certificates]* の順に選択します。証明書の詳細を表示するには、その証明書に対応する行にある *[証明書の詳細表示]* アイコンを選択します。

[Local Certificates] ページ

デフォルトのローカル証明書だけでなく、インポートされた証明書も表示します。また、このページから証明書を生成することもできます。

[Generate]	ローカル証明書要求を生成します。詳細については、192 ページの「証明書要求の生成」を参照してください。
[Import]	署名済みローカル証明書をインポートします。詳細については、194 ページの「署名済みサーバ証明書のインポート」を参照してください。
[Name]	既存のローカル証明書および保留中の証明書要求の名前。
[Subject]	署名済みローカル証明書の識別名 (DN)。
[Comments]	この証明書の説明。
[Status]	このローカル証明書のステータス。*[PENDING]* は、ダウンロードして署名する必要のある証明書要求を示します。
[証明書の詳細表示]	証明書の名前、発行者、件名、有効な証明書の日付などの証明書の詳細を表示します。
[Delete]	選択された証明書要求またはインストールされたサーバ証明書を FortiGate の設定から削除します。これは、証明書のステータスが *[PENDING]* である場合にのみ使用できます。
[Download]	証明書要求のコピーをローカル コンピュータに保存します。FortiGate ユニットの署名済みサーバ証明書を取得するために、この要求を CA に送信できます (SCEP ベースの証明書のみ)。
[Edit Comments]	この証明書の説明を編集する場合に選択します。

デジタル証明書の取得およびインストールに関する詳細と手順については、『*FortiGate 証明書管理ユーザ ガイド*』を参照してください。

証明書要求の生成

FortiGate ユニットは、FortiGate ユニットを識別するために入力された情報に基づいて、証明書要求を生成します。生成された要求は、[Local Certificates] リストに [PENDING] のステータスとともに表示されます。証明書要求を生成した後、その要求を FortiGate ユニットへの管理アクセスが可能なコンピュータにダウンロードし、さらに CA に転送することができます。

証明書要求を作成するには、*[System]*、*[Certificates]*、*[Local Certificates]* の順に選択して *[Generate]* を選択し、下の表のフィールドに入力する必要があります。証明書要求をダウンロードして CA に送信するには、193 ページの「証明書要求のダウンロードおよび送信」を参照してください。

[Generate Certificate Signing Request] ページ

証明書を設定するための各設定を提供します。この証明書は、FortiGate ユニットに関連付けられます。

[Certification Name]	証明書の名前を入力します。これは通常、FortiGate ユニットの名前です。後で、必要に応じて署名済み証明書を PKCS12 ファイルとしてエクスポートできるようにするために、名前にはスペースを含めないでください。
[Subject Information]	この FortiGate ユニットを識別するために必要な情報を入力します。
[Host IP]	FortiGate ユニットにスタティック IP アドレスが割り当てられている場合は、[Host IP] を選択し、この FortiGate ユニットのパブリック IP アドレスを入力します。FortiGate ユニットにパブリック IP アドレスが割り当てられていない場合は、代わりに電子メール アドレス (使用可能な場合はドメイン名) を使用します。
[Domain Name]	FortiGate ユニットにスタティック IP アドレスが割り当てられ、かつダイナミック DNS サービスに登録されている場合は、この FortiGate ユニットを識別するためのドメイン名を使用します (使用可能な場合)。[Domain Name] を選択した場合は、この FortiGate ユニットの完全修飾ドメイン名を入力します。プロトコル仕様 (http://) や、ポート番号またはパス名は含めないでください。ドメイン名が使用できず、かつ FortiGate ユニットがダイナミック DNS サービスに登録されている場合は、この FortiGate ユニットのパブリック IP アドレスが変更されるたびに、ユーザのブラウザに "unable to verify certificate" (証明書を確認できません) というメッセージが表示されることがあります。
[E-Mail]	[E-Mail] を選択した場合は、この FortiGate ユニットの所有者の電子メール アドレスを入力します。
[Optional Information]	説明に従って入力するか、または空白のままにします。
[Organization Unit]	部門 (1 つまたは複数) の名前を入力します。最大 5 つの組織単位を入力できます。組織単位を追加または削除するには、プラス (+) またはマイナス (-) のアイコンを使用します。
[Organization]	企業または組織の正式名称を入力します。
[Locality (City)]	FortiGate ユニットが設置されている市または町の名前を入力します。
[State/Province]	FortiGate ユニットが設置されている都道府県または州の名前を入力します。
[Country]	FortiGate ユニットが設置されている国を選択します。
[e-mail]	連絡先の電子メール アドレスを入力します。
[Key Type]	RSA のみがサポートされています。
[Key Size]	[1024 Bit]、[1536 Bit]、または [2048 Bit] を選択します。キーのサイズを大きくするほど生成に時間がかかりますが、セキュリティは向上します。
[Enrollment Method]	次のいずれかの方法を選択します。
[File Based]	証明書要求を生成する場合に選択します。
[Online SCEP]	SCEP ベースの署名済み証明書をネットワーク経由で自動的に取得する場合に選択します。 **[CA Server URL]:** CA 証明書を取得するために使用する SCEP サーバの URL を入力します。 **[Challenge Password]:** CA サーバのチャレンジ パスワードを入力します。

証明書要求のダウンロードおよび送信

CA に証明書要求を送信する前に、必要な項目を入力し、証明書要求を生成する必要があります。詳細については、192 ページの「証明書要求の生成」を参照してください。

証明書要求をダウンロードして送信するには

1 *[System]*、*[Certificates]*、*[Local Certificates]* の順に選択します。

2 *[Local Certificates]* リストで、生成された証明書要求に対応する行にある *[ダウンロード]* アイコンを選択します。

3 *[File Download]* ダイアログ ボックスで、*[Save to Disk]* を選択します。

4 ファイルに名前を付け、それをローカル ファイル システムに保存します。
5 次のようにして要求を CA に送信します。
- 管理コンピュータ上で Web ブラウザを使用して、CA の Web サイトを参照します。
- CA の指示に従って、base-64 でエンコードされた PKCS#12 の証明書要求を作成し、その証明書要求をアップロードします。
- CA の指示に従って、その CA のルート証明書と証明書失効リスト（CRL）をダウンロードし、次にそのルート証明書と CRL を各リモート クライアントにインストールします（ブラウザのドキュメントを参照してください）。

6 CA から署名済み証明書を受け取ったら、その証明書を FortiGate ユニットにインストールします。194 ページの「署名済みサーバ証明書のインポート」を参照してください。

署名済みサーバ証明書のインポート

FortiGate ユニットにインストールする署名済みサーバ証明書は、CA から提供されます。CA から署名済みサーバ証明書を受け取ったら、その証明書を、FortiGate ユニットへの管理アクセスが可能なコンピュータに保存します。この証明書ファイルは、PEM または DER のどちらの形式でもかまいません。

署名済みサーバ証明書をインポートするには、*[System]*、*[Certificates]*、*[Local Certificates]* の順に選択します。*[Import]* を選択し、必要な情報を入力して *[OK]* を選択します。

[Import Certificate] ページ

特定の署名済み証明書をインポートするための設定を提供します。[Type] ドロップダウン リストから [Local Certificate] を選択する場合は、次の設定を使用できます。

[Type]	[Local Certificate] を選択します。
[Certificate File]	署名済みサーバ証明書の完全なパスとファイル名を入力します。
[Browse]	あるいは、証明書が保存されている管理コンピュータ上の場所を参照し、その証明書を選択します。

エクスポートされたサーバ証明書と秘密鍵のインポート

証明書ファイルをインポートするには、そのパスワードを知っている必要があります。作業を開始する前に、このファイルのコピーを、FortiGate ユニットへの管理アクセスが可能なコンピュータに保存します。詳細については、『*FortiGate 証明書管理ユーザ ガイド*』を参照してください。

PKCS12 ファイルをインポートするには、*[System]*、*[Certificates]*、*[Local Certificates]* の順に選択します。*[Import]* を選択し、必要な情報を入力して *[OK]* を選択します。

[Import Certificate] ページ

特定の署名済み証明書をインポートするための設定を提供します。[Type] ドロップダウン リストから [PKCS12 Certificate] を選択する場合は、次の設定を使用できます。

[Type]	*[PKCS12 Certificate]* を選択します。
[Certificate with key file]	以前にエクスポートされた PKCS12 ファイルの完全なパスとファイル名を入力します。
[Browse]	あるいは、PKCS12 ファイルが保存されている管理コンピュータ上の場所を参照し、そのファイルを選択して *[OK]* を選択します。
[Password]	PKCS12 ファイルをアップロードするために必要なパスワードを入力します。

個別のサーバ証明書と秘密鍵ファイルのインポート

サーバ証明書要求と秘密鍵が FortiGate ユニットによって生成されなった場合は、それらを個別のファイルとして受け取ります。これらの 2 つのファイルを管理コンピュータにコピーします。

証明書と秘密鍵ファイルをインポートするには、*[System]*、*[Certificates]*、*[Local Certificates]* の順に選択します。*[Import]* を選択し、必要な情報を入力して *[OK]* を選択します。

[Import Certificate] ページ

CA から特定の署名済み証明書をインポートするための設定を提供します。[Type] ドロップダウン リストから [Certificate] を選択する場合は、次の設定を使用できます。

[Type]	*[Certificate]* を選択します。
[Certificate file]	以前にエクスポートされた証明書ファイルの完全なパスとファイル名を入力します。
[Browse]	あるいは、以前にエクスポートされた証明書ファイルの場所を参照し、そのファイルを選択して [OK] を選択します。
[Key file]	以前にエクスポートされた鍵ファイルの完全なパスとファイル名を入力します。
[Browse]	あるいは、以前にエクスポートされた鍵ファイルの場所を参照し、そのファイルを選択して [OK] を選択します。
[Password]	このファイルをアップロードして開くためにパスワードが必要な場合は、そのパスワードを入力します。

注記：証明書ファイルでは、40 ビットの RC2-CBC 暗号化を使用できません。

リモート証明書

動的な証明書の失効には、OCSP (Online Certificate Status Protocol) サーバを使用する必要があります。リモート証明書は、秘密鍵のない公開証明書です。OCSP サーバは、CLI でのみ設定されます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

[Remote Certificates] リストには、インストールされたリモート (OCSP サーバ) 証明書が表示されます。

インストールされたリモート (OCSP サーバ) 証明書を表示したり、リモート (OCSP サーバ) 証明書をインポートしたりするには、*[System]*、*[Certificates]*、*[Remote]* の順に選択します。証明書の詳細を表示するには、その証明書に対応する行にある *[証明書の詳細表示]* アイコンを選択します。

注記：OCSP サーバは、VDOM ごとに 1 つ存在します。

[Remote] ページ

公開証明書を表示します。このページでは、証明書をインポート、削除、および表示することができます。

[Import]	OCSP サーバの公開証明書をインポートします。196 ページの「CA 証明書のインポート」を参照してください。
[Name]	既存のリモート (OCSP サーバ) 証明書の名前。FortiGate ユニットは、リモート (OCSP サーバ) 証明書がインポートされたとき、それらの証明書に一意の名前 (REMOTE_Cert_1、REMOTE_Cert_2、REMOTE_Cert_3 など) を割り当てます。
[Subject]	リモート (OCSP サーバ) 証明書に関する情報。
[Delete]	FortiGate の設定からリモート (OCSP サーバ) 証明書を削除します。
[証明書の詳細表示]	証明書の詳細を表示します。
[Download]	リモート (OCSP サーバ) 証明書のコピーをローカル コンピュータに保存します。

リモート (OCSP サーバ) 証明書のインポート

システムは、各リモート (OCSP サーバ) 証明書に一意の名前を割り当てます。これらの名前には、連続した番号が付けられます (REMOTE_Cert_1、REMOTE_Cert_2、REMOTE_Cert_3 など)。

リモート (OCSP サーバ) 証明書をインポートするには、*[System]*、*[Certificates]*、*[Remote]* の順に選択し、*[Import]* を選択します。

[Upload Remote Certificate]
リモート証明書を FortiGate ユニットにアップロードするための設定を提供します。

[Local PC]	公開証明書をアップロードするための管理 PC 内の場所を入力します。
[Browse]	あるいは、証明書が保存されている管理コンピュータ上の場所を参照し、その証明書を選択して [OK] を選択します。

CA 証明書

リモート クライアントにインストールするための署名済みの個人証明書またはグループ証明書を申請する場合は、発行 CA から、対応するルート証明書と CRL を取得する必要があります。

証明書を受け取ったら、ブラウザのドキュメントに従って、その証明書をリモート クライアントにインストールします。発行 CA から取得した対応するルート証明書と CRL を FortiGate ユニットにインストールします。

CA 証明書は、期限が切れる前にオンラインで自動的に更新できます。これは、CLI で設定する必要があります。『*FortiGate CLI リファレンス*』にある `vpn certificate local` コマンドを参照してください。

[CA Certificates] リストには、インストールされた CA 証明書が表示されます。Fortinet_CA 証明書を削除することはできません。インストールされた CA ルート証明書を表示したり、CA ルート証明書をインポートしたりするには、*[System]*、*[Certificates]*、*[CA Certificates]* の順に選択します。証明書の詳細を表示するには、その証明書に対応する行にある *[証明書の詳細表示]* アイコンを選択します。

デジタル証明書の取得およびインストールに関する詳細と手順については、『*FortiGate 証明書管理ユーザ ガイド*』を参照してください。

[CA Certificates] ページ
デフォルトの CA 証明書だけでなく、作成した CA 証明書も表示します。また、CA 証明書をインポートすることもできます。

[Import]	CA ルート証明書をインポートします。196 ページの「CA 証明書のインポート」を参照してください。
[Name]	既存の CA ルート証明書の名前。FortiGate ユニットは、CA 証明書がインポートされたとき、それらの証明書に一意の名前 (`CA_Cert_1`、`CA_Cert_2`、`CA_Cert_3` など) を割り当てます。
[Subject]	発行 CA に関する情報。
[Delete]	FortiGate の設定から CA ルート証明書を削除します。
[証明書の詳細表示]	証明書の詳細を表示します。
[Download]	CA ルート証明書のコピーをローカル コンピュータに保存します。

CA 証明書のインポート

CA のルート証明書をダウンロードしたら、その証明書を、FortiGate ユニットへの管理アクセスが可能な PC に保存します。

[SCEP] を選択した場合は、*[OK]* を選択するとすぐに、システムによって取得プロセスが開始されます。

システムは、各 CA 証明書に一意の名前を割り当てます。これらの名前には、連続した番号が付けられます (CA_Cert_1、CA_Cert_2、CA_Cert_3 など)。

CA ルート証明書をインポートするには、*[System]*、*[Certificates]*、*[CA Certificates]* の順に選択し、*[Import]* を選択します。

[Import CA Certificate]
SCEP サーバまたはローカル PC を使用して証明書をインポートするための設定を提供します。

[SCEP]	SCEP サーバを使用して CA 証明書にアクセスし、ユーザ認証を行う場合に選択します。CA 証明書を取得するために使用する SCEP サーバの URL を入力します。必要に応じて、CA の識別情報 (ファイル名など) を入力します。[OK] を選択します。
[Local PC]	ローカル管理者の PC を使用して公開証明書をアップロードする場合に選択します。証明書が保存されている管理コンピュータ上の場所を入力するか、またはその場所を参照して証明書を選択し、[OK] を選択します。

CRL

証明書失効リスト (CRL) とは、CA が発行した証明書と、その証明書のステータスをリストにしたものです。[CRL] リストには、インストールされた CRL が表示されます。FortiGate ユニットは、CRL を使用して、CA やリモート クライアントに属する証明書が有効であることを確認します。

インストールされた CRL を表示するには、*[System]*、*[Certificates]*、*[CRL]* の順に選択します。

[CRL] ページ

個々の CRL を表示します。このページでは、CRL をインポート、表示、またはダウンロードすることができます。

[Import]	CRL をインポートします。詳細については、197 ページの「証明書失効リストのインポート」を参照してください。
[Name]	既存の証明書失効リストの名前。FortiGate ユニットは、証明書失効リストがインポートされたとき、それらのリストに一意の名前 (CRL_1、CRL_2、CRL_3 など) を割り当てます。
[Subject]	証明書失効リストに関する情報。
[Delete]	選択された CRL を FortiGate の設定から削除します。
[証明書の詳細表示]	発行者名や CRL 更新日などの CRL の詳細を表示します。
[Download]	CRL のコピーをローカル コンピュータに保存します。

証明書失効リストのインポート

証明書を取り消されたクライアントが FortiGate ユニットとの接続を確立できないようにするために、CA の Web サイトからの証明書失効リストを定期的に更新された状態に保つ必要があります。CA の Web サイトから CRL をダウンロードしたら、その CRL を、FortiGate ユニットへの管理アクセスが可能なコンピュータに保存します。

システムは、各 CRL に一意の名前を割り当てます。これらの名前には、連続した番号が付けられます (CRL_1、CRL_2、CRL_3 など)。

証明書失効リストをインポートするには、*[System]*、*[Certificates]*、*[CRL]* の順に選択し、*[Import]* を選択します。

[Import CRL] ページ

HTTP、LDAP、SCEP サーバ、またはローカル PC から CRL をインポートするための設定を提供します。

[HTTP]	HTTP サーバを使用して CRL を取得する場合に選択します。HTTP サーバの URL を入力します。
[LDAP]	LDAP サーバを使用して CRL を取得した後、リストから LDAP サーバを選択する場合に選択します。
[SCEP]	SCEP サーバを使用して CRL を取得した後、リストからローカル証明書を選択する場合に選択します。CRL を取得するために使用できる SCEP サーバの URL を入力します。
[Local PC]	ローカル管理者の PC を使用して公開証明書をアップロードする場合に選択します。証明書が保存されている管理コンピュータ上の場所を入力するか、またはその場所を参照して証明書を選択し、[OK] を選択します。

注記: CRL が LDAP、HTTP、または SCEP サーバ、あるいはそれらの組み合わせから取得するように設定されているとき、FortiGate ユニットに CRL のコピーが存在しない場合や、現在のコピーの期限が切れている場合は、最新バージョンの CRL がサーバから自動的に取得されます。

システム - メンテナンス

この項では、システム設定を保守する方法や、FDN サービスを有効にしたり、更新したりする方法について説明します。また、FortiGate ユニットに使用できる FDN サービスの種類についても説明します。

FortiGate ユニット上でバーチャル ドメイン (VDOM) を有効にした場合、システム メンテナンスは FortiGate ユニット全体に対してグローバルに設定されます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には、以下のトピックが含まれています。

メンテナンスの概要

メンテナンス メニューは、ファームウェアの保守や管理に関するヘルプ、設定リビジョン、スクリプト ファイル、および FortiGuard サブスクリプション ベースのサービスを提供します。このメニューからは、ファームウェアをアップグレードまたはダウングレードしたり、設定ファイルの履歴バックアップを表示したり、FortiGuard サービスを更新したりすることができます。

メンテナンス メニューには、次のメニューがあります。

- **[Revision Control]** – システム設定のすべてのバックアップを、バックアップされた日付と時刻とともに表示します。リビジョン制御を使用するには、事前に集中管理サーバを設定し、有効にする必要があります。
- **[Firmware]** – 現在 FortiGate ユニット上に格納されているファームウェア イメージや、現在 FortiGate ユニット上で実行されているファームウェア イメージを表示します。
- **[Advanced]** – スクリプト、USB 自動インストールのための詳細設定を表示するとともに、デバッグ ログのダウンロードを可能にします。
- **[FortiGuard]** – アンチウイルスおよび IPS 定義や FortiGuard Analysis and Management Service などの、すべての FDN サブスクリプション サービスを表示します。また、このタブでは、アンチウイルス、IPS、Web フィルタリング、およびアンチスパム サービスのための設定オプションも提供されます。
- **[License]** – VDOM の最大数を増やすことができます (一部の FortiGate モデル)。
- **[Disk]** – 複数のローカル ディスクのステータスに関する詳細情報を表示します。

システム設定をバックアップすると、Web コンテンツ ファイルと電子メール フィルタリング ファイルも含まれます。設定を管理コンピュータ、FortiGate ユニットに USB ポートが装備されている場合は USB ディスク (202 ページの「USB ディスクのフォーマット」を参照)、またはローカル ハード ディスクに保存できます。また、*[Backup & Restore]* メニューで、以前にダウンロードしたバックアップ ファイルからシステム設定を復元することもできます。

バーチャル ドメイン設定が有効になっている場合、バックアップ ファイルの内容は、そのファイルを作成した管理者アカウントによって異なります。super_admin アカウントからのシステム設定のバックアップには、グローバル設定と、各 VDOM に含まれている設定が含まれます。このファイルから設定を復元できるのは、super_admin だけです。標準管理者アカウントからシステム設定をバックアップした場合、バックアップ ファイルには、グローバル設定と、その標準管理者が属する VDOM の設定が含まれます。このファイルから設定を復元できるユーザ アカウントは、標準管理者だけです。

一部の FortiGate モデルは、ユーザがダウンロードできる FortiClient イメージを格納することによって FortiClient をサポートしています。*[Backup & Restore]* の [FortiClient] セクションは、使用している FortiGate モデルで FortiClient がサポートされている場合に使用できます。

ヒント： バックアップと復元のオプションを含むファームウェアの管理や、FortiGate ユニットのファームウェアのアップロードおよびダウンロードに関する簡素化された手順については、61 ページの「ファームウェア管理方法」を参照してください。

[Configuration Revision]

[Configuration Revisions] メニューでは、設定ファイルの複数のバージョンを管理できます。リビジョン制御には、設定された集中管理サーバ、またはローカルのハード ドライブのどちらかが必要です。集中管理サーバは、FortiManager ユニットまたは FortiGuard Analysis and Management Service のどちらにすることもできます。

FortiGate ユニット上に集中管理が設定されていない場合は、次のいずれかを実行するよう求めるメッセージが表示されます。

- 集中管理を有効にする（183 ページの「集中管理」を参照）
- 有効なライセンスを取得する

FortiGate ユニット上でリビジョン制御が有効になっており、かつ設定がバックアップされている場合は、これらのバックアップされた設定の保存済みのリビジョンのリストが表示されます。

設定リビジョンを表示するには、*[System]*、*[Maintenance]*、*[Configuration Revision]* の順に選択します。

[Configuration Revision] ページ

すべての設定リビジョンを表示します。このページでは、設定ファイルを削除、編集、またはアップロードすることができます。また、コメントを変更したり、リビジョン間の違いを表示したり、以前の設定に戻したりこともできます。

[OS Version <firmware_version_build>] (このページ上のセクションとして表示される)	このページのセクションであり、指定された FortiOS のファームウェア バージョンとビルド番号に属する設定ファイルを含みます。たとえば、4.0 MR1 (ビルド 178) に 4 つの設定リビジョンがある場合、それらのリビジョンは [Configuration Revision] ページのセクション [OS Version 4.00 build178] に表示されます。
[Revision]	設定が保存された順序を示す増分番号。設定が削除された場合は、連続した番号ではない可能性があります。 リストの先頭には、最新の、最も大きな番号が表示されます。
[Date/Time]	この設定が FortiGate ユニットに保存された日付と時刻。
[Administrator]	このリビジョンをバックアップするために使用された管理者アカウント。
[Comments]	このリビジョンが保存された理由、保存したユーザ、日付がある場合は領域を解放するために削除できる時期などの、このリビジョンに関して保存された任意の関連情報。
[Diff]	2 つのリビジョンを比較する場合に選択します。 選択されたリビジョンを表示し、次のいずれかと比較できるウィンドウが表示されます。 ・ 現在の設定 ・ リビジョン履歴とテンプレートを含む表示されたリストから選択されたリビジョン ・ 指定されたリビジョン番号
[Download]	このリビジョンをローカル PC にダウンロードします。

[Revert]	以前の選択されたリビジョンを復元します。この操作を確認するよう求められます。
[Delete]	リストから設定リビジョンを削除する場合に選択します。
[Details]	設定リビジョンの CLI 設定を表示する場合に選択します。
[Change Comments]	説明を変更する場合に選択します。
[Upload]	設定ファイルを FortiGate ユニットにアップロードする場合に選択します。その後、このファイルはリストに追加されます。

[Firmware]

[Firmware] メニューを使用すると、FortiGate ユニットにファームウェアをインストールしたり、後日インストールするためにファームウェア イメージをアップロードしたりすることができます。また、このメニューからは、現在 FortiGate ユニット上で実行されているファームウェアを表示することもできます。

ファームウェア イメージを表示したり、イメージをアップロードおよびインストールしたりするには、*[System]*、*[Maintenance]*、*[Firmware]* の順に選択します。

[Firmware] ページ

FortiGate ユニットにアップロードされたすべてのファームウェア イメージを表示します。

[Currently Running Firmware]	現在 FortiGate ユニット上で実行されているファームウェア イメージを表示します。
[Delete]	このファームウェア イメージをリストから削除する場合に選択します。
[Change Comments]	このファームウェア イメージの説明を変更する場合に選択します。
[Upgrade]	FortiGate ユニットにイメージをインストールするには、リスト内のそのファームウェア イメージを選択する必要があります。
[Upload]	[Upload] を選択すると、[Upload] ページに自動的にリダイレクトされます。このページでは、アップロードするファームウェア イメージを選択したり、[Boot New Firmware] を有効にしたり (これにより、選択されたファームウェアが FortiGate ユニットにインストールされます)、目的のファームウェアに関する任意の説明を入力したりすることができます。
[Firmware Version]	このファームウェア イメージのファームウェア バージョン番号。
[Date]	このファームウェア イメージが作成された日付。
[Create by]	このファームウェア イメージをアップロードした管理者。
[Comments]	このイメージに関する説明。

このトピックには、以下の内容が含まれています。

- 設定ファイルのバックアップと復元
- USB ディスクのフォーマット
- FortiManager のリモートでのバックアップと復元のオプション
- FortiGuard のリモートでのバックアップと復元のオプション

設定ファイルのバックアップと復元

FortiGate の設定を、管理 PC、集中管理サーバ、あるいは USB ディスクにバックアップまたは復元できます。FortiGate ユニットに USB ポートが装備されていて、その USB ポートに USB ディスクを接続している場合は、USB ディスクに設定をバックアップおよび復元できます。FortiGate ユニットは、USB キーや外付け USB ハード ディスクを含め、ほとんどの USB ディスクをサポートしています (202 ページの「USB ディスクのフォーマット」を参照)。FortiGate ユニットの接続先の任意のリモート管理サービスが集中管理サーバになります。たとえば、FortiGate-60 上の現在の設定が FortiManager ユニットにバックアップされた場合は、その FortiManager ユニットが集中管理サーバになります。

[Backup & Restore] セクションでこれらのオプションを使用できるようにするには、その前に *[System]*、*[Admin]*、*[Central Management]* の順に選択して表示される画面で集中管理を設定する必要があります。詳細については、183 ページの「集中管理」を参照してください。

バックアップと復元の設定は、CLI でのみ使用できます。`execute backup config` コマンドと `execute restore config` コマンドは、FortiGate ユニットの設定ファイルをバックアップおよび復元するために使用されます。

USB ディスクのフォーマット

注意：USB ディスクをフォーマットすると、そのディスク上のすべての情報が削除されます。ディスク上のすべての情報を確実に回復できるようにするために、フォーマットの前に USB ディスク上の情報をバックアップしてください。

USB ポートを備えた FortiGate ユニットは、USB ディスクでの設定のバックアップと復元をサポートしています。

FortiUSB と一般的な USB ディスクがサポートされますが、一般的な USB ディスクは FAT16 ディスクとしてフォーマットする必要があります。その他のパーティションの種類はサポートされていません。

USB ディスクは、CLI または Windows システムの 2 つの方法のどちらかを使用してフォーマットできます。CLI では、`exe usb-disk format` のコマンド構文を使用して USB ディスクをフォーマットできます。Windows システムを使用してディスクをフォーマットする場合は、コマンド プロンプトで "`format <drive_letter>: /FS:FAT /V:<drive_label>`" と入力します。ここで、`<drive_letter>` はフォーマットする接続済みの USB ドライブのドライブ名であり、`<drive_label>` は識別のためにその USB ドライブに付ける名前です。

FortiManager のリモートでのバックアップと復元のオプション

FortiGate ユニットは、FortiManager ユニットによってリモートで管理できます。FortiGate ユニットは、FortiGuard-FortiManager プロトコルを使用して接続します。このプロトコルは FortiGate ユニットと FortiManager ユニットの間の通信を提供し、IPv4/TCP ポート 541 を使用して SSL 経由で動作します。

FortiManager ユニットをインストールする方法の詳細な手順については、『*FortiManager インストール ガイド*』を参照してください。

FortiGate ユニットから FortiManager ユニットに正常に接続したら、FortiManager ユニットに設定をバックアップできます。また、設定を復元することもできます。

自動設定バックアップは、FortiManager ユニット上でローカル モードでのみ使用できます。

リモートの場所から設定を復元する場合は、リビジョンのリストが表示されます。このリストにより、復元する設定を選択できます。

FortiGuard のリモートでのバックアップと復元のオプション

FortiGate ユニットは、FortiGuard Analysis and Management Service に登録すると使用できる集中管理サーバによってリモートで管理できます。FortiGuard Analysis and Management Service はサブスクリプション ベースのサービスであり、サポートに問い合わせることによって購入されます。FortiGate ユニットを FortiGuard Analysis and Management Service に登録する方法を含む追加情報は、『*FortiGuard Analysis and Management Service ユーザ ガイド*』に記載されています。

登録した後、設定をバックアップまたは復元できます。FortiGuard Analysis and Management Service は、FortiManager ユニットを使用することなく複数の FortiGate ユニットを管理する場合に有効です。

FortiGuard Analysis and Management Service を使用すると、FortiGate ユニット上のファームウェアをアップグレードすることもできます。ファームウェアのアップグレードは、バックアップと復元メニューの *[Firmware Upgrade]* セクションで使用できます。バックアップと復元メニューからファームウェアをアップグレードする方法の詳細については、42 ページの「FortiGate の変更」を参照してください。

ヒント： バックアップと復元のオプションを含むファームウェアの管理や、FortiGate ユニットのファームウェアのアップロードおよびダウンロードに関する簡素化された手順については、61 ページの「ファームウェア管理方法」を参照してください。

リモートの場所から設定を復元する場合は、復元する設定ファイルを選択できるように、リビジョンのリストが表示されます。

注記： FortiGuard-FortiManager プロトコルは、FortiGuard Analysis and Management Service に接続する場合に使用されます。このプロトコルは IPv4/TCP ポート 541 を使用して SSL 経由で動作し、次の機能を含んでいます。

- FortiGate ユニットの停止または動作中のステータスの検出
- 管理サービスの停止または動作中のステータスの検出
- 設定変更、AV/IPS データベース更新、およびファイアウォール変更に関する FortiGate ユニットへの通知

[FortiGuard]

FortiGuard Distribution Network (FDN) および FortiGuard サービスを使用するように FortiGate ユニットを設定するには、*[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択します。FDN は、アンチウイルス定義、IPS 定義、およびアンチスパム ルール セットに対する更新を提供します。FortiGuard サービスには、FortiGuard Web フィルタリングおよび FortiGuard Analysis and Management Service が含まれています。

このトピックには、以下の内容が含まれています。

- FortiGuard Distribution Network
- FortiGuard サービス
- FortiGate ユニットでの FDN および FortiGuard サブスクリプション サービスの設定

FortiGuard Distribution Network

FDN は、FortiGuard Distribution Server (FDS) の世界規模のネットワークです。FDN は、アンチウイルス (グレーウェアを含む) 定義、IPS 定義、およびアンチスパム ルール セットに対する更新を提供します。FortiGate ユニットは、FDN に接続すると、現在のタイムゾーン設定に基づいて最も近い FDS に接続します。

FortiGate ユニットは、次の更新オプションをサポートしています。

- FDN からユーザが実行する更新
- 1 時間、1 日、または 1 週間ごとの、FDN からのアンチウイルス定義、IPS 定義、およびアンチスパム ルール セットの定期更新
- FDN からのプッシュ更新
- バージョン番号、終了日、および更新日時を含む更新ステータス
- NAT デバイスを介したプッシュ更新

「Fortinet Support」Web ページで FortiGate ユニットを登録すると、有効なライセンス契約と FDN への接続が提供されます。「Fortinet Support」Web ページで、「Product Registration」にアクセスしてその指示に従います。

定期更新を受信するには、FortiGate ユニットが、ポート 443 上で HTTPS を使用して FDN に接続できる必要があります。詳細については、209 ページの「定期更新を有効にするには」を参照してください。

また、プッシュ更新を受信するように FortiGate ユニットを設定することもできます。FortiGate ユニットがプッシュ更新を受信する場合は、FDN が、UDP ポート 9443 を使用して FortiGate ユニットにパケットをルーティングできる必要があります。詳細については、210 ページの「プッシュ更新の有効化」を参照してください。FortiGate ユニットが NAT デバイスの背後にある場合は、211 ページの「NAT デバイスを介したプッシュ更新の有効化」を参照してください。

FortiGuard サービス

世界を網羅する FortiGuard サービスは、FortiGuard サービス ポイントによって提供されます。FortiGate ユニットは、FDN に接続しているとき、最も近い FortiGuard サービス ポイントに接続しています。フォーティネットは、必要に応じて新しいサービス ポイントを追加します。

何らかの理由でその最も近いサービス ポイントに接続できなくなった場合、FortiGate ユニットは別のサービス ポイントに接続し、数秒以内に情報が入手可能になります。FortiGate ユニットは、デフォルトでは、ポート 53 上で UDP を介してサービス ポイントと通信します。あるいは、*[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択することによって、サービス ポイントとの通信に使用される UDP ポートをポート 8888 に切り替えることもできます。

デフォルトの FortiGuard サービス ポイントのホスト名を変更する必要がある場合は、CLI コマンド `system fortiguard` で `hostname` キーワードを使用します。Web ベース マネージャを使用して FortiGuard サービス ポイント名を変更することはできません。

FortiGuard サービスの詳細については、FortiGuard Center の Web ページを参照してください。

FortiGuard アンチスパム サービス

FortiGuardアンチスパムは、FortiGateユニットにダウンロードされるアンチスパム ルール セットに含まれている IP アドレス ブラック リスト、URL ブラック リスト、電子メール フィルタリング ツールを包含する、フォーティネットのアンチスパム システムです。IP アドレス ブラック リストには、スパムを生成する既知の電子メール サーバの IP アドレスが含まれています。URL ブラック リストには、スパム電子メールで見つかった URL が含まれています。

FortiGuard アンチスパムの処理は、フォーティネットによって完全に自動化および設定されています。常時監視と動的な更新により、FortiGuard アンチスパムは常に最新の状態に保たれています。FortiGuard アンチスパムは、[Firewall] メニューのプロテクション プロファイルで有効または無効にすることができます。

FortiGate ユニットにはすべて、30 日間無料の FortiGuard アンチスパム トライアル ライセンスが付属しています。FortiGuard アンチスパムのライセンス管理は、フォーティネット サーバによって実行されるため、ライセンス番号を入力する必要はありません。FortiGuard アンチスパムを有効にすると、FortiGate ユニットは自動的に FortiGuard アンチスパム サービス ポイントに接続します。無償トライアルの期限が切れた後に FortiGuard アンチスパム ライセンスを更新するには、フォーティネット テクニカル サポートにお問い合わせください。

[System]、*[Maintenance]*、*[FortiGuard]* の順に選択した後、*[UTM]*、*[Email Filtering]*、*[Profile]* の順に選択して表示される画面で電子メール フィルタリング オプションを設定することによって、FortiGuard アンチスパム (電子メール フィルタ) をグローバルに有効にすることができます。

FortiGuard Web フィルタリング サービス

FortiGuard Web フィルタリングは、フォーティネットが提供するマネージド Web フィルタリング ソリューションです。FortiGuard Web フィルタリングは、数億もの Web ページを、ユーザが許可、ブロック、または監視できる広範囲のカテゴリに分類します。FortiGate ユニットは、最も近い FortiGuard Web フィルタリング サービス ポイントにアクセスして、要求された Web ページのカテゴリを決定した後、そのユーザまたはインタフェースのために設定されたファイアウォール ポリシーに従います。

FortiGate ユニットにはすべて、30 日間無料の FortiGuard Web フィルタリング トライアル ライセンスが付属しています。FortiGuard のライセンス管理は、フォーティネット サーバによって実行されます。ライセンス番号を入力する必要はありません。FortiGuard カテゴリ ブロッキングを有効にすると、FortiGate ユニットは自動的に FortiGuard サービス ポイントに接続します。無償トライアルの後に FortiGuard ライセンスを更新するには、フォーティネット テクニカル サポートにお問い合わせください。

[System]、*[Maintenance]*、*[FortiGuard]* の順に選択した後、*[UTM]*、*[Web Filtering]*、*[Profile]* の順に選択して表示される画面で FortiGuard Web フィルタリング オプションを設定することによって、FortiGuard Web フィルタリングをグローバルに有効にすることができます。

FortiGuard Analysis and Management Service

FortiGuard Analysis and Management Service は、すべての FortiGate ユニットに対するロギングおよびレポート機能を含むリモート管理サービスを提供する、サブスクリプション ベースのサービスです。これらのサービスは以前、FortiAnalyzer ユニットと FortiManager ユニットでのみ使用できました。

サブスクリプション ベースのサービスは、FortiGuard Analysis and Management Service のポータル Web サイトから使用できます。この Web サイトでは、ロギングおよびレポート機能やリモート管理を設定したり、毎日のクォータやサービスの終了日などのサブスクリプション契約情報を表示したりするための中央の場所が提供されます。

FortiGate ユニットでの FDN および FortiGuard サブスクリプション サービスの設定

FDN 更新および FortiGuard サービスは、*[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択して表示される画面で設定されます。FDN のページには、FortiGuard サービスの次の 4 つのセクションが含まれています。

- サポート契約および FortiGuard サブスクリプション サービス
- アンチウイルスおよび IPS 更新のダウンロード
- Web フィルタリングおよび電子メール フィルタリング オプションの設定
- FortiGuard Analysis and Management Service オプションの設定

サポート契約および FortiGuard サブスクリプション サービス

サポート契約および FortiGuard サブスクリプション サービスのセクションは、[Status] ページに省略された形式で表示されます。38 ページの「ダッシュボードの概要」を参照してください。

FortiGuardオプションを表示するには、*[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択します。

[FortiGuard Distribution Network] ページ

FortiGate ユニットのサポート契約および FortiGuard サブスクリプション サービスに関する詳細情報を表示します。このページではまた、Analysis and Management Service の連絡先アカウント ID のほか、アンチウイルスおよび IPS オプション、Web フィルタリングや電子メール フィルタリングのオプションも入力できます。

[Support Contract]
FortiGate ユニットのサポート契約の有効性またはステータス。表示されるステータスは、*[Unreachable]*、*[Not Registered]*、*[Valid Contract]* のいずれかです。
[Valid Contract] が表示されている場合は、FortiOS のファームウェア バージョンと契約の終了日が表示されます。また、緑色のチェックマークも表示されます。

[Register]
FortiGate ユニットのサポート契約を登録する場合に選択します。
このオプションは、サポート契約が登録されていない場合にのみ使用できます。

[FortiGuard Subscription Services]
次のような、各 FortiGuard サブスクリプション サービスの有効性とステータスの情報。
- [AntiVirus]
- [Intrusion Protection]
- [Vulnerability Compliance and Management]
- [Web Filtering]
- [AntiSpam]
- [Analysis & Management Service]

[Availability]
この FortiGate ユニット上のこのサービスの有効性。サービスのサブスクリプションによって異なります。このステータスは、*[Unreachable]*、*[Not Registered]*、*[Valid License]*、*[Valid Contract]* のいずれかです。
[Availability] が *[Not Registered]* の場合は、*[Subscribe]* オプションが表示されます。
[Availability] の期限が切れている場合は、*[Renew]* オプションが表示されます。

[Update]
FortiGate ユニット上のこのサービスを手動で更新する場合に選択します。これにより、ローカル コンピュータから更新ファイルをダウンロードするよう求められます。直接 FDN から最新の更新を直ちにダウンロードするには、*[Update Now]* を選択します。

[Register]	このサービスを登録する場合に選択します。これは、Analysis and Management Service で表示されます。
ステータス アイコン	サブスクリプション サービスのステータスを示します。このアイコンは、有効性の説明に対応しています。 灰色 (**[Unreachable]**) — FortiGate ユニットはサービスに接続できません。 オレンジ色 (**[Not Registered]**) — FortiGate ユニットは接続できますが、このサービスに登録されていません。 黄色 (**[Expired]**) — FortiGate ユニットのライセンスは有効でしたが、期限が切れています。 緑色 (**[Valid License]**) — FortiGate ユニットは FDN に接続でき、サポート契約にも登録されています。 ステータス アイコンが緑色の場合は、終了日が表示されます。
[Version]	このサービスのための、FortiGate ユニットに現在インストールされている定義ファイルのバージョン番号。
[Last update date and method]	最後の更新の日付と、このサービスのための定義の更新をダウンロードする最後の試行に使用された方法。
[Date]	FortiGate ユニットがこのサービスのための更新を最後にチェックしたローカル システムの日付。

アンチウイルスおよび IPS 更新のダウンロード

[Antivirus and IPS Options] セクションでは、アンチウイルスおよび IPS 更新をスケジュールしたり、オーバーライド サーバを設定したり、プッシュ更新を許可したりすることができます。これらのオプションには、展開の矢印を選択することによってアクセスできます。

プッシュ更新を有効にしたときに FortiGate ユニットによって送信される SETUP メッセージには、FDN の接続先の FortiGate インタフェースの IP アドレスが含まれています。FortiGate ユニットが NAT デバイスの背後にある場合は、*[Use override push IP]* オプションを使用します。FortiGate ユニットは、FDS に NAT デバイスの IP アドレスとポート番号を送信します。また、NAT デバイスも、FDS トラフィックをポート 9443 上で FortiGate ユニットに転送するように設定されている必要があります。

詳細については、211 ページの「NAT デバイスを介したプッシュ更新の有効化」を参照してください。

[FortiGuard Distribution Network] ページの [Antivirus and IPS Options] セクション

更新をスケジュールしたり、オーバーライド サーバを設定したり、プッシュ更新を許可したりするための設定を提供します。

[Use override server address]	FDN に接続できない場合、または組織が独自の FortiGuard サーバを使用して更新を提供している場合に、オーバーライド サーバを設定するために選択します。 選択する場合は、FortiGuard サーバの IP アドレスまたはドメイン名を入力し、*[Apply]* を選択します。FDN ステータスが、依然として FDN に接続されていないことを示している場合は、208 ページの「FDN 接続性のトラブルシューティング」を参照してください。
[Allow Push Update]	プッシュ更新を許可する場合に選択します。これにより、使用可能になった更新が自動的に FortiGate ユニットに送信されるため、更新が使用可能かどうかをチェックする必要がなくなります。
[Allow Push Update] ステータス アイコン	プッシュ更新を受信するための FortiGate ユニットのステータス。 灰色 (**[Unreachable]**) - FortiGate ユニットはプッシュ更新サービスに接続できません。 黄色 (**[Not Available]**) - 現在のサポート ライセンスでは、プッシュ更新サービスは使用できません。 緑色 (**[Available]**) - プッシュ更新サービスが許可されています。210 ページの「プッシュ更新の有効化」を参照してください。 このアイコンが灰色または黄色の場合は、208 ページの「FDN 接続性のトラブルシューティング」を参照してください。

[Use override push IP]	*[Use override server address]* と *[Allow Push Update]* の両方が有効になっている場合にのみ使用できます。 受信した FDS プッシュ更新を FortiGate ユニットにリダイレクトするフォワーディング ポリシーを作成できるようにする場合に選択します。 FortiGate ユニットの前にある NAT デバイスの IP アドレスを入力します。FDS は、FortiGate ユニットに到達しようとするときにこのデバイスに接続します。 NAT デバイスは、FDS トラフィックを UDP ポート 9443 上で FortiGate ユニットに転送するように設定されている必要があります。211 ページの「NAT デバイスを介したプッシュ更新の有効化」を参照してください。
[Port]	FDS プッシュ更新を受信する NAT デバイス上のポートを選択します。このポートは、FortiGate ユニット上の UDP ポート 9443 に転送される必要があります。 *[Use override push IP]* が有効になってている場合にのみ使用できます。
[Schedule Updates]	定期更新を有効にするには、このチェック ボックスをオンにします。
[Every]	1 ～ 23 時間ごとに 1 回更新を試みます。各更新要求の間の時間数を選択します。
[Daily]	1 日に 1 回更新を試みます。更新をチェックする時間を指定できます。更新の試行が、選択された時間内のランダムに決定された時間に実行されます。
[Weekly]	1 週間に 1 回更新を試みます。更新をチェックする曜日と時間を指定できます。更新の試行が、選択された時間内のランダムに決定された時間に実行されます。
[Update Now]	FDN 更新を手動で開始する場合に選択します。
[Submit attack characteristics...] (推奨)	このチェック ボックスをオンにすることをお勧めします。IPS シグネチャの品質向上に役立ちます。

Web フィルタリングおよび電子メール フィルタリング オプションの設定

この項には、展開の矢印を選択して *[Web Filtering]* および *[Email Filtering]* オプションを表示することによってアクセスできます。

[FortiGuard Distribution Network] ページの [Web Filtering and Email Filtering Options] セクション

FortiGuard Web フィルタ サービス、キャッシュ、および電子メール フィルタ サービスを有効にするための設定を提供します。

[Enable Web Filter]	FortiGuard Web フィルタ サービスを有効にする場合に選択します。
[Enable Cache]	Web フィルタ クエリのキャッシュを有効にする場合に選択します。 これにより、FortiGuard サーバへの FortiGate ユニットの要求が減るため、パフォーマンスが向上します。このキャッシュでは、FortiGate のメモリの 6% が使用されます。キャッシュがいっぱいになると、最も以前に使用された IP アドレスまたは URL が削除されます。 *[Enable Web Filter]* が選択されている場合に使用できます。
[TTL]	TTL (Time to Live)。再びサーバに接続するまでに、ブロックされた IP アドレスや URL をキャッシュ内に格納する秒数。TTL は、300 ～ 86400 秒の範囲にある必要があります。 *[Enable Web Filter]* と *[Enable Cache]* の両方が選択されている場合にのみ使用できます。
[Enable Email Filter]	FortiGuard アンチスパム サービスを有効にする場合に選択します。
[Enable Cache]	アンチスパム クエリのキャッシュを有効にする場合に選択します。 これにより、FortiGuard サーバへの FortiGate ユニットの要求が減るため、パフォーマンスが向上します。このキャッシュでは、FortiGate のメモリの 6% が使用されます。キャッシュがいっぱいになると、最も以前に使用された IP アドレスまたは URL が削除されます。 *[Enable Email Filter]* が選択されている場合にのみ使用できます。
[TTL]	TTL (Time to Live)。再びサーバに接続するまでに、ブロックされた IP アドレスや URL をキャッシュ内に格納する秒数。TTL は、300 ～ 86400 秒の範囲にある必要があります。
[Port Section]	Web フィルタリングとアンチスパムの要件を満たす次のいずれかのポートを選択します。
[Use Default Port (53)]	FortiGuard アンチスパム サーバへの送信にポート 53 を使用する場合に選択します。

[Use Alternate Port (8888)]	FortiGuard アンチスパム サーバへの送信にポート 8888 を使用する場合に選択します。
[Test Availability]	サーバへの接続をテストする場合に選択します。結果は、ボタンの下とステータス インジケータに表示されます。
[To have a URL's category rating re-evaluated, please click here.]	FortiGuard Web フィルタ サービスでの URL のカテゴリ評価を再評価する場合に選択します。

FortiGuard Analysis and Management Service オプションの設定

[Analysis and Management Service Options] セクションには、アカウント ID や、FortiGuard Analysis and Management Service に関連したその他のオプションが含まれています。

この項には、展開の矢印を選択することによってアクセスできます。

***[FortiGuard Distribution Network]* ページの *[Analysis and Management Service Options]* セクション**

FortiGuard Analysis and Management Service サブスクリプション サービスの追加の設定のための各設定を提供します。

[Account ID]	このアカウントを識別する Analysis and Management Service の名前を入力します。 登録時に [Account ID] フィールドに入力したアカウント ID がこのフィールドで使用されます。
[To launch the service portal, please click here]	FortiGuard Analysis and Management Service のポータル Web サイトに直接移動してログまたは設定を表示する場合に選択します。また、ここを選択して、FortiGate ユニットを FortiGuard Analysis and Management Service に登録することもできます。
[To configure FortiGuard Analysis Service options, please click here]	*[please click here]* リンクを選択して、FortiGuard Analysis and Management サーバへのロギングを設定したり、有効にしたりします。このリンクにより、*[Log&Report]*、*[Log Config]*、*[Log Setting]* の順に選択して表示される画面にリダイレクトされます。 このサービスに登録した後でのみ表示されます。
[To purge logs older than *n* months, please click here]	これらのログを FortiGuard Analysis and Management サーバから削除する月数をリストから選択し、*[please click here]* リンクを選択します。たとえば、2 か月を選択すると、過去 2 か月からのログがサーバから削除されます。 また、このオプションを使用して、現在のレポートに表示される可能性のあるログを削除することもできます。 ロギングが有効になり、ログ メッセージが FortiGuard Analysis サーバに送信された後でのみ表示されます。

- 集中管理

FDN 接続性のトラブルシューティング

FortiGate ユニットが FDN に接続できない場合、設定を確認します。たとえば、FortiGate ルーティング テーブルにルートを追加したり、FortiGate ユニットがポート 443 上で HTTPS を使用してインターネットに接続できるようにネットワークを設定したりすることが必要になる場合があります。

更新を受信するために、FortiGuard オーバーライド サーバに接続しなければならない場合があります。詳細については、210 ページの「オーバーライド サーバを追加するには」を参照してください。これが成功しない場合は、設定をチェックして、FortiGate ユニットから FortiGuard オーバーライド サーバに接続できることを確認します。

次のような場合、プッシュ更新が使用できないことがあります。

- FortiGate ユニットを登録していない場合 (FortiGate ユニットをまだ登録していない場合は、「Product Registration」にアクセスして Web サイトの指示に従います)。
- FortiGate ユニットと FDN の間に NAT デバイスが設置されている場合 (211 ページの「NAT デバイスを介したプッシュ更新の有効化」を参照)。
- FortiGate ユニットがプロキシ サーバを使用してインターネットに接続している場合 (210 ページの「プロキシ サーバを介した定期更新を有効にするには」を参照)。

アンチウイルスおよび攻撃定義の更新

FDN に接続してアンチウイルス (グレーウェアを含む) 定義と IPS 攻撃定義を更新するように FortiGate ユニットを設定するには、次の手順を使用します。

注記: アンチウイルスおよび IPS 攻撃定義を更新すると、FortiGate ユニットが新しいシグネチャ定義を適用している間、トラフィック スキャンにごく短時間の中断が発生することがあります。中断を最小限に抑えるために、トラフィックが少ない時間帯に更新をスケジュールすることをお勧めします。

FortiGate ユニットが FDN に接続できることを確認するには

1 *[System]*、*[Dashboard]*、*[Status]* の順に選択し、*[System Information]* セクションの *[System Time]* 行にある *[Change]* を選択します。

タイム ゾーンが、FortiGate ユニットが設置されている地域に対応して正しく設定されていることを確認します。

2 *[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択します。

3 使用可能なオプションを表示するには、*[Web Filtering and Email Filtering Options]* の横にある展開の矢印を選択します。

4 *[Test Availability]* を選択します。

FortiGate ユニットによって、FDN への接続がテストされます。このテスト結果は、[FortiGuard] ページの一番上に表示されます。

アンチウイルスおよび攻撃定義を更新するには

1 *[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択します。

2 使用可能なオプションを表示するには、*[Antivirus and IPS Options]* の横にある展開の矢印を選択します。

3 *[Update Now]* を選択して、アンチウイルスおよび攻撃定義を更新します。

FDN またはオーバーライド サーバへの接続に成功すると、Web ベース マネージャに次のようなメッセージが表示されます。

```
Your update request has been sent.Your database will be updated in a few minutes.Please check your update page for the status of the update.
```

数分後、更新が使用可能になると、[FortiGuard] ページに、アンチウイルス定義と IPS 攻撃定義の新しいバージョン情報のリストが表示されます。このページにはまた、更新された定義およびエンジンの新しい日付とバージョン番号も表示されます。更新が成功したかどうかを示すメッセージがイベント ログに記録されます。

定期更新を有効にするには

1 *[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択します。

2 使用可能なオプションを表示するには、*[Antivirus and IPS Options]* の横にある展開の矢印を選択します。

3 *[Scheduled Update]* チェック ボックスをオンにします。

4 次のいずれかを選択します。

[Every]	1 ～ 23 時間ごとに 1 回。各更新要求間の時間数と分数を選択します。
[Daily]	1 日に 1 回。更新をチェックする時間を指定できます。
[Weekly]	1 週間に 1 回。更新をチェックする曜日と時間を指定できます。

5 *[Apply]* を選択します。

FortiGate ユニットは、新しい更新スケジュールに従って次の定期更新を開始します。

FortiGate ユニットが定期更新を実行する場合は常に、各イベントが FortiGate のイベント ログに記録されます。

FDN に接続できない場合、または組織が独自の FortiGuard サーバを使用してアンチウイルスおよび IPS 攻撃の更新を提供している場合は、次の手順を使用して FortiGuard オーバーライド サーバの IP アドレスを追加できます。

オーバーライド サーバを追加するには

1 *[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択します。
2 使用可能なオプションを表示するには、*[Antivirus and IPS Options]* の横にある展開の矢印を選択します。
3 *[Use override server address]* チェック ボックスをオンにします。
4 FortiGuard サーバの完全修飾ドメイン名または IP アドレスを入力します。
5 *[Apply]* を選択します。

FortiGate ユニットは、オーバーライド サーバへの接続をテストします。

FortiGuard Distribution Network の有効性アイコンが灰色から緑色に変化した場合は、FortiGate ユニットがオーバーライド サーバに正常に接続しています。

FortiGuard Distribution Network の有効性アイコンが灰色のままの場合は、FortiGate ユニットがオーバーライド サーバに接続できません。FortiGate の設定やネットワーク設定をチェックして、FortiGate ユニットが FortiGuard オーバーライド サーバに接続できない設定になっていないどうかを確認してください。

プロキシ サーバを介した定期更新を有効にするには

FortiGate ユニットがプロキシ サーバを介してインターネットに接続する必要がある場合は、`config system autoupdate tunneling` のコマンド構文を使用して、FortiGate ユニットのプロキシ サーバを使用した FDN への接続（またはトンネリング）を許可することができます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

プッシュ更新の有効化

重大な状況にできるだけすばやく対応できるようにするために、FDN は FortiGate ユニットに更新をプッシュできます。FortiGate ユニットでプッシュ更新を受信できるようにするには、事前にユニットを登録する必要があります。FortiGate ユニットを登録するには、Fortinet のサポート Web サイトの「Product Registration」に移動し、指示に従います。

プッシュ更新を許可するように FortiGate ユニットを設定すると、その FortiGate ユニットから FDN に SETUP メッセージが送信されます。次回新しいアンチウイルスまたは IPS 攻撃定義がリリースされたとき、FDN では、プッシュ更新が設定されたすべての FortiGate ユニットに新しい更新が入手できることを通知します。プッシュ通知を受信してから 60 秒以内に、FortiGate ユニットは FDN に更新を要求します。

ネットワーク設定によって許可されている場合は、定期更新に加えて、プッシュ更新を設定することをお勧めします。定期更新によって FortiGate ユニットが最新の更新を受信することが保証されますが、プッシュ更新も設定した場合は通常、FortiGate ユニットは新しい更新をより迅速に受信できます。

更新を取得するための唯一の方法としてプッシュ更新を有効にすることはお勧めできません。FortiGate ユニットでプッシュ通知が受信されない可能性があります。FortiGate ユニットは、プッシュ通知を受信する場合、FDN に接続して更新をダウンロードする試みを 1 回しか行いません。

FortiGate ユニットの IP アドレスが変更される場合のプッシュ更新の有効化

プッシュ更新を有効にしたときに FortiGate ユニットによって送信される SETUP メッセージには、FDN の接続先の FortiGate インタフェースの IP アドレスが含まれています。プッシュ更新に使用されるインタフェースは、スタティック ルーティング テーブルのデフォルト ルートで設定されたインタフェースです。

次の場合は、FortiGate ユニットによって SETUP メッセージが送信されます。

- このインタフェースの IP アドレスを手動で変更した場合
- インタフェースのアドレッシング モードが DHCP または PPPoE に設定されているときに、DHCP または PPPoE サーバによって IP アドレスが変更された場合

FortiGate ユニットがプッシュ更新メッセージを受信できるように、FDN はこの IP アドレスに接続できる必要があります。FortiGate ユニットが NAT デバイスの背後にある場合は、211 ページの「NAT デバイスを介したプッシュ更新の有効化」を参照してください。

インターネットへの冗長接続が設定されている場合は、1 つのインターネット接続がダウンし、FortiGate ユニットが別のインターネット接続にフェールオーバーしたときも、FortiGate ユニットによって SETUP メッセージが送信されます。

トランスペアレント モードでは、管理 IP アドレスを変更した場合も、そのアドレスの変更を FDN に通知するために FortiGate ユニットによって SETUP メッセージが送信されます。

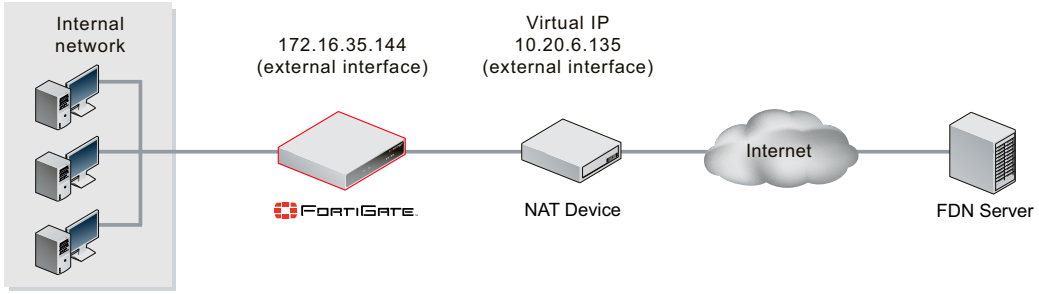
NAT デバイスを介したプッシュ更新の有効化

FDN が NAT デバイスを介してのみ FortiGate ユニットに接続する場合は、その NAT デバイス上でポート フォワーディングを設定し、そのポート フォワーディング情報をプッシュ更新の設定に追加する必要があります。ポート フォワーディングを使用すると、FDN は、ポート 9443 またはユーザが指定したオーバーライド プッシュ ポート上で UDP を使用して FortiGate ユニットに接続できます。

NAT デバイスの外部 IP アドレスが動的 (PPPoE または DHCP) である場合、FortiGate ユニットは、NAT デバイスを介してプッシュ更新を受信できません。

次の手順では、NAT デバイスを介して更新をプッシュするように FortiGate ユニットを設定します。また、この手順には、NAT デバイスへのポート フォワーディング仮想 IP とファイアウォール ポリシーの追加も含まれています。

図 4: ネットワークの例 : NAT デバイスを介したプッシュ更新



全体的なプロセスは次のとおりです。

1 内部ネットワーク上の FortiGate ユニットを、最新のサポート ライセンスを備え、プッシュ更新を受信できるように登録します。

2 内部ネットワーク上の FortiGate ユニットで、次の FortiGuard オプションを設定します。
   - *[Allow push updates]* を有効にします。
   - *[Use override push IP]* を有効にして、IP アドレスを入力します。通常、これは NAT デバイスの外部インタフェースの IP アドレスです。
   - 必要に応じて、オーバーライド プッシュ更新のポートを変更します。

3 NAT デバイスにポート フォワーディング仮想 IP を追加します。
- 仮想 IP の外部 IP アドレスを、オーバーライド プッシュ更新の IP と一致するように設定します。通常、これは NAT デバイスの外部インタフェースの IP アドレスです。

ポート フォワーディング仮想 IP を含む FortiGate の NAT デバイスにファイアウォール ポリシーを追加します。

注記： FortiGate ユニットがプロキシ サーバを使用して FDN に接続する必要がある場合、プッシュ更新はサポートされません。詳細については、210 ページの「プロキシ サーバを介した定期更新を有効にするには」を参照してください。

内部ネットワーク上の FortiGate ユニットで FortiGuard オプションを設定するには

1 *[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択します。
2 使用可能なオプションを表示するには、*[Antivirus and IPS Options]* の横にある展開の矢印を選択します。
3 *[Allow Push Update]* チェック ボックスをオンにします。
4 *[Use override push IP]* チェック ボックスをオンにします。
5 NAT デバイスの外部インタフェースの IP アドレスを入力します。
UDPポート9943は、ブロックされているか、または使用されている場合にのみ変更されます。
6 *[Apply]* を選択します。

外部サービス ポートの外部 IP アドレスが変更された場合は、プッシュ オーバーライド設定に変更できます。更新されたプッシュ情報が FortiGate ユニットから FDN に送信されるようにするには、*[Apply]* を選択します。

FortiGate ユニットがオーバーライド プッシュの IP アドレスとポートを FDN に送信すると、FDN は、FortiGate ユニットへのプッシュ更新にこの IP アドレスとポートを使用します。ただし、NAT デバイスがプッシュ更新パケットを受け付けて内部ネットワーク上の FortiGate ユニットに転送できるようにその NAT デバイスに仮想 IP が追加されるまで、実際にはプッシュ更新は動作しません。

その NAT デバイスも FortiGate ユニットである場合は、FortiGate の NAT デバイスにポート フォワーディング仮想 IP を追加するにはの手順によって、ポート フォワーディングを使用して、FDN から内部ネットワーク上の FortiGate ユニットに更新接続をプッシュするように NAT デバイスを設定できます。

FortiGate の NAT デバイスにポート フォワーディング仮想 IP を追加するには

1 *[Firewall]*、*[Virtual IP]*、*[Virtual IP]* の順に選択します。
2 *[Create New]* を選択します。
3 次の該当する情報を入力します。

[Name]	この仮想 IP の名前を入力します。
[External Interface]	リストから外部インタフェースを選択します。これは、インターネットに接続するインタフェースです。
[External IP Address/Range]	IP アドレスまたは範囲、あるいはその両方を入力します。これは、FDN がプッシュ更新を送信する先の IP アドレスです。これは通常、NAT デバイスの外部インタフェースの IP アドレスです。この IP アドレスは、内部ネットワーク上の FortiGate ユニットの *[User override push update]* にある IP アドレスと同じである必要があります。
[Mapped IP Address/Range]	内部ネットワーク上の FortiGate ユニットの IP アドレスまたは範囲、あるいはその両方を入力します。
[Port Forwarding]	*[Port Forwarding]* を選択します。*[Port Forwarding]* を選択すると、*[Protocol]*、*[External Services Port]*、および *[Map to Port]* のオプションが表示されます。
[Protocol]	*[UDP]* を選択します。

[External Service Port]	外部サービス ポートを入力します。外部サービス ポートは、FDN の接続先のポートです。プッシュ更新の外部サービス ポートは通常、9443 です。内部ネットワーク上の FortiGate ユニットの FortiGuard 設定でプッシュ更新のポートを変更した場合は、外部サービス ポートをその変更したプッシュ更新のポートに設定する必要があります。
[Map to Port]	9443 を入力します。これは、NAT の FortiGate ユニットが、仮想 IP を介して受信したプッシュ更新を送信する先のポート番号です。FortiGate ユニットは、ポート 9443 上でプッシュ更新通知を予測します。

4 *[OK]* を選択します

FortiGate の NAT デバイスにファイアウォール ポリシーを追加するには

1 *[Firewall]*、*[Policy]*、*[Policy]* の順に選択します。

2 *[Create New]* を選択します。

3 外部から内部へのファイアウォール ポリシーを設定します。

[Source Interface/Zone]	インターネットに接続するインタフェースの名前を選択します。
[Source Address]	*[All]* を選択します。
[Destination Interface/Zone]	内部ネットワークに接続する NAT デバイスのインタフェースの名前を選択します。
[Source Address]	NAT デバイスに追加された仮想 IP を選択します。
[Schedule]	*[Always]* を選択します。
[Service]	*[ANY]* を選択します。
[Action]	*[Accept]* を選択します。
[NAT]	*[NAT]* を選択します。

4 *[OK]* を選択します

[System]、*[Maintenance]*、*[FortiGuard]* の順に選択し、*[Web Filtering and AntiSpam Options]* で *[Test Availability]* を選択することによって、内部ネットワーク上の FortiGate ユニットへのプッシュ更新が動作していることを確認します。*[Push Update]* のインジケータが緑色に変化します。

[Advanced]

[Advanced] メニューを使用すると、スクリプト ファイルを設定してアップロードしたり、USB 自動インストールの機能を設定したり、デバッグ ログをダウンロードしたりすることができます。

スクリプトは、CLI コマンド シーケンスを含むテキスト ファイルです。複雑なコマンド シーケンスを容易に実行するために、これらのファイルをアップロードして実行できます。スクリプトを使用すると、多数のデバイスに同一の設定を展開できます。たとえば、すべてのデバイスで同一の管理者プロファイルを使用する場合は、その管理者プロファイルを作成するために必要なコマンドをスクリプト内に入力した後、そのスクリプトを、それらの同じ設定を使用するすべてのデバイスに展開することができます。

FortiManager ユニットまたは FortiGuard Analysis and Management Service なしで FortiGate ユニットを使用している場合、アップロードしたスクリプトは実行された後、破棄されます。スクリプトを複数回実行する場合は、管理 PC 上にコピーを保持する必要があります。

FortiGate ユニットが FortiManager ユニットを使用するように設定されている場合は、スクリプトを FortiManager ユニットにアップロードした後、FortiManager ユニットを使用するように設定されている任意の FortiGate ユニットからそれらのスクリプトを実行できます。スクリプトを FortiGate ユニットに直接アップロードした場合、そのスクリプトは実行された後、破棄されます。

FortiGate ユニットが FortiGuard Analysis and Management Service を使用するように設定されている場合、アップロードしたスクリプトは実行された後、格納されます。アップロードされたスクリプトは、FortiGuard Analysis and Management Service アカウントを使用して設定されている任意の FortiGate ユニットから実行できます。アップロードされたスクリプト ファイルは、FortiGuard Analysis and Management Service のポータル Web サイトに表示されます。

スクリプトを実行した後、スクリプト ページでスクリプト実行履歴を表示できます。このリストには、最後に実行された 10 個のスクリプトが表示されます。

スクリプトや USB 自動インストールを設定したり、デバッグ ログをダウンロードしたりするには、*[System]*、*[Maintenance]*、*[Advanced]* の順に選択します。

[Advanced] ページ

スクリプトや USB 自動インストールを設定したり、デバッグ ログをダウンロードしたりするためのすべての設定を表示します。

[Scripts] セクション

スクリプト ファイルをアップロードするための設定を提供します。また、このセクションからスクリプト実行履歴を表示することもできます。

[Execute Script from] スクリプトは、管理 PC から FortiGate ユニットに直接アップロードできます。FortiManager ユニットまたは FortiGuard Analysis and Management Service のどちらかを設定している場合は、リモートで格納されたスクリプトをその FortiGate ユニット上で実行することもできます。

[Upload Bulk CLI Command File] *[Browse]* を選択してスクリプト ファイルを見つけた後、*[Apply]* を選択してそのファイルをアップロードおよび実行します。
FortiGate ユニットが FortiGuard Analysis and Management Service を使用するように設定されている場合、スクリプトは、後で使用するためにサーバ上に保存されます。

[Select From remote management station] FortiManager ユニットまたは FortiGuard Analysis and Management Service からスクリプトを実行する場合に選択します。リモートで格納されたすべてのスクリプトのリストから、実行するスクリプトを選択します。

[Script Execution History (past 10 scripts)] 最近実行された 10 個のスクリプトのリスト。

[Name] このスクリプト ファイルの名前。

[Type] このスクリプト ファイルの発信元。ローカル ファイルは、管理 PC から FortiGate ユニットに直接アップロードされ、実行されます。リモート ファイルは、FortiManager ユニットまたは FortiGuard Analysis and Management Service から送信された後、FortiGate ユニット上で実行されます。

[Time] このスクリプト ファイルが実行された日付と時刻。

[Status] 実行が成功したか失敗したかを示す、このスクリプト ファイルのステータス。

[Delete] このスクリプト エントリをリストから削除します。

[USB Auto-Install section]

システムの再起動時に常に、特定のファームウェア イメージおよび設定ファイルをアップロードするための設定を提供します。この機能が動作するには、FortiGate ユニット上の USB ポートに USB キーが挿入されている必要があります。

[On system restart ...] システムの再起動時に特定のファームウェア イメージをアップロードする場合に選択します。フィールドにファームウェア イメージの名前を入力します。
システムが再起動すると、FortiGate ユニットは、USB キー上でそのファームウェア イメージ名を探します。

[On system restart ...] システムの再起動時に特定の設定ファイルをアップロードする場合に選択します。フィールドに設定ファイルの名前を入力します。
システムが再起動すると、FortiGate ユニットは、USB キー上でその設定ファイル名を探します。

[Download Debug Log] セクション

診断のためのデバッグ ログのルールを提供します。このデバッグ ログをフォーティネット テクニカル サポートに送信して、FortiGate ユニットに関する問題の診断に役立てることができます。

[Download Debug Log] 暗号化されたデバッグ ログ ファイルをローカル PC にダウンロードする場合に選択します。

スクリプト ファイルの作成

スクリプト ファイルは、CLI コマンド シーケンスを含むテキスト ファイルです。スクリプト ファイルが FortiGate ユニットにアップロードされると、これらのコマンドは順番に実行されます。

スクリプト ファイルを作成するには

1 テキスト エディタ アプリケーションを開きますスクリプト ファイルは、Windows 上のメモ帳、Linux 上の GEdit、Mac 上の Textedit、またはプレーンテキストを保存する任意のエディタで作成できます。

2 実行する CLI コマンドを入力します。

これらのコマンドは、1 行に 1 コマンドずつ、順番に入力する必要があります。

3 このファイルをメンテナンス PC に保存します。

ヒント : 暗号化されていない設定ファイルでは、スクリプト ファイルと同じ構造および構文が使用されています。設定ファイルを保存し、必要な部分を新しいファイルにコピーして、必要な任意の編集を行うことができます。この方法により、スクリプト ファイルをよりすばやく生成できます。

スクリプト ファイルのアップロード

注意 : コマンド ラインに入力したときに FortiGate ユニットの再起動が必要なコマンドは、スクリプトに含めた場合にも再起動を強制します。

スクリプト ファイルを作成した後、*[System]*、*[Maintenance]*、*[Advanced]* の順に選択して表示される画面でそのファイルをアップロードできます。アップロードされたそのスクリプトは、自動的に実行されます。

スクリプトを実行するには

1 *[System]*、*[Maintenance]*、*[Advanced]* の順に選択します。

2 *[Upload Bulk CLI Command File]* が選択されていることを確認します。

3 *[Browse]* を選択してスクリプト ファイルを見つけます。

4 *[Apply]* を選択します。

FortiGate ユニットがリモート管理用に設定されていない場合、または FortiManager ユニットを使用するように設定されている場合、アップロードされたスクリプトは実行後に破棄されます。これらのスクリプト ファイルを後で再び実行する場合は、管理 PC に保存します。

FortiGate ユニットが FortiGuard Analysis and Management Service を使用するように設定されている場合、スクリプト ファイルは、後で再利用するためにリモート サーバに保存されます。このスクリプトは、FortiGuard Analysis and Management Service のポータル Web サイトから表示したり、実行したりできます。アップロードされたスクリプトのポータル Web サイトでの表示または実行の詳細については、『*FortiGuard Analysis and Management Service ユーザ ガイド*』を参照してください。

VDOM ライセンスの追加

ハイエンドの FortiGate ユニットの場合は、フォーティネットからライセンス キーを購入して、VDOM の最大数を 25、50、100、または 250 に増やすことができます。FortiGate ユニットでは、デフォルトで最大 10 個の VDOM がサポートされています。

ライセンス キーとは、フォーティネットが提供する 32 文字の文字列です。フォーティネットは、ライセンス キーを生成するために FortiGate ユニットのシリアル番号が必要になります。

このライセンス キーは、*[System]*、*[Maintenance]*、*[License]* の順に選択して表示される画面の *[Input License Key]* フィールドで入力されます。このフィールドは、ハイエンドの FortiGate モデルでのみ表示されます。

[License] ページ

FortiGate ユニット上で許可されているバーチャル ドメインの現在の最大数や、バーチャル ドメインを増やすためにライセンス キーを入力するフィールドを表示します。

[Current License]	バーチャル ドメインの現在の最大数。
[Input License Key]	フォーティネットが提供するライセンス キーを入力し、*[Apply]* を選択します。

注記： 登録された FortiGate ユニット上で作成された VDOM は、接続されているすべての FortiAnalyzer ユニットによって実際のデバイスとして認識されます。FortiAnalyzer ユニットには、登録済みデバイスの総数の VDOM が含まれています。たとえば、3 つの FortiGate ユニットが FortiAnalyzer ユニットに登録され、合計で 4 つの VDOM を含んでいる場合、FortiAnalyzer ユニット上に登録されている FortiGate ユニットの総数は 7 です。詳細については、『*FortiAnalyzer 管理ガイド*』を参照してください。

[Disk]

[System]、*[Maintenance]*、*[Disk]* の順に選択して表示される画面から、FortiGate ユニット上の使用可能な各ローカル ディスクのステータスを表示できます。[Disk] メニューを使用すると、現在残されているストレージ領域の容量のほか、格納されているデータの内容や、そのデータが占有しているストレージ領域の容量などを表示できます。このメニューでは、次の機能ごとのストレージ領域に関する詳細情報が提供されます。

- ディスク ロギング
- SQL データベース
- 履歴レポート
- IPS パケットのアーカイブ
- 隔離
- WAN 最適化および Web キャッシュ

[Disk] メニューではまた、上の機能ごとのクォータ使用率に関する情報も提供されます。[Disk] メニューは、複数のディスクを備えた FortiGate モデルでのみ表示されます。

[Disk] ページ

各ディスクのステータスに関する詳細情報と、各ディスクがディスクへの情報の格納をどのように管理しているかを表示します。このページの [Disk Management] セクションでは、機能ごとの情報の格納を表示できます。

[Disk Status] セクション

このディスク上のストレージ領域を説明している円グラフを表示します。その FortiGate ユニットに現在搭載されているディスクごとに円グラフがあります。

#	リスト内のこのディスクの順序。
[Name]	このディスクの名前 (internal など)。
[Total]	このディスク上の使用可能なディスク領域の合計容量。
[Used]	このディスク上ですでに使用されている領域の合計容量。
[Free]	格納するために使用できる領域の合計容量。このディスクをフォーマットするには、[Format] を選択できます。ただし、ディスクをフォーマットすると、このディスクのすべてのデータが削除されます。

[Disk Management] セクション

使用されているディスク領域の容量、使用可能な空き領域、およびクォータ使用率に関する詳細情報を提供します。

[Feature]	このディスク上に情報を格納する機能。使用可能な機能を次に示します。 · ディスク ロギング · DLP アーカイブ · 履歴レポート · IPS パケットのアーカイブ · 隔離 · SQL データベース · WAN 最適化および Web キャッシュ
[Storage Size]	このディスク上のストレージ領域のサイズ。
[Allocated]	機能を格納するために許可されている領域の容量。
[Used]	機能の情報を格納するために使用されている領域の現在の容量。
[Quota Usage]	現在使用されているクォータの容量。この数値はパーセンテージで表されます。クォータがまったく使用されていない場合、この数値は 100% です。
[Edit]	使用されている領域の現在の容量を変更する場合に選択します。

AMC モジュールの設定

この項では、FortiGate ユニット上で AMC モジュールを設定する方法について説明します。これには、AMC ブリッジ モジュールの自動バイパスと回復が含まれます。

この項には、以下のトピックが含まれています。

注記： AMC スロットを備えたほとんどの FortiGate モデルには、シングル幅またはデュアル幅の AMC スロットが 1 つあります。FortiGate-3810A には、シングル幅の AMC スロットが 2 つ、デュアル幅の AMC スロットが 2 つあります。

AMC モジュールの設定

デフォルトでは、FortiGate ユニットは AMC スロットに装着されている AMC モジュールを自動的に認識するか、または AMC スロットが空であることを自動的に認識します。そのモジュールにインタフェースがある場合は、FortiOS によって、それらのインタフェースが FortiGate の設定に自動的に追加されます。そのモジュールにハード ディスクが含まれている場合は、そのハード ディスクが設定に自動的に追加されます。ただし、FortiGate ユニットの電源が切断された後にスロットからモジュールが取り外された場合、FortiGate ユニットは再起動時にそのスロットが空であることを自動的に認識するため、失われたモジュールの設定は保持されません。

このデフォルトの動作は、ほとんどの場合は許容可能です。ただし、スロット内にモジュールが存在するときに、そのモジュールの名前を FortiGate の設定に追加すると有効な場合があります。それにより、そのモジュールに障害が発生した場合や、スロットから一時的に取り外された場合でも、FortiGate ユニットにモジュールの設定が保持されるため、そのモジュールを交換したときに再設定は必要なくなります。

スロットにモジュールの名前をすでに追加しているときに、そのモジュールを取り外して別の種類のモジュールに交換する（たとえば、FortiGate-ASM-S08 を取り外し、それを FortiGate-ASM-FX2 に交換する）ことを計画または実行している場合は、モジュールを取り外す前にスロットをデフォルト設定にリセットする必要があります。次に、新しいモジュールを追加した後、その名前をスロットに追加する必要があります。

AMC スロットの設定は、FortiGate の CLI から `config system amc` コマンドを使用して設定します。このコマンドについては、『*FortiGate CLI リファレンス*』を参照してください。

次の手順は、FortiGate-ADM-FB8 を最初のダブル幅の AMC スロット（dw1）に追加する方法、およびモジュールの名前をスロットの設定に追加する方法を示しています。

AMC スロットのデフォルト設定を変更するには

1 FortiGate-ADM-FB8 モジュールを挿入するスロットがデフォルト設定に設定されていることを確認するには、次の CLI コマンドを入力します。

このコマンドは、AMC スロットと、各 AMC スロットの設定の一覧を表示します。ダブル幅の AMC スロットが空である FortiGate-5001A に対するコマンド出力の例を次に示します。

```
get system amc
dw1       : auto
```

2 FortiGate ユニットの電源を切ります。

3 FortiGate-ADM-FB8 モジュールをダブル幅の AMC スロットに挿入します。

4 FortiGate ユニットの電源を入れます。

FortiGate-ADM-FB8 モジュールを挿入したスロットが auto に設定されている限り、FortiGate ユニットは、電源投入時にそのモジュールを自動的に検出します。

5 FortiGate-ADM-FB8 モジュールの名前を FortiGate の設定に追加します。

```
config system amc
  set dw1 adm-fb8
end
```

AMC ブリッジ モジュールの自動バイパスと回復

FortiGate-ASM-CX4 および FortiGate-ASM-FX2 モジュールは、トランスペアレント モードで動作している、シングル幅の AMC スロットを備えた FortiGate ユニットのインタフェース ペアに対するフェールオープン保護を提供します。FortiGate-ASM-CX4 または FortiGate-ASM-FX2 モジュールは、FortiGate インタフェースをブリッジし、インタフェースにトラフィック障害がないかどうかを監視します。さらに、インタフェースまたは FortiGate ユニット全体に障害が発生するか、または何らかの理由でインタフェース間でトラフィックを転送できない場合はパススルー デバイスとして動作します。障害が発生した場合は、トラフィックが FortiGate ユニットをバイパスして FortiGate-ASM-CX4 または FortiGate-ASM-FX2 モジュールを通過することで、FortiGate の障害の後もネットワークが引き続きトラフィックを処理できるようになります。

この項では、FortiGate-ASM-CX4 または FortiGate-ASM-FX2 モジュールを使用して FortiGate インタフェースをブリッジするように FortiGate ユニットを設定する方法について説明します。FortiGate ユニットは、トランスペアレント モードで動作する必要があります。また、FortiGate-ASM-CX4 および FortiGate-ASM-FX2 モジュールは FortiGate HA と互換性がありません。

FortiGate-ASM-CX4 および FortiGate-ASM-FX2 モジュールには、ブリッジされた FortiGate インタフェースを通してトラフィックが流れていることを継続的に確認するバイパス ウォッチドッグが含まれています。トラフィックの流れが停止した場合（たとえば、FortiGate ユニットに障害が発生した場合）や、バイパス ウォッチドッグによってこの状態が検出された場合は、ネットワーク上のトラフィック フローを保証するためにブリッジ モジュールはバイパス モードに切り替えます。

バイパス モードでは、すべてのトラフィックが FortiGate-ASM-CX4 および FortiGate-ASM-FX2 モジュール上のインタフェース間を流れ、FortiGate ユニットを通過しません。ブリッジされた FortiGate インタフェースがトラフィックを処理できないことを確認するように回復ウォッチドッグを設定できます。問題を修正するか、または問題が自然に修正された場合は、回復ウォッチドッグがトラフィックの再開が可能なことを自動的に検出し、バイパス モードを無効にすることによってモジュールを元の通常の動作に戻します。

FortiGate ユニットを FortiGate-ASM-CX4 または FortiGate-ASM-FX2 モジュールとともに動作するように設定するには

1 FortiGate ユニットをトランスペアレント モードで動作するように切り替えます。

```
config system settings
  set opmode transparent
  set manageip <management_IPv4> <netmask_ipv4>
  set gateway <gateway_ipv4>
end
```

短時間の一時停止の後、FortiGate ユニットはトランスペアレント モードで動作します。

2 FortiGate-ASM-CX4 または FortiGate-ASM-FX2 モジュールを挿入するスロットが auto に設定されていることを確認するには、次のコマンドを入力します。

このコマンドは、AMC スロットと、各 AMC スロットの設定の一覧を表示します。AMC スロットが空である FortiGate-620B に対するコマンド出力の例を次に示します。

```
get system amc
sw1      : auto
```

3 FortiGate ユニットの電源を切ります。

4 FortiGate-ASM-CX4 または FortiGate-ASM-FX2 モジュールをシングル幅の AMC スロットに挿入します。

5 FortiGate ユニットの電源を入れます。

モジュールを挿入したスロットが auto に設定されている限り、FortiGate ユニットは、電源投入時にそのモジュールを自動的に検出します。

6 そのモジュールの名前を FortiGate の設定に追加し、バイパスと回復の設定を設定します。

次のコマンドでは、FortiGate-ASM-CX4のシングル幅のAMCスロット1（sw1）を設定します。

このコマンドではまた、バイパス ウォッチドッグを有効にし、バイパス タイムアウトをデフォルト値の 10 秒から 60 秒に増やします。つまり、障害が発生した場合、ブリッジ モジュールは、バイパス ウォッチドッグが障害を検出してから 60 秒後にバイパス モードに変更します。

このコマンドではまた、ウォッチドッグ回復を有効にし、ウォッチドッグ回復の期間を 30 秒に設定します。つまり、障害が発生した場合、FortiGate-ASM-CX4 モジュールによって接続が AMC にブリッジされている間、バイパス ウォッチドッグは FortiGate プロセスを監視し、FortiGate ユニットが障害から回復した場合は通常の動作モードに戻します（つまり、FortiGate-ASM-CX4 モジュールによるインタフェースのブリッジを無効にします）。

```
config system amc
  set sw1 asm-cx4
  set bypass-watchdog enable
  set bypass-timeout 60
  set watchdog-recovery enable
  set watchdog-recovery-period 30
end
```

AMC ブリッジ モジュールのバイパス モードの有効化または無効化

FortiGate ユニット内のシングル幅の AMC スロットに装着されている FortiGate-ASM-CX4 または FortiGate-ASM-FX2 モジュールの通常モードとバイパス モードとを切り替えるには、execute amc bypass コマンドを使用します。通常、FortiGate-ASM-CX4 および FortiGate-ASM-FX2 モジュールはバイパス モードが無効な状態で動作し、トラフィックは FortiGate-ASM-CX4 または FortiGate-ASM-FX2 モジュールによってブリッジされた FortiGate インタフェースを通過します。このコマンドを手動で使用すると、バイパス モードを有効にし、強制的にトラフィックに FortiGate インタフェースをバイパスして FortiGate-ASM-CX4 または FortiGate-ASM-FX2 モジュールを通過させるようにすることができます。

また、バイパス モードが（このコマンドを使用して、または障害のために）有効になっている場合は、このコマンドを使用して手動でバイパス モードを無効にし、通常の動作を再開することもできます。この操作は、障害の原因になった問題が修正され、通常の動作を再開できるようになった場合に有効です。

バイパス モードを手動で有効にするには

1 バイパス モードを手動で有効にするには、次のコマンドを使用します。

```
execute amc bypass enable
```

2 FortiGate ユニットに装着されている AMC モジュールのステータス（バイパス モードで動作しているかどうかを含む）を表示するには、次の診断コマンドを使用します。

たとえば、FortiGate-ASM-CX4 モジュールを FortiGate-3810A の AMC スロット 2 に装着していて、バイパス モードが有効になっている場合は、次のコマンドを入力します。

```
diagnose sys amc bypass status
ASM-CX4 in slot 2:
        amc-sw2/1 <--> amc-sw2/2: mode=bypass (admin action)
        amc-sw2/3 <--> amc-sw2/4: mode=bypass (admin action)
```

```
Daemon heartbeat status: normal
Last heartbeat received: 0 second(s) ago
```

3 Web ベース マネージャにログインして、*[System]*、*[Dashboard]*、*[Status]* の順に選択し、*[Unit Operation]* ウィジェットを表示して AMC ブリッジ モジュールのステータスを表示します。

バイパス モードを手動で無効にするには

1 バイパス モードを手動で無効にするには、次のコマンドを使用します。

```
execute amc bypass disable
```

2 FortiGate ユニットに装着されている AMC モジュールのステータス（バイパス モードで動作しているかどうかを含む）を表示するには、次の診断コマンドを使用します。

たとえば、FortiGate-ASM-CX4 モジュールを FortiGate-3810A の AMC スロット 2 に装着していて、バイパス モードが無効になっている場合は、次のコマンドを入力します。

```
diagnose sys amc bypass status
ASM-CX4 in slot 2:
        amc-sw2/1 <--> amc-sw2/2: mode=normal
        amc-sw2/3 <--> amc-sw2/4: mode=normal

Daemon heartbeat status: normal
Last heartbeat received: 1 second(s) ago
```

3 Web ベース マネージャにログインして、*[System]*、*[Dashboard]*、*[Status]* の順に選択し、*[Unit Operation]* ウィジェットを表示して AMC ブリッジ モジュールのステータスを表示します。

RAID の設定

この項では、複数のディスクがサポートされている FortiGate ユニット上で RAID を設定する方法について説明します。RAID アレイは、選択されている RAID レベルに応じて、より高速なディスク アクセス、または部分的な障害が発生した場合の冗長性、あるいはその両方を提供できます。

この項には、以下のトピックが含まれています。

RAID アレイの設定

注意 : RAID アレイの同期中にディスクを取り外さないでください。格納されている情報が失われる可能性があります。また、これによってアレイのデグレードも発生し、再構築が必要になります。
デグレードした状態にある RAID アレイでは、冗長性が提供されません。RAID がデグレードした状態にある間に何らかのディスク障害が発生すると、データが消失します。

一部の FortiGate モデルでは、ログ メッセージを FortiGate ユニット上にローカルに格納するために、RAID アレイ内に 2 台以上のディスク ドライブが設定されます。RAID アレイは、選択されている RAID レベルに応じて、より高速なディスク アクセス、または部分的な障害が発生した場合の冗長性、あるいはその両方を提供できます。

RAID レベルの切り替え中に、"RAID status is OK and RAID is doing background synchronization"（RAID ステータスは正常であり、RAID はバックグラウンド同期を実行しています）というメッセージが表示されることがあります。アレイ内のディスクの同期には、かなりの時間がかかります。アレイの規模が大きいほど、またディスクのストレージ容量が大きいほど長い時間がかかります。

RAID ディスクの設定

RAID アレイを設定するには、*[System]*、*[Dashboard]*、*[Status]* の順に選択し、[RAID Monitor] ウィジェットで *[Configure]* を選択します。

[RAID level]	RAID のレベルを選択します。オプションには次のものがあります。 **[RAID-0]** —（ストライピング）より高いパフォーマンス、冗長性はなし **[RAID-1]** —（ミラーリング）ストレージ容量は半分になるが、完全な冗長性 **[RAID-5]** — パリティ チェック付きストライピング、および冗長性 使用可能な RAID レベル オプションは、使用可能なハード ディスクの数によって異なります。RAID 0 または RAID 1 には、2 台以上のディスクが必要です。 RAID レベルの変更は、[Apply] が選択されたときに有効になります。 RAID レベルを変更すると、アレイに格納されているログ情報がすべて消去され、FortiGate ユニットが再起動されます。ユニットは、RAID アレイを再設定している間オフラインのままになります。再起動された後、完全な動作状態にするには、アレイを同期する必要があります。 RAID レベルの詳細については、224 ページの「RAID レベル」を参照してください。

[Status]	RAID アレイのステータスまたは稼働状態。このステータスは、次のいずれかになります。 **[OK]** — 標準のステータスであり、すべてが正常です。 **[OK (Background-Synchronizing) (%)]** — RAID レベルを変更した後、ディスクを同期しています。同期の進行状況バーに進行状況が表示されます。 **[Degraded]** — アレイ内の 1 台以上のディスクが故障しているか、削除されたか、または正常に機能していません。この状態では冗長性がないことについての警告が表示されます。また、デグレードしたアレイは正常なアレイより低速でもあります。アレイを修正するには、*[Rebuild RAID]* を選択します。 **[Degraded (Background-Rebuilding) (%)]** — [Degraded] と同じですが、RAID アレイがバックグラウンドで再構築されています。再構築が完了するまで、アレイは引き続き脆弱な状態にあります。
[Size]	ギガバイト (GB) 単位の RAID アレイのサイズ。アレイのサイズは、選択された RAID レベルと、アレイ内のディスクの数によって異なります。
[Rebuild RAID]	アレイに新しいディスクが追加された後、または故障したディスクが交換された後にアレイを再構築する場合に選択します。 ディスクが少なすぎる状態で RAID アレイを再構築しようとすると、再構築エラーが表示されます。機能しているディスクを挿入した後、再構築が開始されます。 このボタンは、RAID アレイがデグレードした状態にあり、かつ再構築するための十分なディスクが存在する場合にのみ使用できます。 再構築がすでに進行中のときに、再構築を再起動することはできません。 **注記 :** ディスクが故障すると、機能しているディスクの数が、RAID レベルの動作にとって十分でなくなる可能性があります。この場合は、RAID アレイを再構築するために、故障したディスクを機能しているディスクに交換してください。
[Disk#]	このディスクのアレイ内の位置。これは、そのディスクの物理スロットに対応します。 ディスクが FortiGate ユニットから取り外された場合、そのドライブ ベイに新しいディスクが挿入されるまで、そのディスクはアレイのメンバではないとしてマークされますが、その位置は保持されます。
[Status]	このディスクのステータス。オプションには、[OK] と [unavailable] があります。 ディスクは、削除されるか、または故障すると [unavailable] になります。
[Member]	選択されたディスクが RAID アレイに含まれているかどうかを表示します。 チェックマークの付いた緑色のアイコンは、このディスクがアレイに含まれていることを示します。 ラ印の付いた灰色のアイコンは、このディスクが RAID アレイに含まれていないことを示します。 ディスクは、RAID アレイ内のメンバでない場合でも、ダッシュボードの表示には正常として表示される可能性があります。 ディスクは、使用可能であっても、RAID アレイで使用されていない可能性があります。たとえば、RAID 1 アレイ内に 3 台のディスクが存在する場合は、2 台のみが使用されます。
[Capacity]	このドライブが RAID アレイに提供しているストレージ容量。 このディスクの完全なストレージ容量が、自動的に RAID アレイに使用されます。 RAID アレイの合計ストレージ容量は、ディスクの容量と数、およびアレイの RAID レベルによって異なります。

RAID レベル

RAID レベルを変更する場合、使用可能なレベルは、そのユニット内に実際に存在する、機能しているディスクの数によって異なります。たとえば、ディスクが 3 台未満のユニット上では RAID 5 は使用できません。ディスクが故障するか、破損するか、または取り外された場合は、RAID アレイを再構築する必要があります。詳細については、225 ページの「RAID アレイの再構築」を参照してください。

FortiGate ユニットに 1 台のディスクしか搭載されていない場合、1 台のディスクだけでは RAID アレイを設定できないため、[RAID Monitor] ウィジェットは表示されません。

使用可能な RAID レベルには次のものがあります。

- RAID 0
- RAID 1
- RAID 5

RAID 0

RAID 0 アレイは、ストライピングとも呼ばれます。FortiGate ユニットは、すべてのハード ディスクにわたって均等に情報を書き込みます。使用可能な合計の領域は、RAID アレイ内のすべてのディスクの領域です。冗長性は使用できません。いずれか 1 台のドライブに障害が発生した場合、そのドライブ上のデータは回復できません。この RAID レベルでは、FortiGate ユニットがディスク書き込みを複数のディスクに分散できるので、処理速度が向上するメリットがあります。

たとえば、FortiGate ユニットにそれぞれが 1 TB の容量を持つ 3 台のディスクが搭載されている場合、RAID 0 アレイの容量は 3 TB になります。

RAID 1

RAID 1 アレイは、ミラーリングとも呼ばれます。FortiGate ユニットは、1 台のハードディスクに情報を書き込み、その全情報のコピー (ミラー イメージ) を他のすべてのハードディスクに書き込みます。使用可能な合計のディスク領域は 1 台のハードディスクの領域だけであり、その他のハードディスクはミラーリングにのみ使用されます。これにより、単一障害点のない、冗長なデータ ストレージが提供されます。いずれかのハード ディスクに障害が発生した場合は、使用可能なバックアップ ハード ディスクが複数存在します。たとえば、1 台のディスクに障害が発生しても、ユニットは引き続き他の 3 台のハード ディスクにアクセスし、機能し続けることができます。

RAID 1 アレイでは、容量が 1 TB のディスクが 4 台搭載されている場合、アレイの容量は 2 TB になります。RAID 1 ではミラーリングのためにディスクをペアにするため、ディスクの数が奇数の場合、1 台のディスクは使用されません。3 台のディスクがある場合、RAID 1 アレイでは 2 台のみが使用されます。

RAID 5

RAID 5 アレイでは、ストライピングをパリティ チェックとともに使用します。RAID 0 と同様に、FortiGate ユニットはすべてのドライブにわたって均等に情報を書き込みますが、同じストライプ上に追加のパリティ ブロックが書き込まれます。このパリティ ブロックは、各ストライプで互い違いになります。合計のディスク領域は、アレイ内のディスクの総数から、パリティ ストレージのための 1 台のディスクを引いた分になります。たとえば、ハード ディスクが 4 台の場合、使用可能な総容量は、実際には 3 台のハード ディスクの合計になります。RAID 5 のパフォーマンスは一般に、書き込みに比べて読み取りの方が優れています。ただし、1 台のディスクが故障するか、または欠けているとパフォーマンスが低下します。RAID 5 では、1 台のディスクが故障してもデータは失われません。1 台のドライブが故障しても交換が可能なため、FortiGate ユニットは、パリティ ボリュームからの参照情報を使用して新しいディスク上にデータを復元します。

RAID アレイの再構築

RAID アレイには複数のディスクが搭載され、それらのディスクへの書き込みが分散されているため、アレイ内の 1 台のディスクに障害が発生しても、アレイは引き続き、格納されているすべての情報を提供できます。RAID では、一部の形式を除いて冗長性が提供されます。

ディスクに障害が発生するか、または RAID アレイがデグレードした状態になった場合

[System]、*[Dashboard]*、*[Status]* の順に選択して表示される画面にある [Alert Message Console] ウィジェットには、故障したハード ディスクなど緊急の注意が必要なイベントまたはアクティビティに関するすべてのメッセージが表示されます。このウィジェットは、イベントまたはアクティビティの日付と時刻や、発生した状態に関する説明を含む詳細なメッセージを提供します。

この項には、以下のトピックが含まれています。

- RAID アレイを再構築する理由
- RAID アレイを再構築する方法

RAID アレイを再構築する理由

RAID アレイに冗長性があり、アレイ内の 1 台のディスクが故障するか、破損するか、または取り外された場合、そのアレイはデグレードした状態になります。デグレードした状態でも、アレイは引き続き機能できますが、変わる点がいくつかあります。2 つの主な変化として、冗長性がなくなることと、アレイへのアクセスに以前に比べて長い時間がかかる点があります。

冗長性がなくなるのは、アレイから 1 台のディスクを取り外した場合、そのディスク上に格納されていた情報はアレイ内のその他のディスクを使用して取得できるためです。ただし、アレイから別のディスクを取り外すと、バックアップやパリティ データがない情報は削除されます。この 2 番目のディスクの取り外しはデータ消失につながり、アレイは障害の状態になります。この RAID アレイの注意を要する状態は、ステータスが警告の形式でデグレードしたときに、[RAID Monitor] ダッシュボード上に警告メッセージで表示されます。

アレイのデータ アクセスに以前より長い時間がかかるのは、予測された形式と順序でデータが取得されるのではなく、アレイがデータをあちこちから見つけたり、場合によっては失われたデータをパリティ情報から再作成したりする必要があるためです。これらの処理のすべてに、通常の単純な読み取り操作だけの場合より長い時間がかかり、RAID アレイが再構築されるまでこの状態が続行されます。

RAID アレイを再構築する理由には次のものがあります。

- ディスクが故障した
- アレイが破損した
- ディスクが取り外された
- RAID アレイの再構築
- RAID アレイを再構築する方法

RAID アレイを再構築する方法

RAID アレイが通常の正常な状態にある場合は、その必要性がないため、アレイを再構築するオプションは存在しません。アレイを再構築する必要があるのは、アレイがデグレードした状態にあり、データが失われる恐れがある場合のみです。

ディスクの故障がデグレードしたアレイの原因である場合は、RAID アレイを再構築する前に、その故障したディスクの交換用ディスクを用意する必要があります。ディスクが欠けているアレイを再構築することはできません。交換用ディスクは、交換対象のディスクと同じストレージ容量である必要があります。

また、可能であれば、アレイを再構築する前にデータをバックアップすることも必要です。可能な場合は、RAID アレイがデグレードした状態になったらすぐにそのアレイをバックアップして、データ消失を防止する必要があります。

RAID アレイを再構築するには

1 *[System]*、*[Dashboard]*、*[Status]* の順に選択し、[RAID Monitor] ウィジェットで *[Configure]* を選択します。

2 RAID アレイのステータスが [Degraded] であり、[Rebuild] ボタンが灰色で表示されていないことを確認します。

3 FortiGate ユニットから故障したディスクを取り外します。
   - 正常なディスクが用意されていることを確認します。
   - 緑色のボタンを押して、ディスクのロックを解除します。
   - レバーを静かに左の端まで押して、ディスクを切り離します。
   - レバーを引いて、FortiGate ユニットからディスクを取り外します。

4 新しいディスクを、故障したディスクを交換している FortiGate ユニットに挿入します。
   - ディスクを慎重に FortiGate ユニットに挿入します。
   - ディスクのフロント　パネルを押して接続を行います。レバーが右に移動し始めます。ディスクの両端が他のディスクと揃っていることを確認してください。
   - 所定の位置にある場合は、緑色のボタンがカチッと音がするまで、バーを完全に右に押します。
5 表示を更新して、新しいディスクが正しく搭載されたことを確認します。ディスクが認識されない場合は、新しいディスクで手順 3 と 4 を繰り返して、正しく搭載されたことを確認します。
6 設定画面で、*[Rebuild RAID]* を選択します。

   RAID アレイの再構築には通常、数時間かかります。ダッシュボード上の [RAID Monitor] の表示で進行状況を確認できます。
7 再構築が完了したら、RAID アレイのステータスが [OK] に変化します。

ルータ - スタティック

この項では、いくつかの一般的なルーティングの概念、およびスタティック ルートとルート ポリシーを定義する方法について説明します。

ルートは、ネットワーク上の特定の宛先にパケットを転送するのに必要な情報を FortiGate ユニットに提供します。パケットは、スタティック ルートによって、工場出荷時に設定されているデフォルト ゲートウェイ以外の宛先へと転送されます。

工場出荷時に設定済みのスタティック デフォルト ルートは、デフォルト ゲートウェイを設定するための出発点となります。工場出荷時に設定済みのスタティック デフォルト ルートを変更して異なるデフォルト ゲートウェイを FortiGate ユニットに設定するか、または工場出荷時に設定済みのルートを削除して、デフォルト ゲートウェイを示すスタティック デフォルト ルートを FortiGate ユニットに設定する必要があります。詳細については、233 ページの「デフォルト ルートおよびデフォルト ゲートウェイ」を参照してください。

スタティック ルートは手動で定義します。FortiGate ユニットから送出されるトラフィックはスタティック ルートが制御しますが、パケットを送出するインタフェースとパケットの転送先のデバイスはユーザが指定できます。

オプションでルート ポリシーを定義することができます。ルート ポリシーは、着信パケットのプロパティを分析するための基準を追加指定するものです。ルート ポリシーを使用すると、パケット ヘッダ内の IP 発信元および宛先アドレスや、パケットが受信されたインタフェース、パケットを送信するために使用されるプロトコル（サービス）とポートなどのその他の条件に基づいてパケットをルーティングするように FortiGate ユニットを設定できます。

FortiGate ユニット上でバーチャル ドメイン（VDOM）を有効にした場合、スタティック ルーティングはバーチャル ドメインごとに別々に設定されます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には、以下のトピックが含まれています。

ルーティングの概念

FortiGate ユニットはネットワーク上のセキュリティ デバイスとして機能し、パケットはこのユニットを通過する必要があります。FortiGate ユニットを適切に設定するには、いくつかの基本的なルーティングの概念を理解する必要があります。

管理するネットワークの規模の大小を問わず、この項は FortiGate ユニットがどのようにルーティング機能を実行するのかを理解するのに役立ちます。

このトピックには、以下の内容が含まれています。

ルーティング テーブルの成立ち

FortiGate ユニットが各種のアドレスを接続するたびにそのルートを検出しなくても済むように、ルーティング テーブルには、それらのアドレスへのルートが格納されます。工場出荷のデフォルト設定では、FortiGate ルーティング テーブルにはスタティック ルート、つまりデフォルト ルートが 1 つ設定されています。別のスタティック ルートを定義することにより、ルーティング テーブルにルーティング情報を追加できます。このテーブルには、同じ宛先への異なるルートをいくつか含めることができます。これらのルート、またはこれらのルートに関連付けられている FortiGate インタフェースで指定されているネクストホップ ルータの IP アドレスは、それぞれ異なることがあります。

FortiGate ユニットは、ルーティング テーブルの情報を評価することで、パケットに「最良」のルートを選択します。宛先への最良のルートは通常、FortiGate ユニットとそれに最も近いネクストホップ ルータの間の最短のディスタンスに関連しています。最良のルートが使用できない場合は、その次に最良のルートが選択されることがあります。FortiGate ユニットは、使用可能な最良のルートを、そのユニットのルーティング テーブルのサブセットであるユニットのフォワーディング テーブル内に設定します。パケットは、フォワーディング テーブルの情報に基づいて転送されます。

ルーティングの決定方法

パケットが FortiGate ユニットのいずれかのインタフェースに到着すると常に、そのユニットは、パケット ヘッダ内の発信元 IP アドレスを使用して逆引きを行うことにより、そのパケットが正当なインタフェース上で受信されたかどうかを判断します。FortiGate ユニットが、そのパケットが受信されたインタフェースを介して発信元 IP アドレスにあるコンピュータと通信できない場合、ハッキングの試みである可能性があるため、FortiGate ユニットはそのパケットを破棄します。

宛先アドレスがローカル アドレスと一致した場合 (かつ、ローカル設定で配信が許可されている場合)、FortiGate ユニットはそのパケットをローカル ネットワークに配信します。そのパケットが別のネットワークに宛てられている場合、FortiGate ユニットは、ポリシー ルートおよび FortiGate フォワーディング テーブルに格納されている情報に従って、そのパケットをネクストホップ ルータに転送します。詳細については、243 ページの「ポリシー ルート」を参照してください。

マルチパス ルーティングと最良のルートの決定

マルチパス ルーティングは、同じ宛先へのエントリがルーティング テーブルに複数存在する場合に発生します。マルチパス ルーティングが発生すると、FortiGate ユニットは着信パケットに複数の宛先を使用できることになり、どのネクストホップが最良か判断を迫られます。

同じ宛先への複数のルートという問題を手動で解決するには、一方のルートのディスタンスを小さくするか、または両方のルートにプライオリティを設定するという 2 つの方法があります。FortiGate ユニットがプライマリ (優先) ルートを選択するようにするには、優先ルートに関連付けられたディスタンスを手動で小さくします。

ディスタンス

ディスタンスは、特定のルートの予測される信頼性に基づいています。このディスタンスは、発信元からのホップの数と、使用されているルーティング プロトコルの組み合わせによって決定されます。発信元からのホップの数が多いことは、障害ポイントが生まれる可能性が高いことを示します。ディスタンスは 1 ～ 255 の範囲の値であり、数値が小さいほど優先されます。255 のディスタンスは無制限と見なされ、ルーティング テーブルには設定されません。

ここで、ディスタンスのしくみを説明するための例を示します。トラフィックが 2 つの宛先の中から選択できる、ディスタンスがそれぞれ 5 (常時使用可能) と 31 (使用できない場合がある) の 2 つの可能性のあるルートがある場合、トラフィックは、可能であれば常にディスタンスが 5 のルートを使用します。デフォルトのディスタンスは、ルーティング プロトコルごとに異なります。これらのどのルーティング プロトコルもデフォルトのディスタンスを設定できます。ルーティング プロトコルに関連付けられたディスタンスの変更の詳細については、『*FortiGate CLI リファレンス*』にある config routing を参照してください。

表 47: ルーティング プロトコルのデフォルトのディスタンス

ルーティング プロトコル	デフォルトのディスタンス
直接の物理的な接続	1
スタティック	10
EBGP	20
OSPF	110
RIP	120
IBGP	200

同じ宛先への複数のルートを手動で解決するための別の方法として、両方のルートのプライオリティを手動で変更する方法があります。FortiGate ユニット上の 2 つのルートのネクストホップ ディスタンスが等しい場合は、パケットがどのルートを選択するかが明確でないことがあります。これらの各ルートのプライオリティを設定すると、ディスタンスが等しい場合にどのネクストホップが使用されるかが明確になります。ルートのプライオリティは、CLI からのみ設定できます。プライオリティの値が小さい方が優先されます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

ルーティング テーブル内のエントリはすべて、ディスタンスに関連付けられています。ルーティング テーブルに、同じ宛先を指す複数のエントリが含まれている場合（各エントリのゲートウェイまたはインタフェースの関連付けは異なることがあります）、FortiGate ユニットはこれらのエントリのディスタンスを比較し、ディスタンスの最も小さいエントリを選択して、それらのエントリを FortiGate フォワーディング テーブル内にルートとして設定します。その結果、FortiGate フォワーディング テーブルには、各宛先への、ディスタンスの最も小さいルートのみが含まれます。スタティック ルートに関連付けられたディスタンスを変更する方法については、236 ページの「ルーティング テーブルへのスタティック ルートの追加」を参照してください。

ルート プライオリティ

FortiGate ユニットが、各ディスタンスに基づいてフォワーディング テーブルのスタティック ルートを選択した後、これらのルートのプライオリティ フィールドによってルーティングの優先順位が決定されます。

このプライオリティ フィールドは、CLI を使用して設定します。プライオリティ フィールド内の値が最も小さいルートが、最良のルートおよびプライマリ ルートと見なされます。プライオリティ フィールドを設定するコマンドは、`config router static` コマンドの下にある `set priority <integer>` です。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

まとめると、CLI を使用して、スタティック ルートを定義するときに使用するプライオリティ フィールドの設定を指定できるため、そのプライオリティ フィールドの設定に従って同じ宛先へのルートに優先順位を付けることができます。スタティック ルートを優先ルートにするには、`config router static` CLI コマンドを使用してルートを作成し、そのルートに低いプライオリティを指定する必要があります。2 つのルートのディスタンスとプライオリティの両方が同じ場合、これらのルートは等価コスト マルチパス (ECMP) ルートです。同じ宛先への複数のルートが存在することになるため、どのルートを設定したり、使用したりするかが紛らわしくなる場合があります。ただし、ECMP ルート間でセッションを負荷分散する方法を制御するために、ECMP ルートのフェールオーバーと負荷分散を設定できます。237 ページの「ECMP ルートのフェールオーバーと負荷分散」を参照してください。

ブラックホール ルート

ブラックホール ルートとは、送信されたすべてのトラフィックを破棄するルートのことです。Linux プログラミングでの /dev/null インタフェースにとてもよく似ています。

ブラックホール ルートは、疑わしい問い合わせに応答することなく、パケットを廃棄するために使用されます。これにより、発信元が対象のネットワークから何も情報を得られないため、セキュリティが強化されます。

ブラックホール ルートはまた、サブネット上のトラフィックも制限できます。一部のサブネット アドレスが使用されていない場合は、これらのアドレスへのトラフィック（ 有効なトラフィックまたは悪意のあるトラフィック ）をブラックホールに転送することで、セキュリティの強化とサブネット上のトラフィックの削減を実現できます。

トラフィックを転送しない仮想インタフェースであるループバック インタフェースを使用すると、ブラックホール ルーティングの設定が容易になります。通常のインタフェースと同様に、このループバック インタフェースも設定するパラメータがほとんどなく、送信されたすべてのトラフィックがそこで停止します。ハードウェア接続やリンク ステータスの問題が起こり得ないため、常に使用可能であり、その他のダイナミック ルーティングの役割に有効に使用できます。設定した後は、ファイアウォール ポリシーやルーティングなど、インタフェースを参照するその他の場所でループバック インタフェースを使用できます。ループバック インタフェースは、Web ベース マネージャと CLI のどちらからも設定できます。詳細については、95 ページの「ループバック インタフェースの追加」または『*FortiGate CLI リファレンス*』のシステムの章を参照してください。

スタティック ルート

スタティック ルートは、FortiGate ユニットで中継するパケットの宛先 IP アドレスとネットマスクを定義し、それらのパケットの（ゲートウェイ）IP アドレスを指定することによって設定します。ゲートウェイ アドレスは、トラフィックがルーティングされるネクストホップ ルータを指定します。

スタティック ルートの操作

スタティック ルート リストには、パケットをルーティングするために FortiGate ユニットがパケット ヘッダと比較する情報が表示されます。最初、このリストには工場出荷時に設定済みのスタティック デフォルト ルートが含まれています。詳細については、233 ページの「デフォルト ルートおよびデフォルト ゲートウェイ」を参照してください。新しいエントリを手動で追加できます。

スタティック ルート リストにスタティック ルートを追加すると、FortiGate ユニットは、一致するルートと宛先が FortiGate ルーティング テーブル内にすでに存在するかどうかを判定するためのチェックを実行します。一致が見つからなかった場合、FortiGate ユニットは、そのルートをルーティング テーブルに追加します。

Web ベース マネージャで IPv6 が有効になっている場合は、スタティック ルート リストに IPv6 ルートが表示されるため、新しいスタティック ルートを作成するときに IPv6 を選択できます。それ以外の場合、IPv6 ルートは表示されません。IPv6 の詳細については、184 ページの「設定」または 186 ページの「FortiGate の IPv6 サポート」を参照してください。

スタティック ルート リストを表示するには、*[Router]*、*[Static]*、*[Static Route]* の順に選択します。

[Static Route] ページ

作成したすべてのスタティック ルート（デフォルトのスタティック ルートを含む）を表示します。このページでは、新しいスタティック ルートを編集、削除、または作成することができます。

[Create New]	スタティック ルート リストにスタティック ルートを追加します。詳細については、236 ページの「ルーティング テーブルへのスタティック ルートの追加」を参照してください。 IPv6 スタティック ルートを作成するには、オプションの下矢印を選択します。
[Edit]	スタティック ルート内の設定を変更する場合に選択します。
[Delete]	リストからスタティック ルートを削除する場合に選択します。
[ECMP Route Failover & Load Balance Method]	ECMP ルートの負荷分散とフェールオーバーの方法を選択します。237 ページの「ECMP ルートのフェールオーバーと負荷分散」を参照してください。
[Source based]	FortiGate ユニットは、負荷分散されるセッションの発信元 IP アドレスに基づいて、ECMP ルート間でセッションを負荷分散します。これがデフォルトの負荷分散方法です。発信元 IP の負荷分散をサポートするために、設定変更は必要ありません。

[Weighted]	FortiGate ユニットは、ECMP ルートに追加された重み付けに基づいて、ECMP ルート間でセッションを負荷分散します。重み付けの大きいルートに、より多くのトラフィックが転送されます。 重み付けベースの方法を選択した後、スタティック ルートに重み付けを追加する必要があります。詳細については、241 ページの「重み付けされたスタティック ルートの負荷分散の設定」を参照してください。
[Spill-over]	FortiGate ユニットは、ルートに関連付けられた FortiGate インタフェースのビジー状態に基づいて、ECMP ルート間でセッションを分散します。 スピルオーバーの方法を選択した後、ECMP ルートに追加されたインタフェースにルートの *[Spillover Thresholds]* を追加します。詳細については、101 ページの「ゲートウェイ負荷分散のためのインタフェース ステータス検出の設定」を参照してください。 このインタフェースで処理される帯域幅がスピルオーバーしきい値に達するまで、FortiGate ユニットは、ECMP によってルーティングされるすべてのセッションを最も小さい番号のインタフェースに送信します。その後、FortiGate ユニットは、以降のセッションをその次に小さい番号のインタフェースに送信します。 各インタフェースが選択される順序を含む詳細については、、238 ページの「スピルオーバーまたは使用状況ベースの ECMP の設定」を参照してください。
[Apply]	ECMP ルートのフェールオーバーと負荷分散の方法を保存する場合に選択します。
[Route]	IPv4 スタティック ルートの表示と非表示を切り替えるには、展開の矢印を選択します。デフォルトでは、これらのルートは表示されています。
[IPv6 Route]	IPv6 スタティック ルートの表示と非表示を切り替えるには、展開の矢印を選択します。デフォルトでは、これらのルートは非表示になっています。 これは、Web ベース マネージャで IPv6 が有効になっている場合にのみ表示されます。
[IP/Mask]	FortiGate ユニットが中継するパケットの宛先 IP アドレスとネットワーク マスク。
[Gateway]	中継されたパケットが転送されるネクストホップ ルータの IP アドレス。
[Device]	中継されたパケットが送受信される FortiGate インタフェースの名前。
[Distance]	各ルートに関連付けられたディスタンス。これらの値は、ネクストホップ ルータへのディスタンスを表します。
[Weight]	[ECMP Route Failover & Load Balance Method] が *[Weighted]* に設定されている場合は、各ルートの重み付けを追加します。負荷分散時により多くのセッションを割り当てるルートには、より大きな重み付けを追加します。詳細については、241 ページの「重み付けされたスタティック ルートの負荷分散の設定」を参照してください。

[New Static Route] ページ

FortiGate ユニットで中継するパケットの宛先 IP アドレスとネットマスクを定義し、それらのパケットの（ゲートウェイ）IP アドレスを指定するための設定を提供します。

[Destination IP/Mask]	FortiGate ユニットで中継するパケットの宛先 IP アドレスとネットマスクを入力します。
[Device]	中継されたパケットが送受信されるインタフェースを選択します。
[Gateway]	FortiGate ユニットで中継するパケットのゲートウェイの IP アドレスを入力します。
[Distance]	ネクストホップ ルータへのディスタンスを表す数値を入力します。
[Priority]	このスタティック ルートのプライオリティの数値を入力します。

注記： 特に指定されていない限り、スタティック ルートの例や手順は IPv4 スタティック ルートのためのものです。
IPv6 トラフィックのスタティック ルートを追加、編集、または削除するには、`config router static6` CLI コマンドを使用できます。詳細については、『*FortiGate CLI リファレンス*』の "router" の章を参照してください。

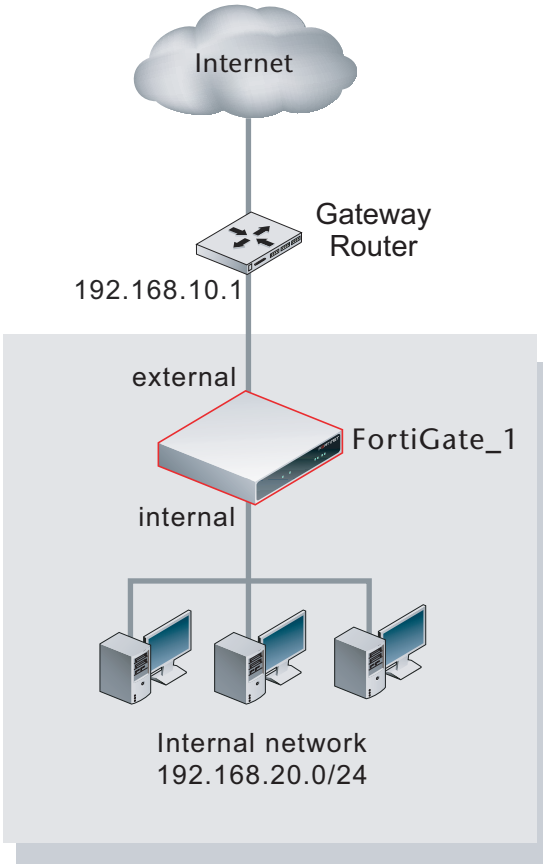
デフォルト ルートおよびデフォルト ゲートウェイ

工場出荷のデフォルト設定では、スタティック ルート リスト内のエントリ番号 1 は、すべての宛先を示す 0.0.0.0/0.0.0.0 の宛先アドレスに関連付けられています。このルートは、「スタティック デフォルト ルート」と呼ばれます。ルーティング テーブル内に他のルートが存在せず、パケットを FortiGate ユニットを超えて転送する必要がある場合は、工場出荷時に設定済みのスタティック デフォルト ルートによって、FortiGate ユニットはそのパケットをデフォルト ゲートウェイに転送します。

これを防ぐには、工場出荷時に設定済みのスタティック デフォルト ルートを編集して FortiGate ユニットの別のデフォルト ゲートウェイを指定するか、または工場出荷時に設定済みのルートを削除し、FortiGate ユニットのデフォルト ゲートウェイを指す独自のスタティック デフォルト ルートを指定する必要があります。

たとえば、図 5 は、ルータに接続されている FortiGate ユニットを示しています。ルータを超えた任意のネットワーク宛てのすべての送信パケットが正しい宛先に確実にルーティングされるようにするには、工場出荷のデフォルト設定を編集して、そのルータを FortiGate ユニットのデフォルト ゲートウェイにする必要があります。

図 5: ルータをデフォルト ゲートウェイにする



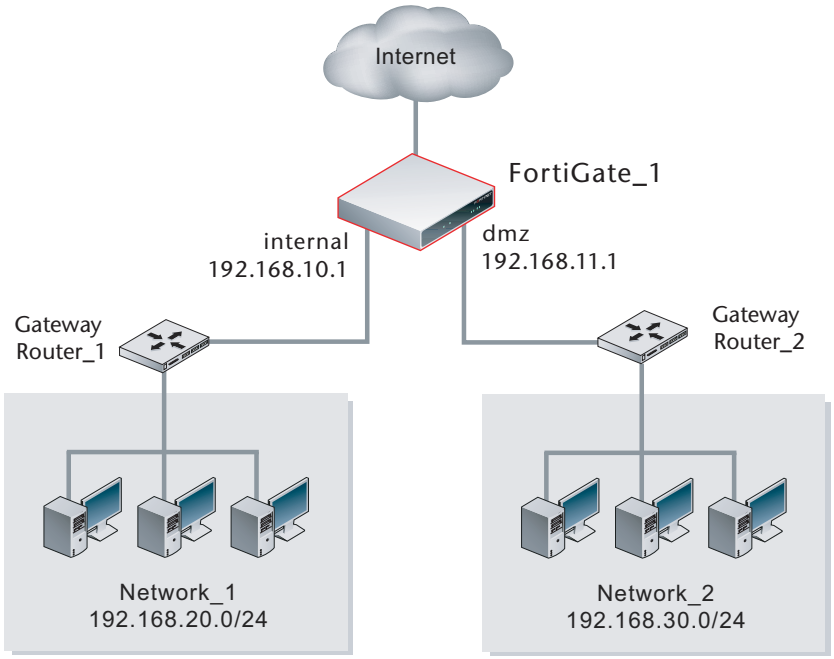
送信パケットを内部ネットワークから、ネットワーク 192.168.20.0/24 上に存在しない宛先にルーティングするには、デフォルト ルートを編集して、次の設定を含めます。

- [Destination IP/mask]: 0.0.0.0/0.0.0.0
- [Gateway]: 192.168.10.1
- [Device]: ネットワーク 192.168.10.0/24 に接続されているインタフェースの名前 (この例では、"external")
- [Distance]: 10

[Gateway] 設定は、FortiGate の外部インタフェースへのネクストホップ ルータ インタフェースの IP アドレスを指定します。ルータ (192.168.10.1) に接続されているインタフェースは、FortiGate_1 のデフォルト ゲートウェイです。

場合によっては、FortiGate ユニットの背後にルータが存在することがあります。パケットの宛先 IP アドレスがローカル ネットワーク上には存在せず、それらのいずれかのルータの背後にあるネットワーク上に存在する場合は、FortiGate ルーティング テーブルにそのネットワークへのスタティック ルートが含まれている必要があります。たとえば、図 6 の場合、FortiGate ユニットがパケットを Network_1 と Network_2 に転送するには、このユニットに、それぞれインタフェース 192.168.10.1 と 192.168.11.1 へのスタティック ルートが設定されている必要があります。また、ファイアウォール ポリシーも、トラフィックがこれらのルートに沿って FortiGate ユニットを通過できるように設定されている必要があります。詳細については、268 ページの「ファイアウォール ポリシーの設定」を参照してください。

図 6: 内部ルータの背後にあるネットワーク上の宛先



パケットを Network_1 から Network_2 にルーティングするには、Router_1 は、デフォルト ゲートウェイとして FortiGate の Internal インタフェースを使用するように設定されている必要があります。FortiGate ユニット上で、新しいスタティック ルートを次の設定で作成します。

[Destination IP/mask]	192.168.30.0/24
[Gateway]	192.168.11.1
[Device]	dmz
[Distance]	10

パケットを Network_2 から Network_1 にルーティングするには、Router_2 は、デフォルト ゲートウェイとして FortiGate の dmz インタフェースを使用するように設定されている必要があります。FortiGate ユニット上で、新しいスタティック ルートを次の設定で作成します。

[Destination IP/mask]	192.168.20.0/24
[Gateway]	192.168.10.1
[Device]	internal
[Distance]	10

デフォルト ルートのゲートウェイの変更

デフォルト ゲートウェイは、デフォルト ルートに一致するパケットの転送先を決定します。

FortiGate ユニット上のモデム インタフェースを介して DHCP または PPPoE を使用している場合は、このインタフェース上でのスタティック ルートの設定で問題が発生する可能性があります。DHCP ライセンスの更新または PPPoE 接続の再接続のどちらかを試した後、CLI に移動し、モデム インタフェースの `config system interface` の下にある `dynamic-gateway` を有効にします。これにより、このインタフェースのルートのゲートウェイを指定する必要がなくなります。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

注記：ネットワーク トラフィックを通過させるには、正しいルートが設定されている場合でも、適切なファイアウォール ポリシーが設定されている必要があります。詳細については、268 ページの「ファイアウォール ポリシーの設定」を参照してください。

デフォルト ルートのゲートウェイを変更するには

1 *[Router]*、*[Static]*、*[Static Route]* の順に選択します。
2 1 行目にある *[編集]* アイコンを選択します。
3 FortiGate ユニットが、*[Device]* フィールドで現在選択されているインタフェース以外のインタフェースを介してネクストホップ ルータに到達する場合は、*[Device]* フィールドからインタフェースの名前を選択します。
4 *[Gateway]* フィールドに、送信トラフィックの転送先として使用できるネクストホップ ルータの IP アドレスを入力します。
5 *[Distance]* フィールドで、必要に応じてディスタンスの値を調整します。
6 *[OK]* を選択します

ルーティング テーブルへのスタティック ルートの追加

ルートは、FortiGate ユニットに、パケットを特定の宛先に転送するために必要な情報を提供します。パケットは、スタティック ルートによって、デフォルト ゲートウェイ以外の宛先へと転送されます。

スタティック ルートは手動で定義します。FortiGate ユニットから送出されるトラフィックはスタティック ルートが制御しますが、パケットを送出するインタフェースとパケットの転送先のデバイスはユーザが指定できます。

スタティック ルートのエントリを追加するには

1 *[Router]*、*[Static]*、*[Static Route]* の順に選択します。
2 *[Create New]* を選択します。
3 IP アドレスとネットマスクを入力します。

   たとえば、`172.1.2.0/255.255.255.0` は、サブネット 172.1.2.x 上のすべてのアドレスのルートになります。
4 このサブネットに最も近いか、またはこのサブネットに接続されている FortiGate ユニット インタフェースを入力します。
5 ゲートウェイの IP アドレスを入力します。先の例を続けると、`172.1.2.11` は有効なアドレスになります。
6 このルートのディスタンスを入力します。

   ディスタンスを使用すると、あるルートを別のルートより優先されるように重み付けすることができます。これは、あるルートが信頼できない場合に有効です。たとえば、ルート A のディスタンスが 30 で、ルート B のディスタンスが 10 の場合、優先ルートはディスタンスが小さい方の 10 のルート A です。ルート A が信頼できないことがわかった場合は、ルート A のディスタンスを 10 から 40 に変更できます。これにより、ルート B が優先ルートになります。
7 *[OK]* を選択して、新しいスタティック ルートを確認し、保存します。

Web ベース マネージャでスタティック ルートを追加すると、FortiGate ユニットによって、そのエントリがスタティック ルート リストに追加されます。

"internal" という名前のインタフェースを持つ FortiGate ユニットの [Edit Static Route] ダイアログ ボックスを示しています。FortiGate ユニット上の実際のインタフェースの名前はこれとは異なる場合があります。

[Destination IP/Mask]	FortiGate ユニットで中継する必要のあるパケットの宛先 IP アドレスおよびネットワーク マスクを入力します。 0.0.0.0/0.0.0.0 の値は、 デフォルト ルートに予約されています。
[Gateway]	中継したパケットを FortiGate ユニットが転送するネクストホップ ルータの IP アドレスを入力します。
[Device]	中継したパケットをネクストホップ ルータにルーティングするために使用できる FortiGate インタフェースの名前を選択します。
[Distance]	ルートのディスタンスを 1 ～ 255 の範囲の値で入力します。このディスタンスの値は任意であり、ネクストホップ ルータへのディスタンスが反映されている必要があります。値が小さいほど、より優先されるルートであることを示します。
[Weight]	各ルートの重み付けを追加します。負荷分散でより多くのセッションを割り当てるルートには、より大きな重み付けを追加します。241 ページの「重み付けされたスタティック ルートの負荷分散の設定」を参照してください。 [ECMP Route Failover & Load Balance Method] が *[Weighted]* に設定されている場合に使用できます。

ECMP ルートのフェールオーバーと負荷分散

FortiOS は、 等価コスト マルチパス (ECMP) を使用して、トラフィックをインターネットや別のネットワークなどの同じ宛先に分散します。 ECMP を使用すると、 複数のルートを同じ宛先に追加し、これらの各ルートに同じディスタンスとプライオリティを割り当てることができます。

ただし、同じ宛先への複数のルート プライオリティは同じで、ディスタンスが異なる場合は、ディスタンスの最も小さいルートが使用されます。同じ宛先への複数のルートのディスタンスは同じで、プライオリティが異なる場合は、プライオリティの最も低いルートが使用されます。ディスタンスはプライオリティより優先されます。同じ宛先への複数のルートのディスタンスとプライオリティの両方が異なる場合は、たとえプライオリティが最も高いとしても、ディスタンスの最も小さいルートが常に使用されます。

ECMP を使用すると、複数の ECMP ルートが使用可能な場合に、通信セッションに使用されるルートの FortiGate ユニットによる選択方法を設定できます。1 つの ECMP ルートのみが使用可能な場合 (たとえば、インタフェース ステータス検出で、設定されたサーバからの応答が受信されないためにインタフェースがトラフィックを処理できない場合など) は、すべてのトラフィックがこのルートを使用します。

以前のバージョンの FortiOS は、ECMP ルートに対して発信元 IP ベースの負荷分散を提供していました。FortiOS 4.0 MR1 には、ECMP ルートのフェールオーバーと負荷分散のための次の 3 つの設定オプションが含まれています。

[Source based] (発信元 IP ベースとも呼ばれる)	FortiGate ユニットは、負荷分散されるセッションの発信元 IP アドレスに基づいて、ECMP ルート間でセッションを負荷分散します。これがデフォルトの負荷分散方法です。発信元 IP の負荷分散をサポートするために、設定変更は必要ありません。
[Weighted] (重み付けベースとも呼ばれる)	FortiGate ユニットは、ECMP ルートに追加された重み付けに基づいて、ECMP ルート間でセッションを負荷分散します。重み付けの大きいルートに、より多くのトラフィックが転送されます。 重み付けベースの方法を選択した後、スタティック ルートに重み付けを追加する必要があります。241 ページの「重み付けされたスタティック ルートの負荷分散の設定」を参照してください。
[Spill-over] (使用状況ベースとも呼ばれる)	FortiGate ユニットは、ルートに追加された FortiGate インタフェースのビジー状態に基づいて、ECMP ルート間でセッションを分散します。 スピルオーバーの方法を選択した後、ECMP ルートに追加されたインタフェースにルートの *[Spillover Thresholds]* を追加します。このインタフェースで処理される帯域幅がスピルオーバーしきい値に達するまで、FortiGate ユニットは、ECMP によってルーティングされるすべてのセッションを最も小さい番号のインタフェースに送信します。その後、FortiGate ユニットは、以降のセッションをその次に小さい番号のインタフェースに送信します。 *[Spillover Thresholds]* の範囲は 0 ～ 2097000 KBps です。 各インタフェースが選択される順序を含む詳細については、、238 ページの「スピルオーバーまたは使用状況ベースの ECMP の設定」を参照してください。

1 つの VDOM 内で設定できる ECMP ルートのフェールオーバーと負荷分散の方法は、これらのうちの 1 つだけです。FortiGate ユニットで複数の VDOM での動作が設定されている場合は、各 VDOM に独自の ECMP ルートのフェールオーバーと負荷分散を設定できます。

Web ベース マネージャから ECMP ルートのフェールオーバーと負荷分散の方法を設定するには

1 *[Router]*、*[Static]*、*[Static Route]* の順に選択します。
2 *[ECMP Route Failover & Load Balance Method]* を *[Source based]*、*[Weighted]*、または *[Spill- over]* に設定します。
3 [Apply] を選択します。

CLI から ECMP ルートのフェールオーバーと負荷分散の方法を設定するには

次のコマンドを入力します。

```
config system settings
  set v4-ecmp-mode {source-ip-based | usage-based |
     weight-based}
end
```

同じ宛先 IP アドレスへの同時セッションの ECMP ルーティング

FortiGate ユニットがセッションの ECMP ルートを選択すると、そのセッションの宛先 IP アドレスを含むルートに一致するルート キャッシュが作成されます。そのルートがキャッシュからフラッシュされるまで、同じ宛先 IP アドレスへのすべての新しいセッションが同じルートを使用します。その宛先 IP アドレスへの新しいセッションが受信されなくなってから一定の期間が経つと、ルートはキャッシュからフラッシュされます。

ルート キャッシュによって、FortiGate ユニットがルーティング テーブル内のルートを検索する頻度が削減されるため、FortiGate のルーティング パフォーマンスが向上します。

FortiGate ユニットが同じ宛先 IP アドレスを含む多数のセッションを受信している場合は、これらのすべてのセッションが同じルートによって処理されるため、ECMP ルートのフェールオーバーと負荷分散の設定に従ってセッションが分散されていないように見えることがあります。

スピルオーバーまたは使用状況ベースの ECMP の設定

スピルオーバーまたは使用状況ベースの ECMP の方法では、新しいセッションを、設定された帯域幅の制限 (*[Spillover Threshold]* またはルート スピルオーバーしきい値と呼ばれる) に達していないインタフェースにルーティングします。スピルオーバーまたは使用状況ベースの ECMP ルーティングを設定するには、スピルオーバー ECMP の方法を有効にして、ECMP ルートを追加し、ECMP ルートによって使用されるインタフェースに *[Spillover Threshold]* を追加します。各インタフェースで処理される帯域幅の量を制限するには、*[Spillover Thresholds]* を設定します。

スピルオーバーの ECMP ルーティングが設定されている場合、各インタフェースが設定済みの *[Spillover Threshold]* に達するまで、FortiGate ユニットは新しいセッションを ECMP ルートによって使用されるインタフェースにルーティングします。その後、そのインタフェースのしきい値に達すると、新しいセッションは、ECMP ルートによって使用される他のいずれかのインタフェースにルーティングされます。

使用状況ベースの ECMP ルーティングを有効にするには、次の手順を使用します。FortiGate インタフェースの port3 と port4 にスピルオーバーしきい値を追加した後、デバイスを port3 と port4 に設定した EMCP ルートを設定します。

Web ベース マネージャからインタフェースにスピルオーバーしきい値を追加するには

1 *[Router]*、*[Static]*、*[Static Route]* の順に選択します。
2 *[ECMP Route Failover & Load Balance Method]* を *[usage-based]* に設定します。
3 *[Router]*、*[Static]*、*[Static Route]* の順に選択します。
4 port3 と port4 の ECMP ルートを追加します。

[Destination IP /Mask]	192.168.20.0/24
[Device]	port3
[Gateway]	172.20.130.3
[Distance]	9

[Destination IP /Mask]	192.168.20.0/24
[Device]	port4
[Gateway]	172.20.140.4
[Distance]	9

5 *[System]*、*[Network]*、*[Interface]* の順に選択します。

6 port3 と port4 を編集し、次のスピルオーバーしきい値を追加します。

[Interface]	port3
[Spillover Threshold (KBps)]	100

[Interface]	port4
[Spillover Threshold (KBps)]	200

7 ルーティング テーブルを表示するには、*[Router]*、*[Monitor]* の順に選択します。
ルートは、表 48 に示す順序で表示できます。

表 48: [Routing Monitor] に表示される ECMP ルートの例

[Type]	[Network]	[Distance]	[Metric]	[Gateway]	[Interface]
[Static]	192.168.20.0/24	9	0	172.20.130.3	port3
[Static]	192.168.20.0/24	9	0	172.20.140.4	port4

この例では、FortiGate ユニットは、すべてのセッションを port3 を介して 192.168.20.0 ネットワークに送信します。port3 が 100 Kbps のスピルオーバーしきい値を超えると、FortiGate ユニットは、すべての新しいセッションをport4を介して192.168.20.0ネットワークに送信します。

CLI からインタフェースにルート スピルオーバーしきい値を追加するには

1 ECMP ルートのフェールオーバーと負荷分散の方法を使用状況ベースに設定するには、次のコマンドを入力します。

```
config system settings
  set v4-ecmp-mode usage-based
end
```

2 3 つのインタフェースに 3 つのルート スピルオーバーしきい値を追加するには、次のコマンドを入力します。

```
config system interface
  edit port1
    set spillover-threshold 400
  next
  edit port2
    set spillover-threshold 200
  next
  edit port3
    set spillover-threshold 100
  end
```

3 各インタフェースに 1 つ、3 つの ECMP デフォルト ルートを追加するには、次のコマンドを入力します。

```
config router static
  edit 1
    set dst 0.0.0.0/0.0.0.0
    set gwy 172.20.110.1
    set dev port1
  next
  edit 2
    set dst 0.0.0.0/0.0.0.0
    set gwy 172.20.120.2
    set dev port2
  next
  edit 3
    set dst 0.0.0.0/0.0.0.0
    set gwy 172.20.130.3
    set dev port3
  end
```

4 ルーティング テーブル内のスタティック ルートを表示するには、次のコマンドを入力します。

```
get router info routing-table static
S        0.0.0.0/0 [10/0] via 172.20.110.1, port1
                   [10/0] via 172.20.120.2, port2
                   [10/0] via 172.20.130.3, port3
```

この例では、FortiGate ユニットは、すべてのセッションを port1 を介してインターネットに送信します。port1 が 400 KBps のスピルオーバーしきい値を超えると、FortiGate ユニットは、すべての新しいセッションを port2 を介してインターネットに送信します。port1 と port2 の両方がスピルオーバーしきい値を超えると、FortiGate ユニットは、すべての新しいセッションを port3 を介してインターネットに送信します。

スピルオーバー ECMP でのルートの選択方法の詳細な説明

ECMP ルートを追加すると、これらのルートは、[Routing Monitor] または `get router info routing-table static` コマンドによって表示される順序でルーティング テーブルに追加されます。この順序は、設定された帯域幅の制限には関係ありません。

FortiGate ユニットは、ルーティング テーブル内の最初のルートを見つけた後、設定されたルート スピルオーバー制限を超えるトラフィックを処理していない FortiGate インタフェース上でセッションを送信することによって、新しいセッションの ECMP ルートを選択します。

たとえば、インタフェース port3 と port4 の両方が別の ISP を介してインターネットに接続された FortiGate ユニットを考えてみます。ECMP ルーティングは使用状況ベースに設定されており、ルート スピルオーバーは port3 が 100 KBps、port4 が 200 KBps です。port3 に 1 つと、port4 に 1 つの、2 つの ECMP デフォルト ルートが追加されます。

ルーティング テーブル内で port3 へのルートの方が port4 へのルートより上にある場合、port3 が 100 KBps のデータを処理するまで、FortiGate ユニットはすべてのデフォルト ルート セッションを port3 から送信します。port3 が設定済みの帯域幅の制限に達すると、FortiGate ユニットは、すべてのデフォルト ルート セッションを port4 から送信します。port3 の帯域幅使用率が 100 KBps を下回ると、FortiGate は再び、すべてのデフォルト ルート セッションを port3 から送信します。

ただし、すでにルーティング キャッシュ内にある IP アドレスを指定する新しいセッションは、キャッシュされているルートを使用します。つまり、port3 が帯域幅の制限を超えていても、その宛先アドレスがすでにルーティング キャッシュ内にある場合は、新しいセッションが引き続き port3 から送信されることがあります。その結果、新しいセッションが port4 から送信されるのは、port3 が帯域幅の制限を超えており、かつルーティング キャッシュに新しいセッションの宛先 IP アドレスのルートが含まれていない場合だけです。port4 に対する制限は、スピルオーバーのための追加のインタフェースが存在する場合にのみ重要です。

また、port4 への切り替えも、port3 が帯域幅の制限を超えるとすぐに実行されるわけではありません。切り替えが実行されるには、帯域幅使用率が一定期間、制限を超えている必要があります。この期間中に port3 の帯域幅使用状況が帯域幅の制限を下回ると、セッションは port4 には切り替えられません。この遅延により、ルート フラッピングが削減されます。ルート フラッピングは、ルートがステータスを頻繁に変更することにより、ルータに連続的なルーティング テーブルの変更および新しい情報のブロードキャストを強制する場合に発生します。

FortiGate の使用状況ベースの ECMP ルーティングでは、ルートが FortiGate インタフェース間で均等に分散されないため、実際には負荷分散されていません。トラフィック量に応じて、ほとんどのトラフィックは通常、最初のインタフェースによって処理され、スピルオーバー トラフィックのみがその他のインタフェースによって処理されます。

使用状況ベースの ECMP を設定する場合は、たいてい、ECMP ルートを含むすべてのインタフェースにスピルオーバーしきい値を追加する必要があります。デフォルトのスピルオーバーしきい値は 0 です。つまり、帯域幅の制限はありません。いずれかのインタフェースのスピルオーバーしきい値が 0 の場合、インタフェースが停止するか、または切断されない限り、セッションはリスト内の下の方のインタフェースにはルーティングされません。インタフェースは、*[Detect Interface Status for Gateway Load Balancing]* で、設定されたサーバからの応答が受信されない場合に停止することがあります。

注記: すでにルーティング キャッシュ内にエントリがある宛先IPアドレスへの新しいセッションは、その宛先アドレス用にすでにキャッシュに追加されているルートを使用してルーティングされます。詳細については、238 ページの「同じ宛先 IP アドレスへの同時セッションの ECMP ルーティング」を参照してください。

インタフェースがスピルオーバーしきい値を超えているかどうかの判定

`diagnose netlink dstmac list` CLI コマンドを使用すると、インタフェースがスピルオーバーしきい値を超えているかどうかを判定できます。このコマンドで *over_bps=1* が表示される場合、インタフェースはしきい値を超えています。*over_bps=0* の場合、インタフェースはしきい値を超えていません。

重み付けされたスタティック ルートの負荷分散の設定

各ルートの重み付けを追加することによって、FortiGate ユニットによる ECMP ルート間でのセッションの分散方法を制御するには、重み付けされた負荷分散を設定します。負荷分散でより多くのセッションを割り当てるルートには、より大きな重み付けを追加します。ルートに重み付けが割り当てられていない場合、そのルートの重み付けはデフォルトで0に設定されます。

ECMP の負荷分散方法が [Weighted] に設定されている場合、FortiGate ユニットは、選択するルートを決定するためにランダムな値を生成することによって、異なる宛先 IP を含むセッションを分散します。あるルートを別のルートより優先して選択する確率は、各ルートの重み付けの値に基づいています。重み付けの大きいルートは、選択される可能性が高くなります。

ルートの重み付けの値に従って、多数のセッションが ECMP ルート間で均等に分散されます。すべての重み付けが同じである場合、セッションは均等に分散されます。ただし、少数のセッションの分散は均等にならないことがあります。たとえば、同じ重み付けの 2 つの ECMP ルートが存在する場合は、異なる IP アドレスへの 2 つのセッションが同じルートを使用する可能性があります。これに対して、異なる宛先 IP を含む 10,000 のセッションは、2 つのルート間で等しい割合で均等に負荷分散されるはずです。この分散は、5000:5000 または 5001:4999 になる可能性があります。また、2 つのルートの重み付けが 100 と 200 である場合、異なる宛先 IP アドレスを含む 10,000 のセッションは 3333:6667 のように負荷分散されるはずです。

重み付けは、新しい宛先 IP アドレスへのセッションに対してルートが選択される方法にのみ影響を与えます。すでにルーティング キャッシュ内にある IP アドレスへの新しいセッションは、すでにキャッシュ内にあるセッションのルートを使用してルーティングされます。そのため、セッションは実際には、必ずしもルーティングの重み付けによる分散に従って分散されるとは限りません。

Web ベース マネージャからスタティック ルートに重み付けを追加するには

1 *[Router]*、*[Static]*、*[Static Route]* の順に選択します。

2 *[ECMP Route Failover & Load Balance Method]* を *[Weighted]* に設定します。

3 *[Router]*、*[Static]*、*[Static Route]* の順に選択します。

4 スタティック ルートを新規に追加するか、または編集し、それらのルートに重み付けを追加します。

次の例は、重み付けが追加された 2 つの ECMP ルートを示しています。

[Destination IP /Mask]	192.168.20.0/24
[Device]	port1
[Gateway]	172.20.110.1
[Distance]	10
[Weight]	100

[Destination IP /Mask]	192.168.20.0/24
[Device]	port2
[Gateway]	172.20.120.2
[Distance]	10
[Weight]	200

この例では、次のようになります。

- 192.168.20.0 ネットワークへのセッションの 1/3 は最初のルートを使用し、IP アドレスが 172.20.110.1 のゲートウェイに port1 から送信されます。
- 192.168.20.0 ネットワークへのセッションのその他の 2/3 は 2 番目のルートを使用し、IP アドレスが 172.20.120.2 のゲートウェイに port2 から送信されます。

CLI からスタティック ルートに重み付けを追加するには

1 ECMP ルートのフェールオーバーと負荷分散の方法を重み付けに設定するには、次のコマンドを入力します。

```
config system settings
  set v4-ecmp-mode weight-based
end
```

2 3 つの ECMP スタティック ルートを追加し、各ルートに重み付けを追加するには、次のコマンドを入力します。

```
config router static
  edit 1
    set dst 192.168.20.0/24
    set gwy 172.20.110.1
    set dev port1
    set weight 100
  next
  edit 2
    set dst 192.168.20.0/24
    set gwy 172.20.120.2
    set dev port2
    set weight 200
  next
  edit 3
    set dst 192.168.20.0/24
    set gwy 172.20.130.3
    set dev port3
    set weight 300
  end
```

注記：この例では、3 つのすべてのルートについて priority は 0 に、また distance は 10 に設定されたままになります。distance が 10 に設定されているその他のルートはすべて、weight が設定されないため、0 の weight が割り当てられ、負荷分散には含まれません。

この例では、次のようになります。

- 192.168.20.0 ネットワークへのセッションの 1/6 は最初のルートを使用し、IP アドレスが 172.20.110.1 のゲートウェイに port1 から送信されます。
- 192.168.20.0 ネットワークへのセッションの 1/3 は 2 番目のルートを使用し、IP アドレスが 172.20.120.2 のゲートウェイに port2 から送信されます。
- 192.168.20.0 ネットワークへのセッションの 1/2 は 3 番目のルートを使用し、IP アドレスが 172.20.130.3 のゲートウェイに port3 から送信されます。

ポリシー ルート

ルーティング ポリシーを使用すると、スタティック ルートから離れてトラフィックをリダイレクトできます。この機能は、特定の種類のネットワーク トラフィックを異なった方法でルーティングする場合に有効なことがあります。受信トラフィックのプロトコル、発信元アドレスまたはインタフェース、宛先アドレス、ポート番号などを使用して、トラフィックの送信先を決定できます。たとえば、一般にネットワーク トラフィックはサブネットのルータに転送されますが、そのサブネットに宛てられた SMTP または POP3 トラフィックをメール サーバに直接転送することもできます。

FortiGate ユニットにルーティング ポリシーが設定されていて、その FortiGate ユニットにパケットが到着した場合、FortiGate ユニットは [Policy Route] リストの先頭から開始して、そのパケットをポリシーと一致させようと試みます。一致が見つかり、そのポリシーにパケットをルーティングするための十分な情報（少なくともネクストホップ ルータの IP アドレスと、そのルータにパケットを転送するための FortiGate インタフェース）が含まれている場合、FortiGate ユニットはポリシー内の情報を使用してパケットをルーティングします。そのパケットに一致するポリシー ルートが存在しない場合、FortiGate ユニットはルーティング テーブルを使用してパケットをルーティングします。

ほとんどのポリシー設定はオプションであるため、一致するポリシーだけでは、パケットを転送するための十分な情報が提供されない可能性があります。FortiGate ユニットは、パケット ヘッダ内の情報をルーティング テーブル内のルートと照合しようとして、ルーティング テーブルを参照することがあります。たとえば、ポリシーに送信インタフェースの項目しか存在しない場合、FortiGate ユニットはネクストホップ ルータの IP アドレスをルーティング テーブル内で検索します。この状況は、インタフェースが動的（DHCP や PPPoE など）であり、かつネクストホップ ルータの IP アドレスを指定したくないか、または指定できない場合に発生することがあります。

ポリシー ルートのオプションによって、着信パケットのどの属性でポリシー ルーティングを実行するかが定義されます。パケットの属性が指定されたすべての条件に一致した場合、FortiGate ユニットは指定されたインタフェースを介して、指定されたゲートウェイにパケットをルーティングします。

ポリシー ルートを追加するには、*[Router]*、*[Static]*、*[Policy Route]* の順に選択し、*[Create New]* を選択します。

サービスの種類の詳細については、245 ページの「サービスの種類」を参照してください。図 は、"external" と "internal" という名前のインタフェースを備えた FortiGate ユニットに属するポリシー ルート リストを示しています。FortiGate ユニット上の実際のインタフェースの名前はこれとは異なる場合があります。

[Policy Route] ページ

作成したすべてのポリシー ルートを表示します。このページでは、新しいポリシー ルートを編集、削除、または作成することができます。

[Create New]	ポリシー ルートを追加します。245 ページの「ポリシー ルートの例」を参照してください。
#	設定されたルート ポリシーの ID 番号。これらの番号は、テーブル内でポリシーが移動されていない限り、連番となります。
[Incoming]	ルート ポリシーの対象となるパケットを受信するインタフェース。
[Outgoing]	ポリシーによってルーティングされるパケットをルーティングするインタフェース。
[Source]	ポリシー ルーティングを実行する IP 発信元アドレスおよびネットワーク マスク。
[Destination]	ポリシー ルーティングを実行する IP 宛先アドレスおよびネットワーク マスク。
[Delete]	ポリシー ルートを削除します。
[Edit]	ポリシー ルートを編集します。

[New Routing Policy] ページ

スタティック ルートから離れてトラフィックをリダイレクトする方法を設定するための各設定を提供します。

[If incoming traffic matches:]

[Protocol]	パケットのプロトコル フィールド内の値に基づいてポリシー ルーティングを実行するには、一致するプロトコル番号を入力します。インターネット プロトコル番号は、IP パケット ヘッダ内に含まれています。プロトコル番号は RFC 5237 に記述されており、割り当てられたプロトコル番号のリストはここで見つけることができます。範囲は 0 ～ 255 です。0 の値を指定すると、この機能は無効になります。 **ヒント**：一般に使用される *[Protocol]* の設定には、TCP セッションをルーティングするための 6、UDP セッションのための 17、ICMP セッションのための 1、GRE セッションのための 47、マルチキャスト セッションのための 92 などがあります。 6 と 17 以外のプロトコルでは、ポート番号は無視されます。
[Incoming interface]	ポリシーの対象となる着信パケットが経由するインタフェースの名前を選択します。
[Source address/mask]	パケットの IP 発信元アドレスに基づいてポリシー ルーティングを実行するには、一致する発信元アドレスとネットワーク マスクを入力します。0.0.0.0/0.0.0.0 の値を指定すると、この機能は無効になります。
[Destination address/mask]	パケットの IP 宛先アドレスに基づいてポリシー ルーティングを実行するには、一致する宛先アドレスとネットワーク マスクを入力します。0.0.0.0/0.0.0.0 の値を指定すると、この機能は無効になります。
[Destination ports]	パケットを受信するポートに基づいてポリシー ルーティングを実行するには、[From] フィールドと [To] フィールドに同じポート番号を入力します。ポートの範囲にポリシー ルーティングを適用するには、開始のポート番号を [From] フィールドに、終了のポート番号を [To] フィールドに入力します。0 の値を指定すると、この機能は無効になります。 [Destination ports] フィールドは、TCP および UDP プロトコルにのみ使用されます。その他のプロトコルではすべて、これらのポートはスキップされます。
[Type of Service]	2 桁の 16 進数のビット パターンを使用してサービスを一致させるか、または 2 桁の 16 進数のビット マスクを使用してマスク除外します。詳細については、245 ページの「サービスの種類」を参照してください。

[Force traffic to:]

[Outgoing interface]	ポリシーの影響を受けるパケットがルーティングされるインタフェースの名前を選択します。
[Gateway Address]	FortiGate ユニットが指定されたインタフェースを介してアクセスできるネクストホップ ルータの IP アドレスを入力します。0.0.0.0 の値は無効です。

ポリシー ルートの例

port1 で受信されたすべての FTP トラフィックを、port10 インタフェースから IP アドレスが 172.20.120.23 のネクストホップ ルータに送信するには、次のポリシー ルートを設定します。FTP トラフィックをルーティングするには、プロトコルを 6 (TCP 用) に設定し、両方の宛先ポートを 21 (FTP ポート) に設定します。

[Protocol]	6
[Incoming interface]	port1
[Source address/mask]	0.0.0.0/0.0.0.0
[Destination address/mask]	0.0.0.0/0.0.0.0
[Destination ports]	21 から 21 まで
[Type of Service]	ビット パターン : 00 (16 進数) ビット マスク : 00 (16 進数)
[Outgoing interface]	port10
[Gateway Address]	172.20.120.23

サービスの種類

サービスの種類 (TOS) は、遅延、優先順位、信頼性、最小のコストなどの品質を使用して IP データグラムの配信方法を決定できるようにするための、IP ヘッダ内の 8 ビット フィールドです。

各品質により、ゲートウェイは、データグラムをルーティングするための最適な方法を決定できるようになります。ルータは、ルーティング テーブル内のルートごとに TOS 値を保持しています。最もプライオリティの低い TOS は 0 で、最もプライオリティの高い TOS は 7 (ビット 3、4、および 5 がすべて 1 に設定されている) です。ルータは、データグラムの TOS を、宛先への可能性のあるいずれかのルートの TOS と一致させようと試みます。一致が存在しない場合、データグラムは 0 の TOS ルートを介して送信されます。

高い品質を使用した場合は、パフォーマンスを向上させようとして限られたネットワーク リソースが消費されることがあるため、配信のコストが増える可能性があります。詳細については、RFC 791 および RFC 1349 を参照してください。

表 49: IP ヘッダの TOS 8 ビット フィールド内の各ビットの役割

ビット 0、1、2	**優先順位**	一部のネットワークでは、優先順位の高いトラフィックをより重要なトラフィックとして扱います。優先順位は 1 つのネットワーク内でのみ使用する必要があり、ネットワークごとに異なった方法で使用できます。通常、これらのビットを気にする必要はありません。
ビット 3	**遅延**	1 に設定されている場合、このビットは、短い遅延が優先されることを示します。これは、遅延によって音の品質が低下する VoIP などのサービスに有効です。
ビット 4	**スループット**	1 に設定されている場合、このビットは、高いスループットが優先されることを示します。これは、ビデオ会議などの、多くの帯域幅が必要なサービスに有効です。
ビット 5	**信頼性**	1 に設定されている場合、このビットは、高信頼性が優先されることを示します。これは、DNS サーバなどの、サービスを常に使用できる必要がある場合に有効です。
ビット 6	**コスト**	1 に設定されている場合、このビットは、低コストが優先されることを示します。一般に、ビット 3、4、または 5 を有効にすると関連する配信コストが高くなります。ビット 6 は、最もコストの低いルートを使用することを示します。
ビット 7	**将来の使用のために予約済み**	現時点では使用されていません。

たとえば、遅延が受け入れられない VoIP アプリケーションのために短い遅延と高信頼性を割り当てる場合は、xxx1x1xx のビット パターンを使用します。ここで、"x" は、ビットを任意の値にできることを示します。設定されていないビットがあるため、これはビット マスクの適切な使用です。0x14 に設定されたマスクは、短い遅延と高信頼性のために設定されている任意の TOS パケットに一致します。

ルータ - ダイナミック

この項では、[Routing] メニューにあるダイナミック ルーティングについて説明します。ダイナミック ルーティングの詳細については、『*FortiOS ハンドブック*』の「ダイナミック ルーティング」の章を参照してください。

ダイナミック ルーティング プロトコルを使用すると、FortiGate ユニットは、ルートに関する情報の隣接ルータとの共有や、それらのルータによってアドバタイズされたルートおよびネットワークについての学習を自動的に行うことができます。FortiGate ユニットは、次のダイナミック ルーティング プロトコルをサポートしています。

- RIP (Routing Information Protocol)
- OSPF (Open Shortest Path First)
- BGP (Border Gateway Protocol)

FortiGate ユニット上でバーチャル ドメイン (VDOM) を有効にした場合、ダイナミック ルーティングはバーチャル ドメインごとに別々に設定されます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には、以下のトピックが含まれています。

注記： FortiGate ユニットは、ルート バーチャル ドメイン内で PIM (Protocol Independent Multicast) バージョン 2 ルータとして動作できます。FortiGate ユニットは、PIM スパース モードおよびデンス モードをサポートしており、FortiGate インタフェースが接続されているネットワーク セグメント上のマルチキャスト サーバまたはレシーバにサービスを提供できます。PIM は、スタティック ルート、RIP、OSPF、または BGP を使用して、マルチキャスト パケットを宛先に転送できます。

RIP

RIP (Routing Information Protocol) は、小規模で、比較的均質なネットワークを対象にした、ディスタンス ベクトルのルーティング プロトコルです。FortiGate での RIP の実装は、RIP バージョン 1 (RFC 1058 を参照) および RIP バージョン 2 (RFC 2453 を参照) をサポートしています。

RIP は、*[Routing]*、*[Dynamic]*、*[RIP]* の順に選択して表示される画面で設定されます。

[RIP] ページ

作成したすべてのネットワークおよびインタフェースを表示します。このページではまた、基本的な RIP 設定 (インタフェースやネットワークの作成を含む) を設定することもできます。

[RIP Version] FortiGate ユニットで必要な RIP 互換性のレベルを選択します。RIP が有効なネットワークに接続されたすべての FortiGate インタフェース上でグローバルな RIP 設定を有効にすることができます。
[1] — RIP バージョン 1 のパケットを送受信します。
[2] — RIP バージョン 2 のパケットを送受信します。
必要に応じて、特定の FortiGate インタフェースのグローバル設定を置き換えることができます。詳細については、249 ページの「RIP が有効なインタフェース」を参照してください。

[Advanced Options] RIP 詳細設定オプションの表示と非表示を切り替えるには、展開の矢印を選択します。詳細については、248 ページの「RIP 詳細設定オプション」を参照してください。

[RIP] ページの [Networks] セクション

RIP を実行している (FortiGate ユニットに接続された) 主要なネットワークの IP アドレスとネットワークマスク。[Networks] リストにネットワークを追加すると、そのネットワークに含まれている FortiGate インタフェースが RIP 更新でアドバタイズされます。RIP ネットワーク アドレス空間に一致する IP アドレスを持つすべての FortiGate インタフェース上で RIP を有効にすることができます。

[IP/Netmask]	RIP が有効なネットワークを定義する IP アドレスとネットマスクを入力します。
[Add]	[Networks] リストにネットワーク情報を追加する場合に選択します。
[Delete]	RIP ネットワークのリストからネットワークを削除する場合に選択します。

[RIP] ページの [Interfaces] セクション

FortiGate インタフェース上の RIP 動作を調整するために必要な任意の追加の設定。

[Create New]	インタフェースの新しい RIP 動作パラメータを追加します。これらのパラメータによって、そのインタフェースのグローバルな RIP 設定が置き換えられます。詳細については、249 ページの「RIP が有効なインタフェース」を参照してください。
[Interface]	このユニットの RIP インタフェースの名前。
[Send Version]	各インタフェースを介して更新を送信するために使用される RIP のバージョンであり、*[1]*、*[2]*、*[both]* のいずれか。
[Receive Version]	各インタフェース上で更新を待機するために使用される RIP のバージョンであり、*[1]*、*[2]*、*[both]* のいずれか。
[Authentication]	このインタフェース上で使用される認証のタイプであり、*[None]*、*[Text]*、*[MD5]* のいずれか。
[Passive]	このインタフェース上の RIP ブロードキャストのための権限。緑色のチェックマークは、RIP ブロードキャストがブロックされていることを示します。
[Edit]	RIP インタフェースの設定を変更する場合に選択します。
[Delete]	[RIP Interface] リストから RIP インタフェースを削除する場合に選択します。

RIP 詳細設定オプション

RIP 詳細設定オプションを使用すると、RIP タイマの設定を指定したり、FortiGate ユニットが RIP 更新以外の何らかの手段によって学習したルートを再配布するためのメトリックを定義したりすることができます。たとえば、ユニットが OSPF または BGP ネットワークに接続されている場合や、FortiGate ルーティング テーブルにスタティック ルートを手動で追加する場合は、これらのルートを RIP が有効なインタフェース上でアドバタイズするようにユニットを設定できます。

追加の詳細設定オプションは、カスタマイズ可能な GUI ウィジェットおよび CLI を使用して設定できます。たとえば、受信した更新または送信する更新を、ルート マップ、アクセス リスト、またはプレフィックス リストを使用してフィルタ処理できます。FortiGate ユニットではまた、指定されたオフセットをルートのメトリックに追加するオフセット リストもサポートされています。カスタマイズ可能な GUI ウィジェットの詳細については、260 ページの「」を参照してください。CLI ルーティング コマンドの詳細については、『*FortiGate CLI リファレンス*』の "router" の章を参照してください。

RIP 詳細設定オプションは、*[Router]*、*[Dynamic]*、*[RIP]* の順に選択して表示されるページの [Advanced Options] で設定されます。これらの詳細設定オプションを設定できるように、非表示になった設定を表示するには、[Advanced Options] を展開する必要があります。

[RIP] ページの [Advanced Options] セクション

[Advanced Options]	詳細設定オプションの表示と非表示を切り替えるには、 展開の矢印を選択します。
[Default Metric]	FortiGate ユニットが、FortiGate ルーティング テーブルに追加されたルートに割り当てるデフォルトのホップ カウントを入力します。 範囲は 1 ～ 16 です。 このメトリックはホップ カウントであり、1 が最適または最短であることを示します。 特に指定されていない限り、この値は [Redistribute] にも適用されます。
[Default-information-originate]	FortiGate ユニットの RIP が有効なネットワークへのデフォルト ルートを生成してアドバタイズする場合に選択します。生成されるルートは、ダイナミック ルーティング プロトコルを介して学習されたルート、ルーティング テーブル内のルート、またはその両方に基づいている可能性があります。

[RIP Timers]	デフォルトの RIP タイマ設定を置き換えるための新しい値を入力します。これらのデフォルト設定は、ほとんどの設定で有効です。これらの設定を変更する場合は、新しい設定がローカル ルータやアクセス サーバと互換性があることを確認してください。 [Update] タイマが [Timeout] または [Garbage] タイマより小さい場合は、エラーが表示されます。
[Update]	FortiGate ユニットが RIP 更新を送信する間に待つ時間 (秒単位) を入力します。
[Timeout]	ルートに関する更新が受信されなくても、そのルートが到達可能と見なされる最長時間 (秒単位) を入力します。これは、ルートに関する更新が受信されなくても、FortiGate ユニットがその到達可能なルートをルーティング テーブル内に保持する最長時間です。[Timeout] の期間が切れる前に FortiGate ユニットがそのルートに関する更新を受信すると、タイマは再起動されます。 [Timeout] の期間は、[Update] の期間の少なくとも 3 倍の長さにする必要があります。
[Garbage]	FortiGate ユニットがルーティング テーブルからルートを削除するまでにそのルートを到達不可としてアドバタイズする時間 (秒単位) を入力します。この値によって、到達不可のルートがルーティング テーブル内に保持される期間が決定されます。
[Redistribute]	RIP を介して学習されなかったルートに関する RIP 更新を再配布するには、1 つ以上のオプションを選択します。FortiGate ユニットは、RIP を使用して、直接接続されたネットワーク、スタティック ルート、OSPF、および BGP から学習されたルートを再配布できます。
[Connected]	直接接続されたネットワークから学習されたルートを再配布する場合にオンにします。これらのルートのホップ カウントを指定するには、[Metric] を選択し、[Metric] フィールドにホップ カウントを入力します。ホップ カウントの有効な範囲は 1 ～ 16 です。
[Static]	スタティック ルートから学習されたルートを再配布する場合にオンにします。これらのルートのホップ カウントを指定するには、[Metric] を選択し、[Metric] フィールドにホップ カウントを入力します。範囲は 1 ～ 16 です。
[OSPF]	OSPF を介して学習されたルートを再配布する場合にオンにします。これらのルートのホップ カウントを指定するには、[Metric] を選択し、[Metric] フィールドにホップ カウントを入力します。範囲は 1 ～ 16 です。
[BGP]	BGP を介して学習されたルートを再配布する場合にオンにします。これらのルートのホップ カウントを指定するには、[Metric] を選択し、[Metric] フィールドにホップ カウントを入力します。範囲は 1 ～ 16 です。

RIP が有効なインタフェース

RIP インタフェース オプションを使用すると、RIP が有効なネットワークに接続されたすべての FortiGate ユニット インタフェースに適用されるグローバルな RIP 設定を置き換えることができます。たとえば、RIP が有効なネットワークのサブネットに接続されたインタフェース上の RIP アドバタイズを抑制する場合は、そのインタフェースを受動的に動作するように設定できます。受動的なインタフェースは RIP 更新を待機しますが、RIP 要求には応答しません。

インタフェース上で RIP バージョン 2 が有効になっている場合は、FortiGate ユニットが隣接ルータからの更新を受け付ける前にそのルータを確実に認証できるようにパスワード認証を選択することもできます。ユニットと隣接ルータの両方に同じパスワードが設定されている必要があります。認証によって、更新パケットの正当性が保証されますが、パケット内のルーティング情報の機密性は保証されません。

RIP が有効なインタフェースは、*[Router]*、*[Dynamic]*、*[RIP]* の順に選択して表示される画面で設定されます。

注記：スプリット ホライズンやキー チェーンなどの追加オプションは、CLI を使用してインタフェースごとに設定できます。詳細については、『*FortiGate CLI リファレンス*』の `router` の章を参照してください。

[New/Edit RIP Interface] ページ

RIP インタフェースを設定するための各設定を提供します。[RIP] ページの [Interfaces] セクションで [Create New] を選択すると、[New/Edit RIP Interface] ページに自動的にリダイレクトされます。

[Interface]	これらの設定を適用する FortiGate インタフェースの名前を選択します。このインタフェースは、RIP が有効なネットワークに接続されている必要があります。このインタフェースには、仮想 IPSec または GRE インタフェースを指定できます。
[Send Version]、[Receive Version]	このインタフェースを介して更新を送受信するためのデフォルトの RIP 互換性設定を置き換える場合に、RIP バージョンを [1]、[2]、または [Both] から選択します。
[Authentication]	指定したインタフェースでの RIP 交換の認証方法を選択します。 **[None]** — 認証を無効にします。 **[Text]** — このインタフェースが、RIP バージョン 2 を実行しているネットワークに接続されている場合に選択します。*[Password]* フィールドに、パスワード (最大 35 文字) を入力します。FortiGate ユニットと RIP 更新ルータの両方に同じパスワードが設定されている必要があります。このパスワードは、ネットワーク上をクリア テキストで送信されます。 **[MD5]** — MD5 を使用して交換を認証します。
[Password]	認証のためのパスワードを入力します。
[Passive Interface]	指定したインタフェースを介した FortiGate ユニットのルーティング情報のアドバタイズを抑制する場合に選択します。このインタフェースが RIP 要求に正常に応答できるようにするには、このチェック ボックスをオフにします。

OSPF

OSPF (Open Shortest Path First) は、同じ自律システム (AS) 内のルータ間でルーティング情報を共有するために、大規模な異種ネットワークで最もよく使用されているリンク状態ルーティング プロトコルです。FortiGate ユニットは、OSPF バージョン 2 (RFC 2328 を参照) をサポートしています。

OSPF の主な利点は、 指定された間隔ごとにではなく、 隣接機器の状態が変更された場合にのみルートをアドバタイズするため、 ルーティングのオーバーヘッドが削減される点にあります。

このトピックには、以下の内容が含まれています。

- OSPF AS の定義 - 概要
- 基本的な OSPF 設定
- OSPF 詳細設定オプション
- OSPF エリアの定義
- OSPF ネットワーク
- OSPF インタフェースの動作パラメータ

OSPF AS の定義 - 概要

OSPF 自律システム (AS) の定義には、次の操作が含まれます。

- 1 つ以上の OSPF エリアの特性の定義
- 定義した OSPF エリアと、その OSPF AS に含めるローカル ネットワークの間の関連付けの作成
- 必要に応じて、OSPF が有効なインタフェースの設定の調整

Web ベース マネージャを使用してこれらのタスクを実行する場合は、下に要約されている手順に従ってください。

基本的な OSPF 設定

OSPF 設定を設定する場合は、OSPF を有効にする AS を定義するとともに、その AS に参加する FortiGate インタフェースを指定する必要があります。AS の定義の一部として、AS エリアを指定し、それらのエリアに含めるネットワークを指定します。また、FortiGate インタフェース上の OSPF 動作に関連付けられた設定を調整することもできます。

OSPF 設定は、*[Router]*、*[Dynamic]*、*[OSPF]* の順に選択して表示される画面で設定されます。

[OSPF] ページ

OSPF のために作成したすべてのエリア、ネットワーク、およびインタフェースを表示します。

[Router ID] FortiGate ユニットを他の OSPF ルータと区別するための一意のルータ ID を入力します。慣例により、ルータ ID は、OSPF AS 内のいずれかの FortiGate インタフェースに割り当てられた数値的に最も大きい IP アドレスです。
インタフェース上に OSPF が設定されている間にルータ ID を変更すると、OSPF 隣接機器へのすべての接続が一時的に停止します。これらの接続は自動的に再確立されます。
ルータ ID が明示的に設定されていない場合は、VDOM またはユニットの最も大きい IP アドレスが使用されます。

[Advanced Options] OSPF 詳細設定の表示と非表示を切り替えるには、展開の矢印を選択します。詳細については、252 ページの「OSPF 詳細設定オプション」を参照してください。

[OSPF] ページの [Areas] セクション

OSPF AS を構成しているエリアに関する情報。OSPF パケットのヘッダには、AS 内にあるパケットの発信元の識別に役立つエリア ID が含まれています。

[Create New] 新しい OSPF エリアを定義して [Areas] リストに追加します。詳細については、253 ページの「OSPF エリアの定義」を参照してください。

[Edit] エリアの設定を変更する場合に選択します。

[Delete] [Areas] リストからエリアを削除する場合に選択します。

[Area] ドット区切り 10 進数で表記された、AS 内にあるエリアの一意の 32 ビット識別子。エリア ID 0.0.0.0 は AS のバックボーンを参照しており、 変更や削除はできません。

[Type] AS 内のエリアの種類には、次のものがあります。
- *[Regular]* - 通常の OSPF エリア
- *[NSSA]* - NSSA
- *[Stub]* - スタブ エリア

詳細については、253 ページの「OSPF エリアの定義」を参照してください。

[Authentication] 各エリアにリンクされているすべてのFortiGateインタフェースを介して送受信された OSPF パケットを認証するための方法。
[None] — 認証は無効になります。
[Text] — テキスト ベースの認証が有効になります。
[MD5] — MD5 認証が有効になります。
[Interfaces] に表示されているように、エリア内の一部のインタフェースに対して別の認証設定が適用される可能性があります。たとえば、あるエリアで単純なパスワードを認証に使用している場合は、そのエリア内の 1 つ以上のネットワークに対して別のパスワードを設定できます。

[OSPF] ページの [Networks] セクション

OSPF AS 内のネットワークと、それぞれのエリア ID。[Networks] リストにネットワークを追加すると、そのネットワークに含まれているすべての FortiGate インタフェースが OSPF リンク状態アドバタイズメントでアドバタイズされます。OSPF ネットワーク アドレス空間に一致する IP アドレスを持つすべての FortiGate インタフェース上で OSPF を有効にすることができます。詳細については、253 ページの「OSPF ネットワーク」を参照してください。

[Create New] AS にネットワークを追加し、そのエリア ID を指定して、その定義を [Networks] リストに追加します。

[Edit] エリアの設定を変更する場合に選択します。

[Delete] [Areas] リストからエリアを削除する場合に選択します。

[Network] OSPF を実行している AS 内のネットワークの IP アドレスとネットワーク マスク。FortiGate ユニットは、そのネットワークに接続された物理または VLAN インタフェースを備えている可能性があります。

[Area] OSPF ネットワーク アドレス空間に割り当てられたエリア ID。

[OSPF] ページの [Interfaces] セクション

FortiGate インタフェース上の OSPF 動作を調整するために必要な任意の追加の設定。詳細については、254 ページの「OSPF インタフェースの動作パラメータ」を参照してください。

[Create New] ユニット インタフェースの追加または別の OSPF 動作パラメータを作成し、その設定を [Interfaces] リストに追加します。

[Edit] エリアの設定を変更する場合に選択します。

[Delete] [Areas] リストからエリアを削除する場合に選択します。

[Name] OSPF インタフェース定義の名前。

[Interface]	同じエリア内の他のすべてのインタフェースに割り当てられたデフォルト値とは異なる OSPF 設定を持つ FortiGate 物理または VLAN インタフェースの名前。
[IP]	追加または別の設定を持つ OSPF が有効なインタフェースの IP アドレス。
[Authentication]	OSPF が有効な特定のインタフェース上で送受信された LSA 交換を認証するための方法。これらの設定によって、そのエリアの [Authentication] 設定が置き換えられます。

OSPF 詳細設定オプション

OSPF 詳細設定オプションを選択することによって、FortiGate ユニットが OSPF リンク状態アドバタイズメント以外の何らかの手段によって学習したルートを再配布するためのメトリックを指定できます。たとえば、FortiGate ユニットが RIP または BGP ネットワークに接続されている場合や、FortiGate ルーティング テーブルにスタティック ルートを手動で追加する場合は、これらのルートを OSPF が有効なインタフェース上でアドバタイズするようにユニットを設定できます。

追加の詳細設定オプションは、カスタマイズ可能な GUI ウィジェットおよび CLI を使用して設定できます。たとえば、受信した更新または送信する更新を、ルート マップ、アクセス リスト、またはプレフィックス リストを使用してフィルタ処理できます。FortiGate ユニットではまた、指定されたオフセットをルートのメトリックに追加するオフセット リストもサポートされています。カスタマイズ可能な GUI ウィジェットの詳細については、260 ページの「」を参照してください。CLI ルーティング コマンドの詳細については、『*FortiGate CLI リファレンス*』の "router" の章を参照してください。

OSPF 詳細設定オプションは、*[Router]*、*[Dynamic]*、*[RIP]* の順に選択して表示される画面にあります。これらのオプションにアクセスするには、このページで [Advanced Options] を展開する必要があります。

[OSPF] ページ上の [Advanced Options]

[Router ID]	FortiGate ユニットを他の OSPF ルータと区別するための一意のルータ ID を入力します。
展開の矢印	[Advanced Options] の表示と非表示を切り替える場合に選択します。
[Default Information]	OSPF AS へのデフォルト（ 外部 ）ルートを生成してアドバタイズします。 生成されるルートは、ダイナミック ルーティング プロトコルを介して学習されたルート、ルーティング テーブル内のルート、 またはその両方に基づくことができます。
[None]	デフォルト ルートが生成されないようにします。
[Regular]	OSPF AS へのデフォルト ルートを生成し、そのルートが FortiGate ルーティング テーブルに格納される場合のみ、そのルートを隣接する自律システムにアドバタイズします。
[Always]	OSPF AS へのデフォルト ルートを生成し、そのルートが FortiGate ルーティング テーブルに格納されない場合であっても、そのルートを隣接する自律システムに無条件にアドバタイズします。
[Redistribute]	OSPF を介して学習されなかったルートに関する OSPF リンク状態アドバタイズメントを再配布するには、表示されている 1 つ以上のオプションを選択します。FortiGate ユニットは、OSPF を使用して、直接接続されたネットワーク、スタティック ルート、RIP、および BGP から学習されたルートを再配布できます。
[Connected]	直接接続されたネットワークから学習されたルートを再配布する場合にオンにします。 [Metric] フィールドに、これらのルートのコストを入力します。範囲は 1 ～ 16,777,214 です。
[Static]	スタティック ルートから学習されたルートを再配布する場合にオンにします。 [Metric] フィールドに、これらのルートのコストを入力します。範囲は 1 ～ 16,777,214 です。
[RIP]	RIP を介して学習されたルートを再配布する場合にオンにします。 [Metric] フィールドに、これらのルートのコストを入力します。範囲は 1 ～ 16,777,214 です。
[BGP]	BGP を介して学習されたルートを再配布する場合にオンにします。 [Metric] フィールドに、これらのルートのコストを入力します。範囲は 1 ～ 16,777,214 です。

OSPF エリアの定義

エリアによって、OSPF AS の一部が論理的に定義されます。各エリアは、ドット区切り 10 進数表記 (たとえば、192.168.0.1) で表現された 32 ビットのエリア ID によって識別されます。エリア ID 0.0.0.0 は、OSPF ネットワーク バックボーンのために予約されています。AS の残りのエリアを、通常、スタブ、または NSSA として分類できます。

通常エリアには、そのエリアへの OSPF が有効なインタフェースを、それぞれが少なくとも 1 つは備えた複数のルータが含まれます。

OSPF バックボーンに到達するには、スタブ エリア内のルータはパケットをエリア境界ルータに送信する必要があります。OSPF 以外のドメインにつながるルートは、スタブ エリア内のルータにはアドバタイズされません。エリア境界ルータは、OSPF AS に、スタブ エリアへの単一のデフォルト ルート (宛先は 0.0.0.0) をアドバタイズします。これにより、特定のルートに該当しない OSPF パケットはすべてデフォルト ルートに従うことが保証されます。スタブ エリアに接続されたルータはすべて、そのスタブ エリアの一部と見なされます。

NSSA (Not-So-Stubby Area) では、そのエリアから出て OSPF 以外のドメインにつながるルートが OSPF AS に通知されます。ただし、そのエリア自体は、AS の他の部分によって引き続きスタブ エリアのように扱われます。

通常エリアとスタブ エリア (NSSA を含む) は、エリア境界ルータを介して OSPF バックボーンに接続されます。

OSPF の定義は、*[Router]*、*[Dynamic]*、*[OSPF]* の順に選択して表示される画面で設定されます。

注記： 必要に応じて、OSPF バックボーンへの物理的な接続が失われたエリアへの仮想リンクを定義できます。仮想リンクは、エリア境界ルータとして機能する 2 つの FortiGate ユニット間にのみ設定できます。仮想リンクの詳細については、『*FortiGate CLI リファレンス*』を参照してください。

[New/Edit OSPF Area] ページ

OSPF エリアを定義するための設定を提供します。[OSPF] ページの [Areas] セクションで [Create New] を選択すると、[New/Edit OSPF Area] ページに自動的にリダイレクトされます。

[Area] このエリアの 32 ビット識別子を入力します。この値は、ドット区切り 10 進数表記の IP アドレスと同じ形式にする必要があります。OSPF エリアを作成した後、エリア IP の値を変更することはできません。そのエリアを削除して、やり直す必要があります。

[Type] そのエリアに割り当てられるネットワークの特性を分類するためのエリアの種類を選択します。
[Regular] — エリアに、そのエリアへの OSPF が有効なインタフェースをそれぞれが少なくとも 1 つは備えた複数のルータを含める場合。
[NSSA] — 外部の OSPF 以外のドメインへのルートを OSPF AS に通知するが、そのエリアは AS の他の部分によってスタブ エリアのように扱われるようにする場合。
[STUB] — エリア内のルータがバックボーンに到達するにはパケットをエリア境界ルータに送信する必要があり、OSPF 以外のドメインへのルートがエリア内のルータにアドバタイズされないようにする場合。

[Authentication] エリア内のすべてのインタフェースを介して送受信された OSPF パケットを認証するための方法を選択します。
[None] — 認証を無効にします。
[Text] — プレーン テキストのパスワードを使用して LSA 交換を認証するためにテキスト ベースのパスワード認証を有効にします。このパスワードは、ネットワーク上をクリア テキストで送信されます。
[MD5] — MD5 暗号化ハッシュ (RFC 1321) を使用して、MD5 ベースの認証を有効にします。
必要に応じて、そのエリア内の 1 つ以上のインタフェースに対してこの設定を置き換えることができます。詳細については、254 ページの「OSPF インタフェースの動作パラメータ」を参照してください。

OSPF ネットワーク

OSPF エリアによって、いくつかの隣接ネットワークがグループ化されます。 ネットワーク アドレス空間にエリア ID を割り当てると、 そのエリアの属性がネットワークに関連付けられます。

ネットワークへの OSPF エリア ID の割り当ては、*[Router]*、*[Dynamic]*、*[OSPF]* の順に選択して表示される画面で設定されます。ネットワークに OSPF エリア ID を割り当てるには、このページの [Networks] セクションを使用する必要があります。

[New/Edit OSPF Network] ページ

エリア ID に割り当てられたネットワークを設定するための各設定を提供します。[OSPF] ページの [Networks] セクションで [Create New] を選択すると、[New/Edit OSPF Network] ページに自動的にリダイレクトされます。

[IP/Netmask] OSPFエリアに割り当てるローカル ネットワークのIPアドレスとネットワークマスクを入力します。

[Area] このネットワークのエリア ID を選択します。このエリアの属性は、指定したネットワークの特性およびトポロジに一致している必要があります。エリア ID を選択する前に、エリアを定義する必要があります。詳細については、253 ページの「OSPF エリアの定義」を参照してください。

OSPF インタフェースの動作パラメータ

OSPF インタフェース定義には、FortiGate の OSPF が有効なインタフェースの特定の動作パラメータが含まれています。この定義には、インタフェースの名前 (たとえば、external または VLAN_1)、インタフェースに割り当てられた IP アドレス、インタフェースを介して LSA 交換を認証するための方法、および OSPF の Hello パケットや停止間隔パケットを送受信するためのタイマ設定が含まれます。

OSPF が有効なネットワーク エリアに一致する IP アドレスを持つすべての FortiGate インタフェース上で OSPF を有効にすることができます。たとえば、0.0.0.0 のエリアを定義し、OSPF ネットワークを 10.0.0.0/16 として定義します。次に、vlan1 を 10.0.1.1/24 として、vlan2 を 10.0.2.1/24 として、vlan3 を 10.0.3.1/24 として定義します。これらの 3 つの VLAN がすべて、エリア 0.0.0.0 で OSPF を実行できます。すべてのインタフェースを有効にするには、OSPF ネットワーク 0.0.0.0/0 を作成します。

インタフェースの MD5 キーの動作パラメータを入力するとき、次の特殊文字はサポートされません。

- < >
- #
- ( )
- "
- '

インタフェースに複数のIPアドレスが割り当てられている場合は、同じFortiGateインタフェースに対して異なる OSPF パラメータを設定できます。たとえば、異なるサブネットを介して、2 つの隣接機器に同じ FortiGate インタフェースを接続できます。ある隣接機器の設定との互換性のために、Hello および停止間隔パラメータの 1 つのセットを含む OSPF インタフェース定義を設定すると同時に、2 つ目の隣接機器の設定との互換性を保証するために、同じインタフェースの 2 つ目の OSPF インタフェース定義を設定できます。

OSPF 動作パラメータは、*[Router]*、*[Dynamic]*、*[OSPF]* の順に選択して表示されるページの [Interfaces] セクションで設定されます。

[New/Edit OSPF Interface] ページ

OSPF インタフェースを設定するための各設定を提供します。[OSPF] ページの [Interfaces] セクションで [Create New] を選択すると、[New/Edit OSPF Interface] ページに自動的にリダイレクトされます。

[Name] OSPF インタフェース定義を識別するための名前を入力します。たとえば、そのインタフェースのリンク先の OSPF エリアを示す名前にすることができます。

[Interface] この OSPF インタフェース定義に関連付ける FortiGate インタフェースの名前 (たとえば、port1、external、VLAN_1) を選択します。FortiGate ユニットは、OSPF が有効なネットワークに接続された物理、VLAN、仮想 IPSec、または GRE インタフェースを備えている可能性があります。

[IP] OSPF が有効なインタフェースに割り当てられている IP アドレスを入力します。このインタフェースは、IP アドレスが OSPF ネットワーク アドレス空間に一致するため、OSPF が有効なインタフェースになります。
たとえば、`172.20.120.0/24` の OSPF ネットワークを定義しており、port1 に IP アドレス `172.20.120.140` が割り当てられている場合は、「`172.20.120.140`」を入力します。

[Authentication] 指定したインタフェースでの LSA 交換のための認証方法を選択します。
[None] — 認証を無効にします。
[Text] — プレーン テキストのパスワードを使用して LSA 交換を認証します。このパスワードは最大 35 文字であり、ネットワーク上をクリア テキストで送信されます。
[MD5] — 1 つ以上のキーを使用して MD5 暗号化ハッシュを生成します。

[Password] プレーン テキストのパスワードを入力します。最大 15 文字の英数字の値を入力します。この FortiGate インタフェースにリンク状態アドバタイズメントを送信する OSPF 隣接機器にも、同じパスワードが設定されている必要があります。このフィールドは、プレーン テキスト認証を選択した場合にのみ使用できます。

[MD5 Keys] [ID] フィールドに (最初の) パスワードのキー識別子 (範囲は 1 ～ 255) を入力した後、[Key] フィールドにそれに関連付けられたパスワードを入力します。このパスワードは、最大 16 文字の英数字文字列で表された 128 ビットのハッシュです。これらの文字を入力するとき、< >、( )、#、″、および ' はサポートされていないため、これらの文字を使用しないでください。
この FortiGate インタフェースにリンク状態アドバタイズメントを送信する OSPF 隣接機器にも、同じ MD5 キーが設定されている必要があります。OSPF 隣接機器が MD5 ハッシュの生成に複数のパスワードを使用している場合は、[Add] アイコンを選択してリストに MD5 キーを追加します。
このフィールドは、MD5 認証を選択した場合にのみ使用できます。

[Hello Interval] 必要に応じて、すべての OSPF 隣接機器上の [Hello Interval] 設定と互換性があるように [Hello Interval] を設定します。
この設定によって、FortiGate ユニットがこのインタフェースを介して Hello パケットを送信する間に待つ期間 (秒単位) が定義されます。

[Dead Interval] 必要に応じて、すべての OSPF 隣接機器上の [Dead Interval] 設定と互換性があるように [Dead Interval] を設定します。
この設定によって、FortiGate ユニットがこのインタフェースを介して OSPF 隣接機器から Hello パケットを受信するまでに待つ期間 (秒単位) が定義されます。指定された時間内に FortiGate ユニットが Hello パケットを受信しない場合、FortiGate ユニットは、この隣接機器をアクセス不可として宣言します。
慣例により、[Dead Interval] の値は一般に [Hello Interval] の値の 4 倍です。

BGP

BGP (Border Gateway Protocol) は、異なる ISP ネットワーク間でルーティング情報を交換するために ISP によって一般に使用されるインターネット ルーティング プロトコルです。たとえば、BGP を使用すると、ISP ネットワークと、RIP や OSPF、またはその両方を使用して自律システム (AS) 内でパケットをルーティングしている AS の間でネットワーク パスを共有できます。FortiGate での BGP の実装は BGP-4 をサポートしており、RFC 1771 および RFC 2385 に準拠しています。

注記: グレースフル リスタートやその他の詳細設定は、CLI コマンドを使用してのみ設定できます。BGP 詳細設定の詳細については、『*FortiGate CLI リファレンス*』の `router` の章を参照してください。

BGP を設定する場合は、FortiGate ユニットが属している AS を指定するとともに、このユニットを他の BGP ルータと区別するためのルータ ID を入力する必要があります。また、FortiGate ユニットの BGP 隣接機器を識別し、それらの BGP 隣接機器に FortiGate ユニットのどのローカル ネットワークをアドバタイズするかを指定することも必要です。

BGP 設定は、*[Router]*、*[Dynamic]*、*[BGP]* の順に選択して表示される画面で設定されます。Web ベース マネージャによって、基本的な BGP オプションを設定するための簡略化されたユーザ インタフェースが提供されます。また、CLI を使用して多くの BGP 詳細設定オプションを設定することもできます。詳細については、『*FortiGate CLI リファレンス*』の `router` の章を参照してください。

[BGP] ページ

作成したすべての隣接機器およびネットワークを表示します。このページではまた、隣接機器、ネットワーク、およびローカル AS を設定することもできます。また、4 バイトの AS パスも設定できます。4 バイトの AS パスの設定に関する追加情報が必要な場合は、RFC 4893 を参照してください。

[Local AS] FortiGate ユニットが属しているローカル AS の番号を入力します。

[Router ID] FortiGate ユニットを他の BGP ルータと区別するための一意のルータ ID を入力します。このルータ ID は、ドット区切り 10 進数の形式（たとえば、192.168.0.1）で記述された IP アドレスです。
インタフェース上に BGP が設定されている間にルータ ID を変更すると、BGP ピアへのすべての接続が一時的に停止します。これらの接続は自動的に再確立されます。
ルータ ID が明示的に設定されていない場合は、VDOM の最も大きい IP アドレスが使用されます。

[BGP] ページの [Neighbors] セクション

隣接する自律システム内にある BGP ピアの IP アドレスと AS 番号。

[IP] BGP が有効なネットワークへの隣接機器インタフェースの IP アドレスを入力します。

[Remote AS] この隣接機器が属している AS の番号を入力します。

[Add/Edit] [Neighbors] リストに隣接機器情報を追加するか、またはリスト内のエントリを編集します。

[Neighbor] BGP ピアの IP アドレス。

[Remote AS] この BGP ピアに関連付けられている自律システムの番号。

[Delete] BGP 隣接機器エントリを削除します。

[BGP] ページの [Networks] セクション

BGP ピアにアドバタイズするネットワークの IP アドレスとネットワーク マスク。FortiGate ユニットは、それらのネットワークに接続された物理または VLAN インタフェースを備えている可能性があります。

[IP/Netmask] アドバタイズされるネットワークの IP アドレスとネットマスクを入力します。

[Add] [Networks] リストにネットワーク情報を追加します。

[Network] BGP ピアにアドバタイズされる主要なネットワークの IP アドレスとネットワークマスク。

[Delete] BGP ネットワーク定義を削除します。

注記：`get router info bgp` CLI コマンドによって、設定された BGP 設定に関する詳細情報が提供されます。コマンド オプションの完全なリストについては、『*FortiGate CLI リファレンス*』の `router` の章を参照してください。

マルチキャスト

FortiGate ユニットは、ルート バーチャル ドメイン内で PIM (Protocol Independent Multicast) バージョン 2 ルータとして動作できます。FortiGate ユニットは、PIM スパース モード (RFC 2362) および PIM デンス モード (RFC 3973) をサポートしており、FortiGate インタフェースが接続されているネットワーク セグメント上のマルチキャスト サーバまたはレシーバにサービスを提供できます。

注記：基本的なオプションは、Web ベース マネージャで設定できます。多くの追加オプションが使用できますが、それらのオプションは CLI からのみ使用できます。CLI コマンドを使用して PIM 設定を設定する方法の詳細な説明および例については、『*FortiGate CLI リファレンス*』の `router` の章にある `multicast` を参照してください。

マルチキャスト (PIM) ルーティングが有効になっている場合は、任意の FortiGate インタフェース上でスパース モードまたはデンス モード動作を設定できます。

PIM 設定は、*[Router]*、*[Dynamic]*、*[Multicast]* の順に選択して表示される画面で設定されます。Web ベース マネージャによって、基本的な PIM オプションを設定するための簡略化されたユーザ インタフェースが提供されます。また、CLI を使用して PIM 詳細設定オプションを設定することもできます。詳細については、『*FortiGate CLI リファレンス*』の "router" の章を参照してください。

[Multicast] ページ

作成した個々のマルチキャスト ルートを表示します。このページではまた、各マルチキャスト ルートを設定したり、RP アドレスを追加したりすることもできます。

[Enable Multicast Routing]	PIM バージョン 2 のルーティングを有効にする場合にオンにします。カプセル化されたパケットやカプセル化解除されたデータが発信元と宛先の間を通過できるようにするには、PIM が有効なインタフェース上でファイアウォール ポリシーを作成する必要があります。
[Static Rendezvous Points (RPs)]	スパース モード動作に必要な場合は、マルチキャスト グループのためのパケット配布ツリーのルートとして使用できるランデブー ポイント (RP) の IP アドレスを入力します。マルチキャスト グループからの結合メッセージや、発信元からのデータが RP に送信されます。 指定された IP のマルチキャスト グループの RP がすでにブート ストラップ ルータ (BSR) に通知されている場合は、BSR に通知されている RP が使用され、指定した静的 RP アドレスは無視されます。
[Apply]	指定した静的 RP アドレスを保存します。
[Create New]	インタフェースの新しいマルチキャスト エントリを作成します。 この新しいエントリを使用して、特定の FortiGate インタフェース上の PIM 動作を微調整したり、特定のインタフェース上のグローバルな PIM 設定を置き換えたりすることができます。詳細については、257 ページの「インタフェース上のマルチキャスト設定の置き換え」を参照してください。
[Interface]	特定の PIM 設定を持つ FortiGate インタフェースの名前。
[Mode]	そのインタフェース上の PIM 動作のモード (*[Sparse]* または *[Dense]*)。
[Status]	このインタフェース上のスパース モード RP 候補のステータス。 インタフェース上の RP 候補のステータスを変更するには、そのインタフェースに対応する行にある [編集] アイコンを選択します。
[Priority]	そのインタフェース上の RP 候補に割り当てられたプライオリティ番号。RP 候補が有効になっている場合にのみ使用できます。
[DR Priority]	このインタフェース上の指定ルータ (DR) 候補に割り当てられたプライオリティ番号。スパース モードが有効になっている場合にのみ使用できます。
[Delete]	このインタフェース上の PIM 設定を削除する場合に選択します。
[Edit]	このインタフェース上の PIM 設定を変更する場合に選択します。

このトピックには、以下の内容が含まれています。

インタフェース上のマルチキャスト設定の置き換え

PIM ドメインに接続された FortiGate インタフェースの動作パラメータを設定するには、マルチキャスト (PIM) インタフェース オプションを使用します。たとえば、PIM が有効なネットワーク セグメントに接続されたインタフェース上でデンス モードを有効にすることができます。スパース モードが有効になっている場合は、インタフェース上のランデブー ポイント (RP) または指定ルータ (DR) 候補のアドバタイズに使用されるプライオリティ番号を調整できます。

インタフェース上のマルチキャスト設定の置き換えは、*[Router]*、*[Dynamic]*、*[Multicast]* の順に選択して表示される画面で設定されます。

[New] ページ

新しいマルチキャスト インタフェースを設定するための各設定を提供します。[Multicast] ページで [Create New] を選択すると、[New] ページに自動的にリダイレクトされます。

[Interface]	これらの設定を適用するルート VDOM FortiGate インタフェースの名前を選択します。このインタフェースは、PIM バージョン 2 が有効なネットワーク セグメントに接続されている必要があります。
[PIM Mode]	動作のモードを [Sparse Mode] または [Dense Mode] から選択します。同じネットワーク セグメントに接続されたすべての PIM ルータが同じ動作モードを実行している必要があります。[Sparse Mode] を選択した場合は、残りのオプションを以下の説明に従って調整します。

[DR Priority]	FortiGate ユニットのインタフェース上の DR 候補をアドバタイズするためのプライオリティ番号を入力します。範囲は 1 ～ 4,294,967,295 です。 ユニットは、この値を同じネットワーク セグメント上の他のすべての PIM ルータの DR インタフェースと比較し、DR プライオリティの最も高いルータを DR として選択します。
[RP Candidate]	このインタフェース上の RP 候補を有効にします。
[RP Candidate Priority]	FortiGateインタフェース上のRP候補をアドバタイズするためのプライオリティ番号を入力します。範囲は 1 ～ 255 です。

マルチキャスト宛先 NAT

マルチキャスト宛先 NAT (DNAT) を使用すると、外部から受信したマルチキャスト宛先アドレスを、組織の内部のアドレッシング ポリシーに従うアドレスに変換できます。

CLI でのみ使用できるこの機能を使用すると、RPF (Reverse Path Forwarding) が正しく機能するように、ルートが変換境界でネットワーク インフラストラクチャに再配布されることを回避できます。また、ネットワーク内の 2 つの入力ポイントから同一のフィードを受信し、それらを独立にルーティングすることもできます。

マルチキャスト DNAT は、CLI で次のコマンドを使用して設定します。

```
config firewall multicast-policy
  edit p1
    set dnat <dnatted-multicast-group>
    set ...
  next
  end
```

詳細については、『*FortiGate CLI リファレンス*』の `firewall` の章を参照してください。

BFD (Bi-directional Forwarding Detection)

BFD (Bi-directional Forwarding Detection) プロトコルは、ネットワーク上のデバイス障害を検出し、これらの障害を回避して再ルーティングするためのきめ細かさがダイナミック ルーティング プロトコルに不足していることに対処するように設計されています。BFD は、障害をミリ秒単位のタイマで検出できるため、これらの障害によりすばやく対応できます。これに対して、他のダイナミック ルーティング プロトコルでは秒単位のタイマでしか検出できません。

ユニットは、OSPF および BGP 動的ネットワーキングの一部として BFD をサポートしています。

注記：BFD は、CLI からのみ設定できます。

このトピックには、以下の内容が含まれています。

- BFD の設定
- FortiGate ユニット上での BFD の設定
- 特定のインタフェースの BFD の無効化

BFD の設定

BFD は、BGP または OSPF ルーティング プロトコルを使用するネットワークを対象にしています。一般に、より小規模なネットワークは除外されます。

FortiGate ユニット上での BFD の設定は、非常に柔軟です。ユニット全体に対して BFD を有効にした後、1 つまたは 2 つのインタフェースに対して無効にすることができます。あるいは、隣接ルータまたはインタフェースごとに個別に BFD を有効にすることができます。どちらの方法を選択するかは、ネットワークに必要な設定の量によって決定されます。

タイムアウト期間によって、ユニットが、ある接続に停止としてラベルを付けるまでに待つ期間が決定されます。このタイムアウト期間の長さは重要です。この期間が短すぎると、接続にあまりにも早く停止としてラベルが付けられます。また、長すぎると、停止している接続からの応答を待つ時間が浪費されます。この数値はネットワークやユニットによって異なるため、単純には決まりません。ハイエンドの FortiGate モデルは、トラフィックによる負荷で停止していない限り、非常にすばやく応答します。また、ネットワークの規模が大きい場合も応答時間が低下します。より小規模なネットワークに比べて、パケットが多くのホップを通過する必要があります。これらの 2 つの要因 (CPU 負荷とネットワーク トラバース時間) が、選択すべきタイムアウト期間の長さに影響を与えます。タイムアウト期間が短すぎる場合、BFD はネットワーク デバイスに接続されませんが、接続を試行し続けます。この状態によって不必要なネットワーク トラフィックが生成されるだけでなく、デバイスが監視されていない状態に置かれたままになります。この状態が発生した場合は、BFD がより多くの時間をかけてネットワーク上のデバイスを検出できるように、より長いタイムアウト期間の設定を試みる必要があります。

FortiGate ユニット上での BFD の設定

この例では、FortiGate ユニット上で、デフォルト値を使用して BFD を有効にしています。つまり、接続が確立された後、BFD ルータを停止していると宣言してトラフィックを再ルーティングするまでに、ユニットはそのルータからの応答を最大 150 ミリ秒 (最小転送間隔 50 ミリ秒 × 検出乗数 3) 待ちます。`bfd-dont-enforce-src-port` の無効化によって示されているように、セキュリティ上の理由から、BFD トラフィックの発信元のポートがチェックされます。

```
config system settings
   set bfd enable
   set bfd-desired-min-tx 50
   set bfd-required-min-rx 50
   set bfd-detect-mult 3
   set bfd-dont-enforce-src-port disable
end
```

注記 : 最小受信間隔 (`bfd-required-min-rx`) と検出乗数 (`bfd-detect-mult`) の組み合わせによって、ユニットが隣接機器を停止していると宣言するまでに応答を待つ期間が決定されます。実際の状況での正しい値は、ネットワークの規模やユニットの CPU 速度によって異なります。この例で使用されている数値が、実際のネットワークでは機能しない可能性があります。

特定のインタフェースの BFD の無効化

前の例では、FortiGate ユニット全体に対して BFD を有効にしました。あるインタフェースが、BFD が有効ないずれかのルータに接続されていない場合は、そのインタフェースの BFD を無効にすることによってネットワーク トラフィックを削減できます。この例では、CLI コマンドを使用して、Internal インタフェースの BFD を無効にしています。

```
config system interface
   edit <interface>
   set bfd disable
end
```

BGP 上での BFD の設定

BGP ネットワーク上で BFD を設定するための手順は 1 つだけです。BFD をグローバルに有効にした後、このプロトコルを実行している各隣接機器に対して BFD を無効にします。

```
   config system settings
     set bfd enable
     end

   config router bgp
     config neighbor
```

```
    edit <ip_address>
    set bfd disable
  end
end
```

OSPF 上での BFD の設定

OSPF ネットワーク上での BFD の設定は、ユニット上での BFD の有効化とほとんど同じです。BFD を OSPF に対してグローバルに有効にした後、インタフェースのレベルでグローバル設定を置き換えることができます。

OSPF 上で BFD を有効にするには、次のコマンドを入力します。

```
configure routing OSPF
  set bfd enable
end
```

インタフェース上で BFD を置き換えるには、次のコマンドを入力します。

```
configure routing OSPF
  configure ospf-interface
  edit <interface_name>
    set bfd disable
  end
end
```

ルータ - モニタ

この項では、[Routing Monitor] リストの読み取り方について説明します。このリストには、FortiGate ルーティング テーブル内のエントリが表示されます。

FortiGate ユニット上でバーチャル ドメイン (VDOM) を有効にした場合、ルータの監視はバーチャル ドメインごとに別々に使用可能になります。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には、以下のトピックが含まれています。

ルーティング情報の表示

デフォルトでは、すべてのルートが [Routing Monitor] リストに表示されます。デフォルトのスタティック ルートは、" 任意の / すべての " パケットの宛先 IP アドレスに一致する、0.0.0.0/0 として定義されます。

ルーティング テーブル内のルートを表示するには、*[Router]*、*[Monitor]*、*[Routing Monitor]* の順に選択します。

[Routing Monitor] ページ

監視されているすべてのルート (デフォルトのスタティック ルートを含む) を表示します。このページではまた、フィルタを適用することによって、このページに表示されている情報をフィルタ処理することもできます。

[IP version] IPv4 または IPv6 ルートを選択します。表示されるフィールドは、選択されている IP バージョンによって異なります。
Web ベース マネージャで IPv6 の表示が有効になっている場合にのみ表示されます。

[Type] 次のいずれかのルート タイプを選択すると、ルーティング テーブルが検索され、選択したタイプのルートのみが表示されます。
[All] — ルーティング テーブル内に記録されているすべてのルートを表示します。
[Connected] — FortiGate インタフェースへの直接接続に関連付けられたすべてのルートを表示します。
[Static] — ルーティング テーブルに手動で追加されたスタティック ルートを表示します。詳細については、232 ページの「スタティック ルート」を参照してください。
[RIP] — RIP を介して学習されたすべてのルート。詳細については、247 ページの「RIP」を参照してください。
[OSPF] — OSPF を介して学習されたすべてのルート。詳細については、250 ページの「OSPF」を参照してください。
[BGP] — BGP を介して学習されたすべてのルート。詳細については、255 ページの「BGP」を参照してください。
[HA] — 高可用性 (HA) クラスタのプライマリ ユニットと副系ユニットの間で同期された RIP、OSPF、および BGP ルートを表示します。HA ルートは、副系ユニット上に保持され、仮想クラスタ内の下位のバーチャル ドメインとして設定されたバーチャル ドメインからルータ モニタを表示している場合にのみ表示されます。
IPv6 の IP バージョンが選択されている場合は表示されません。
HA ルーティングの同期の詳細については、『*FortiGate HA ユーザ ガイド*』を参照してください。

[Network] ルーティング テーブルを検索し、指定したネットワークに一致するルートを表示するための IP アドレスとネットマスク (たとえば、`172.16.14.0/24`) を入力します。
IPv6 の IP バージョンが選択されている場合は表示されません。

[Gateway] ルーティング テーブルを検索し、指定したゲートウェイに一致するルートを表示するための IP アドレスとネットマスク (たとえば、`192.168.12.1/32`) を入力します。
IPv6 の IP バージョンが選択されている場合は表示されません。

[Apply Filter] 指定した検索条件に基づいてルーティング テーブル内のエントリを検索し、一致したルートをすべて表示する場合に選択します。
IPv6 の IP バージョンが選択されている場合は表示されません。

[Type]	FortiGate のルートに割り当てられたタイプの値 ([Static]、[Connected]、[RIP]、[OSPF]、または [BGP])。 IPv6 の IP バージョンが選択されている場合は表示されません。
[Subtype]	該当する場合は、OSPF ルートに割り当てられたサブタイプの分類。 ・ 空の文字列は、エリア内のルートであることを示しています。宛先は、FortiGate ユニットが接続されているエリア内にあります。 ・ *[OSPF inter area]* — 宛先は OSPF AS 内にありますが、FortiGate ユニットがそのエリアに接続されていません。 ・ *[External 1]* — 宛先は OSPF AS の外部にあります。再配布されたルートのメトリックは、外部のコストと OSPF のコストを加算することによって計算されます。 ・ *[External 2]* — 宛先は OSPF AS の外部にあります。この場合、再配布されたルートのメトリックは外部のコストのみと等価であり、OSPF のコストとして表現されます。 ・ *[OSPF NSSA 1]* — [External 1] と同じですが、ルートは NSSA を介して受信されています。 ・ *[OSPF NSSA 2]* — [External 2] と同じですが、ルートは NSSA を介して受信されています。 IPv6 の IP バージョンが選択されている場合は表示されません。
[Network]	FortiGate ユニットが到達できる宛先ネットワークの IP アドレスとネットワーク マスク。
[Distance]	このルートに関連付けられたディスタンス。0 の値は、同じ宛先への他のルートよりこのルートが優先されることを示しています。 スタティック ルートに割り当てられたディスタンスを変更するには、236 ページの「ルーティング テーブルへのスタティック ルートの追加」を参照してください。ダイナミック ルートのこのディスタンスを変更するには、『*FortiGate CLI リファレンス*』を参照してください。
[Metric]	ルート タイプに関連付けられたメトリック。ルートのメトリックは、FortiGate ユニットがそのルートをルーティング テーブルに動的に追加するときの方法に影響します。メトリックの種類と、それらのメトリックが適用されるプロトコルは次のとおりです。 ・ *[Hop count]* — RIP を介して学習されたルート。 ・ *[Relative cost]* — OSPF を介して学習されたルート。 ・ *[Multi-Exit Discriminator (MED)]* — BGP を介して学習されたルート。ただし、宛先ネットワークへの最適なパスを決定するための属性は MED 以外にもいくつかあります。
[Gateway]	宛先ネットワークへのゲートウェイの IP アドレス。
[Interface]	パケットが宛先ネットワークのゲートウェイに転送されるときに使用されるインタフェース。
[Up Time]	RIP、OSPF、または BGP を介して学習されたルートが到達可能になるまでに要した合計の累積時間。 IPv6 の IP バージョンが選択されている場合は表示されません。

FortiGate ルーティング テーブルの検索

フィルタを適用することで、ルーティング テーブルを検索して特定のルートのみを表示できます。たとえば、1 つ以上のスタティック ルート、接続されたルート、RIP/OSPF/BGP を介して学習されたルート、および指定したネットワークまたはゲートウェイに関連付けられたルートを表示できます。

ルート タイプによってルーティング テーブルを検索し、その表示をさらにネットワークまたはゲートウェイに従って制限する場合、そのエントリが表示されるようにするには、検索条件として指定するすべての値が、同じルーティング テーブル エントリ内の対応する値に一致している必要があります (指定するすべての検索パラメータに暗黙のAND条件が適用されます)。

たとえば、FortiGate ユニットがネットワーク 172.16.14.0/24 に接続されているときに、ネットワーク 172.16.14.0/24 に直接接続されたすべてのルートを表示する場合は、[Type] リストから [Connected] を選択し、[Network] フィールドに「`172.16.14.0/24`」を入力した後 [Apply Filter] を選択して、関連付けられた (1 つまたは複数の) ルーティング テーブル エントリを表示する必要があります。[Type] フィールドに "Connected" という単語が含まれ、かつ [Gateway] フィールドに指定した値が含まれたすべてのエントリが表示されます。

FortiGate ルーティング テーブルを検索するには

1 *[Router]*、*[Monitor]*、*[Routing Monitor]* の順に選択します。

2 *[Type]* リストから、表示するルートのタイプを選択します。たとえば、接続されたすべてのルートを表示するには *[Connected]* を、RIP を介して学習されたすべてのルートを表示するには [RIP] を選択します。

3 特定のネットワークへのルートを表示する場合は、[Network] フィールドにそのネットワークの IP アドレスとネットマスクを入力します。

4 特定のゲートウェイへのルートを表示する場合は、*[Gateway]* フィールドにそのゲートウェイの IP アドレスを入力します。

5 *[Apply Filter]* を選択します。

注記：そのエントリが表示されるようにするには、検索条件として指定するすべての値が、同じルーティング テーブル エントリ内の対応する値に一致している必要があります。

ファイアウォール ポリシー

ファイアウォール ポリシーは、FortiGate ユニットを通過しようとするすべてのトラフィックを、FortiGate インタフェース、ゾーン、および VLAN サブインタフェース間で制御する機能です。

ファイアウォール ポリシーは、FortiGate ユニットを通過しようとするトラフィックの接続許可およびパケット処理を決定するための手順として使用されます。ファイウォールで接続パケットが受信されると、パケットの発信元アドレス、宛先アドレス、サービス（ポート番号による）が解析され、パケットに一致するファイアウォール ポリシーが特定されます。

ファイウォール ポリシーには、FortiGate ユニットがポリシーと一致するパケットを受信した際に実行する多数の手順を盛り込むことができます。手順には、パケットを破棄するかまたは受け入れて処理するかを決定する必須の手順と、ロギングおよび認証などオプションの手順があります。

ポリシー手順には、NAT または PAT が含まれる場合があり、仮想 IP または IP プールを使用することにより発信元および宛先 IP アドレスおよびポート番号を変換します。仮想 IP および IP プールの詳しい利用方法については、313 ページの「ファイアウォール仮想 IP」を参照してください。

ポリシー手順には、アプリケーション層インスペクションおよび他の特定プロトコルのプロテクションおよびロギングを指定するために適用される、プロファイルが含まれる場合もあります。プロファイルの使用については、357 ページの「統合脅威管理（UTM）」を参照してください。

FortiGate ユニットでバーチャル ドメイン（VDOM）を有効にする場合は、バーチャル ドメインごとにファイアウォール ポリシーを個別に設定しますが、ポリシーを設定するにはまずバーチャル ドメインにアクセスする必要があります。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には以下のトピックが含まれています。

ポリシー リストの並び順とポリシー照合との関係

いずれかのインタフェースを通過しようとする接続が FortiGate ユニットで受信されるごとに、ファイアウォール ポリシー リストの中から一致するファイアウォール ポリシーが検索されます。

検索は、ポリシー リストの最上位から始まり、下位の項目へ順番に進みます。一致するポリシーが検出されるまで、FortiGate ユニットによりファイアウォール ポリシー リスト内の各ポリシーが検証されます。FortiGate ユニットにより最初に一致ポリシーが検出されると、そのポリシーに指定された処理がパケットに対して施行され、リスト内の以降のファイアウォール ポリシーは適用されません。ファイアウォール ポリシーの一致は、ファイアウォール ポリシーとパケットの以下の属性を照合することで決められます。

- 発信元および宛先インタフェース

- 発信元および宛先のファイアウォール アドレス
- サービス
- 時間 / スケジュール

一致するポリシーが存在しない場合、その接続は破棄されます。

基本的なルールとして、ファイアウォール ポリシー リストでは、最も特定のポリシーから最も一般的なポリシーの順に並べます。ポリシー リストでは、その順序でポリシーが照合され、***最初に***一致するファイアウォール ポリシーのみが接続に適用されるからです。残りのポリシーについては、照合あるいは適用されません。最も特定のポリシーから最も一般的なポリシーの順に並べることで、幅広いトラフィックに一致してしまうポリシーの照合を後回しにして、例外的な条件に一致するポリシーを有効に照合できます。

たとえば、内部ネットワークからインターネットへの接続をすべて許可する一般的な 1 つのポリシーを持ちながら、FTP をブロックする例外を設けるとします。この場合、その一般的なポリシーの上位に、FTP 接続を拒否するポリシーを追加します。

FTP による接続はすぐに拒否ポリシーに一致してブロックされます。その他のサービスは、FTP ポリシーとは一致せず、一般的な一致ポリシーに到達するまで照合が続けられます。このようにポリシーを並べることで、目的の効果が得られます。もしこれら 2 つのポリシーの順序を逆にして、一般的なポリシーを FTP ブロック ポリシーより前に並べると、FTP 接続を含むすべての接続が一般的なポリシーと一致し、FTP をブロックするポリシーは適用されなくなります。したがって、意図する効果は得られません。

同様に、特定のトラフィックに認証、IPSec VPN、または SSL VPN が必要な場合は、これらのポリシーを他の一致しやすいポリシーより上位に並べます。そのように並べない場合は、他の一致しやすいポリシーが常に優先的に適用され、必要な認証、IPSec VPN、SSL VPN はまったく適用されません。

すべての接続を許可するファイアウォール ポリシーが、デフォルトで設定されている場合があります。このようなポリシーは、移動または削除するか、無効に設定できます。このデフォルトのポリシーをファイアウォール ポリシー リストの最下位に移動することで、パケットに一致するポリシーが他にない場合は、接続が受け付けられます。このデフォルト ポリシーを無効に設定するかまたは削除する場合、パケットに一致するポリシーが他になければ、接続は破棄されます。

ポリシー リスト内のポリシー位置の移動

ポリシーと着信するトラフィックを照合する順序を、目的に応じて変更するために、ファイアウォール ポリシー リスト内のポリシーを並べ替えることができます。同じインタフェースのペアに 2 つ以上のポリシーが定義されている場合は、最初に一致するファイアウォール ポリシーがトラフィックのセッションに適用されます。詳細については、265 ページの「ポリシー リストの並び順とポリシー照合との関係」を参照してください。

ファイアウォール ポリシー リスト内でポリシーを移動しても、ポリシーが作成された順番を示すポリシーの ID は変わりません。

リスト内でポリシーを別の位置に移動するには、そのポリシーの場所に進み (たとえば、*[Firewall]*、*[Policy]*、*[DoS Policy]* の順に選択)、次に *[Move]* アイコンを選択し、ポリシーの異動先を設定します。*[OK]* を選択し、変更を確定します。

ポリシーの有効化および無効化

ポリシー リストでは、ポリシーを一時的に有効または無効に設定できます。ポリシーを削除せずに一時的に無効にする場合に便利な機能です。ポリシーを追加し直すことなく、再び有効に設定できます。

ポリシーを有効または無効に設定するには、*[Firewall]*、*[Policy]* の順に選択します。無効にするファイアウォール ポリシーの行で、[Status] カラムのチェック ボックスをオフにします。そのファイアウォール ポリシーが灰色に表示され、無効に設定されます。無効なファイアウォール ポリシーを有効にするには、有効にするファイアウォール ポリシーの行で、[Status] カラムのチェック ボックスをオンにします。そのファイアウォール ポリシーが濃く表示され、有効に設定されます。

マルチキャスト ポリシー

FortiGate ユニットでは、マルチキャスト ポリシーがサポートされます。以下の CLI コマンドを使用することで、マルチキャスト ポリシーを設定および作成できます。

```
config firewall multicast-policy
```

詳しくは、『*FortiOS CLI リファレンス*』および『*FortiGate マルチキャスト テクニカル ノート*』を参照してください。

ファイアウォール ポリシー リストの表示

ファイアウォール ポリシー リストには、それぞれの発信元および宛先インタフェース ペアと優先的に一致する順序で、ファイアウォール ポリシーが表示されます。

FortiGate ユニットで、バーチャル ドメインが有効に設定されている場合は、各バーチャル ドメインごとに個別のファイアウォール ポリシーを設定しますが、ポリシーを設定するにはまずバーチャル ドメインにアクセスする必要があります。バーチャル ドメインにアクセスするには、*[System]*、*[VDOM]* の順に選択し、ポリシーを設定するバーチャル ドメインに該当する行で、[Enter] を選択します。

ポリシー リスト内のポリシーは、追加、削除、編集、および並べ替えが可能です。ファイアウォール ポリシーの順序は、ポリシー照合に影響します。ポリシー リスト内でポリシーを並べる順序については、265 ページの「ポリシー リストの並び順とポリシー照合との関係」および 266 ページの「ポリシー リスト内のポリシー位置の移動」を参照してください。

ポリシー リストを表示するには、*[Firewall]*、*[Policy]*、*[Policy]* の順に選択します。IPv6 ファイアウォール ポリシー リストを表示するには、*[Firewall]*、*[Policy]*、*[IPv6 Policy]* の順に選択します。

[Policy] ページ

このページには、作成した個々のポリシーおよびセクションが表示されます。このページでは、ポリシーまたはセクションのタイトルを編集、削除または新規作成できます。

[Create New] 新しいファイアウォール ポリシーを追加します。*[Create New]* の横にある下向き矢印を選択し、新しいセクションをリストに追加し、ポリシーをグループ化して表示します。[Create New] を選択すると、[New Policy] ページの画面に自動的に移動します。新しいセクション タイトルを追加する下向き矢印を選択すると、[Section Title] ウィンドウが表示されます。
不用意にトラフィックを許容しないように、*[Create New]* を選択すると、新しいポリシーがリストの最下位に追加されます。ポリシーがリストに追加されると、*[Move To]* アイコンを使用してポリシーをリスト内の必要な位置に移動できます。また、*[Insert Policy before]* アイコンを使用し、新しいポリシーをリスト内の特定ポリシーの上に追加できます。265 ページの「ポリシー リストの並び順とポリシー照合との関係」を参照してください。

[Column Settings] テーブルの表示をカスタマイズします。カラムの表示、非表示を選択し、テーブル内のカラムの表示順序を指定することができます。詳細については、34 ページの「表示されるカラムのカラム設定を使用した制御」および 35 ページの「」を参照してください。

[Section View] 発信元および宛先インタフェースにより構成されているファイアウォール ポリシーを表示するとき選択します。
注記: どのポリシーでも発信元または宛先インタフェースとして [Any] が選択される場合は、[Section View] は利用できません。

[Global View] すべてのファイアウォール ポリシーをシーケンス番号の順番に並べるとき選択します。

[Filter] アイコン 指定した条件に応じてポリシー リストをフィルタ処理または並べ替えるための、カラム フィルタを編集します。詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。

[ID] ポリシーの識別子。ポリシーには、ポリシー リストに追加された順序で番号が付けられます。

[From] ポリシーの発信元インタフェース。[Global View] のみで利用できます。

[To] ポリシーの宛先インタフェース。[Global View] のみで利用できます。

[Source]	このポリシーを適用する発信元アドレスまたはアドレス グループ。詳細については、295 ページの「ファイアウォール アドレス」を参照してください。
[Destination]	このポリシーを適用する宛先アドレスまたはアドレス グループ。詳細については、295 ページの「ファイアウォール アドレス」を参照してください。
[Schedule]	このポリシーがアクティブになる時期を制御するためのスケジュール。詳細については、309 ページの「ファイアウォール スケジュール」を参照してください。
[Service]	このポリシーを適用するサービス。詳細については、301 ページの「ファイアウォール サービス」を参照してください。
[Profile]	このポリシーに関連付けられるプロファイル。
[Action]	このポリシーが接続試行に一致したときに実行する応答。
[Status]	このチェック ボックスをオンにしてポリシーを有効にするか、またはオフにしてポリシーを無効にします。詳しくは、266 ページの「ポリシーの有効化および無効化」を参照してください。
[From]	発信元インタフェース。
[To]	宛先インタフェース。
[VPN Tunnel]	VPN ポリシーにより使用される VPN トンネル。
[Authentication]	ポリシーにより使用されるユーザ認証方法。
[Comments]	ポリシーを作成または編集するとき入力するコメント。
[Log]	緑のチェック マークは、そのポリシーではトラフィック ロギングが有効であることを示します。灰色の × 印は、そのポリシーではトラフィック ロギングが無効であることを示します。
[Count]	FortiGate ユニットにより、ファイアウォール ポリシーと一致するパケットおよびバイト数がカウントされます。 たとえば、5/50B は、総計 5 つのパケットおよび 50 バイトがポリシーと一致することを示します。 FortiGate ユニットが再起動したとき、またはポリシーが削除され再設定されたとき、カウンタがリセットされます。
[Delete]	ポリシーをリストから削除します。
[Edit]	ポリシーを編集します。
[Insert Policy Before]	対応するポリシーの上に、新しいポリシーを追加します。このオプションを使用することで、ポリシーの並び順を簡素化します。265 ページの「ポリシー リストの並び順とポリシー照合との関係」*を参照してください。*
[Move To]	対応するポリシーを、リスト内にある別のポリシーの前または後に移動します。詳細については、266 ページの「ポリシー リスト内のポリシー位置の移動」を参照してください。

ファイアウォール ポリシーの設定

ファイアウォール ポリシーを設定することで、どのセッションがポリシーに一致し、一致するセッションのパケットに対して FortiGate ユニットがどのようなアクションを実行するかを定義できます。

パケットおよびポリシー双方の以下のような属性を検証することで、セッションをファイアウォール ポリシーと照合します。

- 発信元インタフェース / ゾーン
- 発信元アドレス
- 宛先インタフェース / ゾーン
- 宛先アドレス
- セッション開始のスケジュールおよび時間
- サービスおよびパケットのポート番号

最初のパケットがファイアウォール ポリシーと一致する場合は、セッションに含まれるすべてのパケットに対して、設定済みのアクションおよび他のオプションが FortiGate ユニットにより実行されます。

パケット処理アクションは、*ACCEPT*、*DENY*、*IPSEC*、または *SSL-VPN* のいずれかになります。

- ACCEPT ポリシー アクションによって、通信セッションが許可されます。さらに ACCEPT ポリシー アクションには、ポリシーを使用するための認証の要求、またはセッションに含まれるパケットのウイルス スキャンなどの機能を適用するプロテクション プロファイルの指定など、他のパケット処理手順がオプションで含まれる場合があります。ACCEPT ポリシーでは、選択された発信元または宛先インタフェースのどちらかが IPSec 仮想インタフェースの場合、インタフェース モードの IPSec VPN トラフィックを適用できます。詳細については、411 ページの「IPsec VPN の概要」を参照してください。
- DENY ポリシー アクションにより、通信セッションがブロックされます。また、DENY ポリシー アクションでは、拒否されたトラフィックがオプションでログ記録される場合があります。
- IPSEC および SSL-VPN ポリシー アクションでは、トンネルモードの IPSec VPN または SSL VPN トンネルが、それぞれ適用されます。また、オプションで NAT が適用され、トラフィックの 1 方向または双方向が許可される場合があります。ファイアウォール 暗号化ポリシーにより許可される場合、ポリシーと一致するパケットが指定されたネットワーク インタフェースに到着するときは常に、トンネルを自動で開始することも可能です。詳細については、275 ページの「IPSec ファイアウォール ポリシーの設定」および 275 ページの「SSL VPN の ID ベース ファイアウォール ポリシーの設定」を参照してください。

ファイアウォール ポリシーを追加または編集するには、*[Firewall]*、*[Policy]*、*[Policy]* の順に選択します。*[Create New]* を選択しポリシーを追加するか、または既存のファイアウォール ポリシー横の編集アイコンを選択します。後述の表およびリファレンスの記述に従って設定し、IPSec、SSL VPN、および他の特定の設定を指定して、*[OK]* を選択します。

DoS ポリシーを作成する場合は、*[Firewall]*、*[Policy]*、*[DoS Policy]* の順に選択し、後述の表に従って設定します。DoS ポリシーはファイアウォール ポリシーとは別個のポリシーで、DoS センサーを FortiGate インタフェースに到達するトラフィックと関連付けるために使用されます。DoS ポリシーは、パケットがファイアウォール ポリシーにより許可される前にこれらのパケットを IPS に提供します。このような運用により、DoS 攻撃からの効率的な保護などのメリットを得ることができます。詳細については、278 ページの「攻撃を検出および防御する DoS ポリシーの使用」を参照してください。

スニファ ポリシーを作成する場合は、*[Firewall]*、*[Policy]*、*[Sniffer Policy]* の順に選択し、後述の表に従って設定します。詳細については、281 ページの「ネットワーク攻撃を検出するワンアーム スニファ ポリシーの使用」を参照してください。

ファイアウォール ポリシーで IPv6 ファイアウォール アドレスを使用する場合は、*[System]*、*[Admin]*、*[Settings]* の順に選択します。*[IPv6 Support on GUI]* を選択します。. 次に、*[Firewall]*、*[Policy]*、*[IPv6 Policy]* の順に選択し、後述のテーブルに従って設定します。IPv6 ポリシーの設定は、IPv4 ポリシーの設定と同様です。IPv6 ファイアウォール ポリシーにプロファイルを追加でき、さらに共有トラフィック シェーピングを設定し許可または拒否されたトラフィックをログ記録できます。IPSec または SSL VPN には IPv6 ファイアウォール ポリシーを作成できず、IPv6 ポリシーには認証を追加できません。

ファイアウォール ポリシーの順序は、ポリシー照合に影響します。ポリシーを作成または編集するごとに、ポリシーがリスト内の適切な位置にあることを確認してください。[Insert Policy before] を選択することで、新しいポリシーを作成した直後にそのポリシーをファイアウォール ポリシー リスト内で既存ポリシーの前に配置できます (267 ページの「ファイアウォール ポリシー リストの表示」を参照)。

注記： Differentiated Services (DSCP) ファイアウォール ポリシー オプションを、CLI により設定できます。詳細については、『*FortiGateCLI リファレンス*』の「ÉtÉ@ÉCÉAÉEÉÅ[Éã」の章を参照してください。

[New Policy] ページ

このページでは、新しいファイアウォール ポリシーを設定できます。

[Source Interface/Zone]

IP パケットが受信される、FortiGate ネットワーク インタフェース、バーチャル ドメイン (VDOM) リンク、またはゾーンの名前を選択します。インタフェースとゾーンは、[System Network] ページで設定されます。詳細については、89 ページの「インタフェースの設定」および 106 ページの「ゾーンの設定」を参照してください。

発信元インタフェースとして *[Any]* を選択すると、ポリシーは発信元インタフェースとしてどのインタフェースとも一致します。

[Action] が [IPSEC] に設定されている場合、このインタフェースは、ローカル プライベート ネットワークに関連付けられます。

[Action] が [SSL-VPN] に設定されている場合、このインタフェースは、リモートの SSL VPN クライアントからの接続に関連付けられます。

[Source Address]

発信元インタフェース / ゾーンと関連付けられるファイアウォール アドレス名を選択します。選択したファイアウォール アドレスと一致する IP アドレスがヘッダに含まれるパケットのみが、このポリシーの対象となります。

このリストから *[Create New]* を選択することにより、ファイアウォール アドレスを作成できます。詳細については、297 ページの「アドレスの設定」を参照してください。

複数のファイアウォール アドレスまたはアドレス グループを発信元インタフェース / ゾーンと関連付ける場合は、*[Source Address]* から *[Multiple]* を選択します。ダイアログ ボックスで、ファイアウォール アドレスまたはアドレス グループを、*[Available Addresses]* セクションから *[Members]* セクションに移動し、*[OK]* を選択します。

If *[Action]* が *[IPSEC]* に設定されている場合、このアドレスは FortiGate ユニットの背後に配置されているホスト、サーバ、またはネットワークのプライベート IP アドレスです。

[Action] が *[SSL-VPN]* に設定されており、これが Web のみモードのクライアントのためのポリシーである場合は、*[all]* を選択します。

[Action] が *[SSL-VPN]* に設定されており、これがトンネル モードのクライアントのためのポリシーである場合は、そのトンネル モードのクライアントのために予約したアドレスの名前を選択します。

[Destination Interface/Zone]

IP パケットが転送される先の、FortiGate ネットワーク インタフェース、バーチャル ドメイン (VDOM) リンク、またはゾーンの名前を選択します。インタフェースとゾーンは、[System Network] ページで設定されます。詳細については、89 ページの「インタフェースの設定」および 106 ページの「ゾーンの設定」を参照してください。

宛先インタフェースとして *[Any]* を選択すると、ポリシーは宛先インタフェースとしてどのインタフェースとも一致します。

[Action] が *[IPSEC]* に設定されている場合、このインタフェースは、VPN トンネルへの入口に関連付けられます。

[Action] が *[SSL-VPN]* に設定されている場合、このインタフェースは、ローカル プライベート ネットワークに関連付けられます。

[Destination Address]

宛先インタフェース / ゾーンと関連付けられるファイアウォール アドレス名を選択します。選択したファイアウォール アドレスと一致する IP アドレスがヘッダに含まれるパケットのみが、このポリシーの対象となります。

このリストから *[Create New]* を選択することにより、ファイアウォール アドレスを作成できます。詳細については、297 ページの「アドレスの設定」を参照してください。

複数のファイアウォール アドレスまたはアドレス グループを宛先インタフェース / ゾーンに関連付ける場合は、[Destination Address] から *[Multiple]* を選択します。ダイアログ ボックスで、ファイアウォール アドレスまたはアドレス グループを、*[Available Addresses]* セクションから *[Members]* セクションに移動し、*[OK]* を選択します。

仮想 IP を選択する場合は、FortiGate ユニットにより NAT または PAT が適用されます。適用される変換は、仮想 IP で指定される設定、および [NAT] (以下を参照) を選択するかどうかにより異なります。仮想 IP の使用については、313 ページの「ファイアウォール仮想 IP」を参照してください。

[Action] が *[IPSEC]* に設定されている場合、このアドレスは、VPN トンネルのリモート エンドポイントにある、パケットの配信先になる可能性のあるプライベート IP アドレスです。

[Action] が *[SSL-VPN]* に設定されている場合は、FortiGate ユニットの背後に配置されている、リモート クライアントがアクセスする必要のあるホスト、サーバ、またはネットワークに対応する IP アドレスの名前を選択します。

[Schedule]

ポリシーが有効になるタイミングを制御する、ワンタイムまたは反復スケジュールまたはスケジュールのグループを選択します。

さらに、このリストから *[Create New]* を選択することにより、スケジュールを作成できます。詳細については、309 ページの「ファイアウォール スケジュール」を参照してください。

[Service] このポリシーをトリガするためにパケットと一致する必要がある、ファイアウォール サービスまたはサービス グループの名前を選択します。
事前に設定された各種のファイアウォール サービスから選択するか、またはこのリストから *[Create New]* を選択することにより、カスタムのサービスまたはサービス グループを作成できます。詳細については、306 ページの「カスタム サービスの設定」および 307 ページの「カスタム サービス グループの設定」を参照してください。
[Service] 横の *[Multiple]* ボタンを選択することにより、複数のサービスまたはサービス グループを選択できます。

[Action] パケットがポリシーの条件に一致したときのファイアウォールの対応を選択します。利用可能なオプションは、この選択に応じて幅広く異なります。

[ACCEPT] このポリシーに一致したトラフィックを受け付けます。NAT およびプロテクション プロファイルの設定、トラフィックのログ記録、トラフィックのトラフィック シェーピング、認証オプションに関する各種設定、またはこのポリシーへのコメント追加を行うことができます。

[DENY] このポリシーに一致したトラフィックを拒否します。設定可能な他のポリシー オプションは、このポリシーで拒否された接続をログ記録する *[Log Violation Traffic]*、およびこのポリシーにコメントを追加する *[Comment]* のみです。

IPSEC IPSec VPN パケットの処理、およびプロテクション プロファイルの設定、トラフィックのログ記録、トラフィックのトラフィック シェーピング、またはポリシーへのコメント追加を行うために、IPSec ファイアウォール暗号化ポリシーを設定できます。詳しくは、275 ページの「IPSec ファイアウォール ポリシーの設定」を参照してください。

[SSL-VPN] SSL-VPN ファイアウォール暗号化ポリシーを設定し、SSL VPN トラフィックを受け付けることができます。このオプションは、SSL VPN ユーザ グループを追加しないと使用できません。NAT およびプロテクション プロファイルの設定、トラフィックのログ記録、トラフィックのトラフィック シェーピング、またはこのポリシーへのコメント追加を行うことができます。詳しくは、275 ページの「SSL VPN の ID ベース ファイアウォール ポリシーの設定」を参照してください。

[NAT] *[Action]* が *[ACCEPT]* または *[SSL-VPN]* に設定されている場合のみ使用できます。.
このポリシーにより受け付けられるパケットの発信元アドレスおよびポートの NAT を、有効または無効に設定します。*[NAT]* が有効に設定される場合は、*[Dynamic IP Pool]* および *[Fixed Port]* を設定できます。
仮想 IP を *[Destination Address]* として選択し *[NAT]* オプションを選択しない場合は、FortiGate ユニットにより完全な NAT ではなく DNAT（宛先 NAT）が実行されます。SNAT（発信元 NAT）は実行されません。

[Dynamic IP Pool] チェック ボックスをオンにして、次に IP プールを選択し、発信元アドレスをその IP プールから無作為に選択された IP アドレスに変換します。
宛先インタフェース、VLAN サブインタフェース、または宛先ゾーン内のインタフェースまたは VLAN サブインタフェースのいずれかが、DHCP または PPPoE を使用して設定されている場合は、*[IP Pool]* を選択できません。
詳細については、327 ページの「IP プールの設定」を参照してください。

[Fixed Port] NAT で発信元ポートを変換しないようにするには、*[Fixed Port]* を選択します。
一部のアプリケーションでは、発信元ポートが変換されてしまうと正しく機能しません。ほとんどの場合、*[Fixed Port]* を選択するとき、*[Dynamic IP Pool]* も選択します。*[Dynamic IP Pool]* を選択しない場合、*[Fixed Port]* が選択されたポリシーは、一度にそのサービスへの接続 1 つに限り許可できます。
注記：*[Fixed Port] は、CLI から有効に設定された場合のみ表示されます。*

[Enable Identity Based Policy] 認証を必要とするファイアウォール ポリシーを設定するために選択します。詳細については、273 ページの「ファイアウォール ポリシーへの認証の追加」を参照してください。この項には、*[Firewall]*、*[Directory Service (FSAE)]*、*[NTLM Authentication]*、および *[Enable Disclaimer and Redirect URL to]* の各オプションについての説明も記述されています。

[UTM] UTM オプションを選択することで、このファイアウォール ポリシーを適用します。利用可能な UTM オプションを選択するには、必ず UTM を有効に設定します。

[Protocol] オプション ドロップダウン リストから、プロトコルを選択します。デフォルトのプロトコルを、デフォルトと呼びます。プロトコル項目には、NNTP および無効証明書のロギングなど、複数の設定が含まれます。新しいプロトコル オプション リスト項目を作成するには、ドロップダウン リストから [Create New] を選択します。

[Enable Antivirus] ドロップダウン リストからアンチウイルス プロファイルを選択します。新しいアンチウイルス プロファイルを作成するには、ドロップダウン リストから [Create New] を選択します。アンチウイルス プロファイルの詳細については、358 ページの「アンチウイルス」を参照してください。

[Enable Web Filter]	ドロップダウン リストから、1 つの Web フィルタリング プロファイルを選択します。新しい Web フィルタリング プロファイルを作成するには、ドロップダウン リストから [Create New] を選択します。Web フィルタリング プロファイルの詳細については、374 ページの「Web フィルタ」を参照してください。
[Enable Email Filter]	ドロップダウン リストから、電子メール フィルタリング プロファイルを選択します。新しい電子メール フィルタリング プロファイルを作成するには、ドロップダウン リストから [Create New] を選択します。電子メール フィルタリング プロファイルの詳細については、386 ページの「電子メール フィルタ」を参照してください。
[Enable DLP Sensor]	ドロップダウン リストから、DLP センサーを選択します。新しい DLP センサーを作成するには、ドロップダウン リストから [Create New] を選択します。DLP センサーの詳細については、395 ページの「情報漏洩防止」を参照してください。
[Enable Application Control]	ドロップダウン リストから、アプリケーション制御ブラック / ホワイト リストを選択します。新しいアプリケーション制御ブラック / ホワイト リストを作成するには、ドロップダウン リストから [Create New] を選択します。アンチウイルス プロファイルの詳細については、405 ページの「アプリケーション制御」を参照してください。
[Enable VoIP]	ドロップダウン リストから、VoIP プロファイルを選択します。新しい VoIP プロファイルを作成するには、ドロップダウン リストから [Create New] を選択します。VoIP プロファイルの詳細については、409 ページの「VoIP」を参照してください。
[Traffic Shaping]	ポリシーの共有トラフィック シェーパーを選択します。新しい共有トラフィック シェーパーを作成することもできます。共有トラフィック シェーパーは、利用可能な帯域幅を制御し、処理対象のトラフィックのプライオリティをポリシーに基づいて設定します。 共有トラフィック シェーパーの設定については、337 ページの「共有トラフィック シェーパーの設定」を参照してください。
[Reverse Direction Traffic Shaping]	逆のトラフィック シェーピングを有効にして、共有トラフィック シェーパーを選択するとき、このオプションを選択します。たとえば、ポリシーで制御されるトラフィックの方向がポート 1 からポート 2 の場合、このオプションを選択すると、ポート 2 からポート 1 へのトラフィックにもポリシー シェーピング設定が適用されます。 共有トラフィック シェーパーの設定については、337 ページの「共有トラフィック シェーパーの設定」を参照してください。
[Per-IP Traffic Shaping]	このポリシーに適用される "IP ごとのトラフィック シェーパー" を選択します。"IP ごとのトラフィック シェーピング" は、ファイアウォール ポリシーに追加した "IP ごとのトラフィック シェーパー" に追加されている IP アドレスから発信されるトラフィックに、トラフィック シェーピングを適用します。 的 P ごとのトラフィック シェーパー狽ｱ設定については、338 ページの「"IP ごとのトラフィック シェーピング" の設定」を参照してください。
[Log Allowed Traffic]	ポリシーにより接続が処理されるときはメッセージをトラフィック ログに必ず記録するとき、このオプションを選択します。ロギング場所 (syslog、WebTrends、使用可能な場合はローカル ディスク、メモリ、または FortiAnalyzer) のトラフィック ログを有効にし、[Log & Report] メニューからロギング レベルを [Notification] 以下に設定する必要があります。詳細については、485 ページの「ログおよびレポート」を参照してください。
[No NAT]	デフォルトで選択されています。選択されている場合、そのファイアウォール ポリシーでは NAT は使用されません。
[Enable NAT]	NAT トラフィックのロギングを有効にするとき選択します。それにより、[Dynamic IP Pool] オプションを利用できます。このオプションを有効にする前に、ダイナミック IP プールを設定する必要があります。
[Use Central NAT Table]	[Central NAT Table] メニューで設定する Central NAT テーブルを使用するロギングを有効にするとき、このオプションを選択します。
[Dynamic IP Pool]	[Enable NAT] を選択したときのみ、利用可能です。
[Enable Endpoint NAC]	エンドポイント NAC 機能を有効にして、適用するエンドポイント NAC プロファイルを選択するとき、このオプションを選択します。詳細については、469 ページの「エンドポイント」を参照してください。 ・ *[User]、[Options]、[Authentication]* で *[Redirect HTTP Challenge to a Secure Channel (HTTPS)]* が有効に設定されている場合、ファイアウォール ポリシーでエンドポイントを有効にできません。 ・ ファイアウォール ポリシーに負荷分散仮想 IP が含まれる場合、エンドポイントのチェックは実行されません。
[Comments]	ポリシーについての情報を追加します。最大の長さは 63 文字です。

ファイアウォール ポリシーへの認証の追加

ファイアウォール ポリシーで *[Enable Identity Based Policy]* を有効にする場合、ネットワーク ユーザは、サポートされるファイアウォール認証プロトコルを含むトラフィックを送信することで、ファイアウォール認証チャレンジを開始し、認証を正常に完了する必要があります。この処理を経て、FortiGate ユニットではファイアウォール ポリシーと一致する他のトラフィックが許可されます。

ユーザ認証は、サポートされる以下のどのプロトコルでも発生します。

- HTTP
- HTTPS
- FTP
- Telnet

認証のスタイルは、サポートされるこれらのプロトコルのうち、どれが選択したファイアウォール サービス グループに含まれているか、およびこれらの有効なプロトコルのうち、ネットワーク ユーザがどれを適用して認証チャレンジを開始するかに応じて異なります。認証のスタイルは、2 種類のいずれかになります。証明書ベース (HTTPS、または HTTPS にリダイレクトされる HTTP のみ) の認証では、カスタマイズ済みの証明書を FortiGate ユニット、および FortiGate ユニットにより照合されるネットワーク ユーザのブラウザにインストールする必要があります。ユーザ名およびパスワード ベース (HTTP、FTP、および Telnet) の認証では、ネットワーク ユーザは FortiGate ユニットから、各自のファイアウォール ユーザー名およびパスワードを入力するように指示されます。

たとえば、SMTP および POP3 トラフィックを許可するために、HTTPS 証明書ベース認証を必要とする場合、SMTP、POP3、および HTTPS のサービスを含むファイアウォール サービスを (ファイアウォール ポリシーで) 選択する必要があります。POP3 または SMTP を使用する前に、ネットワーク ユーザは HTTPS サービスを使用するトラフィックを送信し、FortiGate ユニットはこのサービスを使用してネットワーク ユーザの証明書を確認します。証明書ベース認証が正常に完了した後に、ネットワーク ユーザは電子メールにアクセスできます。

ほとんどの場合、認証なしに FortiGate ユニットを介して、ユーザが DNS を使用できるようにしておきます。DNS を利用できない場合は、ユーザは、サポートされる認証プロトコルを使用して FortiGate ユニットの認証チャレンジを開始するとき、ドメイン名を使用できません。

認証では、アクションが必ず ACCEPT または SSL-VPN のいずれかであり、また最初にユーザを作成しそのユーザをファイアウォールのユーザ グループに割り当て、そのユーザ グループにプロテクション プロファイルを割り当てる必要があります。ユーザ グループの設定については、457 ページの「ユーザ グループ」を参照してください。認証の設定については、273 ページの「ID ベースのファイアウォール ポリシーの設定」および 275 ページの「SSL VPN の ID ベース ファイアウォール ポリシーの設定」を参照してください。

注記: ネットワーク ユーザの Web ブラウザに証明書をインストールしないと、SSL 証明書警告メッセージがユーザに表示され、ユーザはデフォルトの FortiGate 証明書を手動で許可する必要があり、ネットワーク ユーザの Web ブラウザはそれを無効と見なす場合があります。証明書のインストールについては、191 ページの「システム - 証明書」を参照してください。

注記: 証明書ベースの認証を使用する場合、ファイアウォール ポリシーを作成する際に何らかの証明書を指定しないと、FortiGate ユニットでは、使用されるグローバル設定からデフォルトの証明書が使用されます。証明書を指定すると、グローバル設定がポリシー-ごとの設定に置き換わります。グローバル認証の設定については、463 ページの「認証」を参照してください。

ID ベースのファイアウォール ポリシーの設定

非 SSL-VPN ID ベース ポリシーを使用するユーザに対しては、ユーザ グループをポリシーに追加する必要があります。ユーザ グループの設定については、457 ページの「ユーザ グループ」を参照してください。

ID ベースのポリシーを設定するには、*[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、*[Create New]* を選択して、ファイアウォール ポリシーを追加するか、または既存のファイアウォール ポリシーに該当する行で、[Edit] を選択します。*[Action]* が *[ACCEPT]* に設定されていることを確認してください。*[Enable Identity Based Policy]* を選択します。

[New Policy] ページの [Enable Identity Based Policy] セクション

ID ベース ポリシー認証を有効にするとき選択します。
[Action] が *[ACCEPT]* に設定される場合、1 つ以上の 認証サーバ タイプを選択できます。ネットワーク ユーザが認証を行うとき、FortiGate ユニットがユーザの資格情報を確認するためにどのローカルまたはリモート認証サーバに問い合わせるかが、選択されたサーバ タイプにより示されます。

[Add]	必ず認証を行う指定されたユーザ グループに、このポリシーを使用することが許可されます。
[Rule ID]	ルールの名前または識別子。
[User Group]	必ず認証を行う指定されたユーザ グループに、このポリシーを使用することが許可されます。
[Service]	このポリシーをトリガするためにパケットと一致する必要がある、ファイアウォール サービスまたはサービス グループ。
[Schedule]	ポリシーが有効になるタイミングを制御する、ワンタイムまたは反復スケジュール。 さらに、このリストから *[Create New]* を選択することにより、スケジュールを作成できます。詳細については、309 ページの「ファイアウォール スケジュール」を参照してください。
[UTM]	UTM 機能がこのポリシーに選択されているかどうかを示します。
[Traffic Shaping]	このポリシーのトラフィック シェーピング設定。 詳細については、265 ページの「ファイアウォール ポリシー」を参照してください。
[Logging]	ロギングがこのポリシーに選択されているかどうかを示します。
[Delete]	この ID ベース ポリシーを削除するとき選択します。
[Edit]	この ID ベース ポリシーを編集するとき選択します。
[Move To]	ID ベース ポリシー リスト内で ID ベース ポリシーの位置を変更するとき選択します。
[Firewall]	FortiGate ユニットまたは接続されている LDAP および RADIUS サーバでローカルに定義される、ファイアウォール ユーザ グループを含むことができます。このオプションはデフォルトで選択されています。
[Directory Service (FSAE)]	*[User]*、*[User Group]* で定義されたディレクトリ サービス グループを含むことができます。これらのグループは、ドメイン コントローラにより FSAE (Fortinet Server Authentication Extensions) を使用して認証されます。このオプションを選択する場合、FSAE をディレクトリ サービス ドメイン コントローラに必ずインストールします。FSAE については、『*Fortinet Server Authentication Extension 管理ガイド*』を参照してください。. ユーザ グループの設定については、457 ページの「ユーザ グループ」を参照してください。
[NTLM Authentication]	*[User]*、*[User Group]* で定義されたディレクトリ サービス グループを含むことができます。このオプションを選択する場合、NTLM の認証グループのメンバとして、ディレクトリ サービス グループを必ず使用します。ユーザ グループの設定については、457 ページの「ユーザ グループ」を参照してください。
[Certificate]	証明書ベースの認証に限られます。ゲスト アカウントが使用するプロテクション プロファイルを選択します。 ***注記:*** 証明書ベースの認証を実装するには、証明書ベース認証を使用するサポート対象の認証プロトコルのいずれかを含む、ファイアウォール サービス グループを選択する必要があります。また証明書を、ネットワーク ユーザの Web ブラウザに必ずインストールします。詳細については、273 ページの「ファイアウォール ポリシーへの認証の追加」を参照してください。
[Enable Disclaimer and Redirect URL to]	ユーザ認証の後に、*[Authentication Disclaimer]* 差し替えメッセージの HTML ページを表示するとき、このオプションを選択します。ユーザが宛先に接続するには、表示されるユーザ認証免責条項を受け入れる必要があります。ユーザ認証差し替えメッセージのカスタマイズについては、160 ページの「ユーザ認証差し替えメッセージ」を参照してください。 オプションで IP アドレスまたはドメイン名を入力することにより、ユーザ認証免責条項が受け入れられた後にユーザ HTTP 要求をリダイレクトできます。リダイレクト先の URL には、追加情報 (使用条項など) をともなう Web ページが可能です。Web ブラウザのセキュリティ警告が表示されないように、この URL は、通常は FQDN (fully qualified domain name) である指定された `auth-cert` の CN フィールドに一致する必要があります。

ID ベースのファイアウォール ポリシー (非 SSL-VPN) を作成するには

1 *[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、*[Create New]* を選択します。

2 *[Source Interface/Zone]*、*[Source Address]*、*[Destination Interface/Zone]*、*[Destination Address]*、*[Schedule]*、および *[Service]* を設定します。詳細については、268 ページの「ファイアウォール ポリシーの設定」を参照してください。

3 *[Action]* フィールドで、*[ACCEPT]* を選択します。

4 *[Enable Identity Based Policy]* を選択し、ID ベースのポリシーを追加できるようにします。

5 *[Add]* を選択します。

6 *[Available User Groups]* リストから、このポリシーの使用を許可されるために認証を行う必要がある、1 つ以上のユーザ グループを選択します。右矢印を選択し、選択したユーザ グループを *[Selected User Groups]* リストに移動します。

7 *[Available Services]* リストからサービスを選択し、右矢印を選択してそれらのサービスを *[Selected Services]* リストに移動します。

8 *[Schedule]* を選択します。

9 オプションで、1 つ以上の UTM オプションを選択します。

10 オプションで、*[Traffic Shaping]* を選択し、トラフィック シェーパーを選びます。

11 *[Traffic Shaping]* を選択した場合は、*[Reverse Direction Traffic Shaping]* を選択し、トラフィック シェーパーを選びます。

12 *[OK]* を選択します。

IPSec ファイアウォール ポリシーの設定

ファイアウォール ポリシーでは（268 ページの「ファイアウォール ポリシーの設定」を参照）、IPSec の以下の暗号化オプションを利用できます。これらのオプションを設定するには、*[Firewall]*、*[Policy]* の順に選択し、*[Create New]* を選択して、ファイアウォール ポリシーを追加するか、または既存のファイアウォール ポリシーに該当する行で、*[Edit]* を選択します。*[Action]* が *[IPSEC]* に設定されていることを確認してください。以下の表の情報を入力し、*[OK]* を選択します。

詳細については、『*FortiGate IPSec VPN ユーザ ガイド*』の「ファイアウォール ポリシーの定義」の章を参照してください。

[New Policy] ページでの IPSec 設定

[VPN Tunnel]	フェーズ 1 の設定で定義された VPN トンネルの名前を選択します。指定されたトンネルは、このファイアウォール暗号化ポリシーに従います。
[Allow Inbound]	リモート プライベート ネットワーク上のダイヤルアップ クライアントまたはコンピュータからのトラフィックで、トンネルを開始できるようにする場合に選択します。
[Allow outbound]	ローカル プライベート ネットワーク上のコンピュータからのトラフィックでトンネルを開始できるようにする場合に選択します。
[Inbound NAT]	暗号化解除された受信パケットの発信元IPアドレスを、ローカル プライベート ネットワークの FortiGate インタフェースの IP アドレスに変換する場合に選択します。
[Outbound NAT]	送信のクリア テキスト パケットの発信元アドレスを、指定した IP アドレスに変換するために、必ず CLI の `natip` 値と組み合わせて選択します。`natip` 値が指定されている場合、送信 IP パケットの発信元アドレスは、それらのパケットがトンネルを経由して送信される前に置き換えられます。詳細については、『*FortiGateCLI リファレンス*』の「ファイアウォール」の章を参照してください。

注記： ルートベース（インタフェース モード）VPN では、IPSec ファイアウォール ポリシーを設定しません。代わりに、1 つは通信方向、もう 1 つは発信元または宛先インタフェースとしての IPSec 仮想インタフェースの、2 種類の標準的な ACCEPT ファイアウォール ポリシーを設定します。

SSL VPN の ID ベース ファイアウォール ポリシーの設定

SSL-VPN の ID ベース ポリシーを使用するネットワーク ユーザの場合、SSL VPN ユーザを設定し、そのユーザをユーザ グループに追加した上で、ポリシーを設定する必要があります。

詳細については、268 ページの「ファイアウォール ポリシーの設定」を参照してください。

SSL-VPN の ID ベース ファイアウォール ポリシーを作成するには、*[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、*[Create New]* を選択します。次に、以下の表の情報を入力します。*[Action]*、*[SSL VPN]* の順に選択します。

注記：[SSL-VPN] オプションは、SSL VPN ユーザ グループを追加した後に限り、[Action] リストから使用できます。SSL VPN ユーザ グループの追加については、460 ページの「SSL VPN ユーザ グループ」を参照してください。

[New Policy] ページでの SSL-VPN 設定

[Source Interface/Zone] IP パケットが受信される、FortiGate ネットワーク インタフェース、バーチャル ドメイン (VDOM) リンク、またはゾーンの名前を選択します。

[Source Address] 発信元インタフェース / ゾーンと関連付けられるファイアウォール アドレス名を選択します。選択したファイアウォール アドレスと一致する IP アドレスがヘッダに含まれるパケットのみが、このポリシーの対象となります。
このリストから *[Create New]* を選択することにより、ファイアウォール アドレスを作成できます。詳細については、297 ページの「アドレスの設定」を参照してください。
[Action] が *[SSL-VPN]* に設定されており、これが Web のみモードのクライアントのためのポリシーである場合は、*[all]* を選択します。
[Action] が *[SSL-VPN]* に設定されており、これがトンネル モードのクライアントのためのポリシーである場合は、そのトンネル モードのクライアントのために予約したアドレスの名前を選択します。

[Destination Interface/Zone] IP パケットが転送される先の、FortiGate ネットワーク インタフェース、バーチャル ドメイン (VDOM) リンク、またはゾーンの名前を選択します。*[Action]* が *[SSL-VPN]* に設定されている場合、このインタフェースは、ローカル プライベート ネットワークに関連付けられます。

[Destination Address] 宛先インタフェース / ゾーンと関連付けられるファイアウォール アドレス名を選択します。選択したファイアウォール アドレスと一致する IP アドレスがヘッダに含まれるパケットのみが、このポリシーの対象となります。
このリストから *[Create New]* を選択することにより、ファイアウォール アドレスを作成できます。詳細については、297 ページの「アドレスの設定」を参照してください。
複数のファイアウォール アドレスまたはアドレス グループを宛先インタフェース/ゾーンに関連付ける場合は、[Destination Address] から *[Multiple]* を選択します。ダイアログ ボックスで、ファイアウォール アドレスまたはアドレス グループを、*[Available Addresses]* セクションから *[Members]* セクションに移動し、*[OK]* を選択します。
仮想 IP を選択する場合は、FortiGate ユニットにより NAT または PAT が適用されます。適用される変換は、仮想 IP で指定される設定、および [NAT] (以下を参照) を選択するかどうかにより異なります。仮想 IP の使用については、313 ページの「ファイアウォール仮想 IP」を参照してください。
[Action] が *[IPSEC]* に設定されている場合、このアドレスは、VPN トンネルのリモート エンドポイントにある、パケットの配信先になる可能性のあるプライベート IP アドレスです。
[Action] が *[SSL-VPN]* に設定されている場合は、FortiGate ユニットの背後に配置されている、リモート クライアントがアクセスする必要のあるホスト、サーバ、またはネットワークに対応する IP アドレスの名前を選択します。

[Action] SSL-VPN を選択し、SSL VPN トラフィックを許可するためのファイアウォール暗号化ポリシーを設定します。このオプションは、SSL VPN ユーザ グループを追加しないと使用できません。

[SSL Client Certificate Restrictive] (共有されている) グループ証明書の所有者が生成したトラフィックを許可します。グループ証明書の所有者は SSL VPN ユーザ グループのメンバである必要があり、そのユーザ グループの名前が [Allowed] フィールドに存在する必要があります。

[Cipher Strength] SSL暗号化のビット レベルを選択します。リモート クライアント上のWeb ブラウザが、選択するレベルに一致している必要があります。選択可能なレベルは、Any、164 以上の High、または 128 以上の Medium です。

[User Authentication Method]	ユーザ認証に使用される認証サーバを選択します。 **[Any]** ミ 上記の認証方法すべてが適用されます。[Local] が最初に試行され、次に [RADIUS]、[LDAP] の順に試行されます。 **[Local]** ミ このファイアウォール ポリシーに、ローカル ユーザ グループが結びつけられる場合に選択します。 **[RAIDUS]** 外部 LADP サーバにより認証されるリモート クライアントの場合に選択します。 **[LDAP]** ミ 外部 LDAP サーバにより認証されるリモート クライアントの場合に選択します。 **[TACACS+]** ミ 外部TACACS+サーバにより認証されるリモート クライアントの場合に選択します。
[No NAT]	デフォルトで選択されています。選択されている場合、そのファイアウォール ポリシーでは NAT は使用されません。
[Dynamic IP Pool]	ダイナミック IP プールを有効にするとき選択します。
[Enable NAT]	このポリシーにより受け付けられるパケットの発信元アドレスおよびポートの NAT を、有効または無効に設定します。*[NAT]* が有効に設定される場合は、*[Dynamic IP Pool]* および *[Fixed Port]* を設定できます。 仮想 IP を *[Destination Address]* として選択し *[NAT]* オプションを選択しない場合は、FortiGate ユニットにより完全な NAT ではなく DNAT (宛先 NAT) が実行されます。SNAT (発信元 NAT) は実行されません。 **ヒント** :NAT を選択する場合、FortiGate ユニットの送信インタフェースの IP アドレスが、SSL VPN により開始される新しいセッションの発信元アドレスとして使用されます。
[Use Central NAT Table]	[Central NAT Table] メニューで設定したNATルールを使用するとき選択します。FortiOS ユニットは、このテーブルを参照し、パケットを変換する方法を判断します。
[Enable Identity Based Policy]	ID ベース ポリシー認証を有効にするとき選択します。 *[Action]* が *[ACCEPT]* に設定される場合、1 つ以上の 認証サーバ タイプを選択できます。ネットワーク ユーザが認証を行うとき、FortiGate ユニットがユーザの資格情報を確認するためにどのローカルまたはリモート認証サーバに問い合わせるかが、選択されたサーバ タイプにより示されます。 詳細については、273 ページの「ID ベースのファイアウォール ポリシーの設定」を参照してください。
[Comments]	ポリシーについての情報を追加します。最大の長さは 63 文字です。

Central NAT Table の設定

Central NAT Table により、ユーザは NAT ルールを作成できるとともに、グローバル ファイアウォール テーブルにより設定される NAT マッピングを表示できます。ファイアウォール ポリシー内で [Use Central NAT Table] オプションを選択することにより、そのポリシーに対してこれらの NAT ルールを使用できます。

NAT ルールを設定するには、*[Firewall]*、*[Policy]*、*[Central NAT Table]* の順に選択し、*[Create New]* を選択するかまたは既存の NAT ルールを編集します。

[Central NAT Table] ページ

このページには、作成済みの NAT ルールが一覧表示されます。このページでは、NAT ルールの編集、削除、または新規作成が可能です。

[Create New]	新しい NAT ルール セットを作成するとき選択します。
[Edit]	NAT ルールを編集するとき選択します。
[Delete]	[Central NAT Table] ページから NAT ルールを削除するとき選択します。
[Enable]	NAT ルールを有効にするとき選択します。
[Disable]	NAT ルールを無効にするとき選択します。
[Insert]	新しい NAT ルールを挿入するとき選択します。このアイコンは、[Create New] と同じです。
[Move]	リスト内で NAT ルールを別の位置に移動するとき選択します。

[New NAT] ページ

このページで、NAT ルールを設定できます。

[Source Address]	ドロップダウン リストから発信元 IP アドレスを選択します。ドロップダウン リストから [Multiple] を選択することで、発信元 IP アドレスのグループをオプションで作成できます。ドロップダウン リストから [Create New] を選択することで、新しい発信元 IP アドレスを作成できます。
[Translated Address]	ドロップダウン リストから、ダイナミック IP プールを選択します。
[Original Port]	アドレスが発生するポートを入力します。
[Translated Port]	変換されるポート番号を入力します。[From] フィールドの数は、[To] フィールドに入力されるより小さいポート番号より必ず大きくなります。

攻撃を検出および防御する DoS ポリシーの使用

DoS ポリシーは主に、ネットワーク トラフィックが送受信される FortiGate インタフェース、および発信元および宛先のアドレスに基づいて、DoS センサーをそのネットワーク トラフィックに適用するために使用されます。DoS センサーは、トラフィックの一般的なパターンおよび動作に当てはまらないネットワーク トラフィックを特定する、トラフィック アノマリ検出機能を備えています。異常なトラフィックの代表的な例に、DoS 攻撃があります。DoS は、攻撃側システムから標的システムに対して異常に多数のセッションが開始されることで発生します。多数のセッションにより、標的システムの処理速度を低速または機能停止の状態にして、正規ユーザがそのシステムを使用できないようにします。

DoS ポリシーでは、ネットワーク保護のために FortiGate ユニットにより展開される保護対策の最初期の段階で、ネットワーク トラフィックが調査されます。このような DoS ポリシーの特性により、少ないリソースでネットワークを効率的に保護する効果を得ることができます。ファイアウォール ポリシー検索、アンチウイルス スキャン、その他、集中的に資源を消費する保護機能を必要とせずに、上述の DoS を検知し、そのパケットを破棄できます。

この項では、DoS ポリシー設定の基礎について説明します。詳細については、『*FortiGate UTM ユーザ ガイド*』を参照してください。

DoS ポリシー リストの表示

DoS ポリシー リストには、それぞれのインタフェース、発信元 / 宛先アドレス ペア、およびサービスとの一致の優先順に、DoS ポリシーが表示されます。

FortiGate ユニットで、バーチャル ドメインが有効に設定されている場合は、各バーチャル ドメインごとに個別の DoS ポリシーを設定しますが、ポリシーを設定するにはまずバーチャル ドメインにアクセスする必要があります。バーチャル ドメインにアクセスするには、*[System]*、*[VDOM]* の順に選択し、ポリシーを設定するバーチャル ドメインに該当する行で、*[Enter]* を選択します。

DoS ポリシー リスト内のポリシーは、追加、削除、編集、および並べ替えが可能です。DoS ポリシーの順序は、ポリシー照合に影響します。ファイアウォール ポリシーと同様に、DoS ポリシー リストに表示される順序で一度に 1 つずつ、上位から下位へ DoS ポリシーがトラフィックと照合されます。一致するポリシーが見つかると、そのポリシーが使用され、以降の DoS ポリシー照合は中止されます。

DoS ポリシー リストを表示するには、*[Firewall]*、*[Policy]*、*[DoS Policy]* の順に選択します。

[DoS Policy] ページ

このページには、作成済みの DoS ポリシーが一覧表示されます。このページでは、DoS ポリシーの編集、削除、または新規作成が可能です。

[Create New]	新しい DoS ポリシーを追加します。[Create New] の横にある下向き矢印を選択し、新しいセクションをリストに追加し、ポリシーをグループ化して表示します。
[Column Settings]	テーブルの表示をカスタマイズします。カラムの表示、非表示を選択し、テーブル内のカラムの表示順序を指定することができます。詳しくは、34 ページの「表示されるカラムのカラム設定を使用した制御」を参照してください。
[Section View]	インタフェースにより構成されている DoS ポリシーを表示するとき選択します。

[Global View]	すべての DoS ポリシーをシーケンス番号の順番に並べるとき選択します。
[Filter] アイコン	指定した条件に応じてポリシー リストをフィルタ処理または並べ替えるための、カラム フィルタを編集します。詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。
[ID]	ポリシーごとに固有の識別子。ポリシーには、作成された順序で番号が付けられます。
[Source]	このポリシーを適用する発信元アドレスまたはアドレス グループ。詳細については、295 ページの「ファイアウォール アドレス」を参照してください。
[Destination]	このポリシーを適用する宛先アドレスまたはアドレス グループ。詳細については、295 ページの「ファイアウォール アドレス」を参照してください。
[Service]	このポリシーを適用するサービス。詳細については、301 ページの「ファイアウォール サービス」を参照してください。
[DoS]	このポリシーで選択される DoS センサー。
[Interface]	このポリシーを適用するインタフェース。
[Status]	このオプションをオンにすると、DoS ポリシーが有効になります。このポリシーを無効にするには、このチェック ボックスをオフにします。詳しくは、266 ページの「ポリシーの有効化および無効化」を参照してください。
[Delete]	ポリシーをリストから削除します。
[Edit]	ポリシーを編集します。
[Insert]	対応するポリシーの上に新しいポリシーを追加する場合に選択します ([New Policy] 画面が表示されます)。
[Move]	対応するポリシーを、リスト内にある別のポリシーの前または後に移動します。

DoS ポリシーの設定

DoS ポリシー設定では、インタフェース、発信元アドレス、宛先アドレス、およびサービスを指定できます。ポリシーをトリガするには、指定された属性すべてがネットワーク トラフィックに一致する必要があります。

また、`config firewall interface-policy` CLI コマンドを使用することで、CLI から DoS ポリシーを追加できます。この CLI コマンドを使用して、IPS センサーまたはアプリケーション制御ブラック / ホワイト リストを、DoS ポリシーに追加することもできます。詳細については、『*FortiGateCLI リファレンス*』を参照してください。

`config firewall interface-policy6` コマンドを使用し、IPv6 スニファ ポリシーを追加できます。FortiGate IPv6 サポートの詳細については、186 ページの「FortiGate の IPv6 サポート」を参照してください。

DoS ポリシーを設定するには、*[Firewall]*、*[Policy]*、*[DoS Policy]* の順に選択し、[Create New] を選択して、DoS ポリシーの情報を入力します。*[OK]* を選択して、新しい DoS ポリシーを保存します。

[New Policy] ページ

このページでは、新しい DoS ポリシーを設定できます。[DoS Policy] ページで [Create New] を選択すると、このページの画面に自動的に移動します。

[Source Interface/Zone]	監視されるインタフェースまたはゾーン。
[Source Address]	アドレス、アドレス範囲、またはアドレス グループを選択し、トラフィック監視を指定のアドレスまたは範囲から送信されるネットワーク トラフィックに限定します。複数のアドレスまたは範囲を含む場合は、*[Multiple]* を選択します。[Create New] を選択することで、新しいアドレスまたはアドレス グループを追加できます。
[Destination Address]	アドレス、アドレス範囲、またはアドレス グループを選択し、トラフィック監視を、指定のアドレスまたは範囲に送信されるネットワーク トラフィックのみに限定します。複数のアドレスまたは範囲を含む場合は、*[Multiple]* を選択します。[Create New] を選択することで、新しいアドレスまたはアドレス グループを追加できます。

[Service]	定義済みのファイアウォール サービスまたはカスタム サービスを選択し、トラフィック監視を選択したサービスのみに限定します。[Create New] を選択することで、カスタム サービスを追加できます。
[DoS Sensor]	DoS センサーを選択、指定し、FortiGate ユニットにより、条件に一致するネットワーク トラフィックにセンサーが適用されるようにします。[Create New] を選択することで、新しい DoS センサーを追加できます。

プロトコルオプションの設定

[Protocol Options] メニューでは、複数のプロトコルを 1 つのプロトコル グループにグループ化しそれをファイアウォール ポリシーに適用するように、特定のプロトコルを設定できます。デフォルトのグループは、scan、strict、unfiltered、および web です。

プロトコルの特定の設定を含むプロトコル グループを設定するには、*[Firewall]*、*[Policy]*、*[Protocol Options]* の順に選択し、*[Create New]* を選択します。プロトコルごとに必要な情報を入力し、*[OK]* を選択します。

[Protocol Options] ページ

このページには、作成済みのプロトコル設定が一覧表示されます。このページでは、プロトコル設定グループの編集、削除、または新規作成が可能です。

[Create New]	[Create New] を選択すると、[Protocol Options Settings] ページの画面に自動的に移動します。
[Edit]	プロトコル設定を編集します。
[Delete]	リストから、プロトコル設定を削除します。
[Name]	このプロトコル グループの名前。このグループは、ファイアウォール ポリシーに適用するとき選択するグループです。
[Comments]	プロトコル グループの説明を記述します。

[Protocol Options Settings] ページ

このページでは、プロトコル グループを構成する個々のプロトコルのオプションを設定できます。

[Name]	このプロトコル グループの名前を入力します。
[Comments]	このプロトコル グループの説明を入力します。(入力はオプションです。)
[Enable Oversized File Log]	サイズ超過ファイルのロギングを可能にするとき選択します。
[Enable Invalid Certificate Log]	無効な証明書のロギングを可能にするとき選択します。
[HTTP] セクション	HTTP プロトコルを設定します。
[Port] (80、88、0-auto など)	IM を除くすべてのプロトコルで利用できます。
[Comfort Clients]	HTTP、FTP、および HTTPS のみで利用できます。 **[Interval] (1 から 900 秒)** ミ時間の間隔を秒単位で入力します。 **[Amount] (1 から 10240 バイト)** ミデータ量をバイト単位で入力します。
[Oversized File/Email]	すべてのプロトコルで利用できます。 **[Threshold]** ミ超過サイズの電子メール メッセージまたはファイルのしきい値量を MB 単位で入力します。
[Monitor Content Information for Dashboard]	[Dashboard] メニューからプロトコルの動作を表示するとき選択します。
[Enable Chunked Bypass]	chunked bypass の設定を有効にするとき選択します。
[FTP] セクション	FTP プロトコルを設定します。FTP セクションに [Enable Chunked Bypass] オプションが含まれないことを除き、FTP および HTTP には同じ設定が含まれています。
[IMAP] セクション	IMAP プロトコルを設定します。
[Allow Fragmented Messages]	

[POP3] セクション	POP3 プロトコルを設定します。このセクションには、IMAP セクションと同じ設定が含まれます。
[SMTP] セクション	SMTP セクションを設定します。
[Append Email Signature]	電子メール メッセージに表示される新しい電子メール シグネチャを入力するオプションを有効にするとき選択します。
[Email Signature Text]	"Yours sincerely" など、電子メール メッセージに表示するシグネチャを入力します。[Append Email Signature] を選択した場合のみ、利用可能です。
[IM] セクション	IM プロトコルを設定します。
[NNTP] セクション	NTTP プロトコルを設定します。
[HTTPS] セクション	HTTPS プロトコルを設定します。
[Allow Invalid SSL Certificate]	無効な SSL 証明書を許可するとき選択します。
[Enable Deep Scanning]	ディープ スキャンを有効にする場合に選択します。
[IMAP]	IMAPS プロトコルを設定します。
[POP3S]	POP3S プロトコルを設定します。このセクションには、IMAPS と同じ設定が含まれます。
[SMTPS]	SMTPS プロトコルを設定します。このセクションには、IMAPS および POP3 と同じ設定が含まれます。

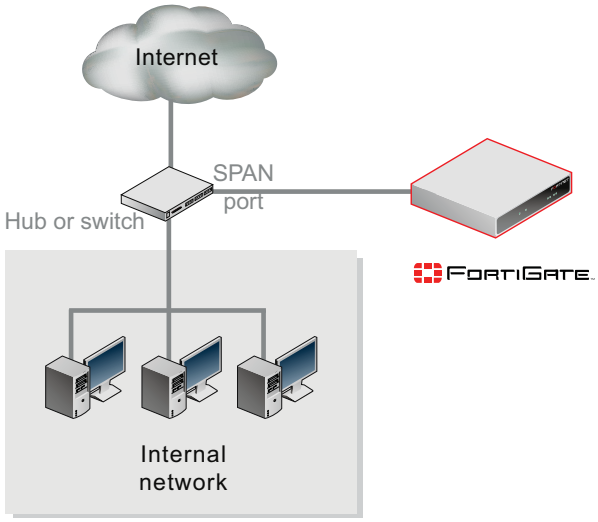
ネットワーク攻撃を検出するワンアーム スニファ ポリシーの使用

スニファ ポリシーを使用することで、実際にパケットを受信または処理することなく攻撃を検出するためにパケットのスニッフィングを行うことができ、これにより FortiGate ユニットインタフェースをワンアーム不正侵入検知システム (IDS) アプライアンスとして機能するように設定できます。

ワンアーム IDS を設定するには、1 つ以上の FortiGate インタフェースをワンアーム スニファ モードで機能するように設定する必要があります。この設定を行うには、*[System]*、*[Network]*、*[Interface]* の順に選択し、インタフェースを編集して、*[Enable one-arm sniffer]* モードを選択します。インタフェースをワンアーム スニファ モードで機能するように設定すると、そのインタフェースを他の目的では使用できなくなります。たとえば、そのインタフェースのファイアウォール ポリシーを追加すること、およびインタフェースをゾーンに追加することは、いずれもできません。

注記：VLAN インタフェースを、ワンアーム スニファ機能に設定されたインタフェースに追加する場合、この VLAN インタフェースによるワンアーム スニファ モードでの機能が可能となり、この VLAN インタフェースのスニファ ポリシーを追加できます。

図 7: ワンアーム IDS トポロジ



インタフェースをワンアーム スニファ モードに設定した後、そのインタフェースをハブ、またはネットワーク トラフィックを処理するスイッチの SPAN ポートに接続します。次に、*[Firewall]*、*[Policy]*、*[Sniffer Policy]* の順に選択し、その FortiGate インタフェースのスニファ ポリシーを追加できます。このインタフェースには、DoS センサー、IPS センサーに加えて、インタフェースがハブまたは SPAN (Switched Port Analyzer) ポートから受信するトラフィックに含まれる攻撃などの挙動を検知するための、アプリケーション ブラック / ホワイト リストが含まれています。

ワンアーム スニファ モードでは、スニファ モード ポリシーによって受け付けられるパケットのみをインタフェースで受信します。スニファ モード ポリシーによって受信されないパケットは、すべて破棄されます。スニファ モード ポリシーにより受信されるすべてのパケットは、IPS インスペクションを経由し、IPS による分析後に破棄されます。

ワンアーム IDS は、トラフィックをブロックできません。しかし、DoS および IPS センサーおよびアプリケーション ブラック / ホワイト リストでロギングを有効にする場合、FortiGate ユニットは検知されたすべての攻撃およびアプリケーションのログ メッセージを記録します。

このトピックでは、スニファ ポリシー設定の基礎について説明します。詳細については、『*FortiGate UTM ユーザ ガイド*』を参照してください。

スニファ ポリシー リストの表示

スニファ ポリシー リストには、それぞれのインタフェース、発信元 / 宛先アドレス ペア、およびサービスとの一致の優先順に、スニファ ポリシーが表示されます。

FortiGate ユニットで、バーチャル ドメインが有効に設定されている場合は、各バーチャル ドメインごとに個別のスニファ ポリシーを設定しますが、ポリシーを設定するにはまずバーチャル ドメインにアクセスする必要があります。バーチャル ドメインにアクセスするには、*[System]*、*[VDOM]* の順に選択し、ポリシーを設定するバーチャル ドメインに該当する行で、*[Enter]* を選択します。

スニファ ポリシー リスト内のポリシーは、追加、削除、編集、および並べ替えが可能です。スニファ ポリシーの順序は、ポリシー照合に影響します。ファイアウォール ポリシーおよび DoS ポリシーと同様に、スニファ ポリシー リストに表示される順序で一度に 1 つずつ、上位から下位へスニファ ポリシー がトラフィックと照合されます。一致するポリシーが見つかると、そのポリシーが使用され、以降のスニファ ポリシー照合は中止されます。どのポリシーとも一致しない場合、パケットは破棄されます。

スニファ ポリシー リストを表示するには、*[Firewall]*、*[Policy]*、*[Sniffer Policy]* の順に選択します。

[Sniffer Policy] ページ

このページには、作成済みのスニファ ポリシーが一覧表示されます。このページでは、スニファ ポリシーの編集、削除、または新規作成が可能です。また、ポリシーの移動または新しいポリシーの挿入が可能です。

[Create New]	新しいスニファ ポリシーを追加します。[Create New] の横にある下向き矢印を選択し、新しいセクションをリストに追加し、ポリシーをグループ化して表示します。
[Column Settings]	テーブルの表示をカスタマイズします。カラムの表示、非表示を選択し、テーブル内のカラムの表示順序を指定することができます。詳しくは、34 ページの「表示されるカラムのカラム設定を使用した制御」を参照してください。
[Section View]	インタフェースにより構成されているファイアウォール ポリシーを表示するとき選択します。
[Global View]	すべてのファイアウォール ポリシーをシーケンス番号の順番に並べるとき選択します。
[Filter] アイコン	指定した条件に応じてポリシー リストをフィルタ処理または並べ替えるための、カラム フィルタを編集します。詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。
[ID]	ポリシーごとに固有の識別子。ポリシーには、作成された順序で番号が付けられます。
[Source]	このポリシーを適用する発信元アドレスまたはアドレス グループ。詳細については、295 ページの「ファイアウォール アドレス」を参照してください。
[Destination]	このポリシーを適用する宛先アドレスまたはアドレス グループ。詳細については、295 ページの「ファイアウォール アドレス」を参照してください。
[Service]	このポリシーを適用するサービス。詳細については、301 ページの「ファイアウォール サービス」を参照してください。
[DoS]	このポリシーで選択される DoS センサー。
[Sensor]	このポリシーで選択される IPS センサー。
[Application Black/White List]	このポリシーで選択されるアプリケーション ブラック/ホワイト リスト。
[Status]	このオプションをオンにすると、DoS ポリシーが有効になります。このポリシーを無効にするには、このチェック ボックスをオフにします。詳しくは、266 ページの「ポリシーの有効化および無効化」を参照してください。
[Delete]	ポリシーをリストから削除します。
[Edit]	ポリシーを編集します。
[Insert Policy Before]	対応するポリシーの上に新しいポリシーを追加する場合に選択します ([New Policy] 画面が表示されます)。
[Move To]	対応するポリシーを、リスト内にある別のポリシーの前または後に移動します。

スニファ ポリシーの設定

スニファ ポリシー設定を使用し、インタフェース、発信元アドレス、宛先アドレス、およびサービスを指定します。ポリシーをトリガするには、指定された属性すべてがネットワーク トラフィックに一致する必要があります。

また、`config firewall sinff-interface-policy` CLI コマンドを使用することで、CLI からスニファ ポリシーを追加できます。詳細については、『*FortiGateCLI リファレンス*』を参照してください。

`config firewall sniff-interface-policy6` コマンドを使用し、IPv6 スニファ ポリシーを追加できます。FortiGate IPv6 サポートの詳細については、186 ページの「FortiGate の IPv6 サポート」を参照してください。

[New Policy] ページ

このページでは、新しいスニファ ポリシーを設定できます。[Sniffer Policy] ページで [Create New] を選択すると、このページの画面に自動的に移動します。

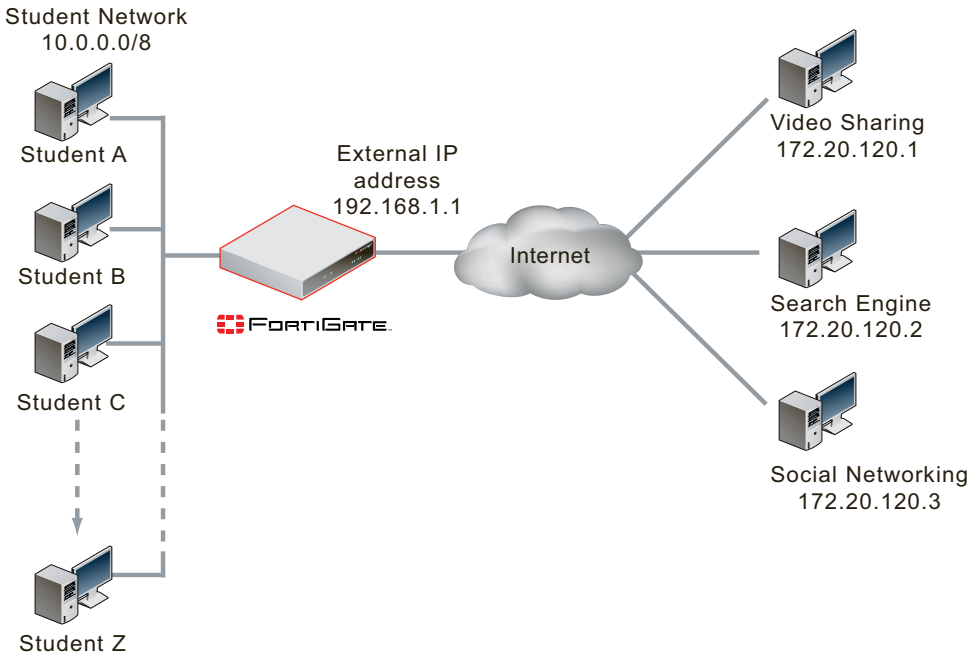
[Source Interface/Zone]	監視されるインタフェースまたはゾーン。

[Source Address]	アドレス、アドレス範囲、またはアドレス グループを選択し、トラフィック監視を指定のアドレスまたは範囲から送信されるネットワーク トラフィックに限定します。複数のアドレスまたは範囲を含む場合は、*[Multiple]* を選択します。[Create New] を選択することで、新しいアドレスまたはアドレス グループを追加できます。
[Destination Address]	アドレス、アドレス範囲、またはアドレス グループを選択し、トラフィック監視を、指定のアドレスまたは範囲に送信されるネットワーク トラフィックのみに限定します。複数のアドレスまたは範囲を含む場合は、*[Multiple]* を選択します。[Create New] を選択することで、新しいアドレスまたはアドレス グループを追加できます。
[Service]	定義済みのファイアウォール サービスまたはカスタム サービスを選択し、トラフィック監視を選択したサービスのみに限定します。[Create New] を選択することで、カスタム サービスを追加できます。
[DoS Sensor]	DoS センサーを選択、指定し、FortiGate ユニットにより、条件に一致するネットワーク トラフィックにセンサーが適用されるようにします。[Create New] を選択することで、新しい DoS センサーを追加できます。
[IPS Sensor]	IPS センサーを選択、指定し、FortiGate ユニットにより、条件に一致するネットワーク トラフィックにセンサーが適用されるようにします。[Create New] を選択することで、新しい IPS センサーを追加できます。
[Application Black/White List]	アプリケーション ブラック / ホワイト リスト センサーを選択、指定し、FortiGate ユニットにより、条件に一致するネットワーク トラフィックにそのリストが適用されるようにします。[Create New] を選択することで、新しいアプリケーション ブラック / ホワイト リストを追加できます。

FortiOS での未使用 NAT ポートの選択方法

次のような、大学での実装に最適なトポロジについて考えてみます。ここでは、学生は FortiGate ユニットを経由してインターネットに接続できます。

図 8: 大学でのインターネット接続トポロジ例



大学からは、グローバル IP アドレスが学生に付与されません。学生は、DHCP を使用し、10.0.0.0/8 の範囲にある IP アドレスを FortiGate ユニットから取得します。FortiGate ユニットでは、NAPT (Network Address Port Translation) によりすべてのトラフィックが変換され、トラフィックが 192.168.1.1 の IP アドレスから送信されていると見なされます。

たとえば、学生 A (IP アドレス 10.78.33.97) が検索エンジン (IP アドレス 172.20.120.2) に接続し、以下の IP アドレスおよびポート番号をともなうパケットを送信しようとする場合を考えます。

```
src-ip: 10.78.33.97
dst-ip: 172.20.120.2
src-port: 10000
dst-port: 80
```

NAT が有効な状態で、このパケットが FortiGate ユニットを通過すると、パケットは以下のように編集されます。

```
src-ip: 192.168.1.1
dst-ip: 172.20.120.2
src-port: 46372
dst-port: 80
```

ここでは、192.168.1.1 は FortiGate ユニットの外部 IP アドレス、46372 は FortiGate ユニットにより選ばれる未使用ポートです。

以下の項では、未使用ポート選択の 3 つのソリューションについて説明します。これら 3 つのソリューションの説明を念頭に、さらに続く項では、FortiOS で使用される未使用ポート選定方法について説明します。

グローバル プール

この方法では、割り当て可能なポートのプールが 1 つあります。ポートが割り当てられると、そのポートがプールから削除されます。ポートがプールから削除されるので、同じポートを 2 回割り当てることはできません。ポートを NAT に使用する必要がなくなると、そのポートがプールに戻され、再び割り当て可能になります。

たとえば、ポートの範囲が 0x7000 (28672) から 0xF000 (61440) の場合、同時に使用可能なポート数は 2^{15} (32,768) となります (この範囲を選んだ理由については後述を参照)。同時に接続可能な最大数は 32,768 ですが、この数はトランスポート プロトコルに関わらず変わりません。

この手法は、実装が容易なために、NAT ポートの選択に最初に使用されたアプローチの 1 つでした。接続数がプールの規模より少ないと考えられる場合、たとえばホーム利用向けの NAT ファイアウォールなどでは、この方法は有効です。一方、大規模な大学または ISP など、数千に及ぶ同時セッションを日常的に処理する場合には、有効なソリューションとはいえません。

このソリューションは、FortiOS で使用される手法ではありません。

プロトコルによるグローバル プール

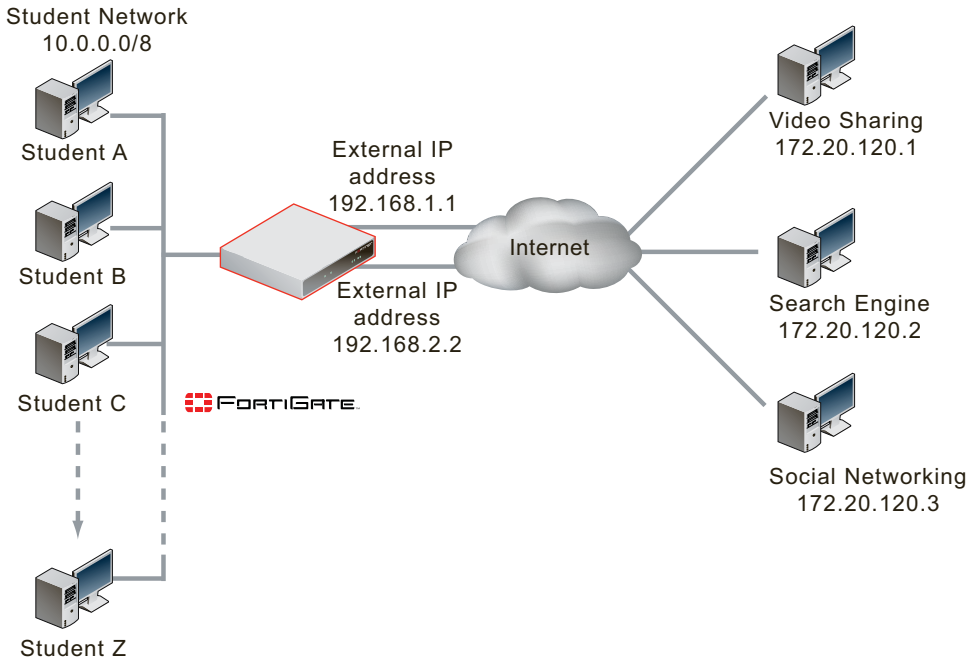
プロトコルによるグローバル プールの場合、TCP および UDP で個別のプールを使用することにより、グローバル プールの手法を拡張します。この手法では、選択されるプールは使用されるプロトコルに応じて決まります。同じ 32,768 ポートの範囲では、UDP に 32,768 ポート、および TCP に 32,768 ポートを使用でき、ポートの総計は 65,536 となります。結果的に使用可能なポートは 2 倍になりますが、大学または ISP にはまだ不十分です。

このソリューションは、FortiOS で使用される手法ではありません。

NAT IP によるプール

NAT IP によるプールの場合、プロトコルによるプールに加えて、NAT IP に応じてプールが決まることにより、ポート選択の手法をより拡張しています。これにより、プールはプロトコルおよび NAT IP に応じて決まります。284 ページの図 8 に示されるトポロジでは、NAT IP は 192.168.1.1 です。NAT IP が 1 つだけ使用されている場合は、この手法はプロトコルによるグローバル プールと変わりません。一方、図 9 に示されるトポロジを見ると、2 つの個別のインターネット接続があり、2 つの NAT IP アドレス、192.168.1.1 および 192.168.2.2 が使用されています。

図 9: 2 つのインターネット接続をともなう大学インターネット接続トポロジ例



FortiGate の構成に等価コスト マルチパス (ECMP) ルーティングが含まれる場合、両方のインターネット接続を同時に使用でき、最大接続数は N*R*P となります。ここでは、N は NAT IP アドレス数、R はポート範囲、*P* はプロトコル数となります。これにより、2 つの NAT IP が使用され、ポート範囲が 32,768、プロトコルが TCP と UDP という上述のケースでは、最大同時接続数は次のようになります。

```
2*32768*2 = 131,072
```

このソリューションは、展開可能な NAT IP の数に応じてスケーリング可能なので、大学または小規模な ISP で問題なく利用できます。

このソリューションは、FortiOS で使用される手法ではありません。

NAT IP、宛先 IP、ポート、およびプロトコルによるプール

FortiOS では、この手法が使用されます。

NAT IP、宛先 IP、ポート、およびプロトコルによるプールでは、プロトコル、NAT IP、宛先 IP、および宛先ポートによりプールが決まるように、ポート選定の手法がさらに拡張されます。

プールを決めるためにこれらの属性を利用するのは、FortiOS ファイアウォールがセッション ベースに設計されているためです。FortiGate ユニットを通過し TCP 接続が確立されると、セッションが作成され、このセッション用に 2 つのインデックスが作成されます。FortiGate ユニットでは、これらのインデックスを使用し、条件と一致するトラフィックをセッションに導きます。

インデックスの 1 つは、セッション作成を開始したパケットと同じ方向のトラフィックに対応します。

```
src-ip: 10.78.33.97
dst-ip: 172.20.120.2
proto:tcp
src-port: 10000
dst-port: 80
```

もう 1 つのインデックスは、逆方向 (返信) のトラフィックに対応します。

```
src-ip: 172.20.120.2
dst-ip: 192.168.1.1
proto:tcp
```

```
src-port: 80
dst-port: 46372
```

ここでは、46372 は選択された NAT ポートです。いずれの場合も、トラフィックがいずれかのインデックスに一致すると、トラフィックが属するセッションを一意に識別できます。

NAT IP、宛先 IP、ポート、およびプロトコルによるプールでは、NAT ポートを選択するとき、FortiOS は、選択されたポートおよび他の 4 項目の属性の組み合わせが、セッションを一意に識別する固有の属性となるようことを保証しさえすればよくなります。たとえば、学生 A が、検索エンジン (宛先 IP アドレス 172.20.120.2) への接続をポート 443 で同時に確立する場合、もう 1 つのセッションが作成され、返信方向のインデックスは以下のようになります。

```
src-ip: 172.20.120.2
dst-ip: 192.168.1.1
proto:tcp
src-port: 443
dst-port:NP
```

5項目の値が組み合わせとして固有であれば、NPはどのような値も可能です。たとえば、FortiOSが再び 46372 を選ぶことも可能です。

```
src-ip: 172.20.120.2
dst-ip: 192.168.1.1
proto:tcp
src-port: 443
dst-port: 46372
```

上記の組み合わせが可能なのは、

```
src-ip: 172.20.120.2
dst-ip: 192.168.1.1
proto:tcp
src-port: 80
dst-port: 46372
```

および

```
src-ip: 172.20.120.2
dst-ip: 192.168.1.1
proto:tcp
src-port: 443
dst-port: 46372
```

に、異なる src-port の値が含まれるためです。

NAT IP、宛先 IP、ポート、およびプロトコルによるプールの手法を使用することで、32,768 ポートのプールを、src-ip、dst-ip、proto、および src-port の固有の組み合わせごとに利用できます。.

サポートされる最大同時接続数は、N*R*P*D*Dp となります。ここでは、N は利用可能な NAT IP アドレスの数、R はポート範囲、P はプロトコルの数、D は固有の宛先 IP アドレスの数、Dp は固有の宛先ポートの数となります。

利用可能な宛先 IP アドレスが多数ある場合は、サポートされる同時接続の数は非常に多くなります。その数がどの程度の大きさかを知るために、宛先 IP アドレスが 1 つ、および NAT IP アドレスが 1 つで計算すると、N=1、R=32,768、P=2、D=1、および Dp=32,768 の条件から、次が得られます。

```
1 * 32,768 * 2 * 1 * 32,768 = 2,147,483,648.
```

この計算の問題点は、32,768 の宛先ポートがすべて使用されるわけではない点です。実際、多くの組織では、必須のインターネット トラフィックは宛先ポート 80 を使用する Web トラフィックで、すべて TCP プロトコルを使用します。このため、TCP プロトコルを使用する 1 つの NAT IP アドレスから 1 つの宛先 IP アドレスの Web トラフィックに対応するプール サイズ限度は、N=1、R=32,768、P=1、D=1、および Dp=1 から、以下が得られます。

```
1* 32,768 * 1 * 1 * 1 = 32,768
```

284 ページの図 8 に示されるトポロジでは、検索エンジン、ソーシャル ネットワーキング、およびビデオ共有サイトに TCP ポート 80 で同時接続する学生の場合、各サイトで 1 つの IP アドレスを使用するとき、各サイトで最大 32,768 の同時接続が可能となり、接続の総計は 32,768 * 3 = 98,304 となります。

多くの大規模なパブリック Web サイトでは、ラウンドロビン DNS を使用することで、4 つ以上の IP アドレスをローテーションすることがあります。検索エンジンおよびビデオ共有サイトでこの方式を使用し、IP 使用負荷を均一にすると、検索エンジンへは最大 4 * 32,768 = 131,072 の接続、ビデオ共有サイトへは 131,072 の接続、ソーシャル ネットワーキング サイトへは 32,768 の接続、総計 294,912 の個別の接続が単一の FortiGate によりサポートされ、1 つの NAT IP および総計 9 つの宛先 IP アドレス、および 1 つの宛先ポートが使用されます。

ファイアウォール ポリシーの例

FortiGate ユニットは、自宅での使用から、SOHO、さらには大規模企業や ISP までの、さまざまなネットワーク要件を完全に満たすことができます。次の 2 つのシナリオでは、SOHO および大規模企業環境におけるファイアウォール ポリシーの実用的な応用を示します。

このトピックには、以下の項目が含まれています。

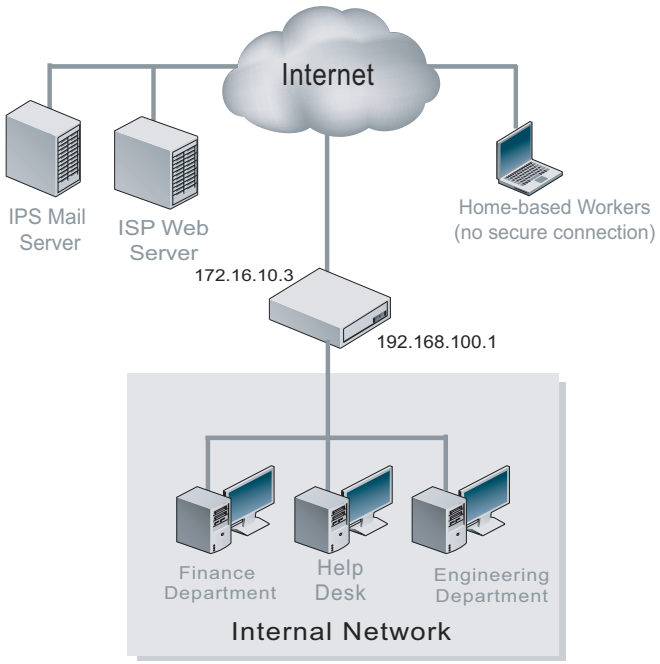
- 例 1:SOHO 規模の企業
- 例 2: 大規模企業
- ファイアウォール ポリシー リストの表示
- ファイアウォール ポリシーの設定

例 1:SOHO 規模の企業

企業 A は、開発を行い、カスタマ サポートを提供している小規模なソフトウェア会社です。15 台のコンピュータから成る内部ネットワークに加えて、フルタイムまたはパートタイムで自宅で作業を行う複数の従業員も抱えています。

現在のネットワーク トポロジでは、15 台の内部コンピュータのすべてがルータの背後に配置されているため、外部の ISP メール サーバや Web サーバにアクセスする必要があります。自宅作業従業員はすべて、セキュリティ保護されていない、オープンなコネクションを介してルータにアクセスします。

図 10: FortiGate をインストールする前の SOHO ネットワークの例



企業 A には、自宅作業者のためのセキュアな接続が必要です。他の多くの企業と同様に、この企業も、ビジネスの遂行を電子メールやインターネット アクセスに大きく依存しています。この企業は、ネットワーク攻撃を検出および阻止し、ウイルスをブロックし、スパムを減らすための総合的なセキュリティ ソリューションを望んでいます。また、異なる部門に対して異なる保護設定を適用したいと考えています。さらに、Web サーバおよび電子メール サーバをそのセキュリティ ソリューションに統合することも希望しています。

最初の要件に対処して、自宅作業者と内部ネットワークの間のセキュアな通信を保証するために、企業 A は、自宅作業者ごとに個別のポリシーを設定します。

1 *[Firewall]*、*[Policy]* の順に選択します。

2 *[Create New]* を選択し、Home_User_1 のための次の設定を入力または選択します。

[Interface/Zone]	[Source]:internal	[Destination]:wan1
[Address]	[Source]:CompanyA_Network	[Destination]:Home_User_1
[Schedule]	Always	
[Service]	ANY	
[Action]	IPSEC	
[VPN Tunnel]	Home1	
[Allow Inbound]	オン	
[Allow outbound]	オン	
[Inbound NAT]	オン	
[Outbound NAT]	オフ	
[Protection Profile]	チェック ボックスをオンにして、[standard_profile] を選択します。	

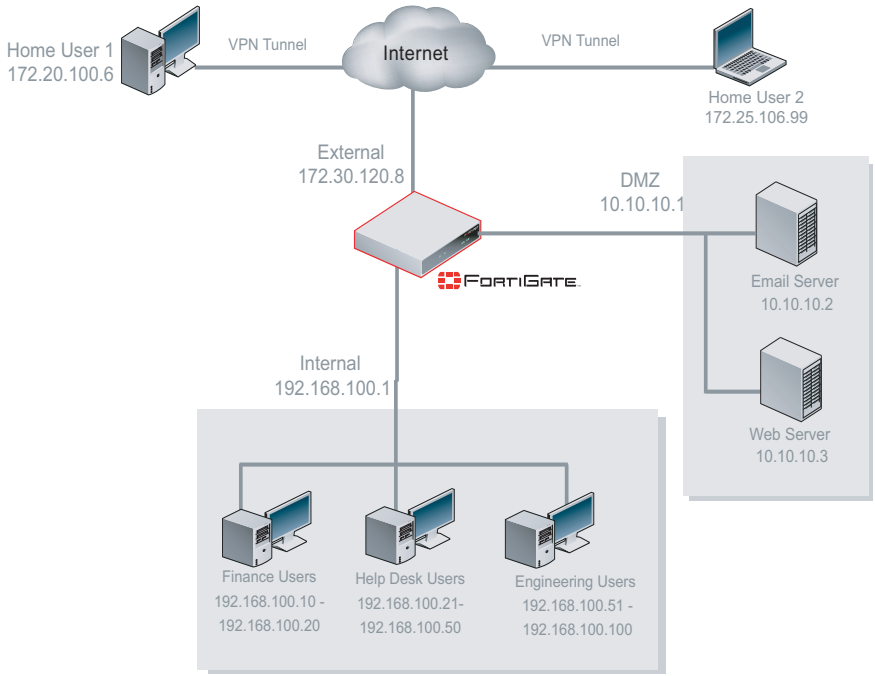
3 *[OK]* を選択します。

4 *[Create New]* を選択し、Home_User_2 のための次の設定を入力または選択します。

[Interface/Zone]	[Source]:internal	[Destination]:wan1
[Address]	[Source]:CompanyA_network	[Destination]:All
[Schedule]	Always	
[Service]	ANY	
[Action]	IPSEC	
[VPN Tunnel]	Home2_Tunnel	
[Allow Inbound]	オン	
[Allow outbound]	オン	
[Inbound NAT]	オン	
[Outbound NAT]	オフ	
[Protection Profile]	チェック ボックスをオンにして、[standard_profile] を選択します。	

5 *[OK]* を選択します。

図 11: FortiGate-100 を使用した SOHO ネットワーク トポロジ



提案されたネットワークは、ForitGate 100A ユニットに基づいています。15 台の内部コンピュータは、FortiGate ユニットの背後に配置されています。これらのコンピュータは現在、DMZ 内にある電子メール サーバおよび Web サーバ (同様に、FortiGate ユニットの背後に配置されている) にアクセスします。すべての自宅作業従業員が、VPN トンネルを経由して、FortiGate ユニットを介してオフィス ネットワークにアクセスするようになりました。

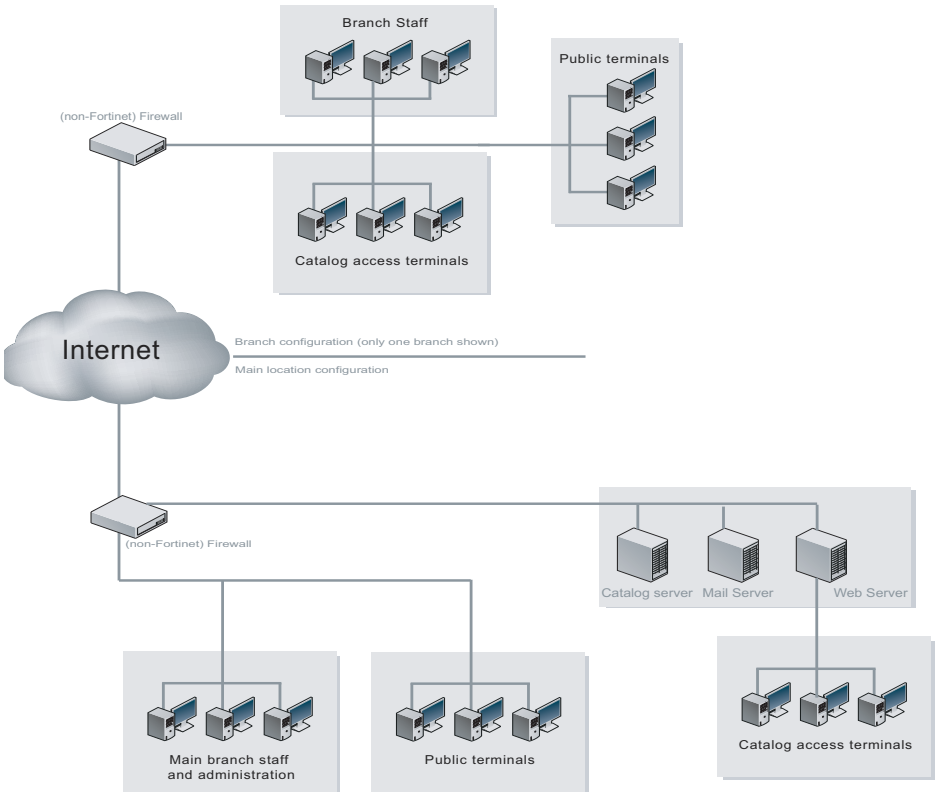
例 2: 大規模企業

大都市に位置する図書館システムは、人口の大多数にサービスを提供している都市中心部の本館を主体とするとともに、10 数の分館が市内全域に分散しています。各分館はインターネットに接続されていますが、専用の接続によって互いにリンクされているところは 1 つもありません。

本館の現在のネットワーク トポロジは、3 つのユーザ グループで構成されています。本館職員や公共端末は、ファイアウォールの背後に位置する DMZ 内のサーバにアクセスします。カタログ アクセス端末は、ファイアウォールを経由することなく、直接カタログ サーバにアクセスします。

分館には、本館にあるサーバに、セキュリティ保護されていないインターネット接続を介してアクセスする 3 ユーザが存在します。

図 12: 図書館システムの現在のネットワーク トポロジ



図書館は、利用者と職員に対して異なるアクセス レベルを設定できる必要があります。

本館職員のための最初のファイアウォール ポリシーでは、インターネットへの常時フル アクセスを許可します。2 番目のポリシーでは、職員の DMZ への直接アクセスを許可します。分館職員にこれと同じアクセスを許可するために、ポリシーの 2 番目のペアが必要です。

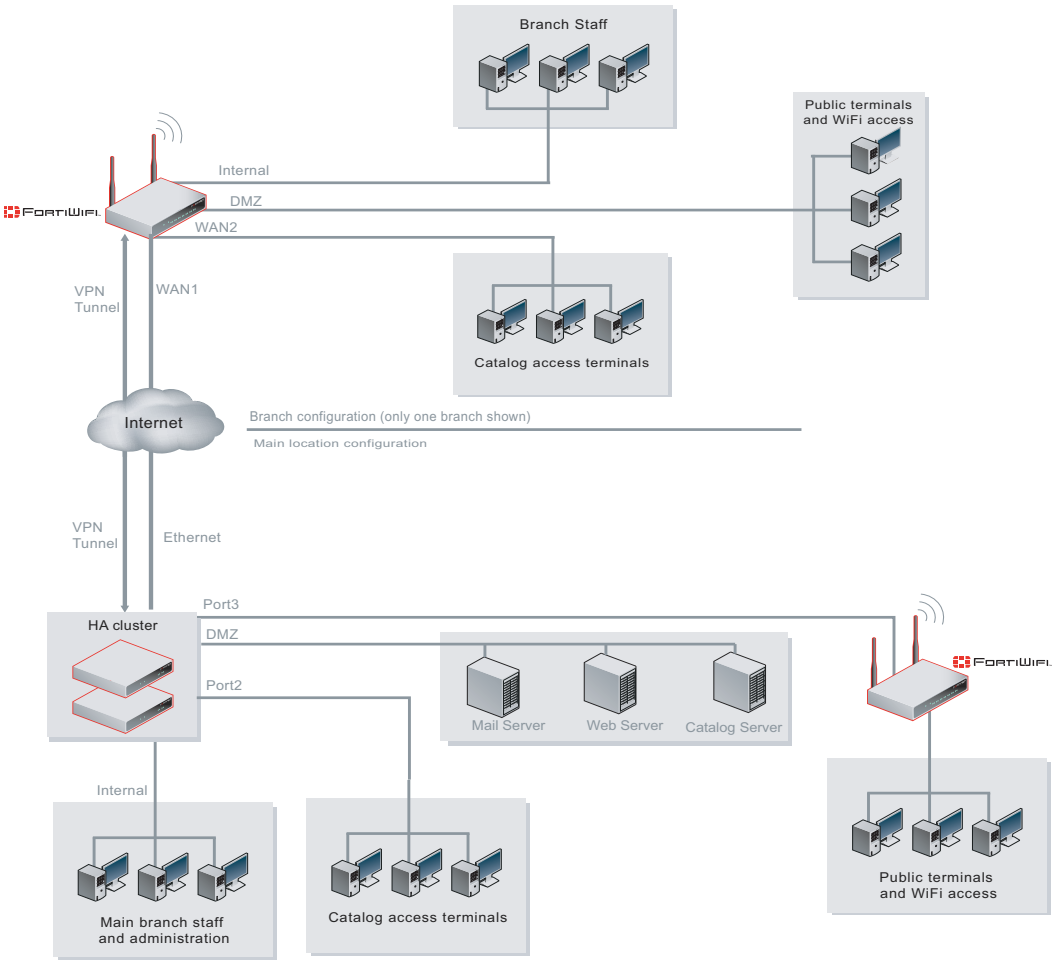
職員のすべてのファイアウォール ポリシーで、職員のアクセス専用に設定されたプロテクション プロファイルを使用します。有効になっている機能には、ウイルス スキャン、電子メール フィルタリング、IPS、および P2P トラフィックすべてのブロッキングが含まれます。また、アドバタイズ、マルウェア、およびスパイウェア サイトをブロックするために、FortiGuard Web フィルタリングも使用されます。

Web サーバやカタログ サーバの設定方法によっては、サーバに関する情報を更新するために、一部のユーザにこれらのサーバへの特殊なアクセスが必要になる可能性があります。この特殊なアクセスは、IP アドレスまたはユーザに基づいて許可されます。

提案されたトポロジの場合、本館職員とカタログ アクセス端末は、FortiGate HA クラスタを経由して、DMZ 内のサーバにアクセスします。公共のアクセス端末は、最初に ForitWiFi ユニットを経由して (ここで、追加のポリシーを適用できます) HA クラスタにアクセスし、最後にサーバに到達します。

分館では、3 ユーザがすべて、VPN トンネルを経由して、ForitWiFi ユニットを介して本館にルーティングされます。

図 13: 提案された図書館システムのネットワーク トポロジ



ポリシーは、*[Firewall]*、*[Policy]*、*[Policy]* の順に選択して設定します。プロファイルは、[UTM] メニューで設定し、たとえばアンチウイルス プロファイルは、*[UTM]*、*[Antivirus]*、*[Profile]* の順に選択して設定します。

本館の " 職員からインターネットへの " ポリシー :

[Source Interface]	Internal
[Source Address]	All
[Destination Interface]	External
[Destination Address]	All
[Schedule]	Always
[Action]	Accept

本館の " 職員から DMZ への " ポリシー :

[Source Interface]	Internal
[Source Address]	All
[Destination Interface]	DMZ
[Destination Address]	Servers
[Schedule]	Always
[Action]	Accept

分館の " 職員からインターネットへの " ポリシー :

[Source Interface]	Branches
[Source Address]	Branch Staff
[Destination Interface]	External
[Destination Address]	All
[Schedule]	Always
[Action]	Accept

分館の " 職員から DMZ への " ポリシー :

[Source Interface]	Branches
[Source Address]	Branch Staff
[Destination Interface]	DMZ
[Destination Address]	Servers
[Schedule]	Always
[Action]	Accept

これらの例の詳細については、次の資料を参照してください。

- *SOHO および SMB の設定サンプル ガイド*
- *Forti の大規模企業の設定例*

ファイアウォール アドレス

ファイアウォール アドレスおよびアドレス グループは、ファイアウォール ポリシーの [Source Address] および [Destination Address] フィールドを設定するときに使用できるネットワーク アドレスです。FortiGate ユニットでは、パケット ヘッダに含まれる IP アドレスとファイアウォール ポリシーの発信元および宛先アドレスを比較することで、ファイアウォール ポリシーがそのトラフィックに一致するかを判定します。IPv4 アドレスおよびアドレス範囲、IPv6 アドレス、および完全修飾ドメイン名 (FQDN) を追加できます。

関連するアドレスをアドレス グループに、および関連する IPv6 アドレスを IPv6 アドレス グループにそれぞれ構成し、ファイアウォール ポリシー リストを簡素化できます。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとにファイアウォール アドレスを個別に設定しますが、アドレスを設定するにはまずバーチャル ドメインにアクセスする必要があります。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には以下のトピックが含まれています。

ファイアウォール アドレスについて

注意: 完全修飾ドメイン名 (FQDN) のファイアウォール アドレスを使用する場合は、注意が必要です。ファイアウォール ポリシーで FQDN を使用すると便利な反面、一部にセキュリティ リスクが発生します。これは、FQDN を使用する場合、ポリシー照合のとき信頼できる DNS サーバに依存するためです。万一 DNS サーバの信頼が失われると、ドメイン名の名前解決を必要とするファイアウォール ポリシーは、正常に機能しなくなる可能性があります。

この項では、ファイアウォール アドレス追加のオプションについて説明します。これらのオプションには、IPv4 アドレス、アドレス範囲、または完全修飾ドメイン名 (FQDN) があります。IPv6 アドレスの追加も可能です。詳しくは、296 ページの「IPv6 ファイアウォール アドレスについて」を参照してください。

1 つのファイアウォール アドレスには、1 つ以上のネットワーク アドレスが含まれます。ネットワーク アドレスは、ネットマスクをともなう IP アドレス、IP アドレス範囲、または完全修飾ドメイン名 (FQDN) によって表すことができます。

ネットマスクをともなう IP アドレスによりホストを表す場合、この IP アドレスで 1 つ以上のホストを表すことができます。たとえば、ファイアウォール アドレスは次のようになります。

- `192.45.46.45` などの、単一のコンピュータ
- クラス C サブネットの `192.168.1.0` などの、サブネットワーク
- `0.0.0.0`、これはあらゆる IP アドレスに該当

ネットマスクは、追加されるアドレスのサブネット クラスに対応し、ドット区切り 10 進数または CIDR 形式のいずれかで表すことができます。FortiGate ユニットは、CIDR 形式のネットマスクをドット区切り 10 進数の形式に自動的に変換します。たとえば、次のような形式になります。

- 単一コンピュータのネットマスク：255.255.255.255、または /32
- クラス A サブネットのネットマスク：255.0.0.0、または /8
- クラス B サブネットのネットマスク：255.255.0.0、または /16
- クラス C サブネットのネットマスク：255.255.255.0、または /24
- すべての IP アドレスを含むネットマスク： 0.0.0.0

有効な IP アドレスおよびネットマスクの形式には、以下があります。

- x.x.x.x/x.x.x.x（192.168.1.0/255.255.255.0 など）
- x.x.x.x/x（192.168.1.0/24 など）

注記：ネットマスク 255.255.255.255 をともなう IP アドレス 0.0.0.0 は、有効なファイアウォール アドレスではありません。

IP 範囲によりホストを表す場合、その範囲は、サブネット内の連続する IP アドレスを持つホストを示し、192.168.1.[2-10]、または 192.168.1.* のようになります。これにより、そのサブネット上のホストの完全な範囲を示します。有効な IP 範囲の形式には、次があります。

- x.x.x.x-x.x.x.x（192.168.110.100-192.168.110.120 など）
- x.x.x.[x-x]（192.168.110.[100-120] など）
- x.x.x.*（192.168.110.* など）

FQDN によりホストを表す場合、ドメイン名は、mail.example.com などのサブドメインが可能です。単一の FQDN ファイアウォール アドレスを使用することにより、負荷分散および高可用性（HA）での設定のように、ファイアウォール ポリシーを複数のホストに適用できます。FortiGate ユニットは、すべてのアドレスを自動的に決定し、FQDN から解決されるすべてのアドレスの記録を保持します。有効な FQDN の形式には、次があります。

- <host_name>.<second_level_domain_name>.<top_level_domain_name>（mail.example.com など）
- <host_name>.<top_level_domain_name>

ファイアウォール ポリシーで FQDN を使用すると、FortiGate ユニットにより DNS TTL を追跡記録し、レコードの変化に対応できるようになるという特長があります。この特長により、ダイナミック IP アドレスに合わせてファイアウォール アドレスを変更する保守作業の要件を軽減できます。さらにこれにより、DHCP を使用するダイナミック アドレスが設定されているネットワークのファイアウォール ポリシーを作成できます。

IPv6 ファイアウォール アドレスについて

デフォルトでは、IPv6 ファイアウォール アドレスは、CLI からのみ設定できます。Web ベースマネージャで IPv6 設定を可能にする方法については、184 ページの「設定」を参照してください。

1 つの IPv6 ファイアウォール アドレスには、1 つの IPv6 アドレス、または IPv6 アドレスとサブネットを含むことができます。IPv6 アドレス範囲を追加することはできません。

IPv6 ファイアウォール アドレスの例。

```
3ffe:ffff:1011:f101:0210:a4ff:fee3:9566/128
```

ネットマスクの /128 は、FortiGate ユニットにより追加されています。

サブネットの IPv6 ファイアウォール アドレスの例。

```
2001:470:1f0e:162::/64
```

[IPv6 Address] フィールドは、34 文字前後に制限されるので、完全な IPv6 アドレスおよびネットマスクは追加できません。このため、例示されるように、短い形式のネットマスクを使用します。

IPv6 アドレスを FortiGate インタフェースに割り当てることはできません。

ファイアウォール アドレス リストの表示

VDOM

リスト中のファイアウォール アドレスは、IP/Netmask、FQDN、または IPv6 の種類ごとにグループ化されています。FortiGate ユニットのデフォルト設定には、あらゆるネットワーク上のすべての IPv4 アドレスを表す *all* アドレスが含まれています。

アドレス リストを表示するには、*[Firewall]*、*[Address]*、*[Address]* の順に選択します。

[Address] ページ

このページには、IP アドレス グループが一覧表示されます。このページでは、IP アドレス グループの編集、削除、または新規作成が可能です。

[Create New]	ファイアウォール アドレスを追加します。[Create New] を選択すると、[New Address] ページの画面に自動的に移動します。 *[IPv6 Support]* が有効に設定されている場合は、*[Create New]* の下向き矢印を選択し、*[IPv6 Address]* を選択して、IPv6 ファイアウォール アドレスを追加できます。Web ベース マネージャで IPv6 サポートを有効にする方法については、184 ページの「設定」を参照してください。
[Name]	ファイアウォール アドレスの名前。
[Address/FQDN]	IP アドレスとネットマスク、IP アドレス範囲、または完全修飾ドメイン名。
[Interface]	IP アドレスを関連づける、インタフェース、ゾーン、またはバーチャル ドメイン (VDOM)。
[IP/Netmask]	IPv4 ファイアウォール アドレスおよびアドレス範囲のリスト。
[FQDN]	完全修飾名ファイアウォール アドレスのリスト。
[IPv6]	IPv6 ファイアウォール アドレスのリスト。
[Delete]	アドレスを削除するとき選択します。*[Delete]* アイコンは、このアドレスがファイアウォール ポリシーまたはアドレス グループにより使用されていない場合のみ表示されます。
[Edit]	アドレスを編集するとき選択します。

アドレスの設定

注意： 完全修飾ドメイン名 (FQDN) のファイアウォール アドレスを使用する場合は、注意が必要です。ファイアウォール ポリシーで FQDN を使用すると便利な反面、一部にセキュリティ リスクが発生します。これは、FQDN を使用する場合、ポリシー照合のとき信頼できる DNS サーバに依存するためです。万一 DNS サーバの信頼が失われると、ドメイン名の名前解決を必要とするファイアウォール ポリシーは、正常に機能しなくなる可能性があります。

ファイアウォール アドレスを追加するには、*[Firewall]*、*[Address]*、*[Address]* の順に選択し、*[Create New]* を選択します。スタティック IP アドレス、IP アドレス範囲、または FQDN の追加が可能です。

[IPv6 Support] が有効に設定されている場合、IPv6 ファイアウォール アドレスを追加するには、*[Firewall]*、*[Address]*、*[Address]* の順に選択し、*[Create New]* の横にある下向き矢印を選択して、*[IPv6 Address]* を選択します。

ヒント： ファイアウォール ポリシーを設定する際にも、ファイアウォール アドレスを追加できます。この場合、*[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、適切なポリシー タブを選択して、*[Create New]* を選択します。*[Source Address]* リストから、*[Address]*、*[Create New]* の順に選択します。

[New Address] ページ

このページでは、IP アドレス範囲から構成される、IP アドレス グループを設定できます。

[Address Name]	ファイアウォール アドレスを識別する名前を入力します。アドレス、アドレス グループ、および仮想 IP には、固有の名前が必要です。
[Type]	アドレスの種類として、*[Subnet/IP Range]* または *[FQDN]* を選択します。IP 範囲、またはサブネット マスクをともなう IP アドレスのいずれかを入力できます。
[Subnet/IP Range]	ファイアウォールの IP アドレスに続いてフォワード スラッシュ (/)、次にサブネット マスクを入力するか、または IP アドレス範囲をハイフンで区切って入力します。詳しくは、295 ページの「ファイアウォール アドレスについて」を参照してください。

[Interface]	IP アドレスを関連づける、インタフェース、ゾーン、またはバーチャル ドメイン (VDOM) リンクを選択します。ファイアウォール ポリシーの作成時に IP アドレスをインタフェース / ゾーンに関連付ける場合は、*[Any]* を選択します。
[IPv6 Address]	ファイアウォール IPv6 アドレスに続いてフォワード スラッシュ (/)、次にサブネット マスクを入力します。詳しくは、296 ページの「IPv6 ファイアウォール アドレスについて」を参照してください。

アドレス グループ リストの表示

複数のファイアウォール アドレスをアドレス グループに構成することにより、ファイアウォール ポリシー リストを簡素化できます。たとえば、関連する異種の 5 つのファイアウォール アドレスに対応する 5 つの同一ポリシーを使用する代わりに、5 つのアドレスを単一のアドレス グループにグループ化し、1 つのファイアウォール ポリシーがこのアドレス グループに対応するように構成できます。

アドレス グループ リストを表示するには、*[Firewall]*、*[Address]*、*[Group]* の順に選択します。

[Group] ページ

このページには、作成済みのアドレス グループが一覧表示されます。このページでは、アドレス グループの編集、削除、または新規作成が可能です。

[Create New]	アドレス グループを追加します。[Create New] を選択すると、[New Address Group] ページの画面に自動的に移動します。 *[IPv6 Support]* が有効に設定されている場合は、*[Create New]* の下向き矢印を選択し、*[IPv6 Address Group]* を選択して、IPv6 ファイアウォール アドレスを追加できます。Web ベース マネージャで IPv6 サポートを有効にする方法については、184 ページの「設定」を参照してください。
[Group Name]	アドレス グループの名前。
[Members]	アドレス グループ内のアドレス。
[Address Group]	ファイアウォール IPv4 アドレス グループのリスト。
[IPv6 Address Group]	ファイアウォール IPv6 アドレス グループのリスト。
[Delete]	アドレス グループを削除するとき選択します。*[Delete]* アイコンは、アドレス グループがファイアウォール ポリシーにより使用されていない場合のみ表示されます。
[Edit]	アドレス グループを編集するとき選択します。

アドレス グループの設定

ファイアウォール ポリシーには同種のネットワーク インタフェースをともなうアドレスが必要なことから、アドレス グループには、必ず同じネットワーク インタフェースまたは *Any* インタフェースに関連づけられるアドレスのみが含まれます。インタフェースに *Any* が選択されているアドレスは、ファイアウォール アドレス作成時ではなくファイアウォール ポリシー作成時にネットワーク インタフェースと関連づけられます。たとえば、アドレス A1 がポート 1、アドレス A2 がポート 2 と関連づけられる場合、これらのアドレスはグループ化できません。一方、アドレス A1 および A2 が *Any* インタフェースをともなう場合、これらのアドレスが異なるネットワークと関連する場合でも A1 および A2 をグループ化できます。

IPv4 ファイアウォール アドレスと IPv6 ファイアウォール アドレスは、同じアドレス グループに混合できません。

アドレスをアドレス グループに構成するには、*[Firewall]*、*[Address]*、*[Group]* の順に選択し、*[Create New]* を選択します。

[IPv6 Support] が有効に設定されている場合、IPv6 ファイアウォール アドレス グループを追加するには、*[Firewall]*、*[Address]*、*[Group]* の順に選択し、*[Create New]* の横にある下向き矢印を選択して、*[IPv6 Address Group]* を選択します。

ヒント： ファイアウォール ポリシーを設定する際にも、ファイアウォール アドレスを作成できます。この場合、*[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、適切なポリシー タブを選択して、*[Create New]* を選択します。*[Source Address]* リストから、*[Address Group]*、*[Create New]* の順に選択します。

[New Address Group] ページ

このページでは、IP アドレス グループに構成される IP アドレスを設定できます。

[Group Name]	アドレス グループを識別する名前を入力します。アドレス、アドレス グループ、および仮想 IP には、固有の名前が必要です。
[Available Addresses]	すべての IPv4 または IPv6 ファイアウォール アドレスのリスト。矢印を使用し、選択されたアドレスを [Available Addresses] および [Members] のリスト間で移動します。IPv4 および IPv6 ファイアウォール アドレスを、同じアドレス グループに追加できません。IPv4 ファイアウォール アドレス グループを追加する場合は、IPv4 アドレスおよび FQDN アドレスのみが表示されます。IPv6 ファイアウォール アドレス グループを追加する場合は、IPv6 アドレスのみが表示されます。
[Members]	アドレス グループに含まれるアドレスのリスト。矢印を使用し、選択されたアドレスを [Available Addresses] および [Members] のリスト間で移動します。

ファイアウォール サービス

ファイアウォール サービスは、サービスごとに関連づけられる 1 つ以上のプロトコルおよびポート番号を定義します。ファイアウォール ポリシーは、サービスの定義に基づいて、セッションの種類を照合します。

関連するサービスをサービス グループに構成することで、ファイアウォール ポリシー リストを簡素化できます。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとにファイアウォール サービスを個別に設定する必要があります。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には以下のトピックが含まれています。

定義済みサービス リストの表示

ファイアウォール サービスには、代表的なトラフィックの種類の多くがあらかじめ定義されています。これらの定義済みサービスはデフォルトで固定されており、編集または削除できません。ただし、異なるサービスが必要な場合は、カスタムのサービスを作成できます。詳細については、306 ページの「カスタム サービスの設定」を参照してください。

定義済みサービス リストを表示するには、[Firewall]、[Service]、[Predefined] の順に選択します。FortiGate の定義済みファイアウォール サービスについては、表 50 の一覧を参照してください。

[Predefined] ページ

このページには、利用可能な定義済みサービスが一覧表示されます。FortiGate ユニットで利用可能な定義済みファイアウォール サービスの一覧および各サービスの説明については、表 50 を参照してください。

[Name] 定義済みサービスの名前。

[Detail] 定義済みサービスのプロトコル (TCP、UDP、IP、ICMP) およびポート番号。

表 50: 定義済みサービス

サービス名	説明	IP プロトコル	ポート
AFS3	AFS 分散ファイル システム プロトコルの Advanced File Security 暗号化ファイル、バージョン 3。	TCP	7000-7009
		UDP	7000-7009
AH	Authentication Header (認証ヘッダ)。AH によって、発信元ホストの認証やデータの整合性が実現されますが、秘密性は実現されません。このプロトコルは、アグレッシブ モードに設定されたIPSecリモート ゲートウェイが認証のために使用します。		51
ANY	IP上のどのプロトコルを使用する接続にも該当します。	all	all
AOL	America Online Instant Message プロトコル。	TCP	5190-5194
BGP	Border Gateway Protocol。BGP は、内部 / 外部ルーティング プロトコルです。	TCP	179
CVSPSERVER	Concurrent Versions System Proxy Server。CSSPServer は、レポジトリへの匿名 CVS アクセスを実現するために最適です。	TCP	2401
		UDP	2401

表 50: 定義済みサービス (続き)

サービス名	説明	IP プロトコル	ポート
DCE-RPC	Distributed Computing Environment / Remote Procedure Calls。DCE-RPC を使用するアプリケーションは、別のアプリケーションからプロシジャをコールでき、このとき、この別アプリケーションがどのホストで実行しているかを把握する必要はありません。	TCP	135
		UDP	135
DHCP	Dynamic Host Configuration Protocol。DHCP は、DHCP サーバからホストにネットワーク アドレスを割り当て、設定パラメータを提供します。	UDP	67 68
DHCP6	IPv6 対応の DHCP。	UDP	546, 547
DNS	Domain Name Service。DNS は、ドメイン名を IP アドレスに解決します。	TCP	53
		UDP	53
ESP	Encapsulating Security Payload。ESP は、暗号化されたデータを通信するために、手動キーおよび AutoIKE IPSec VPN トンネルによって使用されます。AutoIKE VPN トンネルは、IKE によりトンネルを確立した後、ESP を使用します。		50
FINGER	ユーザに関する情報を提供するネットワーク サービス。	TCP	79
FTP	File Transfer Protocol。	TCP	21
FTP_GET	File Transfer Protocol。FTP GET セッションは、FTP サーバから FTP クライアント コンピュータにリモート ファイルを転送します。	TCP	21
FTP_PUT	File Transfer Protocol。FTP PUT セッションは、FTP クライアントからFTPサーバからにローカル ファイルを転送します。	TCP	21
GOPHER	Gopher は、インターネット サーバの内容を、階層的に構造化されたファイルのリストとして構成し、表示します。	TCP	70
GRE	Generic Routing Encapsulation。GRE では、GRE パケット内のプロトコルのパケットをカプセル化することによって、任意のネットワーク プロトコルを、他の任意のネットワーク プロトコルを介して転送できます。		47
GTP	GPRS トンネリング プロトコル (GTP)。GTP を GSM および UMTS ネットワークで使用することにより、ユーザ データを GPRS コア ネットワーク内で伝送できます。FortiOS では、IPv4 GTP パケットを受け入れ、処理できます。	UDP	2123,2152,3386
H323	H.323 マルチメディア プロトコル。H.323 は、複数ネットワーク上でのオーディオ ビジュアル会議データの転送方法を規定している ITU (International Telecommunication Union) によって承認された標準規格です。詳細については、『*FortiGate H.323 サポート テクニカル ノート*』を参照してください。	TCP	1720, 1503
		UDP	1719
HTTP	Hypertext Transfer Protocol。HTTP は、WWW (Word Wide Web) 上の Web ページを閲覧するために使用されます。	TCP	80
HTTPS	SSL (Secure Socket Layer) を備えた HTTP。HTTPS は、Web サーバとのセキュアな通信のために使用されます。	TCP	443
ICMP_ANY	Internet Control Message Protocol。ICMP により、ホストおよびゲートウェイ (インターネット) 間でのメッセージ制御およびエラー レポートが可能となります。	ICMP	Any
IKE	Internet Key Exchange。IKE は、IPSEC の ISAKMP (Internet Security Association and Key Management Protocol) で使用する、認証されたキー作成材料を取得します。	UDP	500, 4500
IMAP	Internet Message Access Protocol。IMAP は、電子メール サーバからメール メッセージを検索するために、電子メール クライアントにより使用されます。	TCP	143

表 50: 定義済みサービス (続き)

サービス名	説明	IP プロトコル	ポート
IMAPS	SSL を備えた IMAP。IMAPS は、電子メール クライアントおよびサーバ間のセキュアな IMAP 通信のために使用されます。IMAPS は、SSL コンテンツ スキャンおよびインスペクションをサポートするFortiGateユニットのみで使用できます。詳しくは、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。	TCP	993
INFO_ADDRESS	ICMP の情報要求メッセージ。	ICMP	17
INFO_REQUEST	ICMP のアドレス マスク要求メッセージ。	ICMP	15
IRC	Internet Relay Chat。IRC により、ユーザはチャット チャネルに参加できます。	TCP	6660-6669
Internet-Locator-Service	Internet-Locator-Service。ILS には、LDAP、User Locator Service、および LDAP over TLS/SSL が含まれます。	TCP	389
L2TP	Layer 2 Tunneling Protocol。L2TP は、リモート アクセスのための PPP ベースのトンネル プロトコルです。	TCP	1701
		UDP	1701
LDAP	Lightweight Directory Access Protocol。LDAP は、情報ディレクトリにアクセスするために使用されるプロトコルです。	TCP	389
MGCP	Media Gateway Control Protocol。MGCP は、分散 VoIP (Voice over IP) システム内部で、コール エージェントおよびメディア ゲートウェイにより使用されるプロトコルです。	UDP	2427, 2727
MS-SQL	Microsoft SQL Server は、Microsoft により開発されたリレーショナル データベース管理システム (RDBMS) であり、その主なクエリ言語は MS-SQL および T-SQL です。	TCP	1433, 1434
MYSQL	MySQL は、複数データベースへのマルチユーザ アクセスを可能にするサーバとして実行する、リレーショナル データベース管理システム (RDBMS) です。	TCP	3306
NFS	Network File System。NFS により、ネットワーク ユーザは共有ファイルを自身のシステムにマウントして扱うことができます。	TCP	111, 2049
		UDP	111, 2049
NNTP	Network News Transport Protocol。NNTP は、USENET メッセージを投稿、配布、および取得するために使用されるプロトコルです。	TCP	119
NTP	Network Time Protocol。NTP は、ホストの時刻をタイム サーバと同期します。	TCP	123
		UDP	123
NetMeeting	NetMeeting を使用すると、ユーザは、インターネットを転送媒体として使用し遠隔会議を実行できます。	TCP	1720
ONC-RPC	Open Network Computing Remote Procedure Call。ONC-RPC は、幅広く展開されているリモート プロシジャ コール システムです。	TCP	111
		UDP	111
OSPF	Open Shortest Path First。OSPF は、一般的なリンク ステート ルーティング プロトコルです。		89
PC-Anywhere	PC-Anywhere は、リモート制御およびファイル転送プロトコルです。	TCP	5631
		UDP	5632
PING	Ping により、ICMP プロトコルの echo メッセージを送信して応答を要求することで、他のホストとの接続性を確認できます。	ICMP	8
PING6	Ping6 により、ICMPv6 プロトコルの echo メッセージをネットワーク ホストに送信し、応答を要求することで、他のホストとの IPv6 接続性を確認できます。		58
POP3	Post Office Protocol version 3。POP は、電子メール メッセージを検索します。	TCP	110

表 50: 定義済みサービス (続き)

サービス名	説明	IP プロトコル	ポート
POP3S	SSL (secure socket layer) を備えた Post Office Protocol version 3。POP3S は、電子メール メッセージのセキュアな検索のために使用されます。POP3S は、SSL コンテンツ スキャンおよびインスペクションをサポートする FortiGate ユニットのみで使用できます。詳しくは、『*FortiOS ハンドブック*』の「*UTM* 」の章を参照してください。	TCP	995
PPTP	Point-to-Point Tunneling Protocol。PPTP は、インターネット上でプライベート ネットワークのホスト同士をトンネル接続するために使用されます。**注記** : IP プロトコル 47 も必要となります。		47
		TCP	1723
QUAKE	Quake のマルチプレーヤーによるコンピュータ ゲームのトラフィック。	UDP	26000, 27000, 27910, 27960
RADIUS	Remote Authentication Dial In User Service。RADIUS は、ネットワーク サービスに接続し使用するユーザまたはコンピュータの、アクセス、認証、およびアカウントを集中的に管理する、ネットワーク プロトコルです。	TCP	1812, 1813
RAUDIO	RealAudio マルチメディア トラフィック。	UDP	7070
RDP	RDP (Remote Desktop Protocol) は、ユーザがネットワーク化されたコンピュータに接続することを可能にする、マルチチャネル プロトコルです。	TCP	3389
REXEC	Rexec トラフィックにより、rexecd サービス (デーモン) を実行するリモート ホスト上で、指定したコマンドを実行できます。	TCP	512
RIP	Routing Information Protocol。RIP は、一般的な距離ベクトル ルーティング プロトコルです。このサービスは、RIPv1 に該当します。	UDP	520
RLOGIN	リモート ログイン トラフィック。	TCP	513
RSH	リモート シェル トラフィックにより、rshd サービス (デーモン) を実行するリモート ホスト上で、指定したコマンドを実行できます	TCP	514
RTSP	RTSP (Real Time Streaming Protocol) は、ストリーミング メディア システムで使用するためのプロトコルです。RTSP により、クライアントからストリーミング メディア サーバをリモート制御できるようになり、再生、停止などビデオデッキのようなコマンドを発行し、サーバ上にあるファイルへのタイムベースのアクセスが可能になります。	TCP	554, 7070, 8554
		UDP	554
SAMBA	SMB (サーバ メッセージ ブロック)。SMB により、クライアントは、対応するホストからファイルおよびプリント共有を利用できます。SMB は、主に Microsoft Windows ホストのために使用されますが、Samba デーモンを実行するオペレーティング システムにも使用されます。	TCP	139
SCCP	Skinny Client Control Protocol。SCCPは、VoIP (voice over IP) で使用するための、Cisco 独自の端末制御プロトコルです。	TCP	2000
SIP	Session Initiation Protocol。SIP により、オーディオ ビジュアル会議データを複数のネットワーク上で転送できます。詳細については、『*FortiGate SIP サポート テクニカル ノート*』を参照してください。	UDP	5060
SIP-MSNmessenger	Session Initiation Protocol。Microsoft Messenger によって、インタラクティブな (一般には) マルチメディア セッションを開始するために使用されます。	TCP	1863
SMTP	Simple Mail Transfer Protocol。SMTP は、電子メール クライアントと電子メール サーバ間、および電子メール サーバ同士で、メール メッセージを送信するために使用されます。	TCP	25

表 50: 定義済みサービス (続き)

サービス名	説明	IP プロトコル	ポート
SMTPS	SSL を備える SMTP。電子メール クライアントと電子メール サーバ間、および電子メール サーバ同士での、セキュアなメール メッセージ送信のために使用されます。SMTPS は、SSL コンテンツ スキャンおよびインスペクションをサポートするFortiGateユニットのみで使用できます。 詳しくは、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。	TCP	465
SNMP	Simple Network Management Protocol。SNMP を使用することにより、複雑なネットワークを監視および管理できます。	TCP	161-162
		UDP	161-162
SOCKS	SOCKetS。SOCKS は、クライアントサーバ アプリケーションがネットワーク ファイアウォールのサービスを透過的に使用できるようにするための、インターネット プロトコルです。	TCP	1080
		UDP	1080
SQUID	プロキシ サーバおよび Web キャッシュのデーモン。その多種多様な用途には、繰り返される要求をキャッシュすることで Web サーバを高速化すること、Web のキャッシュ、DNS および他のコンピュータ ネットワークでネットワーク リソースを共有するユーザ グループの検索、トラフィックのフィルタリングによるセキュリティ支援、などが含まれます。	TCP	3128
SSH	Secure Shell。SSH により、セキュアなリモート管理およびトンネリングが可能になります。	TCP	22
		UDP	22
SYSLOG	リモート ロギングのための Syslog サービス。	UDP	514
TALK	TALK により、2 名以上のユーザ同士の対話が可能になります。	UDP	517-518
TCP	あらゆる TCP ポートを使用する接続に該当します。	TCP	0-65535
TELNET	プレーン テキストによるリモート 管理を可能にします。	TCP	23
TFTP	File Transfer Protocol。TFTP は FTP と類似のプロトコルですが、認証などのセキュリティ機能が含まれていません。	UDP	69
TIMESTAMP	ICMP のタイムスタンプ要求メッセージ。	ICMP	13
TRACEROUTE	IP ネットワーク上でパケット が経由する経路を決めるために使用される、コンピュータ ネットワーク ツール。	TCP	33434
		UDP	33434
UDP	あらゆる UDP ポートを使用する接続に該当します。	UDP	0-65535
UUCP	UNIX 同士のコピー プロトコル。UUCP により、単純なファイル転送が可能です。	UDP	540
VDOLIVE	VDO Live ストリーミング マルチメディア トラフィック。	TCP	7000-7010
VNC	バーチャル ネットワーク コンピューティング。VNC は、RFB プロトコルを使用し別のコンピュータをリモート制御する、グラフィカルなデスクトップ共有システムです。	TCP	5900
WAIS	Wide Area Information Server。WAIS は、Gopher とともに使用される、インターネット検索プロトコルです。	TCP	210
WINFRAME	WinFrameは、Windows NTまたはCitrix WinFrame/MetaFrameを実行するコンピュータ同士の通信を可能にします。	TCP	1494
WINS	WINS (Windows Internet Name Service) は、Microsoft の NetBIOS Name Service (NBNS) 実装で、NetBIOS 名に対応するネーム サーバおよびサービスです。	TCP	1512
		UDP	1512
X-WINDOWS	X Window システム (別称 X11) により、X Window サーバから X Window クライアントにグラフィカル シェルを転送できます。	TCP	6000-6063

カスタム サービスの設定

定義済みサービスリストに含まれていないサービスに対するファイアウォール ポリシーを作成する必要がある場合、カスタム サービスを追加できます。

カスタム サービス リストを表示するには、*[Firewall]*、*[Service]*、*[Custom]* の順に選択します。

カスタム サービスを設定するには、*[Firewall]*、*[Service]*、*[Custom]* の順に選択し、*[Create New]* を選択して、カスタム サービスに必要な情報を入力します。*[OK]* を選択します。

ヒント：ファイアウォール ポリシーを設定する際にも、カスタム サービスを作成できます。この場合、*[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、適切なポリシー タブを選択して、*[Create New]* を選択します。*[Service]* リストから、*[Service]*、*[Create New]* の順に選択します。

[Custom] ページ

このページには、作成済みのカスタム サービスが一覧表示されます。このページでは、カスタム サービスの編集、削除、または新規作成が可能です。

[Create New]	カスタム サービスを追加します。[Create New] を選択すると、[New Custom Service] ページの画面に自動的に移動します。
[Service Name]	カスタム サービスの名前。
[Detail]	各カスタム サービスのプロトコルとポート番号。
[Delete]	カスタム サービスを削除します。*[Delete]* アイコンは、ファイアウォール ポリシーによりこのサービスが使用されていない場合のみ表示されます。
[Edit]	カスタム サービスを編集します。

[New Custom Service] ページ

このページでは、定義済みサービス リストには含まれていないカスタム サービスを設定できます。

[Name]	カスタム サービスの名前を入力します。
[Protocol Type]	カスタム サービスのプロトコルの種類を選択します。
[Protocol]	設定対象のドロップダウン リストから、プロトコルを選択します。
[Source Port]	[Low] と [High] のポート番号を入力することにより、このサービスの [Source Port] の番号範囲を指定します。このサービスでポート番号を 1 つしか使用しない場合は、その番号を *[Low]* と *[High]* の両方のフィールドに入力します。デフォルト値では、任意の発信元ポートを使用できます。
[Destination Port]	[Low] と [High] のポート番号を入力することにより、このサービスの [Destination Port] の番号範囲を指定します。このサービスでポート番号を 1 つしか使用しない場合は、その番号を *[Low]* と *[High]* の両方のフィールドに入力します。
[Add]	作成しているカスタム サービスに複数のポート範囲が必要な場合は、*[Add]* を選択し、さらに発信元と宛先の範囲を入力できるようにします。
[Delete]	プロトコル (TCP、UDP、または SCTP) をリストから削除します。
[Type]	ICMP プロトコル設定の ICMP タイプ番号を入力します。
[Code]	ICMP プロトコル設定の ICMP コード番号を入力します。
[Protocol Number]	IP プロトコル設定のプロトコル番号を入力します。

次の項も参照してください。

- ファイアウォール ポリシー

カスタム サービス グループの設定

複数のファイアウォール サービスをサービス グループに構成することにより、ファイアウォール ポリシー リストを簡素化できます。たとえば、関連する異種の 5 つのファイアウォール サービスに対応する 5 つの同一ポリシーを使用する代わりに、5 つのサービスを単一のサービス グループにグループ化し、1 つのファイアウォール ポリシーがこのサービス グループに対応するように構成できます。

サービス グループには、定義済みサービスおよびカスタム サービスの双方を構成できます。サービス グループには、他のサービス グループを含むことはできません。

サービス グループ リストを表示するには、*[Firewall]*、*[Service]*、*[Group]* の順に選択します。

複数のファイアウォール サービスをサービス グループに構成することにより、ファイアウォール ポリシー リストを簡素化できます。たとえば、関連する異種の 5 つのファイアウォール サービスに対応する 5 つの同一ポリシーを使用する代わりに、5 つのサービスを単一のサービス グループにグループ化し、1 つのファイアウォール ポリシーがこのサービス グループに対応するように構成できます。

サービス グループには、定義済みサービスおよびカスタム サービスの双方を構成できます。サービス グループには、他のサービス グループを含むことはできません。

サービスをサービス グループに構成するには、*[Firewall]*、*[Service]*、*[Group]* の順に選択します。

ヒント：ファイアウォール ポリシーを設定する際にも、カスタム サービス グループを作成できます。この場合、*[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、適切なポリシー タブを選択して、*[Create New]* を選択します。*[Service]* リストから、*[Service Group]*、*[Create New]* の順に選択します。

[Group] ページ

このページには、作成済みのサービス グループが一覧表示されます。このページでは、サービス グループの編集、削除、または新規作成が可能です。

[Create New]	サービス グループを追加します。[Create New] を選択すると、[New Service Group] ページの画面に自動的に移動します。
[Edit]	*[Group Name]* および *[Members]* の情報を編集するとき選択します。
[Delete]	リストからサービス グループを削除します。*[Delete]* アイコンは、ファイアウォール ポリシーでこのサービス グループが選択されていない場合のみ表示されます。
[Group Name]	サービス グループを識別する名前。
[Members]	このサービス グループに追加されたサービス。

[New Service Group] ページ

このページでは、サービス グループに構成されるサービスを設定できます。

[Group Name]	サービス グループを識別する名前を入力します。
[Available Services]	グループに構成されている定義済みサービスのリスト。リスト下部に、カスタム サービスが含まれます。矢印を使用し、選択されたサービスをこのリストと *[Members]* 間で移動できます。
[Members]	グループ内のサービスのリスト。矢印を使用し、選択されたサービスをこのリストと *[Available Services]* 間で移動できます。

次の項も参照してください。

- ファイアウォール ポリシー

ファイアウォール スケジュール

ファイアウォール スケジュールにより、ポリシーをいつ有効にするかを管理できます。作成可能なスケジュールには、ワンタイム スケジュールと反復スケジュールがあります。ワンタイム スケジュールは、スケジュールで指定された期間に 1 回だけ有効になります。反復スケジュールは、指定された曜日の時間に繰り返し有効になります。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとにファイアウォール スケジュールを個別に設定する必要があります。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には以下のトピックが含まれています。

反復スケジュール リストの表示

指定された期間にポリシーが有効になる反復スケジュールを作成できます。たとえば、就業時間を対象とする反復スケジュールを作成することにより、就業時間中のゲームを防止できます。

反復スケジュールの停止時刻が開始時刻より前に設定されると、スケジュールは開始時刻に有効になり、翌日の停止時刻に終了します。このテクニックを使用することで、ある日から翌日にかけて有効期間が続く反復スケジュールを作成できます。たとえば、昼食時間を除きゲームのプレーを防止するには、反復スケジュールの開始時刻を午後 1:00 に設定し停止時刻を正午 12:00 に設定できます。24 時間効力が持続する反復スケジュールを作成するには、開始時刻および停止時刻を 00 に設定します。

反復スケジュール リストを表示するには、*[Firewall]*、*[Schedule]*、*[Recurring]* の順に選択します。

[Recurring] ページ

このページには、作成済みの反復スケジュールが一覧表示されます。このページでは、反復スケジュールの編集、削除、または新規作成が可能です。

[Create New]	反復スケジュールを追加します。
[Name]	反復スケジュールの名前。
[Day]	スケジュールがアクティブになる曜日の頭文字。
[Start]	反復スケジュールの開始時刻。
[Stop]	反復スケジュールの停止時刻。
[Delete]	リストからスケジュールを削除します。*[Delete]* アイコンは、このスケジュールがファイアウォール ポリシーで使用されていない場合にのみ表示されます。
[Edit]	スケジュールを編集します。

反復スケジュールの設定

反復スケジュールを追加するには、*[Firewall]*、*[Schedule]*、*[Recurring]* の順に選択します。以下の表の情報を入力し、*[OK]* を選択します。

ヒント： ファイアウォール ポリシーを設定する際にも、反復スケジュールを作成できます。この場合、*[Firewall]*、*[Policy]* の順に選択し、適切なポリシー タブを選択して、*[Create New]* を選択します。*[Schedule]* リストから、*[Recurring]*、*[Create New]* の順に選択します。

ポリシーが終日有効になるようにするには、スケジュールの開始および停止時刻を 00 に設定します。

[New Recurring Schedule] ページ
このページでは、定期的にアクティブとなるスケジュールを設定できます。

[Name]	反復スケジュールの名前を入力します。
[Select]	このスケジュールがアクティブになる曜日を選択します。
[Start]	この反復スケジュールの開始時刻を選択します。
[Stop]	この反復スケジュールの停止時刻を選択します。

ワンタイム スケジュール リストの表示

指定された期間にポリシーが有効になるワンタイム スケジュールを作成できます。たとえば、インターネット上のすべてのサービスに常時アクセス可能なデフォルトのポリシーをファイアウォールに設定しておいて、さらにワンタイム スケジュールを追加することで休日にインターネットへのアクセスをブロックできます。

ワンタイム スケジュール リストを表示するには、*[Firewall]*、*[Schedule]*、*[One-time]* の順に選択します。

[One-time] ページ
このページには、1 回だけ有効になるスケジュールの一覧が表示されます。このページでは、ワンタイム スケジュールの編集、削除、または新規作成が可能です。

[Create New]	ワンタイム スケジュールを追加します。[Create New] を選択すると、[New One-time Schedule] ページの画面に自動的に移動します。
[Name]	ワンタイム スケジュールの名前。
[Start]	このスケジュールの開始日付および時刻。
[Stop]	このスケジュールの停止日付および時刻。
[Delete]	リストからスケジュールを削除します。*[Delete]* アイコンは、このスケジュールがファイアウォール ポリシーで使用されていない場合にのみ表示されます。
[Edit]	スケジュールを編集します。

ワンタイム スケジュールの設定

ワンタイム スケジュールを追加するには、*[Firewall]*、*[Schedule]*、*[One-time]* の順に選択します。以下の表の情報を入力し、*[OK]* を選択します。

ヒント： ファイアウォール ポリシーを設定する際にも、ワンタイム スケジュールを作成できます。この場合、*[Firewall]*、*[Policy]* の順に選択し、適切なポリシー タブを選択して、*[Create New]* を選択します。*[Schedule]* リストから、*[One-time]*、*[Create New]* の順に選択します。

ポリシーが終日有効になるようにするには、スケジュールの開始および停止時刻を 00 に設定します。

[New One-time Schedule] ページ
このページでは、ワンタイム スケジュールを設定できます。[Create New] を選択すると、このページの画面に自動的に移動します。

[Name]	ワンタイム スケジュールの名前を入力します。

[Start]	このスケジュールの開始日付および時刻を選択します。
[Stop]	このスケジュールの停止日付および時刻を選択します。

スケジュール グループの設定

複数のファイアウォール スケジュールを一つのスケジュール グループに構成することにより、ファイアウォール ポリシー リストを簡素化できます。たとえば、それぞれ異なるファイアウォールスケジュールをもった別々のポリシーを 5 個持つかわりに、5 つのスケジュールをひとつのスケジュールグループにまとめて、このスケジュールグループをファイアーウォールポリシーに適用させることができます。

スケジュール グループには、反復およびワンタイム スケジュールの双方を含むことができます。スケジュール グループには、他のスケジュール グループを含むことはできません。

スケジュールをスケジュール グループに構成するには、*[Firewall]*、*[Schedule]*、*[Group]* の順に選択します。

[Group] ページ

このページには、作成済みのスケジュール グループが一覧表示されます。このページでは、スケジュール グループの編集、削除、または新規作成が可能です。

[Group Name]	スケジュール グループの名前を入力します。
[Available Schedules]	グループに含まれる反復およびワンタイム スケジュールのリスト。矢印を使用し、選択されたスケジュールをこのリストと *[Members]* 間で移動できます。
[Members]	グループ内のスケジュールのリスト。矢印を使用し、選択されたスケジュールをこのリストと *[Available Schedule]* 間で移動できます。

[New Schedule Group] ページ

このページでは、どのスケジュールをメンバとしてグループに含むかを設定できます。

[Group Name]	このスケジュール グループの名前を入力します。
[Available Schedules]	グループにメンバとして含むスケジュールを選択し、下向き矢印を使用してそのスケジュールを [Members] に移動します。
[Members]	グループと関連づけられるスケジュール。[Members] リストからスケジュールを削除するには、スケジュールを選択し、上向き矢印を使用してそのスケジュールを [Available Schedules] に戻します。

ファイアウォール仮想 IP

仮想 IP アドレス (VIP) を利用して、ネットワークインターフェース（モデムインタフェースを含む）上で受信したパケットの IP アドレスとポートを変換するようにファイアーウォールポリシーを設定できます。

FortiGate ユニットが、[Destination Address] フィールドに仮想 IP が指定されているファイアウォール ポリシーと一致するパケットを受信すると、FortiGate ユニットは NAT を適用して、パケットの IP アドレスを仮想 IP にマップされている IP アドレスに変換します。

IP プールを使って NAT を設定できるという点においては仮想 IP と似ていますが、IP プールでは [Destination Interface/Zone] に基づいてパケットの IP アドレスの動的な変換を設定する一方、仮想 IP では [Source Interface/Zone] に基づいてパケットの IP アドレスの静的または動的な変換を設定します。

仮想 IP または IP プールで設定された変換を動作させるには、それを NAT ファイアウォールポリシーに追加する必要があります。詳細については、317 ページの「仮想 IP の設定」を参照してください。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとにファイアウォール仮想 IP を個別に設定します。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には以下のトピックが含まれています。

注記：トランスペアレント モードでは、FortiGate の CLI から、仮想 IP および IP プールを含む NAT ファイアウォール ポリシーを設定できます。詳しくは、332 ページの「トランスペアレント モードでの NAT ファイアウォール ポリシーの追加」を参照してください。

仮想 IP がどのように FortiGate のユニットを通るコネクションをマップするかについて

仮想 IP はインバウンドとアウトバウンドのコネクションの両方にたいして、パケットのポート番号と IP アドレスの両方または一方だけの変換を定義することができます。トランスペアレント モードでは、FortiGate の CLI から仮想 IP を設定できます。

受信接続

仮想 IP を、[Action] が [DENY] に設定されていないファイアウォール ポリシーとともに使用することで、双方向 NAT (受信 NAT とも呼ばれる) を適用できます。

パケットをファイアウォール ポリシー リストと照合して一致するポリシーを特定するとき、ファイアウォール ポリシーの [Destination Address] が仮想 IP の場合は、FortiGate ユニットはパケットの宛先アドレスを仮想 IP の外部 IP アドレスと照合します。これらが一致する場合、FortiGate ユニットでは仮想 I P の受信 NAT マッピングが適用され、FortiGate ユニットによって、パケットのネットワーク アドレスおよびポート番号が、受信（外部）ネットワーク インタフェースから、宛先（マップ先）IP アドレスまたは IP アドレス範囲に接続されるネットワーク インタフェースに、どのように変換されるかを指定します。

インタフェース間の IP アドレスおよびポートのマッピングを指定することに加えて、仮想 IP の設定では、オプションで追加 IP アドレスまたは IP アドレス範囲を受信側のネットワーク インタフェースに関連づけることができます。追加 IP アドレスを関連づけることで、ネットワーク インタフェースに元から設定済みの IP アドレスではなく関連づけられた追加 IP アドレスと一致する宛先を持つパケットに FortiGate ユニットによって適用できるマッピングの組み合わせを、別個に設定できます。

仮想 IP の設定により、そのマッピングは ポート アドレス変換 (PAT)、ポート フォワーディングまたはネットワーク アドレス ポート変換 (NAPT) ともいわれる、と IP アドレスの ネットワーク アドレス変換 (NAT) のいずれかまたは両方を含みます。

仮想 IP およびファイアウォール ポリシーで NAT を設定する場合は、NAT の動作は以下の選択により異なります。

- スタティックまたはダイナミック NAT マッピング
- ダイナミック NAT マッピングを使用する場合、ダイナミック NAT の負荷分散スタイル
- 完全な NAT または宛先 NAT (DNAT)

以下の表は、仮想 IP をともなうファイアウォール ポリシーを設定するとき使用可能な、PAT または NAT あるいは両方の組み合わせについて記述しています。

スタティック NAT	スタティックな、一対一の NAT マッピング。外部 IP アドレスは、必ず同じマップ先 IP アドレスに変換されます。 IP アドレス範囲を使用する場合は、外部 IP アドレス範囲は同じ数の IP アドレスを含んでいるマップ先 IP アドレス範囲に対応し、外部アドレス範囲に含まれる各 IP アドレスは必ずマップ先アドレス範囲内の同じ IP アドレスに変換されます。
ポート フォワーディングをともなうスタティック NAT	ポート フォワーディングをともなう、スタティックな一対一の NAT マッピング。外部 IP アドレスは、必ず同じマップ先 IP アドレスに変換され、外部ポート番号は必ず同じマップ先ポート番号に変換されます。 IP アドレス範囲を使用する場合は、外部 IP アドレス範囲は同じ数の IP アドレスを含んでいるマップ先 IP アドレス範囲に対応し、外部アドレス範囲に含まれる各 IP アドレスは必ずマップ先アドレス範囲内の同じ IP アドレスに変換されます。ポート番号範囲を使用する場合は、外部ポート番号範囲は同じ数のポート番号を含んでいるマップ先ポート番号範囲に対応し、外部ポート番号範囲に含まれる各ポート番号は必ずマップ先ポート番号範囲内の同じポート番号に変換されます。
サーバ ロード バランシング	ダイナミックな、一対多の NAT マッピング。外部 IP アドレスは、より均等なトラフィック分散のために採用される負荷分散アルゴリズムによる決定に従い、マップ先 IP アドレスのいずれかに変換されます。外部 IP アドレスは、必ず同じマップ先 IP アドレスに変換されるとは限りません。 サーバ ロード バランシングでは、1 台以上 8 台までのリアル サーバを設定する必要があります。リアル サーバは、ヘルス チェック モニタとともに構成できます。ヘルス チェック モニタを使用することで、パケットを転送する前にサーバ応答性を計測できます。
ポート フォワーディングによるサーバ ロード バランシング	ポート フォワーディングによるダイナミックな一対多の NAT マッピング。外部 IP アドレスは、より均等なトラフィック分散のための選択された負荷分散アルゴリズムによる決定に従い、マップ先 IP アドレスのいずれかに変換されます。外部 IP アドレスは、必ず同じマップ先 IP アドレスに変換されるとは限りません。 サーバ ロード バランシングでは、1 台以上 8 台までのリアルなサーバを設定する必要があります。リアルなサーバは、ヘルス チェック モニタにより設定できます。ヘルス チェック モニタを使用することで、パケットを転送する前にサーバ応答性を計測できます。

[NAT] チェック ボックスが***オフ***の状態でファイアウォール ポリシーを構成する場合、作成されたポリシーは完全な (発信元および宛先) NAT を実行せず、DNAT (宛先ネットワーク アドレス変換) を実行します。受信トラフィックについては、DNAT によりパケットの宛先アドレスはマップ先プライベート IP アドレスに変換されますが、発信元アドレスは変換***されません***。プライベート ネットワークは、発信元のパブリック IP アドレスを意識します。応答トラフィックについては、FortiGate ユニットはパケットのプライベートネットワークのソース IP アドレスを、セッションテーブルで管理されている最初に発信されたパケットの宛先アドレスに一致するように変換します。

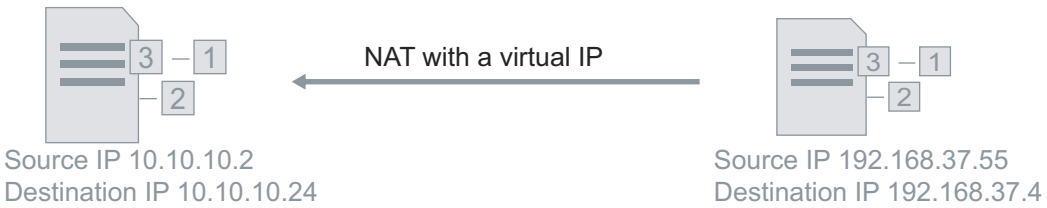
スタティック NAT の代表例は、クライアントがパブリック ネットワークから FortiGate ユニットにより保護されているプライベート ネットワーク上の Web サーバにアクセスすることを許可することです。最も簡潔に表す場合、図 14 に示されるように、この例には 3 台のみのホストが含まれます。これらは、プライベート ネットワーク上の Web サーバ、インターネットなど別のネットワーク上のクライアント コンピュータ、およびこれら 2 つのネットワークを接続する FortiGate ユニットです。

クライアント コンピュータがWebサーバに接続しようとすると、このコンピュータはFortiGate ユニットの外部インタフェース上で仮想 IP を使用します。FortiGate ユニットは、クライアントからのパケットを受信し、パケットに含まれるアドレスはプライベート ネットワーク IP アドレスに変換され、パケットはプライベート ネットワーク上の Web サーバに転送されます。

図 14: 単純なスタティック NAT 仮想 IP の例

クライアント コンピュータから送信されたパケットには、192.168.37.55 という発信元 IP と 192.168.37.4 という宛先 IP が含まれています。FortiGate ユニットは、これらのパケットを外部インタフェースで受信し、その仮想 IP のファイアウォール ポリシーとそれらのパケットを照合します。仮想 IP 設定により 192.168.37.4 が 10.10.10.42 にマッピングされ、FortiGate ユニットはパケットのアドレスを変更します。発信元アドレスは 10.10.10.2 に、宛先は 10.10.10.42 にそれぞれ変更されます。FortiGate ユニットは、内部に保持するファイアウォール セッション テーブルにこの変換を記録します。パケットは、これらの処理を経て、Web サーバに転送されます。

図 15: クライアントからサーバへの NAT 変換におけるパケット アドレス再マッピングの例

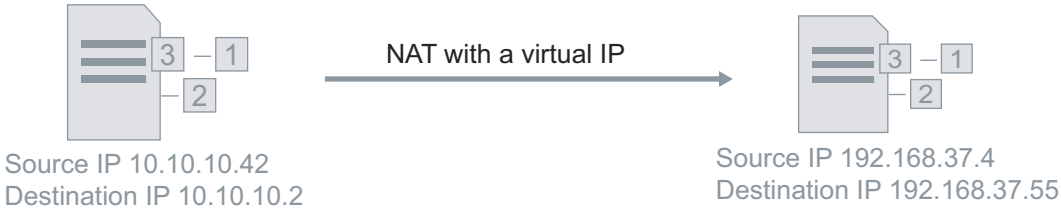


クライアント コンピュータのアドレスは、サーバが受信するパケットには***含まれない***ことに注意してください。FortiGate ユニットでネットワーク アドレスが変換されると、クライアント コンピュータの IP アドレスへの参照はなくなります。ただし、セッション テーブルにはその IP アドレスが残ります。Web サーバは、別のネットワークが存在することを意識せず、すべてのパケットが FortiGate ユニットから送信されるものと認識します。

Web サーバがクライアント コンピュータに応答するとき、同じようにアドレス変換が逆方向で処理されます。Web サーバは、発信元 IP アドレスが 10.10.10.42、宛先アドレスが 10.10.10.2 の応答パケットを送信します。FortiGate ユニットは、これらのパケットを内部インタフェースで受信します。ただし今回は、アドレス変換の宛先アドレスとして、セッション テーブルからクライアント コンピュータの IP アドレスが呼び戻されます。応答パケットでは、発信元アドレスは 192.168.37.4 に、宛先アドレスは 192.168.37.55 にそれぞれ変更されます。パケットは、これらの処理を経てクライアント コンピュータに転送されます。

Web サーバのプライベート IP アドレスは、クライアントが受信するパケットには含まれません。FortiGate ユニットでネットワーク アドレスが変換されると、Web サーバのネットワークへの参照はなくなります。クライアントは、Web サーバの IP アドレスが仮想 IP ではないことを意識せず、FortiGate ユニットの仮想 IP が Web サーバであると認識します。

図 16: サーバからクライアントへの NAT 変換におけるパケット アドレス再マッピングの例



上記の例では、ファイアウォール ポリシーの設定時に、[NAT] チェック ボックスがオンの状態でした。[NAT] チェック ボックスが***オフ***の状態でファイアウォール ポリシーを構成すると、作成されたポリシーは完全な NAT を実行せず、DNAT (宛先ネットワーク アドレス変換) を実行します。

受信トラフィックでは、DNAT によりパケットの宛先アドレスがマップ先プライベート IP アドレスに変換されますが、発信元アドレスは変換***されません***。Web サーバは、クライアントの IP アドレスを意識します。応答トラフィックについては、FortiGate ユニットはパケットのプライベート ネットワークのソース IP アドレスを、セッション テーブルで管理されている最初に発信されたパケットの宛先アドレスに一致するように変換します。

送信接続

仮想 IP は、送信ファイアウォール ポリシーで選択されない場合でも、送信 NAT に影響します。仮想 IP を設定しない場合、FortiGate ユニットは、プライベート ネットワーク IP アドレスからパブリック ネットワーク IP アドレスへの送信接続に、従来の送信 NAT を適用します。一方、仮想 IP 設定が存在する場合、FortiGate ユニットは仮想 IP の受信 NAT マッピングを逆方向に使用することで送信 NAT を適用し、送受信トラフィックの IP アドレス マッピングを対称にします。

たとえば、ネットワーク インタフェースの IP アドレスが 10.10.10.1、関連付けられる仮想 IP の外部IPが10.10.10.2で、受信トラフィックをプライベート ネットワークIPアドレス192.168.2.1 にマッピングする場合、192.168.2.1 からの送信トラフィックは、10.10.10.1 ではなく 10.10.10.2 に変換されます。

仮想 IP、負荷分散仮想サーバ、および負荷分散リアル サーバの制限

仮想 IP、負荷分散仮想サーバ、負荷分散リアル サーバを追加するとき、以下のような制限があります。負荷分散仮想サーバは、実際にはサーバ ロード バランシング仮想 IP です。サーバ ロード バランシング仮想 IP は、CLI から追加できます。

- 仮想 IP の *[External IP Address/Range]* のエントリまたは範囲は、エントリおよび範囲同士、または負荷分散仮想サーバの *[Virtual Server IP]* のエントリとは重複できません。
- 仮想 IP の *[Mapped IP Address/Range]* は、必ず 0.0.0.0 および 255.255.255.255 以外にしなければなりません。
- リアル サーバの *[IP]* は、必ず0.0.0.0および255.255.255.255以外にしなければなりません。
- スタティック NAT 仮想 IP の *[External IP Address/Range]* が 0.0.0.0 の場合、*[Mapped IP Address/Range]* は、必ず単一の IP アドレスにしなければなりません。
- 負荷分散仮想 IP の *[External IP Address/Range]* が 0.0.0.0 の場合、*[Mapped IP Address/Range]* には、アドレス範囲を設定できます。
- ポート フォワーディングでは、マップ先ポート番号および外部ポート番号の数は必ず同じになります。Web ベース マネージャでは、これを自動的に処理できますが、CLI では自動処理できません。
- 仮想 IP および仮想サーバの名前は、ファイアウォール アドレスまたはアドレス グループの名前とは異なるものにしなければなりません。

仮想 IP リストの表示

仮想 IP リストを表示するには、*[Firewall]*、*[Virtual IP]*、*[Virtual IP]* の順に選択します。

[Virtual IP] ページ

このページには、作成済みの仮想 IP が一覧表示されます。このページでは、仮想 IP の編集、削除、または新規作成が可能です。

[Create New]	仮想 IP を追加する場合に選択します。[Create New] を選択すると、[Add New Virtual IP Mapping] ページの画面に自動的に移動します。
[Name]	仮想 IP の名前。
[IP]	関連付けられるネットワーク インタフェースおよび外部 IP アドレスまたは IP アドレス。スラッシュ (/) により区切られます。
[Service Port]	外部ポート番号またはポート番号の範囲。仮想 IP でポート フォワーディングが指定されない場合、このフィールドは空白です。
[Map to IP/IP Range]	宛先ネットワーク上のマップ先 IP アドレスまたはアドレス範囲。
[Map to Port]	マップ先のポート番号またはポート番号の範囲。仮想 IP でポート フォワーディングが指定されない場合、このフィールドは空白です。
[Delete]	リストから仮想 IP を削除します。[Delete] アイコンは、仮想 IP がファイアウォール ポリシーで選択されていない場合にのみ表示されます。
[Edit]	仮想 IP を編集し、仮想 IP 名などの仮想 IP オプションを変更します。

仮想 IP の設定

仮想 IP の外部 IP アドレスとして、単一の IP アドレスまたは IP アドレス範囲を設定し、FortiGate ユニット インタフェースに関連付けることができます。仮想 IP の外部 IP アドレスを FortiGate ユニット インタフェースに関連付けると、デフォルトで、関連付けられた IP アドレスまたは IP アドレス範囲への ARP 要求に対して、そのネットワーク インタフェースが応答します。RFC 1027 の規定に従い、仮想 IP はプロキシ ARP を使用するので、FortiGate ユニットは別のネットワーク上のサーバに対する ARP 要求に応答できます。ARP 応答を無効にする方法については、『*FortiGate CLI Reference* リファレンス』を参照してください。

仮想 IP のマップ先 IP アドレスには、単一 IP アドレスまたは IP アドレス範囲を設定できます。

FortiGate ユニットで、[Destination Address] フィールドに仮想 IP が指定されているファイアウォール ポリシーと一致するパケットが受信されると、FortiGate ユニットは NAT を適用し、パケットの宛先 IP アドレスを仮想 IP のマップ先 IP アドレスと差し替えます。

仮想 IP または IP プールで設定された変換を実装するには、それを NAT ファイアウォール ポリシーに追加する必要があります。たとえば、パブリック ネットワーク アドレスをプライベート ネットワークにマッピングするファイアウォール ポリシーを追加するには、[Destination Address] フィールドに仮想 IP が設定されている外部から内部へのファイアウォール ポリシーを追加します。

仮想 IP を作成する際の制限事項については、317 ページの「仮想 IP、負荷分散仮想サーバ、および負荷分散リアル サーバの制限」を参照してください。

[Add New Virtual IP Mapping] ページ

このページで、仮想 IP を設定できます。

[Name]	仮想 IP を識別するための名前を入力または変更します。混乱を避けるため、アドレス、アドレス グループ、および仮想 IP を同一の名前にすることはできません。
[External Interface]	リストから仮想 IP 外部インタフェースを選択します。外部インタフェースは送信元ネットワークに接続され、宛先ネットワークに転送されるパケットを受信します。FortiGate インタフェース、VLAN サブインタフェース、VPN インタフェース、またはモデム インタフェースの、いずれも選択できます。
[Type]	VIP の種類は、スタティック NAT、読み取り専用です。
[External IP Address/Range]	宛先ネットワーク上のアドレスにマップする外部 IP アドレスを入力します。 すべての IP アドレスの接続を許可するダイナミック仮想 IP を設定するには、外部 IP アドレスを 0.0.0.0 に設定します。スタティック NAT ダイナミック仮想 IP に追加できるマップ先 IP アドレスは 1 つのみです。負荷分散ダイナミック仮想 IP には、単一のマップ先アドレスまたはマップ先アドレス範囲を指定できます。
[Mapped IP Address/Range]	外部 IP アドレスのマップ先となる宛先ネットワーク上のリアル IP アドレスを入力します。 アドレスの範囲を入力して、宛先ネットワーク上の複数の IP アドレスにパケットを転送することもできます。 スタティック NAT 仮想 IP では、マップ先 IP アドレス範囲を追加すると、FortiGate ユニットが外部 IP アドレス範囲を計算し、その IP アドレス範囲が [External IP Address/Range] フィールドに追加されます。 このオプションは、[Type] が [Static NAT] の場合のみ表示されます。
[Port Forwarding]	PAT (ポート アドレス変換) を実行する場合に選択します。
[Protocol]	転送されるパケットのプロトコルを選択します。 このオプションは、[Port Forwarding] が有効なとき表示されます。
[External Service Port]	ポート フォワーディングを設定する外部インタフェース ポート番号を入力します。 このオプションは、[Port Forwarding] が有効なとき表示されます。
[Map to Port]	外部ポート番号のマップ先となる宛先ネットワーク上のポート番号を入力します。 ポート番号の範囲を入力して、宛先ネットワーク上の複数のポートにパケットを転送することもできます。 スタティック NAT をともなう仮想 IP では、ポートの範囲にマップを追加すると、FortiGate ユニットが外部ポート番号の範囲を計算し、そのポート番号の範囲が [External Service Port] フィールドに追加されます。 このオプションは、[Port Forwarding] が有効なとき表示されます。

仮想 IP を設定するには

1 *[Firewall]*、*[Virtual IP]*、*[Virtual IP]* の順に選択します。

2 *[Create New]* を選択します。

3 必要に応じて、ネットワーク インタフェースに関連付けられる仮想 IP アドレスを入力し、マッピングの種類、およびマップ先 IP アドレスまたはポートあるいは双方を選択することにより、仮想 IP を設定します。各種の設定例については、以下を参照してください。

- 319 ページの「単一 IP アドレスに対するスタティック NAT 仮想 IP の追加」
- 320 ページの「IP アドレス範囲に対するスタティック NAT 仮想 IP の追加」
- 322 ページの「単一 IP アドレスおよび単一ポートに対するスタティック NAT ポート フォワーディングの追加」
- 323 ページの「IP アドレス範囲およびポート範囲に対するスタティック NAT ポート フォワーディングの追加」
- 325 ページの「ダイナミック仮想 IP の追加」
- 326 ページの「ポート変換のみの仮想 IP の追加」

4 *[OK]* を選択します。

仮想 IP が、仮想 IP リストに表示されます。

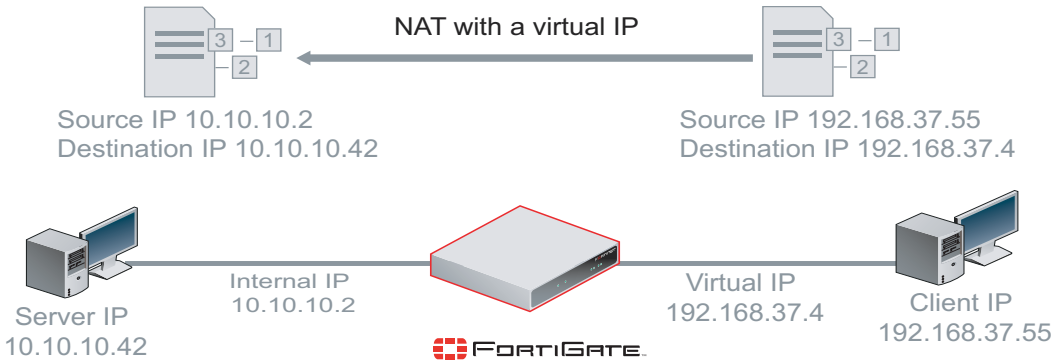
5 仮想 IP を実装するには、ファイアウォール ポリシーで仮想 IP を選択します。

たとえば、パブリック ネットワーク アドレスをプライベート ネットワークにマップするファイアウォール ポリシーを追加するには、外部から内部へのファイアウォール ポリシーを追加し、仮想 IP が関連付けられる [Source Interface/Zone] を選択し、次にポリシーの [Destination Address] フィールドで仮想 IP を選択します。詳細については、268 ページの「ファイアウォール ポリシーの設定」を参照してください。

単一 IP アドレスに対するスタティック NAT 仮想 IP の追加

インターネット上の IP アドレス 192.168.37.4 は、プライベート ネットワーク上の 10.10.10.42 にマッピングされます。インターネットから 192.168.37.4 に接続しようとする通信は、FortiGate ユニットによって 10.10.10.42 に変換され、送信されます。インターネット上のコンピュータからは、この変換は意識されず、プライベート ネットワークを背後に持つ FortiGate ユニットではなく、IP アドレス 192.168.37.4 の 1 台のコンピュータが認識されます。

図 17: 単一 IP アドレスに対するスタティック NAT 仮想 IP の例



次の手順を使用して、インターネット上のユーザが DMZ ネットワーク上の Web サーバに接続できるようにするための仮想 IP を追加します。この例では、FortiGate ユニットの wan1 インタフェースはインターネットに接続され、dmz1 インタフェースは DMZ ネットワークに接続されます。

単一 IP アドレスに対するスタティック NAT 仮想 IP を追加するには

1 *[Firewall]*、*[Virtual IP]*、*[Virtual IP]* の順に選択します。

2 *[Create New]* を選択します。

3 次の情報を入力します。

[Name]	static_NAT
[External Interface]	wan1
[Type]	Static NAT
[External IP Address/Range]	Web サーバのインターネット IP アドレス。 外部 IP アドレスは、通常は Web サーバの ISP から取得されるスタティック IP アドレスです。このアドレスは、別のホストにより使用されない固有の IP アドレスでなければならず、仮想 IP が使用する外部インタフェースの IP アドレスと同一のアドレスにすることはできません。しかし、外部 IP アドレスは選択されたインタフェースへとルーティングされる必要があります。仮想 IP アドレスと外部 IP アドレスは、別々のサブネット上に設定できます。仮想 IP を追加すると、外部インタフェースはその外部 IP アドレスへの ARP 要求に応答します。
[Mapped IP Address/Range]	内部ネットワーク上のサーバの IP アドレス。IP アドレスは 1 つだけなので、2 番目のフィールドは空白のままとします。

4 *[OK]* を選択します。

単一 IP アドレスに対するスタティック NAT 仮想 IP をファイアウォール ポリシーに追加するには

外部から dmz1 への、仮想 IP を使用するファイアウォール ポリシーを追加することで、インターネット上のユーザが Web サーバの IP アドレスに接続しようとしたとき、パケットが FortiGateユニットの外部インタフェースからdmz1インタフェースへと通過するようにします。仮想 IP は、これらのパケットの宛先アドレスを、外部 IP から Web サーバの DMZ ネットワーク IP アドレスに変換します。

1 *[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、*[Create New]* を選択します。

2 ファイアウォール ポリシーを次のように設定します。

[Source Interface/Zone]	external
[Source Address]	All（またはより具体的なアドレス）
[Destination Interface/Zone]	dmz1
[Destination Address]	simple_static_nat
[Schedule]	always
[Service]	HTTP
[Action]	ACCEPT

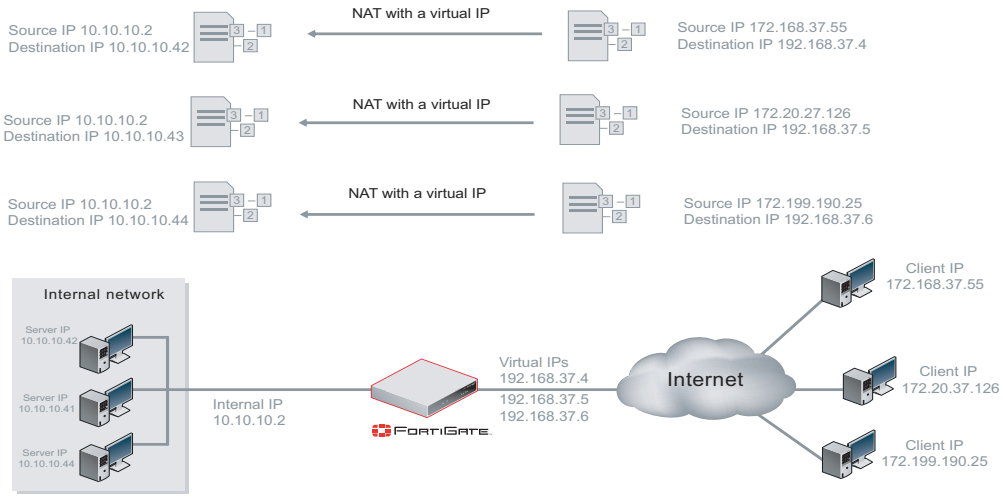
3 *[NAT]* を選択します。

4 *[OK]* を選択します。

IP アドレス範囲に対するスタティック NAT 仮想 IP の追加

インターネット上の IP アドレス範囲 192.168.37.4 ～ 192.168.37.6 は、プライベート ネットワーク上の 10.10.10.42 ～ 10.10.123.44 にマッピングされます。192.168.37.4 と通信しようとするインターネット上のコンピュータからのパケットは、FortiGate ユニットによって 10.10.10.42 に変換され、送信されます。同様に、宛先が 192.168.37.5 のパケットは 10.10.10.43 に、また宛先が 192.168.37.6 のパケットは 10.10.10.44 にそれぞれ変換され、送信されます。インターネット上のコンピュータからは、この変換は意識されず、プライベート ネットワークを背後に持つ FortiGate ユニットではなく、個別の IP アドレスを持つ 3 台のコンピュータが認識されます。

図 18: IP アドレス範囲に対するスタティック NAT 仮想 IP の例



IP アドレス範囲に対するスタティック NAT 仮想 IP を追加するには

1 *[Firewall]*、*[Virtual IP]*、*[Virtual IP]* の順に選択します。

2 *[Create New]* を選択します。

3 次の手順を使用して、インターネット上のユーザが DMZ ネットワーク上の 3 台の Web サーバに接続できるようにするための仮想 IP を追加します。この例では、FortiGate ユニットの wan1 インタフェースはインターネットに接続され、dmz1 インタフェースは DMZ ネットワークに接続されます。

[Name]	static_NAT_range
[External Interface]	wan1
[Type]	Static NAT
[External IP Address/Range]	Web サーバのインターネット IP アドレス範囲。 外部 IP アドレスは、通常は Web サーバの ISP から取得されるスタティック IP アドレスです。これらのアドレスは、別のホストにより使用されない固有の IP アドレスでなければならず、仮想 IP が使用する外部インタフェースの IP アドレスと同一のアドレスにすることはできません。しかし、外部 IP アドレスは選択されたインタフェースへとルーティングされる必要があります。仮想 IP アドレスと外部 IP アドレスは、別々のサブネット上に設定することができます。仮想 IP を追加すると、外部インタフェースは外部 IP アドレスへの ARP 要求に応答します。
[Mapped IP Address/Range]	内部ネットワーク上のサーバの IP アドレス範囲。範囲の最初のアドレスを最初のフィールドに、最後のアドレスを 2 番目のフィールドにそれぞれ入力して、範囲を定義します。

4 *[OK]* を選択します。

IP アドレス範囲に対するスタティック NAT 仮想 IP をファイアウォール ポリシーに追加するには

wan1 から dmz1 への、仮想 IP を使用するファイアウォール ポリシーを追加することで、インターネット上のユーザがサーバ IP アドレスに接続しようとしたとき、パケットが FortiGate ユニットの wan1 インタフェースから dmz1 インタフェースへと通過するようにします。仮想 IP は、これらのパケットの宛先アドレスを、wan1IP からサーバの DMZ ネットワーク IP アドレスに変換します。

1 *[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、*[Create New]* を選択します。

2 ファイアウォール ポリシーを次のように設定します。

[Source Interface/Zone]	wan1
[Source Address]	All（またはより具体的なアドレス）
[Destination Interface/Zone]	dmz1
[Destination Address]	static_NAT_range
[Schedule]	always
[Service]	HTTP
[Action]	ACCEPT

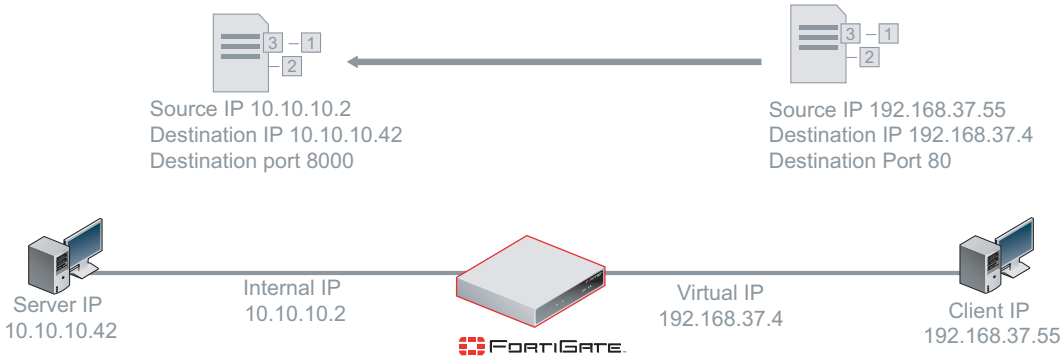
3 *[NAT]* を選択します。

4 *[OK]* を選択します。

単一 IP アドレスおよび単一ポートに対するスタティック NAT ポート フォワーディングの追加

インターネット上の IP アドレス 192.168.37.4、ポート 80 は、プライベート ネットワーク上の 10.10.10.42、ポート 8000 にマッピングされます。インターネットから 192.168.37.4、ポート 80 に接続しようとする通信は、FortiGate ユニットによって 10.10.10.42、ポート 8000 に変換され、送信されます。インターネット上のコンピュータからは、この変換は意識されず、プライベート ネットワークを背後に持つ FortiGate ユニットではなく、IP アドレス 192.168.37.4、ポート 80 の 1 台のコンピュータが認識されます。

図 19: 単一 IP アドレスおよび単一ポートに対するスタティック NAT 仮想 IP ポート フォワーディングの例



単一 IP アドレスおよび単一ポートに対するスタティック NAT 仮想 IP ポート フォワーディングを追加するには

1 *[Firewall]*、*[Virtual IP]*、*[Virtual IP]* の順に選択します。

2 *[Create New]* を選択します。

3 次の手順を使用して、インターネット上のユーザが DMZ ネットワーク上の Web サーバに接続できるようにするための仮想 IP を追加します。この例では、FortiGate ユニットの wan1 インタフェースはインターネットに接続され、dmz1 インタフェースは DMZ ネットワークに接続されます。

[Name]	Port_fwd_NAT_VIP
[External Interface]	wan1
[Type]	Static NAT

[External IP Address/Range]	Web サーバのインターネット IP アドレス。 外部 IP アドレスは、通常は Web サーバの ISP から取得されるスタティック IP アドレスです。このアドレスは、別のホストによって使用されない固有の IP アドレスでなければならず、仮想 IP が使用する外部インタフェースの IP アドレスと同一のアドレスにすることはできません。しかし、外部 IP アドレスは選択されたインタフェースへとルーティングされる必要があります。仮想 IP アドレスと外部 IP アドレスは、別々のサブネット上に設定することができます。仮想 IP を追加すると、外部インタフェースは外部 IP アドレスへの ARP 要求に応答します。
[Mapped IP Address/Range]	内部ネットワーク上のサーバの IP アドレス。IP アドレスは 1 つだけなので、2 番目のフィールドは空白のままとします。
[Port Forwarding]	選択
[Protocol]	TCP
[External Service Port]	インターネットからのトラフィックが使用するポート。Web サーバに対するポートは、通常はポート 80 です。
[Map to Port]	サーバがトラフィックを待つポート。ポートは 1 つだけなので、2 番目のフィールドは空白のままとします。

4 *[OK]* を選択します。

単一 IP アドレスおよび単一ポートに対するスタティック NAT 仮想 IP ポート フォワーディングをファイアウォール ポリシーに追加するには

wan1 から dmz1 への、仮想 IP を使用するファイアウォール ポリシーを追加することで、インターネット上のユーザが Web サーバ IP アドレスに接続しようとしたとき、パケットが FortiGate ユニットの wan1 インタフェースから dmz1 インタフェースへと通過するようにします。仮想 IP は、これらのパケットの宛先アドレスとポートを、外部 IP から Web サーバの dmz ネットワーク IP アドレスに変換します。

1 *[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、*[Create New]* を選択します。

2 ファイアウォール ポリシーを次のように設定します。

[Source Interface/Zone]	wan1
[Source Address]	All（またはより具体的なアドレス）
[Destination Interface/Zone]	dmz1
[Destination Address]	Port_fwd_NAT_VIP
[Schedule]	always
[Service]	HTTP
[Action]	ACCEPT

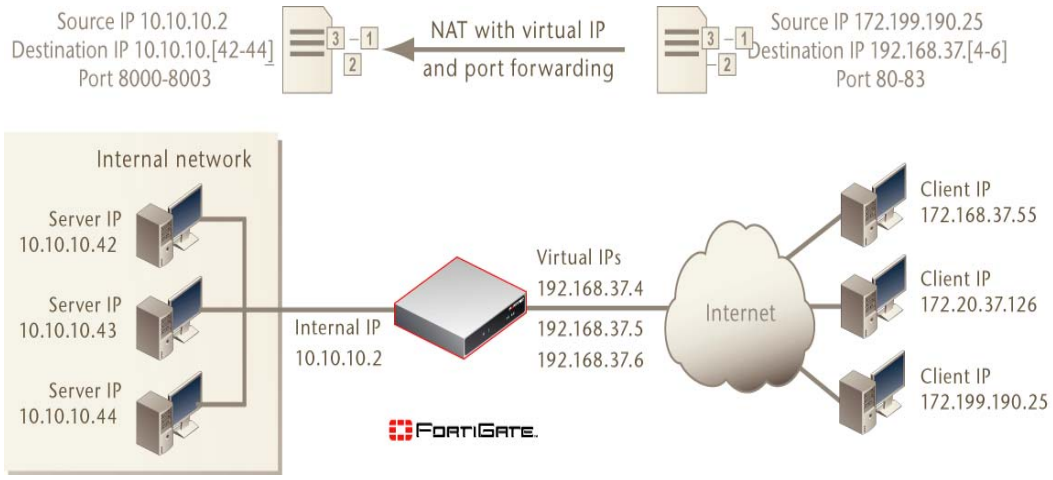
3 *[NAT]* を選択します。

4 *[OK]* を選択します。

IP アドレス範囲およびポート範囲に対するスタティック NAT ポート フォワーディングの追加

インターネット上のアドレス 192.168.37.4 ～ 192.168.37.7 のポート 80 ～ 83 は、プライベートネットワーク上のアドレス 10.10.10.42 ～ 10.10.10.44 のポート 8000 ～ 8003 にマッピングされます。たとえば、インターネットから 192.168.37.5、ポート 82 に接続しようとする通信は、FortiGate ユニットによって 10.10.10.43、ポート 8002 に変換され、送信されます。インターネット上のコンピュータからは、この変換は意識されず、プライベート ネットワークを背後に持つ FortiGate ユニットではなく、IP アドレス 192.168.37.5 の 1 台のコンピュータが認識されます。

図 20: IP アドレス範囲およびポート範囲に対するスタティック NAT 仮想 IP ポート フォワーディングの例



IP アドレス範囲およびポート範囲に対するスタティック NAT 仮想 IP ポート フォワーディングを追加するには

1 *[Firewall]*、*[Virtual IP]*、*[Virtual IP]* の順に選択します。

2 *[Create New]* を選択します。

3 次の手順を使用して、インターネット上のユーザが DMZ ネットワーク上の Web サーバに接続できるようにするための仮想 IP を追加します。この例では、FortiGate ユニットの外部インタフェースはインターネットに接続され、dmz1 インタフェースは DMZ ネットワークに接続されます。

[Name]	Port_fwd_NAT_VIP_port_range
[External Interface]	external
[Type]	Static NAT
[External IP Address/Range]	外部 IP アドレスは、通常は ISP から取得されるスタティック IP アドレスです。このアドレスは、必ず別のホストでは使用されない固有アドレスとなり、仮想 IP が使用する外部インタフェースの IP アドレスと同じアドレスには設定できません。しかし、外部 IP アドレスは選択されたインタフェースへとルーティングされる必要があります。仮想 IP アドレスと外部 IP アドレスは、別々のサブネット上に設定することができます。仮想 IP を追加すると、外部インタフェースは外部 IP アドレスへの ARP 要求に応答します。
[Mapped IP Address/Range]	内部ネットワーク上のサーバの IP アドレス。範囲の最初のアドレスを最初のフィールドに、最後のアドレスを 2 番目のフィールドにそれぞれ入力して、範囲を定義します。
[Port Forwarding]	選択
[Protocol]	TCP
[External Service Port]	インターネットからのトラフィックが使用するポート。Web サーバに対するポートは、通常はポート 80 です。
[Map to Port]	サーバがトラフィックを待つポート。範囲の最初のポートを最初のフィールドに、最後のポートを 2 番目のフィールドにそれぞれ入力して、範囲を定義します。ポートが 1 つのみの場合、2 番目のフィールドは空白のままとします。

4 *[OK]* を選択します。

IP アドレス範囲およびポート範囲に対するスタティック NAT 仮想 IP ポート フォワーディングをファイアウォール ポリシーに追加するには

外部から dmz1 への、仮想 IP を使用するファイアウォール ポリシーを追加することで、インターネット上のユーザがWebサーバIPアドレスに接続しようとしたとき、パケットがFortiGateユニットの外部インタフェースから dmz1 インタフェースへと通過するようにします。仮想 IP は、これらのパケットの宛先アドレスとポートを、外部 IP から Web サーバの dmz ネットワーク IP アドレスに変換します。

1 *[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、*[Create New]* を選択します。

2 ファイアウォール ポリシーを次のように設定します。

[Source Interface/Zone]	external
[Source Address]	All（またはより具体的なアドレス）
[Destination Interface/Zone]	dmz1
[Destination Address]	Port_fwd_NAT_VIP_port_range
[Schedule]	always
[Service]	HTTP
[Action]	ACCEPT

3 *[NAT]* を選択します。

4 *[OK]* を選択します。

ダイナミック仮想 IP の追加

ダイナミック仮想 IP の追加は、仮想 IP の追加と同様です。ただし、外部 IP アドレスがすべての IP アドレスに適合するように、外部 IP アドレスを必ず 0.0.0.0 に設定する点が異なります。

ダイナミック仮想 IP を追加するには

1 *[Firewall]*、*[Virtual IP]*、*[Virtual IP]* の順に選択します。

2 *[Create New]* を選択します。

3 ダイナミック仮想 IP の名前を入力します。

4 リストから、仮想 IP *[External Interface]* を選択します。

外部インタフェースは、送信元ネットワークに接続され、宛先ネットワークに転送されるパケットを受信します。

いずれかのファイアウォール インタフェースまたは VLAN サブインタフェースを選択します。

5 *[External IP Address]* を、0.0.0.0 に設定します。

[External IP Address] に0.0.0.0を設定することで、すべてのIPアドレスに適合します。

6 外部 IP アドレスのマップ先となる IP アドレスを、*[Mapped IP Address]* に入力します。たとえば、内部ネットワーク上の PPTP サーバの IP アドレスです。

7 *[Port Forwarding]* を選択します。

8 *[Protocol]* には、*[TCP]* を選択します。

9 ダイナミック ポート フォワーディングを設定する、*[External Service Port]* 番号を入力します。

外部のサービス ポート番号は、転送されるパケットの宛先ポートに一致する必要があります。たとえば、仮想 IP によりインターネットから PPTP サーバへの PPTP パススルー アクセスを可能にする場合は、外部のサービス ポート番号を 1723（PPTP ポート）に設定する必要があります。

10 パケットが転送される際にパケットに追加される、*[Map to Port]* 番号を入力します。

ポートが変換されない場合は、*[External Service Port]* と同じ番号を入力します。

11 *[OK]* を選択します。

ポート変換のみの仮想 IP の追加

仮想 IP を追加するとき、マップ先 IP アドレスと同じ仮想 IP アドレスを入力しポート フォワーディングを適用する場合は、宛先 IP アドレスは変わりませんが、ポート番号は変換されます。

ポート変換のみをともなう仮想 IP を追加するには

1 *[Firewall]*、*[Virtual IP]*、*[Virtual IP]* の順に選択します。
2 *[Create New]* を選択します。
3 ダイナミック仮想 IP の名前を入力します。
4 リストから、仮想 IP *[External Interface]* を選択します。

外部インタフェースは、送信元ネットワークに接続され、宛先ネットワークに転送されるパケットを受信します。

いずれかのファイアウォール インタフェースまたはVLANサブインタフェースを選択します。

5 リストから、*[External IP Address]* を設定します。
6 外部 IP アドレスをマップする、*[Mapped IP Address]* を入力します。たとえば、内部ネットワーク上の PPTP サーバの IP アドレスです。
7 *[Port Forwarding]* を選択します。
8 *[Protocol]* には、*[TCP]* を選択します。
9 ダイナミック ポート フォワーディングを設定する、*[External Service Port]* 番号を入力します。

外部のサービス ポート番号は、転送されるパケットの宛先ポートに一致する必要があります。たとえば、仮想 IP によりインターネットから PPTP サーバへの PPTP パススルー アクセスを可能にする場合は、外部のサービス ポート番号を 1723（PPTP ポート）に設定する必要があります。

10 パケットが転送される際にパケットに追加される、*[Map to Port]* 番号を入力します。
11 *[OK]* を選択します。

注記：仮想 IP アドレスを外部インタフェースに関連づけずに、その外部インタフェースにポート フォワーディングを適用するには、仮想 IP アドレスの変わりにネットワーク インタフェースのアドレスを入力し、さらにポート フォワーディングを通常のように設定します。

上記の設定を完了した状態で、*外部インタフェース*で受信されたパケットが FortiGate ユニットにより破棄される場合があります。これを防ぐために、FortiGate の CLI にログインし、以下の手順を使用して、ポート変換のみの仮想 IP の ARP 応答を無効にできます。

ARP 応答を無効にするには

1 FortiGate の CLI にログインします。
2 以下のコマンドを入力します。ここでは、<vip_name>

```
config firewall vip
  edit <vip_name>
    set arp-reply disable
  end
```

仮想 IP グループ

複数の仮想 IP を仮想 IP グループ（VIP グループ）に構成することにより、ファイアウォール ポリシー リストを簡素化できます。たとえば、同じネットワーク インタフェース上にある異種の関連する 5 つの仮想 IP に対して、5 つの同一ポリシーを使用する代わりに、5 つの仮想 IP を単一の仮想 IP グループにグループ化し、1 つのファイアウォール ポリシーがこのグループに対応するように構成できます。

VIP グループを使用するファイアウォール ポリシーは、1 つまたは複数のメンバ VIP IP アドレスおよびポート番号の双方と比較、照合されます。

VIP グループ リストの表示

仮想 IP グループ リストを表示するには、*[Firewall]*、*[Virtual IP]*、*[VIP Group]* の順に選択します。

[VIP Group] ページ

このページには、作成済みの VIP グループが一覧表示されます。このページでは、VIP グループの編集、削除、または新規作成が可能です。

[Create New]	新しい VIP グループを追加する場合に選択します。詳しくは、327 ページの「VIP グループの設定」を参照してください。 [Create New] を選択すると、[New VIP Group] ページの画面に自動的に移動します。
[Group Name]	仮想 IP グループの名前。
[Members]	グループのメンバを表示します。
[Interface]	VIP グループが属するインタフェースを表示します。
[Delete]	リストから VIP グループを削除します。[Delete] アイコンは、ファイアウォール ポリシーで VIP グループが使用されていない場合にのみ表示されます。
[Edit]	グループ名やメンバなど、VIP グループ情報を編集します。

VIP グループの設定

VIP グループを追加するには、*[Firewall]*、*[Virtual IP]*、*[VIP Group]* の順に選択し、*[Create new]* を選択します。VIP グループを編集するには、*[Firewall]*、*[Virtual IP]*、*[VIP Group]* の順に選択し、編集する VIP グループの *[Edit]* アイコンを選択します。以下の表の情報を入力し、*[OK]* を選択します。

[New VIP Group] ページ

このページでは、グループに含まれる VIP を設定できます。

[Group Name]	グループ名を入力または編集します。
[Interface]	VIP グループを作成するインタフェースを選択します。グループの編集中は、[Interface] ボックスは灰色に表示されます。
[Available VIPs] および [Members]	上または下向き矢印を選択し、仮想 IP を [Available VIPs] および [Members] 間で移動します。[Members] には、この仮想 IP グループを構成する仮想 IP が表示されます。

IP プールの設定

IP プールを使用することで、発信元アドレスを FortiGate ユニットのインタフェースに割り当てられる IP アドレスではなく、IP プールからランダムに選択されるアドレスに変換する、NAT ポリシーを追加できます。トランスペアレント モードでは、FortiGate の CLI からのみ IP プールを利用できます。

IP プールでは、単一の IP アドレスまたは IP アドレスの範囲が定義されます。IP プールに入力される単一の IP アドレスは、1 つの IP アドレスの範囲になります。たとえば、IP プールに 1.1.1.1 を入力すると、この IP プールは実質的に 1.1.1.1 から 1.1.1.1 のアドレス範囲となります。

FortiGate インタフェースの IP アドレスが、1 つまたは複数の IP プール アドレス範囲と重複する場合は、インタフェースは重複する IP プールに含まれるすべての IP アドレスへの ARP 要求に応答します。

たとえば、FortiGate ユニットに、以下の IP アドレスのポート 1 およびポート 2、

- ポート 1 の IP アドレス : 1.1.1.1/255.255.255.0 (範囲は 1.1.1.0 ～ 1.1.1.255)
- ポート 2 の IP アドレス : 2.2.2.2/255.255.255.0 (範囲は 2.2.2.0 ～ 2.2.2.255)

および以下の IP プールをともなう場合について説明します。

- IP_pool_1: 1.1.1.10–1.1.1.20
- IP_pool_2: 2.2.2.10–2.2.2.20
- IP_pool_3: 2.2.2.30–2.2.2.40

ポート 1 インタフェースと IP_pool_1 の重複する IP 範囲は、次のようになります。

- (1.1.1.0 ～ 1.1.1.255) および (1.1.1.10 ～ 1.1.1.20) の重複部分は、1.1.1.10 ～ 1.1.1.20

ポート 2 インタフェースと IP_pool_2 の重複する IP 範囲は、次のようになります。

- (2.2.2.0 ～ 2.2.2.255) および (2.2.2.10 ～ 2.2.2.20) の重複部分は、2.2.2.10 ～ 2.2.2.20

ポート 3 インタフェースと IP_pool_3 の重複する IP 範囲は、次のようになります。

- (2.2.2.0 ～ 2.2.2.255) および (2.2.2.30 ～ 2.2.2.40) の重複部分は、2.2.2.30 ～ 2.2.2.40

この結果、以下のようになります。

- ポート 1 インタフェースは、1.1.1.10 ～ 1.1.1.20 への ARP 要求に応答します。
- ポート 2 インタフェースは、2.2.2.10 ～ 2.2.2.20 および 2.2.2.30 ～ 2.2.2.40 への ARP 要求に応答します。

ファイアウォール ポリシーから *[NAT]* を選択し、*[Dynamic IP Pool]* を選択します。IP プールを選択し、FortiGate ユニットから送信されるパケットの発信元アドレスを、IP プールからランダムに選択されるアドレスに変換します。

IP プールとダイナミック NAT

ダイナミック NAT に IP プールを使用します。たとえば、ある組織が一定範囲のインターネット アドレスを購入したものの、FortiGate ユニットの外部インタフェースではインターネット接続は 1 つのみという場合があります。

こうした場合、組織のインターネット IP アドレスの 1 つを、FortiGate ユニットの外部インタフェースに割り当てます。FortiGate ユニットが NAT/ ルート モードで機能している場合、組織のネットワークからインターネットへの接続は、すべてこの IP アドレスから行われているように見えます。

すべてのインターネット IP アドレスから接続を開始するには、IP プールにこのアドレス範囲を追加します。次いで、外部インタフェースのすべてのポリシーに、宛先として *[Dynamic IP Pool]* を選択します。各接続に対し、ファイアウォールは IP プールから動的に IP アドレスを選択し、接続の送信元アドレスとします。これにより、インターネットへの接続は、IP プールに含まれるいずれかの IP アドレスから開始されているように見えます。

固定ポートを用いるファイアウォール ポリシーの IP プール

接続に使用されるパケットの送信元ポートが NAT ポリシーにより変換される場合、ネットワーク設定が正しく機能しない場合があります。NAT では、特定のサービスの接続を追跡するため、送信元ポートが変換されます。CLI から、NAT ポリシーの `fixedport` を有効に設定し、発信元ポートの変換を回避できます。ただし、`fixedport` を選択すると、このサービスでは、ファイアウォールによりサポートされる接続は 1 つのみになることを意味します。複数の接続をサポート可能にするには、IP プールを追加した後、ポリシー内で *[Dynamic IP pool]* を選択します。ファイアウォールは IP アドレスを IP プールからランダムに選択して、各接続に割り当てます。この場合、ファイアウォールでサポート可能な接続の数は、IP プール内の IP アドレスの数によって制限されます。

発信元 IP アドレスおよび IP プール アドレスの一致

発信元アドレスが IP プール アドレスに変換されるとき、以下に示される 3 つのケースのいずれかに該当する場合があります。

シナリオ 1: 発信元アドレスの数および IP プール アドレスの数が同じ場合

このケースでは、FortiGate ユニットは必ず IP アドレス同士を一対一で一致させます。

このような場合に、fixedport を有効にすると、FortiGate ユニットは最初の発信元ポートを保持します。同じ IP プールが複数のファイアウォール ポリシーで使用される場合、または同じ IP アドレスが複数の IP プールで使用される場合は、これは競合の原因となります。

最初のアドレス	変換後
192.168.1.1	172.16.30.1
192.168.1.2	172.16.30.2
192.168.1.254	172.16.30.254

シナリオ 2: 発信元アドレスの数および IP プール アドレスの数より多い場合

このケースでは、FortiGate ユニットはラップアラウンドを使用し IP アドレスを変換します。

このような場合に fixedport を有効にすると、FortiGate ユニットは最初の発信元ポートを保持します。しかし、複数のユーザが異なるセッションで同じ TCP の 5 つのタプルを使用する場合には、競合が発生する可能性もあります。

最初のアドレス	変換後
192.168.1.1	172.16.30.10
192.168.1.2	172.16.30.11
192.168.1.10	172.16.30.19
192.168.1.11	172.16.30.10
192.168.1.12	172.16.30.11
192.168.1.13	172.16.30.12

シナリオ 3: 発信元アドレスの数および IP プール アドレスの数より少ない場合

このケースでは、IP プール アドレスの一部が使用され、残りのアドレスは使用されません。

最初のアドレス	変換後
192.168.1.1	172.16.30.10
192.168.1.2	172.16.30.11
192.168.1.3	172.16.30.12
以上の発信元アドレスのみ	172.16.30.13、他のアドレスは使用されない

IP プール リストの表示

FortiGate ユニット上でバーチャル ドメインが有効に設定される場合、IP プールはバーチャル ドメインごとに個別に作成されます。IP プールにアクセスするには、メイン メニューのリストからバーチャル ドメインを選択します。

IP プール リストを表示するには、*[Firewall]*、*[Virtual IP]*、*[IP Pool]* の順に選択します。

[IP Pool] ページ

このページには、作成済みの IP プールが一覧表示されます。このページでは、IP プールの編集、削除、または新規作成が可能です。

[Create New] IP プールを追加する場合に選択します。[Create New] を選択すると、[New Dynamic IP Pool] ページの画面に自動的に移動します。

[Name] IP プールの名前。ファイアウォール ポリシーでこの名前を選択します。

[Start IP] 開始 IP を入力し、IP プール アドレス範囲の最初を指定します。

[End IP] 最終 IP を入力し、IP プール アドレス範囲の最後を指定します。

[Delete]	リストからこのエントリを削除する場合に選択します。[Delete] アイコンは、IP プールがファイアウォール ポリシーで使用されていない場合にのみ表示されます。
[Edit]	IP プールを編集する場合に選択します。[Name]、[Interface]、[IP Range/Subnet] を変更できます。

IP プールの設定

単一の IP アドレスは、通常どおり入力します。たとえば、`192.168.110.100` は有効な IP プール アドレスです。IP アドレス範囲が必要な場合は、以下のいずれかの形式を使用します。

- x.x.x.x-x.x.x.x、たとえば `192.168.110.100-192.168.110.120`
- x.x.x.[x-x]、たとえば `192.168.110.[100-120]`

IP プールを追加するには、*[Firewall]*、*[Virtual IP]*、*[IP Pool]* の順に選択します。

[New Dynamic IP Pool] ページ

このページでは、IP プールの IP アドレス範囲およびサブネットを設定できます。また、IP プールの単一 IP アドレスも入力できます。

[Name]	IP プールの名前を入力します。
[IP Range/Subnet]	IP プールの IP アドレス範囲を入力します。IP 範囲は、アドレス範囲の最初と最後を定義します。範囲の最初は範囲の最後よりも小さくなければなりません。IP 範囲の最初と最後は、IP プールを追加するインタフェースの IP アドレスと同じサブネット上にある必要ありません。

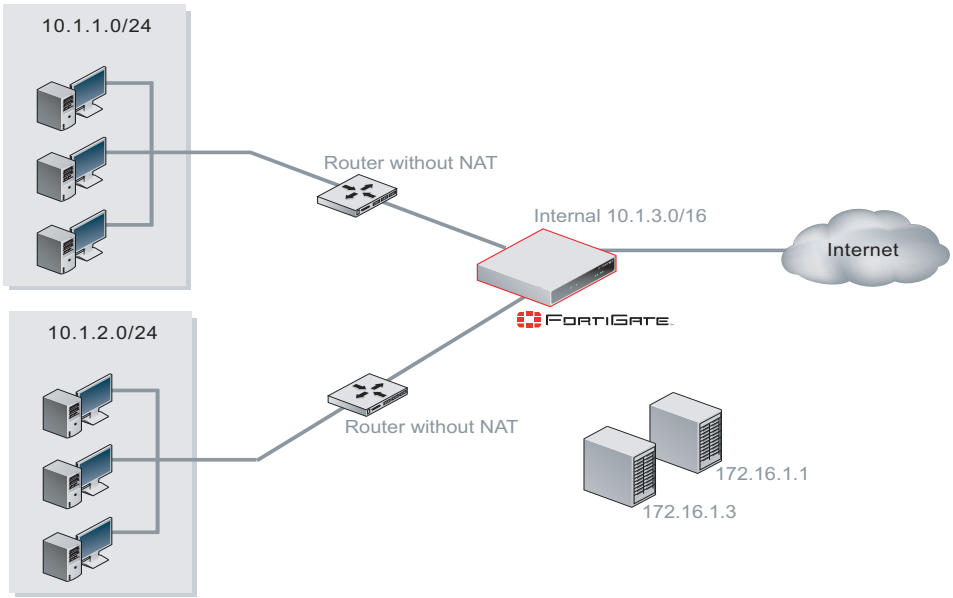
ダブル NAT: IP プールと仮想 IP の組み合わせ

ファイアウォール ポリシーを作成するとき、IP プールおよび仮想 IP の双方を、二重の IP またはポートあるいは双方の変換に使用できます。

ここでは、以下のようなネットワーク トポロジを例に説明します。

- 10.1.1.0/24 サブネット内のユーザが、ポート 8080 を使用しサーバ 172.16.1.1 にアクセス。
- サーバのリスニング ポートは 80。
- 必ず固定ポートを使用。

図 21: ダブル NAT



ローカル ユーザがサーバにアクセスできるようにするには、固定ポートおよび IP プールを使用し、仮想 IP により宛先ポートを 8080 から 80 に変換することで、複数のユーザ接続を可能にできます。

IP プールを作成するには

1 *[Firewall]*、*[Virtual IP]*、*[IP Pool]* の順に選択します。
2 *[Create New]* を選択します。
3 次の情報を入力し、*[OK]* を選択します。

[Name]	pool-1
[IP Range/Subnet]	10.1.3.1-10.1.3.254

ポート変換のみの仮想 IP を作成するには

1 *[Firewall]*、*[Virtual IP]*、*[Virtual IP]* の順に選択します。
2 *[Create New]* を選択します。
3 次の情報を入力し、*[OK]* を選択します。

[Name]	server-1
[External Interface]	Internal
[Type]	Static NAT
[External IP Address/Range]	172.16.1.1 注 : このアドレスはサーバ アドレスと同じになります。
[Mapped IP Address/Range]	172.16.1.1.
[Port Forwarding]	Enable
[Protocol]	TCP
[External Service Port]	8080
[Map to Port]	80

ファイアウォール ポリシーを作成するには

内部から DMZ へのファイアウォール ポリシーを追加します。このポリシーは、仮想 IP を使用して宛先ポート番号を変換し、IP プールを使用して発信元アドレスを変換します。

1 *[Firewall]*、*[Policy]* の順に選択します。
2 *[Create New]* を選択します。
3 ファイアウォール ポリシーを次のように設定します。

[Source Interface/Zone]	internal
[Source Address]	10.1.1.0/24
[Destination Interface/Zone]	dmz
[Destination Address]	server-1
[Schedule]	always
[Service]	HTTP
[Action]	ACCEPT
[NAT]	選択
[Dynamic IP Pool]	選択、および *pool-1* IP プールを選択。

4 *[OK]* を選択します。

トランスペアレント モードでの NAT ファイアウォール ポリシーの追加

NAT/ ルート モードでの機能と同様に、FortiGate ユニットをトランスペアレント モードで使用するとき、ファイアウォール ポリシーを追加し、以下を行うことができます。

- NAT を有効に設定し、パケットが FortiGate ユニットを通過するときパケットの発信元アドレスを変換します。
- 仮想 IP を追加し、パケットが FortiGate ユニットを通過するときパケットの宛先アドレスを変換します。
- 発信元アドレスの変換に必要な IP プールを追加します。

NAT ファイアウォール ポリシーが NAT/ ルート モードで機能するには、異なるネットワーク上に 2 つのインタフェースがあり、2 つの異なるサブネット アドレスをともなう必要があります。これにより、ファイアウォール ポリシーを作成することで、パケットが FortiGate ユニットで一方のインタフェースからもう一方のインタフェースにリレーされるとき、パケットの発信元または宛先アドレスを変換できます。

トランスペアレント モードで機能する FortiGate ユニットにある IP アドレスは、通常は 1 つの管理 IP のみです。NAT をトランスペアレント モードでサポートするために、第 2 の管理 IP を追加できます。これら 2 つの管理 IP は、異なるサブネット上にあることが必要です。2 つの管理 IP アドレスを追加するとき、FortiGate ユニットのすべてのネットワーク インタフェースは、これらの IP アドレスへの接続に応答します。

図 22 に示される例では、内部ネットワーク上 (サブネット アドレス 192.168.1.0/24) のすべての PC は、デフォルトのルートとして 192.168.1.99 に設定されています。FortiGate ユニットの管理 IP の 1 つは、192.168.1.99 に設定されています。この設定では、一般的な NAT モードのファイアウォールが構成されます。内部ネットワーク上のいずれかの PC がインターネットに接続しようとすると、インターネット宛のパケットがその PC のデフォルトのルートで FortiGate ユニットの内部インタフェースに送信されます。

同様に、DMZ ネットワーク (サブネット アドレス 10.1.1.0/24) では、すべての PC にデフォルトのルート 10.1.1.99 があります。

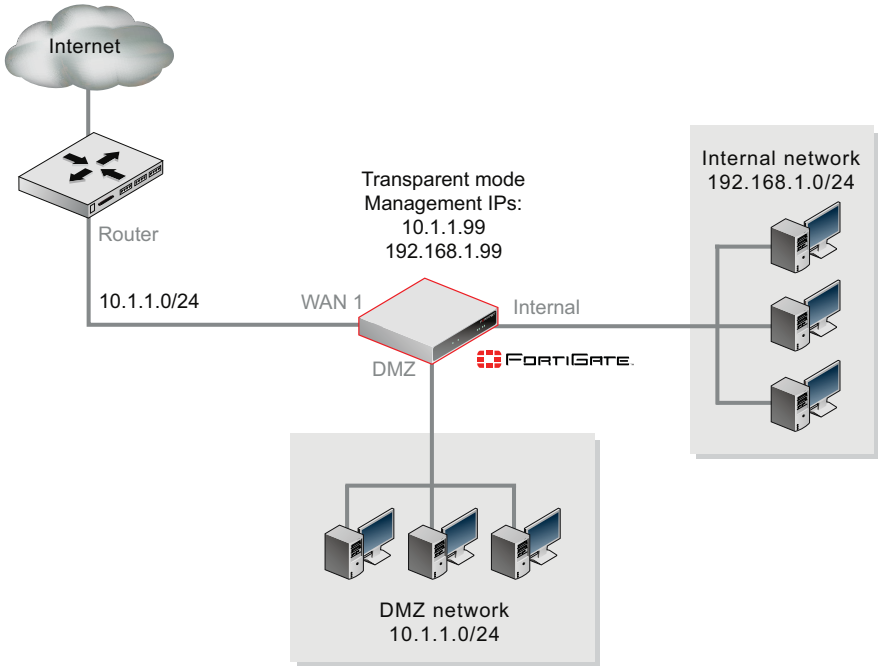
この例では、これらのパケットを内部インタフェースからwan1インタフェースを経てインターネットへリレーするための、内部から wan1 へのファイアウォール ポリシーの追加について説明します。wan1 インタフェースには専用の IP アドレスがないので、送信パケットの発信元アドレスを wan1 インタフェースに接続されるネットワーク上の IP アドレスに変換する wan1 インタフェースに、IP プールを追加する必要があります。

さらにこの例では、単一 IP アドレス 10.1.1.201 をともなう IP プールの追加について説明します。内部ネットワーク上の PC によって送信され、内部から wan1 へのポリシーによって許可されるすべてのパケットは、それらの発信元アドレスが 10.1.1.201 に変換された状態で wan1 インタフェースから伝送されます。この時点で、これらのパケットは、インターネットを経由し宛先まで伝送されることが可能になります。応答パケットは、10.1.1.201 の宛先アドレスを持つので、wan1 に返ります。内部から wan1 への NAT ポリシーは、これらの応答パケットの宛先アドレスを、発信元 PC の IP アドレスに変換し、応答パケットを内部インタフェースから発信元 PC に伝送します。

以下の手順を使用し、トランスペアレント モードで機能する NAT を設定します。

- 2 つの管理 IP を追加する
- wan1 インタフェースに IP プールを追加する
- 内部から wan1 へのファイアウォール ポリシーを追加する

図 22: トランスペアレント モードでの NAT 設定例



トランスペアレント モードで発信元アドレス変換の NAT ポリシーを追加するには

1 以下のコマンドを入力し、2 つの管理 IP を追加します。

2 番目の管理 IP は、内部ネットワークのデフォルトのゲートウェイです。

```
config system settings
  set manageip 10.1.1.99/24 192.168.1.99/24
end
```

2 以下のコマンドを入力して、IP プールを wan1 インタフェースに追加します。

```
config firewall ippool
  edit nat-out
    set interface "wan1"
    set startip 10.1.1.201
    set endip 10.1.1.201
  end
```

3 以下のコマンドを入力し、NAT が有効に設定され IP プールを含む、内部から wan1 へのファイアウォール ポリシーを追加します。

```
config firewall policy
  edit 1
    set srcintf "internal"
    set dstintf "wan1"
    set scraddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ANY"
    set nat enable
    set ippool enable
    set poolname nat-out
  end
```

注記：ウェブ ベース マネージャからファイアウォール ポリシーを追加し、次に CLI から NAT を有効に設定して IP プールを追加できます。

トラフィック シェーピング

トラフィック シェーピングをファイアウォール ポリシーに組み込むことにより、ポリシーに割り当てられる帯域幅を制御し、ポリシーによって処理されるトラフィックのプライオリティを設定できます。トラフィック シェーピングにより、大量のデータが FortiGate ユニットを通過するとき、どのポリシーが最も高いプライオリティをもつか設定できます。たとえば、社内 Web サーバのポリシーを、大部分の従業員が使用するコンピュータのポリシーよりも高いプライオリティに指定できます。また、通常より高速なインターネットアクセスを必要とする従業員には、特別により広い帯域幅を設定した送信ポリシーを許可することもできます。

トラフィック シェーピングは、[Action] を ACCEPT、IPSEC、または SSL-VPN に設定したファイアウォール ポリシーで利用できます。また、H.323、TCP、UDP、ICMP、および ESP など、サポートされるすべてのサービスで使用できます。

保証帯域幅と最大帯域幅をキューイングと組み合わせることで、トラフィックに対する最小帯域幅および最大帯域幅を保証できます。

トラフィック シェーピングを使用しても、利用可能な帯域幅の総量を増やすことはできませんが、帯域を大量に消費するトラフィックや帯域幅の影響を受けやすいトラフィックの品質を向上させることができます。

ファイアウォール ポリシーの詳細については、265 ページの「ファイアウォール ポリシー」を参照してください。トラフィック シェーピングの詳細については、『*FortiGate トラフィック シェーピング テクニカル ノート*』も参考にしてください。

この項には以下のトピックが含まれています。

保証帯域幅と最大帯域幅

トラフィック シェーパーを追加するとき、*[Guaranteed Bandwidth]* フィールドに値を入力すると、選択したネットワーク トラフィックに使用可能な帯域幅の量（キロバイト / 秒単位）を保証します。たとえば、電子商取引トラフィックに対して、より高い保証帯域幅を与えることができます。

トラフィック シェーパーを追加するとき、*[Maximum Bandwidth]* フィールドに値を入力すると、選択したネットワーク トラフィックに使用可能な帯域幅の量（キロバイト / 秒単位）を制限します。たとえば、IM トラフィックで利用される帯域幅を制限して、帯域幅の一部をより重要な電子商取引トラフィックのために確保できます。

トラフィックに使用可能な帯域幅をトラフィック シェーパーで設定すると、制御セッションとデータ セッションの両方で、その帯域幅が双方向のトラフィックに使用されます。たとえば、保証帯域幅を内部および外部への FTP ポリシーに適用した状態で、内部ネットワーク上のユーザが FTP を使用してファイルを put および get すると、put および get の両セッションは、このポリシーが適用されるトラフィックに割り当てられる帯域幅を共有します。

保証帯域幅および最大帯域幅をポリシーに設定すると、この帯域幅は、そのポリシーが適用されるすべてのトラフィックにおいて利用可能な、総帯域幅となります。複数のユーザが、同じポリシーを用いる複数の通信セッションを開始すると、これらすべての通信セッションは、そのポリシーに割り当てられる帯域幅を必ず共有します。

ただし、同じサービスを使用する場合の複数のインスタンスに、それぞれ異なるポリシーが適用される場合は、利用可能な帯域幅はこれらの複数のインスタンス間で共有されません。たとえば、あるネットワーク アドレスに対して、FTP で使える帯域幅を制限するための 1 つの FTP ポリシーを作成すると同時に、別のネットワーク アドレスに対して、別の帯域幅が使えるような別の FTP ポリシーを作成することができます。

注記：保証帯域幅と最大帯域幅の両方を 0（ゼロ）に設定した場合、そのポリシーではどのトラフィックも許可されません。

トラフィック プライオリティ

トラフィック シェーパーを追加するとき、トラフィック プライオリティを設定することにより、異なるトラフィックの種類ごとに相対的なプライオリティを管理できます。遅延に影響されやすい重要なトラフィックには高いプライオリティを割り当て、遅延の影響が少ない重要度の低いトラフィックには低いプライオリティを割り当てる必要があります。

FortiGate ユニットは、プライオリティの高い接続に帯域幅が必要ない場合にのみ、プライオリティの低い接続に帯域幅を提供します。

たとえば、音声トラフィックと電子商取引トラフィックに帯域幅を保証するためのポリシーを追加し、次に音声トラフィックを制御するポリシーには高いプライオリティを、電子商取引トラフィックを制御するポリシーには中程度のプライオリティを割り当てることができます。帯域幅の使用が集中する時間帯に、音声トラフィックと電子商取引トラフィックの両方で帯域幅が競合した場合は、プライオリティの高い音声トラフィックが電子商取引トラフィックの前に送り出されます。

トラフィック シェーピングについて

トラフィック シェーピングは特定の フローを他のフローより優先させるために、トラフィックのピーク / バーストを ″正規化″ しようと試みます。ただし、バッファ処理できるデータの量やその期間には物理的な制限があります。これらのしきい値を超えた状態では、フレームおよびパケットが破棄され、セッションに別の形で影響を与えることになります。たとえば、正しくないトラフィックシェーピングの設定はネットワークフローの余計な品質低下をもたらすことがあります。過剰なパケットの廃棄がエラーから回復しようとする上位レイヤーの余分なオーバーヘッドを引き起こすからです。

トラフィック シェーピングの基本的なアプローチは、破棄されると不都合な特定のトラフィック フローに、他のトラフィックよりも高いプライオリティを設定することです。つまり、プライオリティの低いトラフィックのパフォーマンスおよび安定性をある程度犠牲にしても、プライオリティの高いトラフィックのパフォーマンスおよび安定性を高める、または保証することを意味します。

たとえば、特定のフローに帯域幅の制限を適用する場合は、これらのセッションが制限により悪影響を受ける可能性を認めた上で、制限を適用することになります。

ファイアウォール ポリシーに設定するトラフィック シェーピングは、いずれの方向に流れるトラフィックに対しても適用されます。そのため、あるセッションが、内部のホストから外部のホストに向けて設定されており、内部から外部へのポリシーが適用される場合、データ ストリームが外部から内部への流れであっても、そのセッションに対してトラフィック シェーピングが適用されます。このような例には、FTP の ″get″、または電子メールを取得するために外部サーバに接続する SMTP サーバがあります。

トラフィック シェーピングは、通常のトラフィック レートの標準的な IP トラフィックに対して有効であり、トラフィックが FortiGate ユニットの容量を超えている間は有効でないことに注意してください。 パケットは、トラフィック シェーピングを適用される前に FortiGate ユニットにより受信される必要があるので、 FortiGate ユニットが受信したすべてのトラフィックを処理できない場合は、 パケットが破棄されて、 遅延、 待ち時間が発生する可能性があります。

トラフィック シェーピングが最も効果的に機能するように、イーサネット インタフェースの統計情報にエラー、コリジョン、バッファ オーバーランなどがないことを確認してください。これらのいずれかが発生すると、場合により FortiGate およびスイッチ設定の調整が必要になります。詳細については、『*FortiGate トラフィック シェーピング テクニカル ノート*』を参照してください。

共有トラフィック シェーパーの設定

共有トラフィック シェーパーを設定することで、トラフィック シェーピングおよび逆方向のトラフィック シェーピングをファイウォール ポリシーに追加できます。

共有トラフィック シェーパー リストを表示するには、*[Firewall]*、*[Traffic Shaper]*、*[Shared]* の順に選択します。共有トラフィック シェーパーを追加するには、*[Create New]* を選択します。

FortiGate ユニットには、デフォルトで定義済みの共有トラフィック シェーパーが含まれています。これらのシェーパーをファイアウォール ポリシーにそのまま追加することもカスタマイズすることもでき、あるいは新しい共有トラフィック シェーパーを追加することが可能です。

共有トラフィック シェーパーを作成または編集し、それをファイアウォール ポリシーに追加するには、*[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、新しいファイアウォール ポリシーを追加するかまたはファイアウォール ポリシーを編集します。さらに、*[Firewall]*、*[Policy]*、*[IPv6 Policy]* の順に選択し、新しい Ipv6 ファイアウォール ポリシーを追加するか Ipv6 ファイアウォール ポリシーを編集することで、Ipv6 トラフィックにトラフィック シェーピングを適用できます。

ファイアウォール ポリシーで共有トラフィック シェーピングを有効にするには、*[Traffic Shaping]* を選択し、共有トラフィック シェーパーを選択します。また、*[Reverse Direction Traffic Shaping]* を選択し共有トラフィック シェーパーを選択することで、返信トラフィックに共有トラフィック シェーピングを適用することもできます。

注記：トラフィック シェーピングが最も効果的に機能するように、イーサネット インタフェースの統計情報にエラー、衝突、バッファ オーバーランなどがないことを確認してください。これらのいずれかが発生すると、場合により FortiGate およびスイッチ設定の調整が必要になります。診断コマンドを使用してこの情報を取得する方法については、『*FortiGate トラフィック シェーピング テクニカル ノート*』のトラブルシューティングの項を参照してください。

[Shared] ページ

このページには、作成済みの共有トラフィック シェーパーが一覧表示されます。このページでは、共有トラフィック シェーパーの編集、削除、または新規作成が可能です。

[Create New]	新しい共有トラフィック シェーパーを追加する場合に選択します。
[Name]	このトラフィック シェーパーの名前を入力します。
[Delete]	トラフィック シェーパーを削除するとき選択します。
[Edit]	トラフィック シェーパーを編集するとき選択します。

[New Shared Traffic Shaper] ページ

このページでは、新しい共有トラフィック シェーパーを設定できます。

[Apply Shaping]	*[Per Policy]* を選択すると、トラフィック シェーパーを使用する 1 つのファイアウォール ポリシーにこのシェーパーを適用します。 *[For all policies using this shaper]* を選択すると、このトラフィック シェーパーを使用するすべてのファイアウォール ポリシーにこのシェーパーを適用します。
[Shaping Methods]	共有トラフィック シェーパーにより使用されるトラフィック シェーピングの方法を設定します。
[Guaranteed Bandwidth]	値を選択し、プライオリティの高いサービスが使用可能な帯域幅を十分確保します。すべてのファイアウォール ポリシーの *[Guaranteed Bandwidth]* の総計が、インタフェースの帯域幅容量を大幅に下回るようにしてください。

[Maximum Bandwidth]	帯域幅を必要とするより重要なサービスのために、重要性の低いサービスの帯域幅利用を制限するとき選択します。 *[Guaranteed Bandwidth]* および *[Maximum Bandwidth]* の双方を、ゼロに設定しないでください。両方をゼロに設定すると、この共有トラフィック シェーパーが追加されるファイアウォール ポリシーでは、どのトラフィックも許可されなくなります。
[Traffic Priority]	*[High]*、*[Medium]*、または *[Low]* を選択します。*[Traffic Priority]* を選択し、FortiGate ユニットで、異なるトラフィックの種類ごとに相対的なプライオリティを管理します。たとえば、電子商取引トラフィックのサポートに必要なセキュアな Web サーバへの接続ポリシーには、高いトラフィック プライオリティを割り当て、重要性の低いサービスには低いプライオリティを割り当てます。プライオリティの高い接続に帯域幅が必要ない場合のみ、ファイアウォールによってプライオリティの低い接続に帯域幅が割り当てられます。 すべてのファイアウォール ポリシーで、トラフィック シェーピングを有効にしてください。ポリシーにトラフィック シェーピングのルールを適用しない場合、そのポリシーは、デフォルトで高いプライオリティに設定されます。 ファイアウォール ポリシーを、3 つのプライオリティ キューのすべてに分散させてください。

"IP ごとのトラフィック シェーピング " の設定

ポリシーまたはシェーパーごとではなく IP アドレスごとに適用されるトラフィック シェーピングを設定します。共有トラフィック シェーパーと同様に、ファイアウォール ポリシーで 祢 P ごとのトラフィック シェーパー・ を選択します。

[Firewall]、*[Traffic Shaper]*、*[Per-IP]* の順に選択し、祢 P ごとのトラフィック シェーパー・ を追加します。

"IP ごとのトラフィック シェーピング " をファイアウォール ポリシーに適用するには、*[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、ファイアウォール ポリシーを追加または編集します。*[Per-IP Traffic Shaping]* を選択して "IP ごとのトラフィック シェーパー " を選択します。

[Per-IP] ページ

このページには、作成済みの "IP ごとのトラフィック シェーパー " が一覧表示されます。このページでは、"IP ごとのトラフィック シェーパー " の編集、削除、または新規作成が可能です。

[Create New]	新しい "IP ごとのトラフィック シェーパー " を追加する場合に選択します。
[Name]	この "IP ごとのトラフィック シェーパー " の名前。
[Delete]	"IP ごとのトラフィック シェーパー " を削除するとき選択します。
[Edit]	"IP ごとのトラフィック シェーパー " を編集するとき選択します。

[Per-IP Traffic Shaper] 設定

ここでは、"IP ごとのトラフィック シェーパー " を設定できます。"IP ごとのトラフィック シェーパー " は、トラフィック シェーパーがそれぞれに IP アドレスを設定されて、"IP ごとのトラフィック シェーパー " がファイアウォール ポリシーに適用されます。

[Maximum Bandwidth]	最大限の帯域幅を Kbps 単位で入力します。この制限は、IP アドレスごとに適用されます。範囲は、1 から 2 097 000 です。帯域幅の制限を無効にするには、0 (ゼロ) を入力します。
[IP List] **[IP/Range]**	この "IP ごとのトラフィック シェーパー " が適用される IP アドレスまたは IP アドレス範囲を追加します。
[Delete]	IP アドレスまたはアドレス範囲のエントリを削除します。
[Add]	単一の IP アドレスまたはアドレス範囲を追加します。

ファイアウォール負荷分散

FortiGate の負荷分散機能を使用して受信トラフィックをインターセプトすることで、利用可能な複数のサーバ間でそのトラフィックを分けることができます。そうすることで、FortiGate ユニットは複数のサーバがあたかも一台のデバイスまたはサーバのように応答させることができます。これはつまり、同時により多くのリクエストを処理できることを意味します。

サーバーロードバランスには他にもメリットがあります。まず、負荷が複数のサーバに分散されることで、提供されるサービスの可用性を非常に高くすることができます。一台のサーバが故障しても、他のサーバにより処理されます。さらに、拡張性を増すことができます。負荷がかなり増えたときに、FortiGate ユニットの背後にさらにサーバを追加して負荷の増加に対処できます。

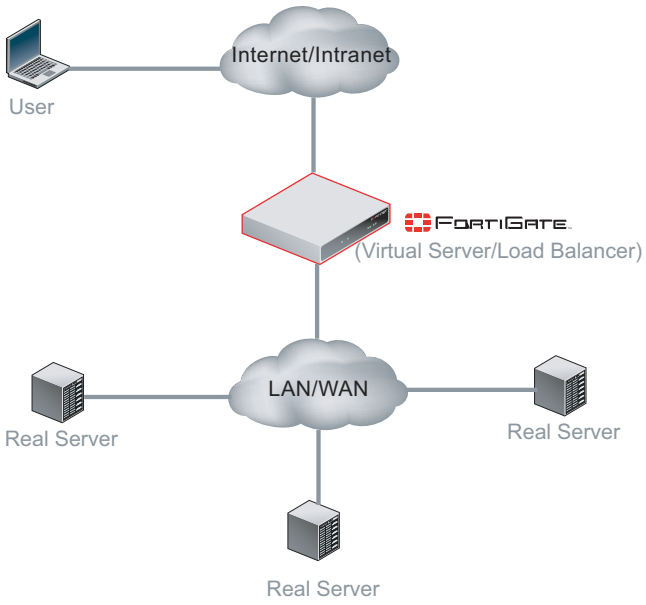
この項には以下のトピックが含まれています。

FortiGate の負荷分散機能の仕組み

[Firewall]、*[Load Balance]*、*[Virtual Server]* の順に選択し、FortiGate ユニット（ロードバランサ）で仮想サーバの設定をおこなえます。次に、*[Firewall]*、*[Load Balance]*、*[Real Server]* の順に選択して、> リアル サーバを追加できます。各リアル サーバは、必ず仮想サーバと関連付けられなければなりません。

１台の仮想サーバにリアル サーバを 8 台まで関連付けることができます。リアル サーバのトポロジはエンドユーザにはトランスペアレントであり、ユーザは仮想サーバのシステムがあたかも仮想サーバの IP アドレスとポート番号をもった一台のサーバであるかのようにやりとりします。リアル サーバ間は高速 LAN で接続されているかもしれないし、または地理的に分散されている WAN によって接続されているかもしれません。FortiGate ユニットはリクエストをリアル サーバ間にスケジュールして、単一の IP アドレスを持っているように見える仮想サーバでパラレルなサービスを作ります。

図 23: 仮想サーバおよびリアル サーバの構成



仮想サーバの設定

仮想サーバの外部 IP アドレスを設定し、それを FortiGate インタフェースにバインドしてください。仮想サーバの外部 IP アドレスを FortiGate ユニットのインタフェースに関連付けると、ネットワーク インタフェースはデフォルトで関連付けられた IP アドレスへの ARP 要求に応答します。仮想サーバは RFC 1027 に定義された プロキシ ARP を使用し、これにより FortiGate ユニットは実際には異なるネットワークにインストールされているリアル サーバへの ARP リクエストに応答することができます。ARP 応答を無効にする方法については、『*FortiGate CLI リファレンス*』を参照してください。

仮想サーバ リストを表示するには、*[Firewall]*、*[Load Balance]*、*[Virtual Server]* の順に選択します。

新しい仮想サーバを作成するには、*[Firewall]*、*[Load Balance]*、*[Virtual Server]* の順に選択し、[Create New] を選択します。[OK] を選択して、新しい仮想サーバを保存します。

仮想サーバを作成する際の制限事項については、317 ページの「仮想 IP、負荷分散仮想サーバ、および負荷分散リアル サーバの制限」を参照してください。

[Virtual Service] ページ

このページには、作成済みの仮想サーバが一覧表示されます。このページでは、仮想サーバの編集、削除、または新規作成が可能です。

[Create New]	仮想サーバを追加するとき選択します。詳細については、340 ページの「仮想サーバの設定」を参照してください。
[Name]	仮想サーバの名前。
[Type]	この仮想サーバにより負荷分散されるプロトコル。
[Comments]	仮想サーバの説明。
[Virtual Server IP]	仮想サーバの IP アドレス。宛先ネットワーク上のアドレスにマップする、外部インタフェース上の IP アドレスです。
[Virtual server Port]	宛先ネットワーク上のポート番号にマップする、外部ポート番号。この宛先ポートとのセッションは、この仮想サーバにより負荷分散されます。
[Load Balance Method]	この仮想サーバの負荷分散方法。
[Health Check]	この仮想サーバに選択されるヘルス チェック モニタ。詳細については、343 ページの「[Health Check]」を参照してください。

[Persistence] この仮想サーバに適用されるパーシスタンスの種類。

[Delete] リストから仮想サーバを削除します。*[Delete]* アイコンは、仮想サーバがリアル サーバに関連付けられていないときのみ表示されます。

[Edit] 仮想サーバを編集し、仮想サーバ名などの仮想サーバのオプションを変更します。

[New Virtual Server] ページ

このページで、仮想サーバを設定できます。

[Name] 仮想サーバの名前を入力します。この名前は、FortiGate ユニットのホスト名ではありません。

[Type] この仮想サーバにより負荷分散されるプロトコルを選択します。*[IP]*、*[TCP]*、または *[UDP]* などの一般的なプロトコルを選択する場合は、仮想サーバによりすべての IP、TCP、または UDP セッションが負荷分散されます。*[HTTP]*、*[HTTPS]*、または *[SSL]* などの特定のプロトコルを選択する場合は、*[Persistence]* および *[HTTP Multiplexing]* など、他のサーバ負荷分散機能を適用できます。

- *[HTTP]* を選択すると、*[Virtual Server Port]* の設定と宛先ポート番号が一致するHTTPセッションのみを負荷分散します。負荷分散されるセッションの宛先ポートと一致するようにバーチャル サーバのポートを変更します (通常は HTTP セッションはポート 80)。*[HTTP Multiplex]* を選択することもできます。また、*[Persistence]* を *[HTTP Cookie]* に設定し、cooki ベースのパーシスタンスを選択できます。高度な HTTP Coookie パーシスタンス オプションの詳細については、『*FortiGate CLI リファレンス*』の `config firewall VIP` コマンドの説明を参照してください。
- *[HTTPS]* を選択すると、*[Virtual Server Port]* の設定と宛先ポート番号が一致する HTTPS セッションのみを負荷分散します。負荷分散されるセッションの宛先ポートと一致するようにバーチャル サーバのポートを変更します (通常は HTTPS セッションはポート 443)。*[HTTP Multiplex]* を選択することもできます。また、*[Persistence]* を *[HTTP Cookie]* に設定し、cooki ベースのパーシスタンスを選択できます。*[Persistence]* を、*[SSL Session ID]* に設定することもできます。高度な HTTP Coookie パーシスタンス オプションおよび SSL オプションの詳細については、『*FortiGate CLI リファレンス*』の `config firewall VIP` コマンドの説明を参照してください。*HTTPS* は、SSL 高速化をサポートする FortiGate ユニットで利用できます。
- *[IP]* を選択すると、この仮想サーバを含んだファイアウォール ポリシーにより許可されるすべてのセッションを負荷分散します。
- *[SSL]* を選択すると、*[Virtual Server Port]* の設定と一致する宛先ポート番号をもった SSL セッションのみを負荷分散します。負荷分散されるセッションの宛先ポートと一致するようにバーチャル サーバのポートを変更します。高度な SSL オプションの詳細については、『*FortiGate CLI リファレンス*』の `config firewall VIP` コマンドの説明を参照してください。
- *[TCP]* を選択すると、*[Virtual Server Port]* の設定と宛先ポート番号をもった TCP セッションのみを負荷分散します。*[Virtual Server Port]* を変更し、負荷分散されるセッションの宛先ポートを一致させます。
- *[UDP]* を選択すると、*[Virtual Server Port]* の設定と宛先ポート番号をもった UDP セッションのみを負荷分散します。*[Virtual Server Port]* を変更し、負荷分散されるセッションの宛先ポートを一致させます。

[Interface] リストから仮想サーバ外部インタフェースを選択します。外部インタフェースは、送信元ネットワークに接続され、宛先ネットワークに転送されるパケットを受信します。

[Virtual Server IP] 仮想サーバの IP アドレス。宛先ネットワーク上のアドレスにマップする、外部インタフェース上の IP アドレスです。

[Virtual server Port] 宛先ネットワーク上のポート番号にマップする、外部ポート番号を入力します。この宛先ポートをもつセッションは、この仮想サーバにより負荷分散されます。

[Load Balance Method] 負荷分散の方法。以下の方法があります。

- *[Static]*。トラフィックの負荷をすべてのサーバに均等に分散し、追加サーバは必要ありません。この負荷分散方法は、同じ発信元アドレスからのすべてのセッションが必ず同じサーバに分散されるので、いくらかの一貫性を提供します。ただし、分散はステートレスなので、リアル サーバを追加または削除（あるいは起動または停止）して分散が変更されると一貫性は失われます。別個のリアル サーバは必要ありません。
- *[Round Robin]*。要求を次のサーバに転送し、応答時間または接続数にかかわらずすべてのサーバを同等に扱います。機能停止したサーバまたは応答なしのサーバへは転送しません。別個のサーバが必要です。
- *[Weighted]*。より大きい重み付けの値を持つサーバが、より大きいパーセンテージで接続されます。サーバを追加するときは、サーバの重み付けを設定します。
- *[First Alive]*。必ず要求を稼働中の最初のリアル サーバに転送します。この場合の「最初」とは、仮想サーバを構成する際のリアル サーバの順番を指します。たとえば、リアル サーバ A、B、C をこの順序で追加した場合、A が稼働していればトラフィックは必ず A に転送されます。A が停止している場合、トラフィックは B に、B が停止している場合は C に転送されます。A が再び起動すると、トラフィックは A に転送されます。リアル サーバは、それらが追加された順序で仮想サーバ構成に順位付けられ、最後に追加されたリアル サーバが最下位となります。順位を変更する場合は、順位に応じてリアル サーバを削除しもう一度追加する必要があります。
- *[Least RTT]*。ラウンド トリップ時間が最短のサーバに、要求を転送します。ラウンド トリップ時間は、Ping ヘルス チェック モニタにより決定され、Ping ヘルス チェック モニタを仮想サーバに加えない場合はデフォルトで 0（ゼロ）に設定されます。
- *[Least Session]*。現在の接続数が最も少ないサーバに、要求を転送します。この方法は、負荷分散されるサーバまたは他の機器が同等の性能をもった環境の場合に、最も効果的に機能します。

[Persistence]

パーシスタンスを設定し、ユーザが同じセッションの中で要求を送信するたびに同一サーバに接続されることを保証します。
パーシスタンスを設定すると、FortiGate ユニットは *[Load Balance Method]* の設定にしたがい、新しいセッションをリアル サーバに負荷分散します。セッションに HTTP クッキーか SSL セッション ID があるときは、FortiGate ユニットは同じ HTTP クッキーまたは SSL セッション ID をもったそれ以後のすべてのセッションを同じサーバに送ります。
[Type] を *[HTTP]*、*[HTTPS]*、または *[SSL]* に設定している場合に、パーシスタンスを設定できます。

- *[None]* を選択すると、パーシスタンスを使用しません。セッションは、*[Load Balance Method]* の設定のみに従い分散されます。*[Load Balance Method]* を *[Static]*（デフォルト）に設定すると、パーシスタンスと同等の動作になります。詳しくは、*[Load Balance Method]* の説明を参照してください。
- *[HTTP Cookie]* を選択すると、同じ HTTP セッション Cookie をともなう HTTP または HTTPS の全セッションは、同じリアル サーバに送信されます。*[HTTP Cookie]* は、*[Type]* を *[HTTP]* または *[HTTPS]* に設定しているとき使用できます。高度な HTTP Coookie パーシスタンス オプションの詳細については、『*FortiGate CLI リファレンス*』の `config firewall VIP` コマンドの説明を参照してください。
- *[SSL Session ID]* を選択すると、同じ SSL セッション ID をともなう全セッションは、同じリアル サーバに送信されます。*[SSL Session ID]* は、*[Type]* を *[HTTPS]* または *[SSL]* に設定しているとき使用できます。

注記：*[Static]* の負荷分散方法では、リアル サーバの台数が変わらない限り、パーシスタンスが有効です。

[HTTP Multiplexing]

FortiGate ユニットを使用して、FortiGate ユニットとリアル サーバ間の複数のクライアントからのコネクションを、ごく少数の接続に多重化するとき使用します。複数のコネクションを確立することによるサーバのオーバーヘッドを減らしてパフォーマンスを改善します。サーバは、HTTP/1.1 に準拠する必要があります。
このオプションは、*[Type]* を *[HTTP]* または *[HTTPS]* に設定している場合のみ表示されます。
注記：CLI から、その他の HTTP Multiplexing オプションを利用できます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

[Preserve Client IP] X-Forwarded-For HTTP ヘッダに、クライアントの IP アドレスを保存するとき選択します。これはリアル サーバでクライアントのオリジナルの IP アドレスをログメッセージに欲しいときに有用です。このオプションを選択しない場合は、ヘッダには FortiGate ユニットの IP アドレスが含まれます。
このオプションは、*[Type]* を *[HTTP]* または *[HTTPS]* に設定しているときのみ表示され、*[HTTP Multiplexing]* を選択しているときのみ利用できます。

[SSL Offloading] FortiGate ユニットを使用し SSL 機能を実行することでサーバへのクライアント SSL 接続を高速化するとき選択し、次に接続のどのセグメントで SSL オフロードを適用するかを選択します。

- *[Client <-> FortiGate]*
  ハードウェアで高速化された SSL を、クライアントと FortiGate ユニット間の部分のコネクションにのみに適用するとき選択します。FortiGate ユニットとサーバの間では、サーバはクリアテキストの通信をおこないます。これにより最もよいパフォーマンスになりますが、フェイルオーバー パスに SSL アクセラレータがないフェイルオーバー構成では使うことはできません。
- *[Client <-> FortiGate <-> Server]*
  ハードウェアで高速化された SSL を、クライアントと FortiGate ユニット間のセグメント、および FortiGate ユニットとサーバ間のセグメントの、両接続部分に適用するとき選択します。ユニットとサーバ間のセグメントでは、暗号化された通信を使用しますが、ハンドシェークは短縮形になります。これにより、パフォーマンスは他のオプションを下回りますが、SSL アクセラレーションのないコミュニケーションよりは改善されます。フェイルオーバー パスに SSL 高速化をもたないフェイルオーバー構成に使用できます。すでに SSL を使用するようにサーバを設定している場合は、サーバの設定を変更せずに SSL 高速化を有効にできます。

SSL 3.0 および TLS 1.0 がサポートされます。
[SSL Offloading] は、*[Type]* を *[HTTPS]* または *[SSL]* に設定している場合のみ、および SSL 高速化をサポートするハードウェアをもった FortiGate モデル上でのみ表示されます。
注記 :CLI から、その他の SSL Offloading オプションを利用できます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

[Certificate] *[SSL Offloading]* で使用する証明書を選択します。証明書の鍵のサイズは、必ず 1024 または 2048 ビットとなります。4096 ビットの鍵は、サポートされません。
このオプションは、*[Type]* を *[HTTPS]* または *[SSL]* に設定しているときのみ表示され、*[SSL Offloading]* を選択しているときのみ利用できます。

[Health Check] どのヘルスチェックモニタ設定を使用しサーバの接続状態を判断するかを選択します。
ヘルスチェックモニタの詳しい設定方法については、344 ページの「ヘルスチェックモニタの設定」を参照してください。

[Comments] この仮想サーバについてのコメントまたは注記。

リアル サーバの設定

リアル サーバを設定し、仮想サーバと関連付けます。

リアル サーバ リストを表示するには、*[Firewall]*、*[Load Balance]*、*[Real Server]* の順に選択します。

リアル サーバを作成する際の制限事項については、317 ページの「仮想 IP、負荷分散仮想サーバ、および負荷分散リアル サーバの制限」を参照してください。

[Real Server] ページ

このページには、作成済みのリアル サーバが一覧表示されます。このページでは、リアル サーバの編集、削除、または新規作成が可能です。

[Create New] リアル サーバを追加するとき選択します。詳細については、343 ページの「リアル サーバの設定」を参照してください。

[IP Address] 仮想サーバ名の横にある青色の矢印を選択することにより、その仮想サーバに関連付けられるリアル サーバの IP アドレスを表示します。

[Port] 外部ポート番号のマップ先となる、宛先ネットワークのポート番号。

[Weight]	リアル サーバの重み付けの値。重み付けの値が大きいほど、サーバが処理するコネクションのパーセンテージは大きくなります。
[Max Connections]	リアル サーバに転送されるアクティブなコネクション数の上限。リアル サーバのコネクションが最大数に達すると、コネクション数が指定された上限より下がるまで、以降のすべてのコネクション要求は FortiGate ユニットにより別のサーバに自動的に切り替えられます。
[Delete]	リストからリアル サーバを削除します。
[Edit]	リアル サーバを編集し、仮想サーバの任意のオプションを変更します。

[New Real Server] ページ

このページでは、リアル サーバを設定し仮想サーバに関連付けることができます。

[Virtual Server]	このリアル サーバを関連付ける仮想サーバを選択します。
[IP]	リアル サーバの IP アドレスを入力します。
[Port]	外部ポート番号のマップ先となる宛先ネットワークのポート番号を入力します。
[Weight]	リアル サーバの重み付けの値を入力します。重み付けの値が大きいほど、サーバが処理するコネクションのパーセンテージは大きくなります。1 ～ 255 の範囲を使用できます。このオプションは、関連付けられる仮想サーバの負荷分散方法が *[Weighted]* の場合のみ利用できます。
[Maximum Connections]	リアル サーバに転送されるアクティブなコネクション数の上限を入力します。1 ～ 99999 の範囲を使用できます。リアル サーバのコネクションが最大数に達すると、コネクション数が指定された上限より下がるまで、以降のすべてのコネクション要求は FortiGate ユニットにより別のサーバに自動的に切り替えられます。 [Maximum Connections] を 0（ゼロ）に設定すると、リアル サーバへのコネクション数は FortiGate ユニットにより制限されません。
[Mode]	リアル サーバのモードを選択します。

ヘルスチェックモニタの設定

ポーリングにより仮想サーバのコネクティビティのステータスを判断するとき、どのヘルス チェック モニタ設定を使用するかを指定できます。

ヘルス チェック モニタ設定では、TCP、HTTP、または ICMP PING を指定できます。ヘルス チェックは、間隔として示される秒数ごとに行われます。制限時間内に応答が受信されず、ヘルス チェックを再試行するように設定している場合は、ヘルス チェックを再度実行します。再試行を設定していない場合は、仮想サーバが応答不能の状態にあると判断され、その仮想サーバが再び応答可能になるまで、そのサーバへトラッフィクを送らないことで負荷分散を継続します。

ヘルスチェックモニタ設定を作成するには、[Firewall]、[Load Balance]、[Health Check Monitor] の順に選択し、[Create New] を選択します。

[Health Check Monitor] ページ

このページには、作成済みのヘルス チェック モニタが一覧表示されます。このページでは、ヘルス チェック モニタの編集、削除、または新規作成が可能です。

[Create New]	ヘルス チェック モニタ設定を追加するとき選択します。
[Name]	ヘルス チェック モニタ設定の名前。名前は、ヘルス チェック モニタの種類ごとにグループ化されます。
[Details]	ヘルス チェック モニタ設定の詳細。ヘルス チェック モニタの種類に応じて異なり、種類にかかわらず共通の設定となる [Interval]、[Timeout]、または [Retry] は含まれません。 このフィールドは、ヘルス チェック モニタの種類が PING の場合は空白です。
[Delete]	ヘルス チェック モニタ設定を削除するとき選択します。このオプションは、現在ヘルス チェック モニタ設定が仮想サーバ設定で使用されていない場合に表示されます。
[Edit]	ヘルス チェック モニタの設定を変更するとき選択します。

[Add New Health Check Monitor]

このページでは、ヘルス チェック モニタを設定できます。

[Name]	ヘルス チェック モニタ設定の名前を入力します。
[Type]	ヘルス チェックの実行に使用するプロトコルを選択します。 ・ TCP ・ HTTP ・ PING
[Port]	ヘルス チェックの実行に使用するポート番号を入力します。*[Port]* を 0 (ゼロ) に設定すると、リアル サーバで定義するポートがヘルス チェック モニタで使用されます。これにより、異なるリアル サーバに、共通のヘルス チェック モニタを使用できます。 このオプションは、*[Type]* を *[PING]* に設定したときは表示されません。
[Interval]	サーバごとのヘルス チェックの間隔を、秒数で入力します。
[URL]	HTTP ヘルスチェックモニタでは、FortiGate ユニットが get 要求を送信し HTTP サーバの状態を確認するとき使用する URL を追加します。この URL は、リアル HTTP サーバの実際の URL と一致する必要があります。URL は、オプションです。 通常は、URL には IP アドレスまたはドメイン名は含まれません。代わりに、/ から始まり、リアル サーバ上にある実際の Web ページのアドレスが続きます。たとえば、リアル サーバの IP アドレスが 1010.10.1 の場合は、/test_page.htm という *URL* により、FortiGate ユニットは HTTP の get 要求を http://10.10.10.1/test_page.htm に送信します。 このオプションは、*[Type]* を *[HTTP]* に設定した場合のみ表示されます。
[Matched Content]	HTTP ヘルス チェック モニタでは、*[URL]* オプションの設定内容に基づいて FortiGate ユニットから送信される get 要求に対して、リアル HTTP サーバから応答が返信されますが、その応答に含まれるフレーズを加えておきます。その *[URL]* から Web ページが返信される場合は、*[Matched Content]* はその Web ページに記載されるテキストの一部と完全に一致する必要があります。*[URL]* および *[Matched Content]* オプションを使用することにより、get 要求に対して想定される Web ページの内容とともに応答が返信されれば、その HTTP サーバが実際に正常に機能していると判断できます。[Matched Content] は、URL を追加する場合のみ必要となります。 たとえば、[URL] オプションにより定義されるリアル HTTP サーバ ページに server test page というフレーズが記載されていれば、*[Matched Content]* に server test page を設定できます。URL get 要求に対する応答として、FortiGate ユニットがその Web ページを受信すると、システムはその Web ページのコンテンツから *[Matched Content]* のフレーズを検索します。 このオプションは、*[Type]* を *[HTTP]* に設定した場合のみ表示されます。
[Timeout]	サーバ ヘルス チェック後に、ヘルス チェックの失敗を表示するために必要な経過時間を、秒単位で入力します。
[Retry]	ヘルス チェック失敗のとき、サーバがアクセス不能状態にあると判断されるまで、ヘルス チェックを再試行する回数 (再試行する場合) を入力します。

サーバの監視

仮想サーバおよびリアル サーバの状態を個別に監視し、リアル サーバの機能を起動または停止できます。

[Monitor] ページ

このページには、現在 FortiGate ユニットにより監視されている個別のサーバおよびリアル サーバが一覧表示されます。

[Virtual Server]	既存の仮想サーバの IP アドレス。
[Real Servers]	既存のリアル サーバの IP アドレス。
[Health Status]	各リアル サーバの状態を、ヘルス チェックの結果に基づいて表示します。緑の矢印は、サーバが稼働していることを示します。赤の矢印は、サーバが機能停止していることを示します。
[Monitor Events]	各リアル サーバの稼働時間および停止時間を表示します。
[Active Sessions]	各リアル サーバのアクティブなセッションを表示します。
[RTT] (ms)	各リアル サーバのラウンド トリップ時間を表示します。デフォルトでは、[RTT] は <1 です。この値は、リアル サーバで PING 監視が有効な場合のみ変更されます。

[Bytes Processed]	各リアル サーバにより処理されたトラフィックを表示します。
[Graceful Stop/Start]	リアル サーバを起動または停止するとき選択します。サーバを停止すると、FortiGate ユニットは新しいセッションを許可せず、アクティブなセッションが終了するのを待ちます。

負荷分散の例

この項には、以下の例が含まれています。

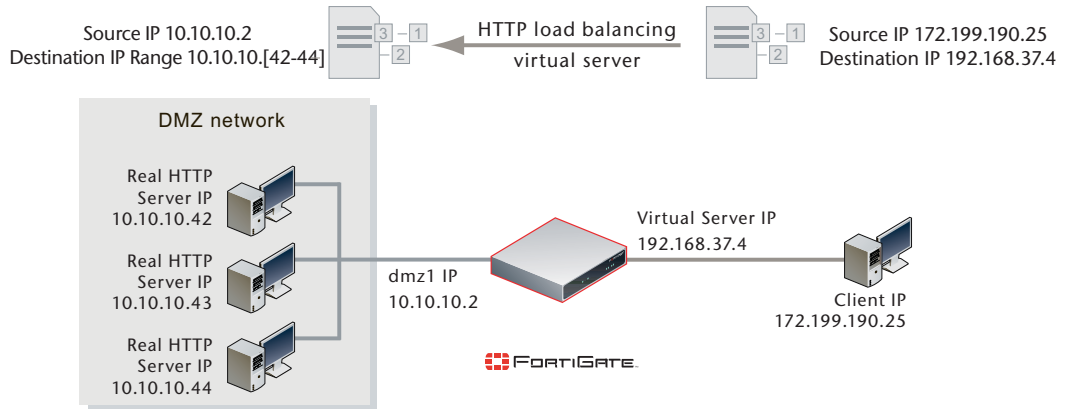
- 3 台のリアル Web サーバによる 1 台の仮想 Web サーバの設定
- サーバ負荷分散ポート フォワーディング仮想 IP の追加
- 重み付けによる負荷分散の設定
- HTTP および HTTPS のパーシスタンスの設定

3 台のリアル Web サーバによる 1 台の仮想 Web サーバの設定

この例では、インターネット上にある IP アドレス 192.168.37.4 の仮想 Web サーバを、FortiGate ユニットの dmz1 インタフェースに接続されている 3 台のリアル Web サーバにマップします。リアル サーバの IP アドレスは、それぞれ 10.10.123.42、10.10.123.43、および 10.10.123.44 です。仮想サーバの負荷分散方法には、*[First Alive]* を設定します。この構成には、HTTP ヘルス チェック モニタが含まれており、FortiGate ユニットではこのヘルス チェック モニタに含まれている URL を get 要求のために使用し、リアル サーバの状態を監視します。

インターネットから IP アドレス 192.168.37.4 の仮想 Web サーバへの接続は、FortiGate ユニットによって変換され、リアル サーバに負荷分散されます。[First alive] の負荷分散方法により、すべてのセッションは最初のリアル サーバに転送されます。インターネット上のコンピュータからはこの変換および負荷分散は意識されず、FortiGate ユニット背後のリアル サーバ 3 台の代わりに、IP アドレス 192.168.37.4 を持つ 1 台の仮想サーバが認識されます

図 24: 仮想サーバの設定例



HTTP ヘルス チェック モニタを追加するには

この例では、HTTP ヘルスチェックモニタに *[URL]* として /index.html を、また *[Matched Phrase]* として Fortinet products を設定します。

1 *[Firewall]*、*[Load Balance]*、*[Health Check Monitor]* の順に選択します。

2 *[Create New]* を選択します。

3 HTTP ヘルス チェック モニタを追加し、このヘルス チェック モニタにより、http://<real_server_IP_address>/index.html に get 要求を送信し、応答される Web ページから Fortinet products というフレーズを検索します。

[Name]	HTTP_health_chk_1
[Type]	HTTP
[Port]	80
[URL]	/index.html
[Matched Content]	Fortinet products
[Interval]	10 秒
[Timeout]	2 秒
[Retry]	3

4 *[OK]* を選択します。

HTTP 仮想サーバを追加するには

1 *[Firewall]*、*[Load Balance]*、*[Virtual Server]* の順に選択します。

2 *[Create New]* を選択します。

3 インターネット上のユーザが内部ネットワーク上のリアル　サーバに接続できるようにするための、HTTP 仮想サーバを追加します。この例では、FortiGate の wan1 インタフェースがインターネットに接続されます。

[Name]	Load_Bal_VS1
[Type]	HTTP
[Interface]	wan1
[Virtual Server IP]	192.168.37.4 Web サーバのパブリック IP アドレス。 仮想サーバの IP アドレスは、通常は Web サーバの ISP から取得されるスタティック IP アドレスです。このアドレスは、別のホストによって使用されない固有の IP アドレスでなければならず、仮想 IP が使用する外部インタフェースのIPアドレスと同一のアドレスにすることはできません。しかし、仮想 IP アドレスは選択されたインタフェースへとルーティングされる必要があります。仮想 IP アドレスと外部 IP アドレスは、別々のサブネット上に設定できます。仮想 IP を追加すると、外部インタフェースは仮想 IP アドレスへの ARP 要求に応答します。
[Virtual server Port]	80
[Load Balance Method]	First Alive
[Persistence]	HTTP cookie
[HTTP Multiplexing]	選択します。 FortiGate ユニットは、FortiGate ユニットおよびリアル HTTP サーバ間での複数のクライアント接続を、少数の接続に多重化します。これにより、複数接続の確立にともなうサーバ オーバーヘッドを削減することで、パフォーマンスを強化できます。
[Preserve Client IP]	選択します。 FortiGate ユニットは、クライアントの IP アドレスを `X-Forwarded-For` HTTP ヘッダに保存します。
[Health Check]	HTTP_health_chk_1 ヘルス チェック モニタを、*[Selected]* リストに移動します。

4 *[OK]* を選択します。

リアル サーバを追加し仮想サーバに関連付けるには

1 *[Firewall]*、*[Load Balance]*、*[Real Server]* の順に選択します。

2 *[Create New]* を選択します。

3 Configure three real servers that include the virtual server Load_Bal_VS1. これらのリアル サーバは、それぞれ内部ネットワーク上のリアル サーバの IP アドレスをともなう必要があります。

最初のリアル　サーバを設定します。

[Virtual Server]	Load_Bal_VS1
[IP]	10.10.10.42
[Port]	80
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0 *[Maximum Connections]* を 0（ゼロ）に設定すると、リアル サーバへの接続数は FortiGate ユニットにより制限されません。仮想サーバに設定されている負荷分散方法は *[First Alive]* なので、各リアル サーバへの接続数を制限し、各サーバで受信されるトラフィック量を制限する必要がある場合が考えられます。この例では、*[Maximum Connections]* は最初に 0（ゼロ）に設定されますが、リアル サーバで膨大な量のトラフィックが受信される場合は、後から設定値を調整できます。

2 番目のリアル サーバを設定します。

[Virtual Server]	Load_Bal_VS1
[IP]	10.10.10.43
[Port]	80
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0 *[Maximum Connections]* を 0（ゼロ）に設定すると、リアル サーバへの接続数は FortiGate ユニットにより制限されません。仮想サーバに設定されている負荷分散方法は *[First Alive]* なので、各リアル サーバの接続数を制限し、各サーバで受信されるトラフィック量を制限する必要がある場合が考えられます。In this example, the*[Maximum Connections]* は最初に 0（ゼロ）に設定されますが、リアル サーバで膨大な量のトラフィックが受信される場合は、後から設定値を調整できます。

3 番目のリアル サーバを設定します。

[Virtual Server]	Load_Bal_VS1
[IP]	10.10.10.44
[Port]	80
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0 *[Maximum Connections]* を 0（ゼロ）に設定すると、リアル サーバへの接続数は FortiGate ユニットにより制限されません。仮想サーバに設定されている負荷分散方法は *[First Alive]* なので、各リアル サーバの接続数を制限し、各サーバで受信されるトラフィック量を制限する必要がある場合が考えられます。この例では、*[Maximum Connections]* は最初に 0（ゼロ）に設定されますが、リアル サーバで膨大な量のトラフィックが受信される場合は、後から設定値を調整できます。

仮想サーバをファイアウォール ポリシーに追加するには

wan1 から dmz1 への、仮想サーバを使用するファイアウォール ポリシーを追加することにより、インターネット上のユーザが Web サーバの IP アドレスに接続しようとしたとき、パケットが FortiGate ユニットの wan1 インタフェースから dmz1 インタフェースへと通過するようにします。仮想 IP は、これらのパケットの宛先アドレスを、仮想サーバの IP アドレスからリアル サーバの IP アドレスに変換します。

1 *[Firewall]*、*[Policy]* の順に選択します。

2 *[Create New]* を選択します。

3 ファイアウォール ポリシーを次のように設定します。

[Source Interface/Zone]	wan1
[Source Address]	All（またはより具体的なアドレス）

[Destination Interface/Zone]	dmz1
[Destination Address]	Load_Bal_VS1
[Schedule]	always
[Service]	HTTP
[Action]	ACCEPT
[NAT]	選択します。
[Log Allowed Traffic]	仮想サーバのトラフィックをログ記録するとき選択します。

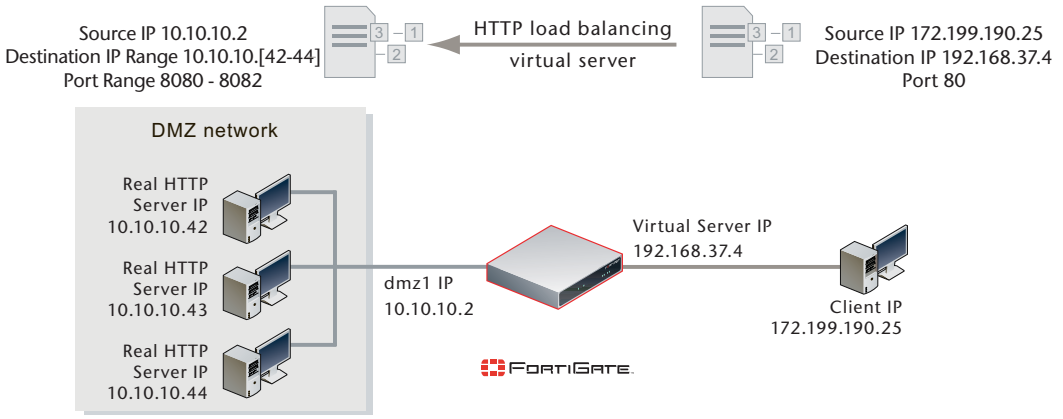
4 必要に応じて、他のファイアウォール オプションを設定します。

5 *[OK]* を選択します。

サーバ負荷分散ポート フォワーディング仮想 IP の追加

この例は、346 ページの「3 台のリアル Web サーバによる 1 台の仮想 Web サーバの設定」に示される例と同じです。ただし、リアル サーバごとに異なるポート番号で HTTP 接続を許可する点が異なります。最初のリアル サーバはポート 8080、2 番目はポート 8081、3 番目はポート 8082 で、それぞれ接続を許可します。

図 25: サーバ負荷分散仮想 IP ポート フォワーディング



この設定の手順は、リアル サーバの設定を除き、346 ページの「3 台のリアル Web サーバによる 1 台の仮想 Web サーバの設定」に示される手順とすべて同じです。

リアル サーバを追加し仮想サーバに関連付けるには

以下の手順を使用し、ポート 8080、8081、8082 上の 3 台のリアル サーバに HTTP パケットをポート フォワーディングするように、FortiGate ユニットを設定します。

1 *[Firewall]*、*[Load Balance]*、*[Real Server]* の順に選択します。

2 *[Create New]* を選択します。

3 仮想サーバ Load_Bal_VS1 をともなう、3 台のリアル サーバを設定します。これらのリアル サーバは、それぞれ内部ネットワーク上のリアル サーバの IP アドレス、および異なるポート番号をともなう必要があります。

最初のリアル サーバを設定します。

[Virtual Server]	Load_Bal_VS1
[IP]	10.10.10.42
[Port]	8080
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0

2 番目のリアル サーバを設定します。

[Virtual Server]	Load_Bal_VS1
[IP]	10.10.10.43
[Port]	8081
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0

3 番目のリアル サーバを設定します。

[Virtual Server]	Load_Bal_VS1
[IP]	10.10.10.44
[Port]	8082
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0

重み付けによる負荷分散の設定

この例では、ファイアウォールの負荷分散を使用し、すべてのトラフィックを 3 台のリアル サーバに負荷分散する方法を示しています。ここでは、インターネットは `port2` に接続され、仮想サーバの仮想 IP アドレスは 192.168.20.20 です。負荷分散方法は、`weighted` を使用します。リアル サーバの IP アドレスは、10.10.10.1、10.10.10.2、および 10.10.10.3 です。リアル サーバの重み付けの値は、1、2、および 3 です。

この設定には、ヘルス チェック モニタは含まれません。

HTTP 仮想サーバを追加するには

1 *[Firewall]*、*[Load Balance]*、*[Virtual Server]* の順に選択します。

2 *[Create New]* を選択します。

3 インターネット上のユーザが内部ネットワーク上のリアル　サーバに接続できるようにするための、IP 仮想サーバを追加します。この例では、FortiGate の port2 インタフェースがインターネットに接続されます。

[Name]	All_Load_Balance
[Type]	IP
[Interface]	port2
[Virtual Server IP]	192.168.20.20
[Load Balance Method]	Weighted

その他すべての仮想サーバの設定は、必要ないかまたは変更できません。

4 *[OK]* を選択します。

リアル サーバを追加し仮想サーバに関連付けるには

1 *[Firewall]*、*[Load Balance]*、*[Real Server]* の順に選択します。

2 *[Create New]* を選択します。

3 仮想サーバ All_Load _Balance をともなう、3 台のリアル サーバを設定します。*[Load Balancing Method]* には *[Weighted]* が使用されるので、リアル サーバごとに重み付けの値が含まれます。より大きな重み付けのサーバでは、転送される接続の割合が大きくなります。

最初のリアル サーバを設定します。

[Virtual Server]	All_Load_Balance
[IP]	10.10.10.1
[Port]	仮想サーバは IP サーバなので設定できません。
[Weight]	1
[Maximum Connections]	0 *[Maximum Connections]* を 0（ゼロ）に設定すると、リアル サーバへの接続数は FortiGate ユニットにより制限されません。仮想サーバに設定されている負荷分散方法は *[First Alive]* なので、各リアル サーバの接続数を制限し、各サーバで受信されるトラフィック量を制限する必要がある場合が考えられます。この例では、*[Maximum Connections]* は最初に 0（ゼロ）に設定されますが、リアル サーバで膨大な量のトラフィックが受信される場合は、後から設定値を調整できます。

2 番目のリアル サーバを設定します。

[Virtual Server]	All_Load_Balance
[IP]	10.10.10.2
[Port]	仮想サーバは IP サーバなので設定できません。
[Weight]	2
[Maximum Connections]	0 *[Maximum Connections]* を 0（ゼロ）に設定すると、リアル サーバへの接続数は FortiGate ユニットにより制限されません。仮想サーバに設定されている負荷分散方法は *[First Alive]* なので、各リアル サーバの接続数を制限し、各サーバで受信されるトラフィック量を制限する必要がある場合が考えられます。この例では、*[Maximum Connections]* は最初に 0（ゼロ）に設定されますが、リアル サーバで膨大な量のトラフィックが受信される場合は、後から設定値を調整できます。

3 番目のリアル サーバを設定します。

[Virtual Server]	All_Load_Balance
[IP]	10.10.10.3
[Port]	仮想サーバは IP サーバなので設定できません。
[Weight]	3
[Maximum Connections]	0 *[Maximum Connections]* を 0（ゼロ）に設定すると、リアル サーバへの接続数は FortiGate ユニットにより制限されません。仮想サーバに設定されている負荷分散方法は *[First Alive]* なので、各リアル サーバの接続数を制限し、各サーバで受信されるトラフィック量を制限する必要がある場合が考えられます。この例では、*[Maximum Connections]* は最初に 0（ゼロ）に設定されますが、リアル サーバで膨大な量のトラフィックが受信される場合は、後から設定値を調整できます。

仮想サーバをファイアウォール ポリシーに追加するには

port2 から port1 への、仮想サーバを使用するファイアウォール ポリシーを追加することにより、インターネット上のユーザが Web サーバの IP アドレスに接続しようとしたとき、パケットが FortiGate ユニットの port1 インタフェースから port2 インタフェースへと通過するようにします。仮想 IP は、これらのパケットの宛先アドレスを、仮想サーバの IP アドレスからリアル サーバの IP アドレスに変換します。

1 *[Firewall]*、*[Policy]* の順に選択します。

2 *[Create New]* を選択します。

3 ファイアウォール ポリシーを次のように設定します。

[Source Interface/Zone]	port2
[Source Address]	All（またはより具体的なアドレス）
[Destination Interface/Zone]	port1
[Destination Address]	All_Load_Balance
[Schedule]	always
[Service]	ANY
[Action]	ACCEPT
[NAT]	選択します。

4 必要に応じて、他のファイアウォール オプションを設定します。

5 *[OK]* を選択します。

CLI による設定

負荷分散は、CLI から `config firewall vip` コマンドを使用し、`type` を `server-load-balance` に指定することにより設定します。デフォルトの重み付けの値は 1 で、最初のリアル サーバでは変更する必要はありません。

以下のコマンドを使用し、仮想サーバおよび重み付けをともなう 3 台のリアル サーバを追加します。

```
config firewall vip
  edit All_Load_Balance
    set type server-load-balance
    set server-type ip
    set extintf port2
    set extip 192.168.20.20
    set ldb-method weighted
      config realservers
        edit 1
          set ip 10.10.10.1
        next
        edit 2
          set ip 10.10.10.2
          set weight 2
        next
        edit 3
          set ip 10.10.10.3
          set weight 3
        end
  end
```

HTTP および HTTPS のパーシスタンスの設定

この例では、ポート 80 を使用し HTTP トラフィックを負荷分散する *Http_Load_Balance* という名前の仮想サーバ、およびポート 443 を使用し HTTPS トラフィックを負荷分散する *Https_Load_Balance* という名前の 2 番目の仮想サーバを追加する方法を示しています。インターネットは port2 に接続され、仮想サーバの仮想 IP アドレスは 192.168.20.20 です。両方のサーバ負荷分散仮想 IP とも、セッションを、10.10.10.2、10.10.10.2、および 10.10.10.3 の IP アドレスを持つ同じ 3 台のリアル サーバに負荷分散します。リアル サーバは、HTTP および HTTPS サービスを提供します。

両方の仮想サーバでは、[Persistence] を *[HTTP Cookie]* に設定することで HTTP cookie パーシスタンスを有効にします。

HTTP および HTTPS 仮想サーバを追加するには

1 *[Firewall]*、*[Load Balance]*、*[Virtual Server]* の順に選択します。

2 HTTP Cookie パーシスタンスをともなう HTTP 仮想サーバを追加します。

[Name]	HTTP_Load_Balance
[Type]	HTTP
[Interface]	port2
[Virtual Server IP]	192.168.20.20
[Virtual server Port]	8080 この例では、仮想サーバは HTTP セッションにポート 80 ではなくポート 8080 を使用します。
[Load Balance Method]	Static
[Persistence]	HTTP cookie

3 *[OK]* を選択します。

4 *[Create New]* を選択します。

5 HTTP Cookie persistence をともなう HTTPS 仮想サーバを追加します。

[Name]	HTTPS_Load_Balance
[Type]	HTTPS
[Interface]	port2
[Virtual Server IP]	192.168.20.20
[Virtual Server Port]	443
[Load Balance Method]	Static
[Persistence]	HTTP cookie

6 *[OK]* を選択します。

リアル サーバを追加し仮想サーバに関連付けるには

1 *[Firewall]*、*[Load Balance]*、*[Real Server]* の順に選択します。

2 *[Create New]* を選択します。

3 仮想サーバ HTTP_Load_Balance をともなう、3 台の HTTP リアル サーバを設定します。

最初の HTTP リアル サーバを設定します。

[Virtual Server]	HTTP_Load_Balance
[IP]	10.10.10.1
[Port]	80
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0

2 番目の HTTP リアル サーバを設定します。

[Virtual Server]	HTTP_Load_Balance
[IP]	10.10.10.2
[Port]	80
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0

3 番目の HTTP リアル サーバを設定します。

[Virtual Server]	HTTP_Load_Balance
[IP]	10.10.10.3
[Port]	80
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0

4 仮想サーバ HTTPS_Load_Balance をともなう、3 台の HTTPS リアル サーバを設定します。

最初の HTTPS リアル サーバを設定します。

[Virtual Server]	HTTPS_Load_Balance
[IP]	10.10.10.1
[Port]	443
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0

2 番目の HTTPS リアル サーバを設定します。

[Virtual Server]	HTTPS_Load_Balance
[IP]	10.10.10.2
[Port]	443
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0

3 番目の HTTPS リアル サーバを設定します。

[Virtual Server]	HTTPS_Load_Balance
[IP]	10.10.10.3
[Port]	443
[Weight]	仮想サーバには重み付けによる負荷分散が含まれないので、設定できません。
[Maximum Connections]	0

仮想サーバをファイアウォール ポリシーに追加するには

port2 から port1 への、仮想サーバを使用するファイアウォール ポリシーを追加することにより、インターネット上のユーザが Web サーバの IP アドレスに接続しようとしたとき、パケットが FortiGate ユニットの port2 インタフェースから port1 インタフェースへと通過するようにします。仮想 IP は、これらのパケットの宛先アドレスを、仮想サーバの IP アドレスからリアル サーバの IP アドレスに変換します。

1 *[Firewall]*、*[Policy]* の順に選択します。

2 *[Create New]* を選択します。

3 HTTP ファイアウォール ポリシーを次のように設定します。

[Source Interface/Zone]	port2
[Source Address]	all
[Destination Interface/Zone]	port1
[Destination Address]	HTTP_Load_Balance
[Schedule]	always
[Service]	HTTP

[Action]	ACCEPT
[NAT]	選択します。

4 必要に応じて、他のファイアウォール オプションを設定します。
5 *[OK]* を選択します。
6 *[Create New]* を選択します。
7 HTTPS ファイアウォール ポリシーを次のように設定します。

[Source Interface/Zone]	port2
[Source Address]	all
[Destination Interface/Zone]	port1
[Destination Address]	HTTPS_Load_Balance
[Schedule]	always
[Service]	HTTPS
[Action]	ACCEPT
[NAT]	選択します。

8 必要に応じて、他のファイアウォール オプションを設定します。
9 *[OK]* を選択します。

CLI による設定： 特定ドメインの persistence を追加

負荷分散は、CLI から `config firewall vip` コマンドを使用し、`type` を `server-load-balance` に指定することにより設定します。

CLI による設定では、両方の仮想サーバの `http-cookie-domain` を `.example.org` に設定します。これは、`example.org` ドメインに HTTP cookie persistence が必要なためです。

まず、HTTP 仮想 IP を以下のように設定します。

```
config firewall vip
  edit HTTP_Load_Balance
    set type server-load-balance
    set server-type http
    set extport 8080
    set extintf port2
    set extip 192.168.20.20
    set persistence http-cookie
    set http-cookie-domain .example.org
      config realservers
        edit 1
          set ip 10.10.10.1
        next
        edit 2
          set ip 10.10.10.2
        next
        edit 3
          set ip 10.10.10.3
        end
  end
```

次に、HTTPS 仮想 IP を以下のように設定します。この設定では、`extport` を `443` に設定する必要はありません。これは、`server-type` を `https` に設定すると、`extport` は自動的に `443` に設定されるからです。

```
config firewall vip
  edit HTTPS_Load_Balance
    set type server-load-balance
```

```
    set server-type https
    set extport 443
    set extintf port2
    set extip 192.168.20.20
    set persistence http-cookie
    set http-cookie-domain .example.org
      config realservers
        edit 1
          set ip 10.10.10.1
        next
        edit 2
          set ip 10.10.10.2
        next
        edit 3
          set ip 10.10.10.3
        end
end
```

統合脅威管理 (UTM)

この項では、[UTM] メニューの基本的な設定について説明します。アンチウイルスの設定方法など、[UTM] メニューの詳しい設定方法については、『*FortiOS ハンドブック*』の「UTM」の章を参照してください。

この項には以下のトピックが含まれています。

統合脅威管理の概要

[UTM] メニューには、アンチウイルスまたは DoS センサーなどの、各種セキュリティ機能の他、ファイアウォール ポリシーに適用されるプロファイルも含まれています。プロファイルに含まれる特定の情報は、ポリシーに基づきトラフィックがどのように検証され、検証に基づいてどのようなアクションが実行されるかを定義します。

[UTM] メニューには、以下の 7 種類の機能が含まれており、これらの機能の一部は、ファイアウォール ポリシーに適用可能なプロファイルを含んでいます。

- アンチウイルス – ウイルスをフィルタリングおよびスキャンするための設定、および隔離設定が含まれています。また、ネットワークの要件に適するアンチウイルス データベースを選択する設定も含まれています。この機能では、プロファイルを利用できます。
- 不正侵入防御 – カスタム シグネチャの作成、IPS センサーおよび DoS センサーの設定などが含まれています。さらに、定義済みシグネチャの詳細情報、およびデフォルトのプロトコル デコーダも表示できます。
- Web フィルタ – Web コンテンツのフィルタリング、および FortiGuard Web フィルタとその FortiGuard Web フィルタリングの上書きを有効にする設定が含まれています。さらに、URL フィルタ、ローカル カテゴリ、ローカル評価の設定が含まれています。この機能では、プロファイルを利用できます。
- 電子メール フィルタリング – アンチスパム機能としても知られる機能ですが、禁止単語、IP アドレス、メール アドレスを、フィルタリングおよびスキャンするための設定が含まれています。この機能では、プロファイルを利用できます。
- 情報漏洩防止 (DLP) – DLP センサーの作成、コンパウンド ルール、および個別ルールの設定が含まれています。プロファイルの代わりに、DLP センサーをファイアウォール ポリシーに適用します。
- アプリケーション制御 – アプリケーション制御ブラック / ホワイト リスト作成の設定が含まれています。さらに [Application List] ページでは、アプリケーション一覧からアプリケーションに関する情報を表示できます。
- VoIP – ファイアウォール ポリシーに適用可能なプロファイルを作成するための設定が含まれています。このプロファイルには、SIP および SCCP トラフィック、およびトラフィック違反のロギングを有効にする設定も含まれています。

アンチウイルス

ここでは、[Antivirus] メニューを使用して設定する、アンチウイルス オプションについて説明します。プロファイルを設定することにより、HTTP、FTP、IMAP、POP3、SMTP、IM、NNTP セッションのファイアウォール ポリシーに、アンチウイルス プロファイルを適用できます。FortiGateユニットがSSLコンテンツ スキャンおよびインスペクションをサポートする場合は、HTTPS、IMAPS、POP3S、SMTPS の各セッションのアンチウイルス プロテクションを設定できます。詳しくは、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとにアンチウイルス オプションを個別に設定します。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

このトピックには、以下の項目が含まれています。

プロファイル

[Profile] ページでは、ファイアウォール ポリシーに適用するためのアンチウイルス プロファイルを設定できます。プロファイルに含まれる特定の情報は、ポリシーに基づきトラフィックがどのように検証され、検証に基づいてどのようなアクションが実行されるかを定義します。

アンチウイルス スキャンのさまざまな要件に応じて、複数のアンチウイルス プロファイルを作成できます。たとえば、POP3 のウイルス スキャンのみを指定するアンチウイルス プロファイルを作成し、そのプロファイルを送信ファイアウォール ポリシーに適用できます。

アンチウイルス プロファイルを設定するには、*[UTM]*、*[Antivirus]*、*[Profile]* の順に選択します。

[Profile] ページ

このページには、作成済みのアンチウイルス プロファイルが一覧表示されます。このページでは、アンチウイルス プロファイルを編集、削除、または新規作成できます。

[Create New]	[Create New] を選択すると、[New Antivirus Profile] ページの画面に自動的に移動します。
編集アイコン	アンチウイルス プロファイルの設定を編集するとき選択します。
削除アイコン	アンチウイルス プロファイルを削除するとき選択します。
[名前]	アンチウイルス プロファイルの名前。
[コメント]	アンチウイルス プロファイルについての説明。

[New Antivirus Profile] ページ

このページでは、新しいアンチウイルス プロファイルを設定できます。また、ウイルス送信者を [Banned User List] に加えるための隔離も設定できます。既存のアンチウイルス プロファイルを編集する場合は、画面が [Edit Antivirus Profile] ページに移動します。このページには、[New Antivirus Profile] ページと同じ設定が含まれています。

[名前]	このプロファイルの名前を入力します。既存のアンチウイルス プロファイルを編集しプロファイル名を変更する場合は、このフィールドに新しい名前を入力します。変更を保存するには、必ず [OK] を選択します。
[コメント]	プロファイルの説明を入力します。この項目はオプションです。既存のアンチウイルス プロファイルを編集し説明内容を変更する場合は、このフィールドに新たな説明を入力します。変更を保存するには、必ず [OK] を選択します。

[Virus Scan]	以下から任意のプロトコルを選択し、これらのプロトコルを使用するとき FortiGate ユニットによりウイルス スキャンが行われるようにします。 ・ HTTP ・ FTP ・ IMAP ・ POP3 ・ SMTP ・ NNTP ・ IM これらのイベントのログ記録が必要な場合は、[Logging] チェック ボックスをオンにします。
[File Filter]	以下から任意のプロトコルを選択し、これらのプロトコルを使用するとき FortiGate ユニットによりファイル フィルタ リストに基づくウイルス スキャンが行われるようにします。 ・ HTTP ・ FTP ・ IMAP ・ POP3 ・ SMTP ・ NNTP ・ IM [Options] ドロップダウン リストから、フィルタを選択します。
[Quarantine Virus Sender (to Banned Users List)]	送信者の隔離を有効にして設定するとき選択します。ウイルスの送信者は、[Banned Users List] (禁止ユーザ リスト) に加えられます。
[Method]	[Quarantine Virus Sender (to Banned Users List)] を選択したとき表示されます。 *[Source IP address]* を選択すると、攻撃者の IP アドレスから送信されるすべてのトラフィックをブロックします。さらに攻撃者の IP アドレスが、[Banned User List] に追加されます。標的のアドレスは、影響を受けません。 *[Virus 痴 Incoming Interface]* を選択すると、攻撃を受けた FortiGate インタフェースに接続しようとするトラフィックを、すべてブロックします。このインタフェースは、[Banned User List] に追加されます。
[Expires]	[Quarantine Virus Sender (to Banned Users List)] を選択したとき表示されます。 ウイルスを無期限に禁止するか、または指定された日数、時間数、または分数に限り禁止するかを選択できます。

ファイル フィルタ

[Filter] メニューを使用し、特定のファイル パターンおよびファイルの種類をブロックするための、フィルタ オプションを設定できます。ファイルは、[有効] に設定されているファイル パターン、次にファイルの種類と、上から順に比較されます。ファイルが、指定されているどのパターンにも一致しない場合、そのファイルはアンチウイルス スキャン (有効な場合) に転送されます。事実上、ファイルは、明示的にブロックされない限り許可されます。さらに FortiGate ユニットによって、ウイルス ログにメッセージが書き込まれ、アラートの電子メール メッセージが送信されます (これらの実行が設定されている場合)。

ファイルが、 設定されているファイル パターンまたはファイル タイプに一致する場合は、 FortiGate ユニットによって、 そのファイルに対し以下のいずれかのアクションが実行されます。

- Allow (許可)。ファイルの通過が許可されます。
- Block （ ブロック ）。ファイルはブロックされ、置換メッセージがユーザに送信されます。ファイル フィルタとウイルス スキャンの双方が有効な場合、[有効] に設定されているファイル フィルタと一致するファイルが、FortiGate ユニットによってブロックされますが、そのファイルに対してウイルス スキャンは実行されません。

許可のアクションを使用する場合、この動作を逆にして、明示的に許可されないファイルをすべてブロックするように処理できます。許可の属性によって通過が許される、すべてのファイル パターンまたは種類を入力します。リストの末尾に、ブロックのアクションをともなう「すべて包含」のワイルドカード (*.*) を追加します。許可されたファイルには引き続きアンチウイルス スキャン (有効な場合) が行われる一方、どの許可パターンにも一致しないファイルは、末尾に追加されたワイルドカードによってブロックされます。通常の運用では、プロファイルでファイル フィルタを無効に設定し、特定の脅威が発生した場合にその脅威をブロックするために、一時的にファイル フィルタを有効に設定できます。

FortiGate ユニットには、ファイル パターンのリストがデフォルトであらかじめ設定されています。

- 実行可能ファイル (*.bat、*.com、および *.exe)
- 圧縮またはアーカイブ ファイル (*.gz、*.rar、*.tar、*.tgz、および *.zip)
- ダイナミック リンク ライブラリ (*.dll)
- HTML アプリケーション (*.hta)
- Microsoft Office ファイル (*.doc、*.ppt、*.xl?)
- Microsoft Works ファイル (*.wps)
- Visual Basic ファイル (*.vb?)
- スクリーン セーバー ファイル (*.scr)
- プログラム情報ファイル (*.pif)
- コントロール パネル ファイル (*.cpl)

FortiGate ユニットは、以下のファイルの種類を検出できます。

表 51: サポートされるファイルの種類

arj	activemime	aspack	base64	bat	binhex	bzip	bzip2
cab	class	cod	elf	exe	fsg	gzip	hlp
hta	html	jad	javascript	lzh	mime	msc	msoffice
petite	prc	rar	sis	tar	upx	uue	zip
unknown	ignored						

注記： unknown は、表に未掲載のあらゆるファイルの種類です。ignored は、FortiGate ユニットにより通常はスキャンされないトラフィックです。この種類には、主にストリーミングの音声およびビデオが含まれます。

以下の基準でファイルをブロックするように、FortiGate ファイル フィルタを設定します。

- ファイル パターン。名前、拡張子、または他の任意のパターンで、ファイルをブロックできます。ファイル パターンによりファイルをブロックする場合、有害と考えられるコンテンツを柔軟にブロックできます。

  ファイル パターンのエントリには、大文字、小文字の区別はありません。たとえば、ファイル パターン リストに `*.exe` を追加すると、末尾が大文字の `.EXE` で表記されるファイルもすべてブロックします。

  デフォルトのビルトイン パターン以外にも、ブロックするファイル パターンを指定できます。詳細については、359 ページの「ファイル フィルタ」を参照してください。
- ファイルの種類。ファイルの種類を示すファイル名とは無関係に、種類に応じてファイルをブロックできます。ファイルの種類を基準にファイルをブロックする場合、FortiGate ユニットのファイル分析によって、ファイル名とは無関係にファイルの種類が特定されます。

ファイル フィルタの設定

複数のファイル フィルタ リストを、アンチウイルス プロファイルに追加できます。ファイル パターンの場合、5,000 までのパターンをリストに追加できます。ファイルの種類の場合、サポートされる種類のみから選択できます。

ファイル フィルタを設定するには、*[UTM]*、*[Antivirus]*、*[File Filter]* の順に選択します。

[File Filter] ページ

このページには、作成済みのファイル フィルタが一覧表示されます。このページでは、ファイル フィルタを編集、削除、または新規作成できます。

[Create New]	カタログに新しいファイル フィルタ リストを追加するには、*[Create New]* を選択します。
[名前]	使用可能なファイル フィルタ リスト。
[# Entries]	各ファイル フィルタ リスト内のファイル パターンまたはファイルの種類の数。
[DLP Rule]	各フィルタ適用の基準となる DLP ルール。
[コメント]	各ファイル フィルタ リストの説明。説明はオプションです。
削除アイコン	カタログからこのファイル フィルタ リストを削除する場合に選択します。
編集アイコン	ファイル フィルタを編集するとき選択します。

[File Filter Settings] ページ

このページでは、ファイル フィルタを構成する複数のファイル パターンおよびファイルの種類を設定できます。また、ファイル フィルタ用に作成済みのファイル パターンおよびファイルの種類が一覧表示されます。ファイル フィルタを編集する場合は、画面がこのページに移動します。

[名前]	ファイル フィルタの名前。この名前を変更するには、[名前] フィールドのテキストを編集し、*[OK]* を選択します。
[コメント]	オプションで入力するコメント。コメントを追加または編集するには、[コメント] フィールドにテキストを入力し、*[OK]* を選択します。
[OK]	リスト名またはコメントに変更を加えた場合は、*[OK]* を選択して変更を保存します。
[Create New]	ファイル フィルタ リストに新しいファイル パターンまたはファイルの種類を追加するには、*[Create New]* を選択します。
[無効]	ファイル パターンまたはファイルの種類を無効にするとき選択します。
削除アイコン	リストからこのファイル パターンまたはファイルの種類を削除する場合に選択します。
編集アイコン	ファイル パターンまたはファイルの種類を編集する場合に選択します。
移動アイコン	このファイル パターンまたはファイルの種類を、リスト内の任意の位置に移動する場合に選択します。
[Filter]	ファイル パターンおよびファイルの種類の現行リスト。
[アクション]	ファイルがファイル パターンおよびファイルの種類に一致する場合、そのファイルに対するアクションを、*[Block]* または *[Allow]* に設定できます。アクションの詳細については、359 ページの「ファイル フィルタ」を参照してください。
[有効]	ファイル パターンまたはファイルの種類を無効にするには、このチェック ボックスをオフにします。

[New File Filter] ページ

[Filter Type]	*[File Name Pattern]* または *[File Type]* を選択します。
[File Type]	リストからファイルの種類を選択します。[Filter Type] で [File Type] を選択している場合のみ表示されます。
[Pattern]	ファイル パターンを入力します。ファイル パターンは、正確なファイル名のみ、またはワイルドカードを加えて入力できます。ファイル パターンを入力する文字数は、80 文字までです。
[アクション]	ドロップ ダウン リストから、*[Block]* または *[Allow]* のアクションを選択します。アクションの詳細については、359 ページの「ファイル フィルタ」を参照してください。
[有効]	フィルタを有効または無効にするときオンまたはオフにします。

注記: デフォルトのファイル パターン リスト カタログは *builtin-patterns* と呼ばれます。

隔離

ローカル ディスクを備える FortiGate ユニットを使用し、ブロックされたファイルおよび感染ファイルを隔離できます。ログ ファイルに記録されているファイルの詳細情報を表示するには、*[Log&Report]*、*[Archive Access]*、*[Quarantine]* の順に選択します。*[AutoSubmit]* リストに特定のファイルを送信しファイル パターンを追加することで、これらのファイルが Fortinet に自動的にアップロードされ、解析されます。

また FortiGate ユニットによって、ブロックされたファイルおよび感染ファイルを FortiAnalyzer ユニットに隔離することも可能です。それらのファイルを表示するには、*[Log&Report]*、*[Archive Access]*、*[Quarantine]* の順に選択します。

隔離の設定

HTTP、FTP、IMAP、POP3、SMTP、IM、および NNTP トラフィックの、隔離オプションを設定できます。FortiGate ユニットが SSL コンテンツ スキャンおよびインスペクションをサポートする場合は、HTTPS、IMAPS、POP3S、および SMTPS トラフィックからブロックされたファイルおよび感染したファイルを隔離できます。詳しくは、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。

隔離を設定するには、*[UTM]*、*[Antivirus]*、*[Quarantine]* の順に選択します。

[Quarantine Configuration] ページ

このページでは、ウイルス スキャンで、感染ファイル、不審なファイル、ブロックされたファイルがあった場合の FortiGate ユニットのアクションを設定できます。これらは、ローカル ディスクまたは FortiAnalyzer ユニットの設定です。これらの設定は、[Quarantine Configuration] ページで表示または変更できます。

[Quarantine Infected Files]	FortiGate ユニットにより検証するプロトコルを選択します。
[Quarantine Suspicious Files]	FortiGate ユニットにより検証するプロトコルを選択します。
[Quarantine Blocked Files]	FortiGate ユニットにより検証するプロトコルのチェック ボックスをオンにします。
[Quarantine To]	ブロックされたファイル、不審なファイル、感染ファイルを、FortiAnalyzer ユニットまたはローカル ディスクに保存する設定を有効にするとき選択します。デフォルトでは、この設定は [None] に設定されており、隔離ファイルを保存する場合は、[FortiAnalyzer] を選択する必要があります。
[Max Filesize to Quarantine]	隔離ファイルの保存場所として、FortiAnalyzer ユニットまたはローカル ディスクが選択されている場合のみ、表示されます。隔離されるファイルの最大サイズを、MB 単位で設定します。設定するサイズが大きすぎると、パフォーマンスに影響する場合があります。
[Disk Age Limit] (ローカル ディスク搭載の FortiGate モデルのみ)	ファイルを隔離場所に保持する時間の制限 (時間単位)。Age Limit は、隔離ファイル リストの [TTL] カラムの値を算出するために使用されます。隔離済みファイル リストは、[Log&Report]、[Archive Access]、[Quarantine] の順に選択して表示します。この Age Limit に達すると、隔離ファイル リストの [TTL] カラムには [EXP] が表示され、ファイルが削除されます (ただし、隔離ファイル リスト内のエントリは保持されます)。0 (ゼロ) の Age Limit を入力すると、[Low Disk Space] で選択されるアクションに応じて、ファイルがディスク上に無期限に格納されます。
[Low Disk space]	ローカル ディスクに空きスペースがないとき、最も古いファイルを上書きするかまたは最新のファイルを破棄するか、いずれかを選択します。
[Enable AutoSubmit] (ローカル ディスク搭載の FortiGate モデルのみ)	自動送信機能を有効にするとき選択します。
[Use File Pattern]	ファイル パターンに一致するファイルの自動アップロードを有効にするとき選択します。
[Use File Status]	[AutoSubmit] リストにあるファイル パターンと一致するファイルの自動アップロードを有効にするとき選択します。
[Heuristics]	ヒューリスティック ステータスに基づくファイル自動アップロードのとき選択します。
[Block Pattern]	ブロック パターン ステータスに基づくファイル自動アップロードのとき選択します。

ウイルス データベース

FortiGate ユニットには複数のアンチウイルス データベースが含まれており、必要に応じたデータベースを選択することにより、ネットワーク環境を最大限に保護できます。ウイルス データベースを使用してネットワーク トラフィックに含まれるウイルスを検出するには、*[UTM]*、*[Antivirus]*、*[Virus Database]* の順に選択します。[Virus Database] ページでは、以下のデータベースを利用できます。

- 通常のウイルス データベース
- Extended ウイルス データベース
- Extreme ウイルス データベース
- Flow ベース ウイルス データベース

[Virus Database] ページでは、グレーウェアの検出を有効に設定できます。グレーウェア検出には、アドウェア、Dial、ダウンローダ、ハッカー ツール、キーロガー、RAT、およびスパイウェアが含まれています。

Extended データベースには、in the wild ウイルス、および最近のウイルス調査では見られない zoo ウイルスが幅広く含まれています。セキュリティ強化を必要とする環境には、この種のデータベースが適しています。Flow ベース データベースには、in the wild ウイルスおよびネットワーク上で一般的に見られるウイルスが含まれています。Flow ベースのウイルス スキャンは、File ベースのウイルス スキャンの代わりに使用され、File ベースのウイルス スキャンよりパフォーマンスに優れますがウイルスのカバー率が下がります。

Extreme アンチウイルス データベースでは、in the wild と最近のウイルス調査では見られない zoo 双方のウイルス スキャン、および現在サポートされているすべてのシグネチャのスキャンが可能です。ネットワークを最大限に保護する柔軟性を持ち、セキュリティ強化を必要とするネットワーク環境に最適です。Extreme アンチウイルス データベースは、AMC 対応プラットフォームおよび大容量ハード ドライブを備える FortiGate モデルのみで利用可能です。

Flow ベース アンチウイルス データベースは、IPS によるマルウェア検出を支援します。Flow ベース データベースには、in the wild ウイルスおよびネットワーク上に一般的に見られるウイルスが含まれています。また、File ベースのウイルス スキャンの代替として機能し、より優れたパフォーマンスも提供します。

FortiGuard のウイルス定義は、最新バージョンのアンチウイルス定義を FortiGate ユニットが FDN から受信した時点で更新されます。

FortiGuard Center Virus Encyclopedia には、FortiGuard ウイルス定義に含まれる情報に基づき FortiGate ユニットにより検出、削除される、ウイルス、ワーム、トロイ、その他の脅威の詳細な説明が含まれています。

FortiGuard アンチウイルス定義は、FortiGuard Distribution Network (FDN) から自動的に更新されます。アンチウイルス定義の自動更新を設定するには、*[System]*、*[Maintenance]*、*[FortiGuard]* の順に選択します。また、アンチウイルス定義をシステム ダッシュボードから手動で更新するには、*[System]*、*[Dashboard]*、*[Status]* の順に選択します。

注記：バーチャル ドメインを有効に設定している場合は、アンチウイルス プロファイルでのファイル フィルタおよびアンチウイルス設定をバーチャル ドメインごとに個別に設定する必要があります。グレーウェアの設定は、FortiOS 4.0 MR2 以降を FortiGate ユニットで実行している場合のみ有効または無効に設定できます。

不正侵入防御

FortiGate の不正侵入防御システムは、シグネチャとアノマリによる侵入検知と防御、および最小限の待ち時間と高い信頼性を両立させています。不正侵入防御では、それぞれがシグネチャに基づく完全な設定をともなう、複数の IPS センサーを作成できます。作成した IPS センサーは、いずれもファイアウォール ポリシーに適用できます。また、DoS センサーを作成し、トラフィックからアノマリに基づく攻撃を割り出すことができます。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとに不正侵入防御を個別に設定します。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

このトピックには、以下の項目が含まれています。

- IPS センサー
- DoS センサー
- 定義済みシグネチャ
- カスタム シグネチャ
- プロトコル デコーダ

IPS センサー

シグネチャを IPS センサーにグループ化することにより、ファイアウォール ポリシーに適用するときシグネチャを容易に選択できるようになります。トラフィックの特定種類に対するシグネチャを個別の IPS センサーに定義し、そのトラフィックの種類を処理するように設計されたプロファイルから、これらのセンサーを選択できます。たとえば、Web サーバ関連のシグネチャすべてを特定の IPS センサーで指定し、FortiGate ユニットにより保護される Web サーバに出入りするすべてのトラフィックを制御するファイアウォール ポリシーに、そのセンサーを適用できます。

FortiGuard サービスでは、定義済みシグネチャが定期的に更新され、新たな脅威を撃退するためのシグネチャが追加されます。フィルタに含まれるシグネチャは、シグネチャ属性を指定することで定義されるので、既存のフィルタ仕様に一致する新しいシグネチャは自動的にこれらのフィルタに組み込まれます。たとえば、Windows オペレーティング システムのすべてのシグネチャを含んでいるフィルタがある場合、新しい Windows シグネチャを追加すると、それらがフィルタに自動的に組み込まれます。

各 IPS センサーは、フィルタ (Filters) および置き換え (Overrides) の 2 部分から構成されています。置き換えは、フィルタの前に必ずチェックされます。

各フィルタは、複数のシグネチャ属性から構成されます。フィルタの実行時に、これらの属性を持つすべてのシグネチャ、およびこれらの属性のみが、トラフィックに対してチェックされます。IPS センサーに複数のフィルタが定義されている場合は、それらのフィルタはトラフィックに対して一度に 1 つずつ上から順にチェックされます。一致するトラフィックが検出されると、FortiGate ユニットにより既定の処理が行われ、その時点でフィルタとの照合は中止されます。

シグネチャ置き換えによって、フィルタに指定されているシグネチャの動作を編集でき、さらに IPS センサーのフィルタに指定されていないシグネチャを追加できます。置き換えを使用し、カスタム シグネチャを IPS センサーに加えることも可能です。

まず置き換えのシグネチャが、ネットワーク トラフィックと比較されます。IPS センサーによってトラフィックの一致が検出されない場合は、フィルタのシグネチャが一度に 1 つのフィルタずつ、上から順にネットワーク トラフィックと比較されます。シグネチャー致が検出されなければ、IPS センサーによってネットワーク トラフィックが許可されます。

フィルタには、指定されているすべての属性と一致するシグネチャのみが含まれます。新しいフィルタを作成すると、すべての属性が *[all]* に設定されている状態なので、そのフィルタにはすべてのシグネチャ含まれることになります。[重要度] を [high] に、[Target] を [server] に変更すると、フィルタにはサーバを標的とするプライオリティの高い攻撃をチェックするシグネチャのみが含まれます。

IPS センサーを設定するには、*[UTM]*、*[Intrusion Protection]*、*[IPS Sensor]* の順に選択します。

[IPS Sensor] ページ

このページには、デフォルトまたはこれまでに作成した IPS センサーが一覧表示されます。このページでは、IPS センサーを編集、削除、または新規作成できます。

[Create New]	[Create New] を選択すると、[New IPS Sensor] ページの画面に自動的に移動します。[New IPS Sensor] ページには、[名前] フィールドおよび [コメント] フィールドが表示されます。[IPS Sensor Settings] ページを表示するには、必ず名前を入力します。
[名前]	各 IPS センサーの名前。
[コメント]	オプションで記述される IPS センサーの説明。
[all_defaults] (デフォルト)	すべてのシグネチャを含みます。IPS センサーは、各シグネチャの [有効] ステータスおよび [アクション] を [Default] で使用するように設定されます。
[all_default_pass] (デフォルト)	すべてのシグネチャを含みます。センサーは、各シグネチャの [有効] ステータスを [Default] で、[アクション] を [pass] で使用するように設定されます。
[protect_client] (デフォルト)	クライアントに対する攻撃を検出するように設計されたシグネチャのみを含み、各シグネチャの [有効] ステータスおよび [アクション] を [Dfault] で使用します。
[protect_email_server] (デフォルト)	サーバおよび SMTP、POP3、または IMAP プロトコルに対する攻撃を検出するように設計されたシグネチャのみを含み、各シグネチャの [有効] ステータスおよび [アクション] を [Default] で使用します。
[protect_http_server] (デフォルト)	サーバおよび HTTP プロトコルに対する攻撃を検出するように設計されたシグネチャのみを含み、各シグネチャの [有効] ステータスおよび [アクション] を [Default] で使用します。
削除アイコン	リストから IPS センサーを削除します。
編集アイコン	IPS センサーを編集します。

[IPS Sensor Settings] ページ

このページでは、IPS センサーを構成する複数のフィルタおよび置き換えを設定できます。[IPS Sensor Settings] ページには、ページ内の [Filters] セクションにフィルタの一覧、[Override] セクションに置き換えの一覧が表示されます。定義済み置き換えを ISP センサーに追加するには [Add Pre-defined Override] を、カスタムの置き換えをセンサーに追加するには [Add Custom Override] を選択します。

[名前]	既存の IPS センサーを編集し名前を変更する場合は、このフィールドに新しい名前を入力します。変更を保存するには、必ず [OK] を選択します。
[コメント]	既存の IPS センサーを編集し説明内容を変更する場合は、このフィールドに新たな説明を入力します。 変更を保存するには、 必ず [OK] を選択します。
[OK]	リストの変更内容を保存するとき選択します。
[Enable Logging]	IPS フィルタおよびパターンをログ記録するとき選択します。これらのログを表示するには、[Log&Report]、[Log Access] の順に選択します。
[Filters]	[IPS Sensor Settings] ページの [Filters] セクション。このセクションには、現在 IPS センサーに設定されているすべてのフィルタが表示されます。このセクションから、各フィルタの編集および新たなフィルタの作成が可能です。
[Create New]	新しいフィルタを追加する場合に選択します。挿入アイコンも使用できます。詳細については、366 ページの「フィルタ」を参照してください。
編集アイコン	フィルタ設定を変更する場合に選択します。
削除アイコン	リストからフィルタを削除する場合に選択します。
挿入アイコン	新しいフィルタを挿入する場合に選択します。
移動アイコン	リスト内でフィルタを移動する場合に選択します。
[View Rules]	フィルタ内のルールを表示します。
[名前]	作成したフィルタの名前。
[重要度]	フィルタの重大度。
[Target]	フィルタに指定された標的。
[プロトコル]	フィルタのプロトコルの種類。
[OS]	オペレーティング システムの種類。

[Application]	Adobe などのソフトウェア アプリケーション。
[有効]	フィルタの設定内で [Enable all] を選択すると、緑色のチェックマークが表示されます。[Disable all] を選択すると、灰色の x が表示されます。
[Logging]	フィルタの設定内で [Enable all] を選択すると、緑色のチェックマークが表示されます。[Disable all] を選択すると、灰色の x が表示されます。
[アクション]	FortiGate ユニットによって実行されるアクションの種類。このアクションには、[Block]、[Pass]、または [Reset] を設定できます。
[Count]	フィルタに含まれるシグネチャの数。置き換えは、総数に含まれません。
[Overrides]	[IPS Sensor Settings] ページの [Overrides] セクション。このセクションには、現在IPSセンサーに設定されているすべての置き換えが表示されます。
編集アイコン	カスタムの置き換えまたは定義済みの置き換えを編集するとき選択します。
削除アイコン	カスタムの置き換えまたは定義済みの置き換えを削除するとき選択します。
[Add Pre-defined Override]	定義済みの置き換えを追加するとき選択します。詳しくは、367 ページの「定義済み置き換えおよびカスタム置き換え」を参照してください。
[Add Custom Override]	カスタムの置き換えを追加するとき選択します。詳しくは、367 ページの「定義済み置き換えおよびカスタム置き換え」を参照してください。

フィルタ

フィルタには、複数のシグネチャ属性が含まれており、これらの属性を必要に応じて設定します。フィルタに指定されている属性すべてをともなうシグネチャが、IPS シグネチャに含まれます。IPS センサーには、複数の IPS フィルタを含むことができます。フィルタの設定には、以下の設定オプションがあります。

IPS センサーでフィルタを設定するには、*[UTM]*、*[Intrusion Protection]*、*[IPS Sensors]* の順に選択します。

[Edit IPS Filter] ページ

このページで、フィルタを設定できます。[IPS Sensor Settings] ページの [Filters] セクションで [Create New] を選択すると、画面が自動的にこのページの表示に移動します。

[名前]	フィルタの名前を入力します。
[重要度]	重大度を選択します。[All] (すべてのレベル) に設定しない場合は、必ずいずれかのレベルを指定します。
[Target]	攻撃の標的となるシステムの種類を選択します。
[OS]	オペレーティング システムの種類を指定します。全種のオペレーティング システムを含む場合は、[All] を選択します。指定可能なオペレーティング システムには、BSD および Solaris が含まれます。 OS 攻撃の属性が「すべての OS」に該当するシグネチャは、あらゆるオペレーティング システムに影響します。このようなシグネチャは、指定されているオペレーティング システムの種類の数にかかわらず、自動的にどのフィルタにも含まれます。
[プロトコル]	いくつかのプロトコルまたは利用可能なすべてのプロトコルを選択します。 特定のプロトコルを選択するには、[Specify] を選択し、必要なプロトコルを [Available] カラムから [Selected] カラムに -> 矢印を使用して移動します。 [Selected] カラムからプロトコルを削除するには、そのプロトコルを選択し、<- 矢印を使用してプロトコルを [Available] カラムに戻します。
[Application]	いくつかのアプリケーション、または利用可能なすべてのアプリケーションを選択します。 特定のアプリケーションを選択するには、[Specify] を選択し、必要なアプリケーションを [Available] カラムから [Selected] カラムに -> 矢印を使用して移動します。 [Selected] カラムからアプリケーションを削除するには、そのアプリケーションを選択し、<- 矢印を使用してアプリケーションを [Available] カラムに戻します。
[Quarantine Attackers (to Banned Users List)]	攻撃者を [Banned Users List] に追加する場合に選択します。

[Method]	[Attacker 痴 IP Address] を選択すると、攻撃者の IP アドレスから送信されるすべてのトラフィックをブロックします。攻撃者の IP アドレスからのトラフィックがブロックされるのは、攻撃者の IP アドレスが [Banned Users List] に追加されているためです。 [Attacker and Victim IP Addresses] を選択すると、攻撃者の IP アドレスから標的 (被害者) の IP アドレスに送信されるすべてのトラフィックをブロックします。攻撃者の IP アドレスから被害者以外の IP アドレスへのトラフィックは許可されます。攻撃者および標的の IP アドレスは、[Banned User List] に 1 つのエントリとして追加されます。 [Attack 痴 Incoming Interface] を選択すると、攻撃を受けた FortiGate インタフェースに接続しようとするトラフィックを、すべてブロックします。このインタフェースは、[Banned User List] に追加されます。
[Logging]	隔離された攻撃者の情報をログ記録する場合に選択します。
[Expires]	攻撃者を無期限に禁止するか、または指定された日数、時間数、または分数に限り禁止するかを選択できます。
[Signature Settings]	フィルタによって、以下のシグネチャ設定が解除されるか、またはシグネチャのデフォルト設定が使用されるかを設定します。
[有効]	フィルタに含まれるシグネチャに対する FortiGate ユニットの動作を指定するために、「すべて有効」、「すべて無効」、または「シグネチャ リストに表示される個別のデフォルト値に応じて有効または無効」の、いずれかのオプションを選択します。
[Logging]	フィルタに含まれるシグネチャのログ エントリを FortiGate ユニットによって作成するか否かを指定するために、「すべて有効」、「すべて無効」、または、「シグネチャ リストに表示される個別のデフォルト値に応じて個々のロギングを有効または無効」の、いずれかのオプションを選択します。
[アクション]	シグネチャと一致するトラフィックに対する FortiGate ユニットの動作を指定するために、「すべてブロック」、「すべてリセット」、または「シグネチャ リストに表示される個別の値に応じてトラフィックをブロックまたは許可」の、いずれかのオプションを選択します。

定義済み置き換えおよびカスタム置き換え

定義済みおよびカスタムの置き換えは、基本的にフィルタと同様に設定し、またフィルタのように機能します。ただしフィルタとは異なり、個々の置き換えは 1 つのシグネチャの動作を定義します。

置き換えは、以下の 2 つの方法で使用できます。

- すでにフィルタに含まれているシグネチャの動作を変更します。たとえば、Web サーバを保護するには、サーバと関連する全シグネチャを含みそれらを有効に設定したフィルタを作成します。必要に応じてこれらのシグネチャの 1 つを無効にする場合、置き換えを作成しシグネチャを無効に指定するのが最も容易な方法です。
- どのフィルタにも含まれない単独シグネチャを、IPS センサーに追加します。これは、カスタムのシグネチャを IPS センサーに追加する、唯一の方法です。

定義済みシグネチャを置き換えに指定する場合、[Dfault] ステータスおよび [アクション] の属性は影響を受けません。置き換えを作成するとき、これらの設定を必ず明示的に設定します。

定義済みまたはカスタムの置き換えの設定には、いずれも以下の設定オプションがあります。

定義済みおよびカスタムの置き換えを設定するには、*[UTM]*、*[Intrusion Protection]*、*[IPS Sensors]* の順に選択し、IPS センサーから設定します。

注記 : ネットワーク トラフィックに対して置き換えを有効にするには、まず置き換えをフィルタに追加し、IPS センサーを選択し、さらにポリシーに適用する必要があります。これらの手順を経ないと、置き換えはネットワーク トラフィックに対して有効に機能しません。

[Configure IPS Override]

ここでは、定義済みおよびカスタムの置き換えを設定できます。[IPS Sensor Settings] ページの [Override] セクションで [Add Pre-defined Override] または [Add Custom Override] を選択すると、画面がこのページに自動的に移動します。

[Signature]	参照アイコンを選択すると、利用可能なシグネチャが一覧表示されます。この一覧から、置き換えを適用するシグネチャを選択し、*[OK]* を選択します。

[有効]	シグネチャの置き換えを有効にするときオンにします。
[アクション]	*[Pass]* 、*[Block]* 、または *[Reset]* を選択します。置き換えを有効に設定すると、[アクション] の設定に応じて、指定のシグネチャを含むトラフィックに対する FortiGate ユニットの動作が決まります。
[Logging]	このチェック ボックスをオンにすると、ネットワーク トラフィックからシグネチャが発見された場合に、ログ エントリを作成します。
[Packet Log]	このチェック ボックスをオンにすると、置き換えをトリガするパケットを FortiGate のハード ドライブに保存します。後からパケットを検証できます。詳細については、373 ページの「パケット ロギング」を参照してください。
[Quarantine Attackers (to Banned Users List)]	このチェック ボックスをオンにすると、この置き換えの NAC 隔離を有効にします。NAC 隔離の詳細については、466 ページの「NAC 隔離および禁止ユーザ リスト」を参照してください。 この設定にかかわらず、攻撃は、IPS センサーまたは DoS センサーの設定に応じて、FortiGate ユニットにより処理されます。
[Method]	*[Attacker 痴 IP address]* を選択すると、攻撃者の IP アドレスから送信されるすべてのトラフィックをブロックします。さらに攻撃者の IP アドレスが、[Banned User List] に追加されます。標的のアドレスは、影響を受けません。 *[Attacker and Victim IP Addresses]* を選択すると、攻撃者の IP アドレスから標的 (被害者) の IP アドレスに送信されるすべてのトラフィックをブロックします。攻撃者の IP アドレスから被害者以外の IP アドレスへのトラフィックは許可されます。攻撃者および標的の IP アドレスは、[Banned User List] に 1 つのエントリとして追加されます。 *[Attack 痴 Incoming Interface]* を選択すると、攻撃を受けた FortiGate インタフェースに接続しようとするトラフィックを、すべてブロックします。このインタフェースは、[Banned User List] に追加されます。
[Logging]	個別のシグネチャをログ記録するとき選択できます。
[Expires]	攻撃者を無期限に禁止するか、または指定された日数、時間数、または分数に限り禁止するかを選択できます。
[Exempt IP]	置き換えから除外する IP アドレスを入力します。これにより、除外に指定された以外のすべての IP アドレスに、置き換えが適用されます。除外される IP アドレスは、発信元および宛先のペアで定義され、その発信元から宛先に移動するトラフィックが置き換えから除外されます。
[Source]	除外される発信元 IP アドレス。すべての発信元 IP アドレスを含むには、`0.0.0.0/0` を入力します。
[Destination]:	除外される宛先IPアドレス。すべての宛先IPアドレスを含むには、`0.0.0.0/0` を入力します。
[Add]	他の除外 IP アドレスを [Add] 下のリストに追加するとき選択します。
#	リスト中の項目の順序を示す番号。
[Source]	入力される発信元 IP アドレスおよびネットマスク。
[Destination]	入力される宛先 IP アドレスおよびネットマスク。
削除アイコン	リストから項目を削除する場合に選択します。

DoS センサー

FortiGateIPS は、トラフィック アノマリ検出機能を使用し、トラフィックの一般的なパターンおよび動作に当てはまらないネットワーク トラフィックを特定します。たとえば、フラッディングの 1 種には DoS 攻撃があります。DoS 攻撃は、攻撃システムが標的のシステムに対して異常に膨大な量のセッションを開始することで発生します。膨大なセッションにより、標的システムの処理速度が著しく低下するか、または機能停止の状態に陥り、正規ユーザがそのシステムを使用できなくなります。このような DoS 攻撃が Dos センサーの名前の由来ですが、DoS センサーは幅広いアノマリ攻撃を検出し防御する機能を備えています。

各トラフィック アノマリのロギングを有効または無効に設定できるとともに、検出しきい値を設定し、その値を超えた場合に実行されるアクションも設定できます。

複数の DoS センサーを作成できます。各センサーには、12 のアノマリ タイプが含まれており、それぞれのアノマリ タイプを設定できます。センサーによりアノマリが検出されると、設定されているアクションが適用されます。DoS ポリシーごとに、使用する 1 つのセンサーを選択し、各インタフェースのアノマリしきい値を個別に設定できます。個々のセンサーは、それらが DoS ポリシーにより追加されるインタフェースの特有の条件に合わせて設定できるので、複数のセンサーを使用することで、非常にきめ細かくアノマリを検出できます。

トラフィック アノマリ検知リストは、FortiGate ファームウェア イメージがアップグレードされた場合にのみ更新できます。

DoS センサーが不適切に設定されると、ネットワーク トラフィックを妨害する原因になるので、FortiGate ユニットは DoS センサーをともなわない状態で出荷されます。まず DoS センサーを独自に作成し、それらを DoS ポリシーで選択する手順を経て、DoS センサーが有効に機能します。新規作成したセンサーのしきい値は、あらかじめ推奨値に設定されており、ネットワークの必要性に応じてその値を調整できます。

FortiGate の CLI から、DoS センサーの NAC 隔離を設定できます。詳細については、466 ページの「NAC 隔離の設定」を参照してください。

注記: デフォルトのアノマリしきい値を変更する前に、正常なネットワーク トラフィックと予測されるネットワーク トラフィックを把握することが重要です。しきい値を低く設定しすぎると誤検知が発生する可能性があり、しきい値を高く設定しすぎると回避可能な攻撃を見逃す可能性があります。

注記: FortiGate ユニットでバーチャル ドメインを有効に設定している場合は、不正侵入防御を各 VDOM で個別に設定する必要があります。すべてのセンサーおよびカスタム シグネチャは、それらが作成された VDOM のみに表示されます。

[DoS Sensor] ページ

このページには、デフォルトおよび作成済みの DoS センサーが一覧表示されます。このページでは、DoS センサーを編集、削除、または新規作成できます。

[Create New]	DoS センサーを新規作成する場合、[New DoS Sensor] ページの画面に自動的に移動します。[New DoS Sensor] ページには、[名前] フィールドおよび [コメント] フィールドがあり、[Edit DoS Sensor] ページを表示するには必ず名前を入力します。
[名前]	DoS センサーの名前。
[コメント]	オプションで記述される、DoS センサーの説明。
削除アイコン	DoS センサーを削除します。
編集アイコン	[アクション]、[重要度]、および [Threshold] の情報を編集します。

[Edit DoS Sensor] ページ

このページでは、アクションの種類、しきい値量の設定、および必要に応じてアノマリのロギングを有効に設定できます。設定可能なアノマリは、デフォルトで 12 種類あります。DoS センサーを編集する場合は、画面がこのページに移動します。

[名前]	DoS センサーの名前を入力または変更します。
[コメント]	オプションで、DoS センサーの説明を入力または変更できます。このフィールドに入力される説明は、DoS センサー リストに表示されます。
[Anomalies Configuration]	
[名前]	アノマリの名前。
[有効]	DoS センサーを有効にして、指定されたアノマリの発生を検出するとき、このチェック ボックスをオンにします。ヘッダ行にあるチェック ボックスをオンにすると、すべてのアノマリを有効にします。
[Logging]	DoS センサーを有効にして、発生したアノマリをログ記録するとき、このチェック ボックスをオンにします。ヘッダ行にあるチェック ボックスをオンにすると、すべてのアノマリのロギングを有効にします。有効に設定されていないアノマリは、ログ記録されません。

[アクション]	[Pass] を選択すると、FortiGate ユニットで検出された異常なトラフィックを許可し、[Block] を選択するとそのようなトラフィックを許可しません。
[Threshold]	[アクション] に指定されているアノマリ対処機能 (Pass または Block) が FortiGate ユニットによりトリガされるまでの、異常な動作が見られるセッション / パケットの数を表示します。必要に応じて、数値を変更できます。設定範囲は、1 ～ 2 147 483 647 です。これらの設定が特定アノマリにどのように影響するかについては、370 ページの表 52 を参照してください。

アノマリについて

DoS センサーには、TCP、UDP、ICMP のプロトコルごとに、4 種類の統計的なアノマリ タイプがあります。これにより DoS センサーには、表 52 に示される合計 12 種類のアノマリ設定項目があります。

表 52: 12 種類のアノマリ設定項目

アノマリ	説明
tcp_syn_flood	1 つの宛先 IP アドレスへの SYN パケット転送速度 (再送信を含む) が、設定されているしきい値を超えると、アクションが実行されます。しきい値は、パケット / 秒の単位で示されます。
tcp_port_scan	1 つの発信元 IP アドレスからの SYN パケット転送速度 (再送信を含む) が、設定されているしきい値を超えると、アクションが実行されます。しきい値は、パケット / 秒の単位で示されます。
tcp_src_session	1 つの発信元 IP アドレスからの同時 TCP 接続の数が、設定されているしきい値を超えると、アクションが実行されます。
tcp_dst_session	1 つの宛先 IP アドレスへの同時 TCP 接続の数が、設定されているしきい値を超えると、アクションが実行されます。
udp_flood	1 つの宛先 IP アドレスへの UDP トラフィックが、設定されているしきい値を超えると、アクションが実行されます。しきい値は、パケット / 秒の単位で示されます。
udp_scan	1 つの発信元 IP アドレスから発生する UDP セッションの数が、設定されているしきい値を超えると、アクションが実行されます。しきい値は、パケット / 秒の単位で示されます。
udp_src_session	1 つの発信元 IP アドレスからの同時 UDP 接続の数が、設定されているしきい値を超えると、アクションが実行されます。
udp_dst_session	1 つの宛先 IP アドレスへの同時 UDP 接続の数が、設定されているしきい値を超えると、アクションが実行されます。
icmp_flood	1 つの宛先 IP アドレスに送信される ICMP パケットの数が、設定されているしきい値を超えると、アクションが実行されます。しきい値は、パケット / 秒の単位で示されます。
icmp_sweep	1 つの発信元 IP アドレスから発生する ICMP パケットの数が、設定されているしきい値を超えると、アクションが実行されます。しきい値は、パケット / 秒の単位で示されます。
icmp_src_session	1 つの発信元 IP アドレスからの同時 ICMP 接続の数が、設定されているしきい値を超えると、アクションが実行されます。
icmp_dst_session	1 つの宛先 IP アドレスへの同時 ICMP 接続の数が、設定されているしきい値を超えると、アクションが実行されます。

定義済みシグネチャ

IPS センサーに必要なシグネチャをグループ化した後は、FortiGate 不正侵入防御システムによってそれらのシグネチャを使用できます。必要に応じて、IPS センサーに指定されているシグネチャのデフォルト設定を置き換えることもできます。FortiGate ユニットには、多数の IPS センサーがあらかじめ内蔵されていますが、IPS センサーを使用する前にそれらの設定をチェックし、ネットワークの要件を満たすかどうかを確かめることが重要です。

必要なシグネチャのみを使用することで、システムのパフォーマンスを強化し、IPS センサーにより作成されるログ メッセージおよびアラート メール メッセージの数を削減できます。たとえば、FortiGate ユニットが Web サーバを保護しない場合は、Web サーバのシグネチャは含まれません。

定義済みのシグネチャ リストは、*[UTM]*、*[Intrusion Protection]*、*[Predefined]* の順に選択して表示できます。このリストには、現在 FortiGuard Center Vulnerability Encyclopedia に含まれているシグネチャが表示されます。このエンサイクロペディアには、[Predefined] メニューには含まれるシグネチャ以外の、他のシグネチャも含まれています。各シグネチャの名前は、Vulnerability Encyclopedia に含まれるそのシグネチャのエントリとリンクしています。Vulnerability Encyclopedia には、シグネチャにより検出された攻撃についての説明があり、推奨されるアクションおよび詳細情報へのリンクが記載されています。

定義済みシグネチャ リストには、攻撃の重大度、プロトコル、各シグネチャに影響されるアプリケーションなどの特性も含まれています。これらの特性は、シグネチャの目的を理解するためのクイック リファレンスとして役立ちます。また、これらの特性をシグネチャ リストの並べ替えに利用し、共通の特性ごとにシグネチャをグループ化できます。シグネチャ リストには、デフォルトのアクション、デフォルトのロギング ステータス、およびシグネチャがデフォルトで有効かどうかも表示されます。シグネチャは、デフォルトで名前を基準に並べられています。

定義済みシグネチャを表示するには、*[UTM]*、*[Intrusion Protection]*、*[Predefined]* の順に選択します。

注記： FortiGate ユニットでバーチャル ドメインを有効に設定している場合は、不正侵入防御を各 VDOM で個別に設定します。すべてのセンサーおよびカスタム シグネチャは、それらが作成された VDOM のみに表示されます。

[Predefined] ページ

このページには、現在 FortiGate ユニットに含まれている定義済みシグネチャが一覧表示されます。シグネチャの名前を選択すると、FortiGuard Center Vulnerability Encyclopedia に記載されているそのシグネチャの詳細な定義の画面に、自動的に移行します。またこのページには、どのシグネチャが有効または無効に設定されているかが表示されます。

[Column Settings]	一覧表示されているシグネチャ情報をカスタマイズする場合に選択します。また、カラムの順序を再調整することもできます。詳細については、34 ページの「表示されるカラムのカラム設定を使用した制御」および 35 ページの「カラム設定と組み合わせたフィルタの使用」を参照してください。
[Clear All Filters]	定義済みシグネチャ リスト表示にフィルタリングを適用している場合は、すべてのフィルタを解除しシグネチャをすべて表示するとき、このオプションを選択します。
[Filter]	指定した条件に応じて定義済みシグネチャ リストをフィルタ処理または並べ替えるための、カラムフィルタを編集します。詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。
[名前]	このシグネチャの名前。各シグネチャの名前は、FortiGuard Center Vulnerability Encyclopedia に含まれるシグネチャの説明にリンクしています。
[重要度]	このシグネチャの重大度。重大度のレベルは、低から高の順に、[Information]、[Low]、[Medium]、[High]、および [Critical] です。
[Target]	このシグネチャの対象。サーバまたはクライアント、あるいはこの双方です。
[Protocols]	このシグネチャが適用されるプロトコル。
[OS]	このシグネチャが適用されるオペレーティング システム。
[Applications]	このシグネチャが適用されるアプリケーション。
[有効]	シグネチャのデフォルトの状態。緑色の円はこのシグネチャが有効なことを示し、灰色の円はシグネチャが有効でないことを示します。
[アクション]	シグネチャのデフォルトのアクション。 *Pass* – 変更を加えずにトラフィックを許可します。 *Drop* – シグネチャが検出されたトラフィックを、宛先まで到達させずに破棄します。ロギングが有効に設定されている場合は、このシグネチャによって生成されるログ メッセージのステータス フィールドにアクションが表示されます。

ヒント： IPS保護機能がネットワーク トラフィックにどのように作用するかを確認するには、必要なシグネチャを有効にして、[アクション] を [Pass] に設定し、ロギングを有効に設定します。トラフィックは中断されませんが、どのシグネチャが検出されたかを詳しく調べることができます。

表示フィルタの使用

デフォルトでは、すべての定義済みシグネチャが表示されます。特定のシグネチャのみを表示するには、フィルタを適用できます。たとえば、Windows シグネチャのみを表示する場合は、OS ステータス フィルタを使用します。詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。

カスタム シグネチャ

注意: カスタム シグネチャは高度な機能です。このドキュメントでは、本書の読者ユーザが不正侵入検知シグネチャ作成の経験者であることを前提にしています。

カスタム シグネチャは、さまざまなネットワーク環境に合わせて FortiGate 不正侵入防御システムをカスタマイズするための、高度な機能と柔軟性を備えています。FortiGate の定義済みシグネチャは、一般的な攻撃をカバーしています。例外的なアプリケーションや特殊なアプリケーション、または一般的でないプラットフォームを使用している場合は、アプリケーションまたはプラットフォームのベンダからリリースされるセキュリティ警告に応じて、カスタム シグネチャを追加できます。

また、P2P プロトコルのブロックに有用なカスタム シグネチャも作成できます。

カスタム シグネチャを作成した後は、トラフィック スキャンのために作成した IPS センサーに、そのシグネチャを指定する必要があります。

カスタム シグネチャは、特定のトラフィックをブロックまたは許可するために使用します。たとえば、公序良俗に反する内容を含むトラフィックをブロックするには、次のようなカスタム シグネチャを追加します。

```
set signature 'F-SBID (--protocol tcp; --flow bi_direction; --
pattern "bad words"; --no_case)'
```

カスタム シグネチャを実際に機能させるには、IPS フィルタのシグネチャ置き換えにそのシグネチャを追加する必要があります。カスタム シグネチャを作成しても、単に作成しただけでは、トラフィックに対して何の効果も作用しません。

カスタム シグネチャを設定するには、*[UTM]*、*[Intrusion Protection]*、*[Custom]* の順に選択します。

注記： FortiGate ユニットでバーチャル ドメインを有効に設定している場合は、不正侵入防御を各 VDOM で個別に設定します。すべてのセンサーおよびカスタム シグネチャは、それらが作成された VDOM のみに表示されます。

[Custom] ページ

このページには、作成済みのカスタム シグネチャが一覧表示されます。このページでは、カスタム シグネチャを編集、削除、または新規作成できます。

[Create New]	[Create New] を選択すると、[New Custom Signature] ページの画面に自動的に移動します。
編集アイコン	カスタム シグネチャを編集する場合に選択します。
削除アイコン	このページのリストからカスタム シグネチャを削除するとき選択します。
[名前]	カスタム シグネチャの名前。
[Signature]	シグネチャ本体。

[New Custom Signature] ページ

[名前]	カスタム シグネチャの名前を入力します。
[Signature]	シグネチャを入力します。

プロトコル デコーダ

FortiGate の不正侵入防御システムは、プロトコル デコーダを使用することにより、プロトコル要件および規格に一致しない異常なトラフィック パターンを特定します。たとえば、HTTP デコーダはトラフィックを監視して、HTTP プロトコル規格と一致しない HTTP パケットを特定します。

リファレンスとして提供されているデコーダ リストは、CLI から設定内容を編集できます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

プロトコル デコーダを表示するには、*[UTM]*、*[Intrusion Protection]*、*[Protocol Decoder]* の順に選択します。

[Protocol Decoder] ページ

このページには、FortiGate ユニットに含まれている現行のプロトコル デコーダが一覧表示されます。FortiGate ユニットは、FDN への問い合わせにより、このリストを自動的に更新します。このリストには、プロトコル デコーダによって監視されるポート番号が含まれています。

[Protocols] プロトコル デコーダの名前。

[Ports] このデコーダが監視する (1 つまたは複数の) ポート番号。

IPS プロトコル デコーダ リストのアップグレード

不正侵入防御システムのプロトコル デコーダは、既存のデコーダ設定を変更したとき、または新しいデコーダを追加したとき、FDN (FortiGuard Distribution Network) により自動的にアップグレードされます。プロトコル デコーダ リストは、FDN によって、既存 IM/P2P の最新バージョンおよび新しいアプリケーションなどの新たな脅威に対する保護を含む、最新の状態に維持されます。

パケット ロギング

パケット ロギングは、カスタム シグネチャをデバッグするための手法であり、あらゆるシグネチャがネットワーク環境でどのように機能するかを知るための手法でもあります。

カスタム置き換えでシグネチャを選択し、パケット ロギングを有効にすると、シグネチャをトリガするすべてのネットワーク パケットが FortiGate ユニットによって、メモリ、内蔵ハード ドライブ (この目的で設置されている場合)、FortiAnalyzer、または FortiGuard Analysis および Management Service に保存されます。これらの保存されたパケットは、後から表示し PCAP 形式で保存して、詳しく検証できます。

パケットのログ記録は、IPS センサーの中で、定義済み置き換えまたはカスタム置き換えで有効に設定できます。IPS センサーを表示するには、*[UTM]*、*[Intrusion Protection]*、*[IPS Sensor]* の順に選択します。

パケット ロギングの設定

パケット ロギングによって、IPS シグネチャに一致するネットワーク パケットが、攻撃ログに保存されます。このログの種類は、診断ツールの一種として使用するためのログです。ロギングされたパケットは、そのログの保存場所として設定されている FortiAnalyzer ユニットなどの場所に、FortiGate ユニットによって保存されます。

パケット ロギングは、シグネチャ置き換えのみで利用でき、IPS センサーまたはフィルタで利用できるオプションではありません。というのも、多数のシグネチャでパケット ロギングを有効にすると、利用不可能な多数のデータを生成する原因になるからです。

パケット ロギングを詳細設定するために、多数の CLI コマンドが用意されています。メモリにロギングするときは、`packet-log-memory` コマンドにより、ロギングされたパケットを保存するための最大メモリ容量を定義します。このコマンドは、メモリにロギングする場合のみ有効です。

シグネチャを含むパケットだけでは問題解決に不十分な場合には、packet-log-history コマンドを使用し、パケットから IPS シグネチャが検出されたときキャプチャするパケットの量を指定できます。この値を 1 より大きく設定すると、シグネチャを含むパケット、およびそのパケットに先行するパケットの双方を、コマンドの設定値と同じ合計数だけパケット ログに保存できます。たとえば、packet-log-history を 7 に設定すると、FortiGate ユニットによって、IPS シグネチャを含むパケット、およびそれに先行する 6 個のパケットが保存されます。

FortiGate ユニットによりロギングされたパケットを、表示または保存できます。ロギングされたパケットは、PCAP 形式で保存できます。PCAP 形式のファイルは、Wireshark などのネットワーク分析ソフトウェアを使用して表示し、詳しく検証できます。

注記: packet-log-history の値を 1 より大きく設定すると、ネットワーク トラフィックをバッファする必要があることから、FortiGate ユニットの性能が制限される場合があります。性能がどの程度制限されるかは、モデル、設定、およびトラフィックの負荷に応じて異なります。

Web フィルタ

ここでは、[Web Filtering] メニューに含まれている FortiGate Web フィルタリング オプションについて説明します。FortiGate ユニットが SSL コンテンツ スキャンおよびインスペクションをサポートする場合は、HTTPS トラフィックの Web フィルタリングを設定できます。詳しくは、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとに Web フィルタリングを個別に設定します。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

このトピックには、以下の項目が含まれています。

プロファイル

[Profile] メニューには、 ファイアウォール ポリシーに適用する Web フィルタ プロファイルの設定が含まれています。プロファイルに含まれる特定の情報は、ポリシーに基づきトラフィックがどのように検証され、 検証に基づいてどのようなアクションが実行されるかを定義します。

FortiGuard カテゴリ機能により SSL プロキシ除外を使用する場合は、[New Web Filter Profile] ページの [Web Filtering] セクションでこの機能を有効にする必要があります。SSL プロキシ除外機能によって、FortiGuard カテゴリに基づく特定の宛先に接続する際に、FortiGuard カテゴリがプロキシ設定を迂回できるようになります。この Web フィルタリング チェックによって、接続を除外する必要があるかどうかはチェックされず、トラフィックのブロッキングまたはロギングが HTTP プロキシで通常どおりに発生します。

Web フィルタ プロファイルを設定するには、*[UTM]*、*[Web Filter]*、*[Profile]* の順に選択します。

[Profile] ページ

このページには、作成済みの Web フィルタ プロファイルが一覧表示されます。このページでは、Web フィルタ プロファイルを編集、削除、または新規作成できます。

[Create New]	新しい Web フィルタ プロファイルを作成するとき選択します。
編集アイコン	Web フィルタ プロファイルの設定を変更するとき選択します。
削除アイコン	Web フィルタ プロファイルを削除するとき選択します。

[名前]	Web フィルタ プロファイルの名前。
[コメント]	Web フィルタ プロファイルの説明。この設定は、オプションです。

[New Web Filter Profile] ページ

このページで、Web フィルタ プロファイルを設定できます。Web コンテンツ フィルタを有効にする場合は Web コンテンツ フィルタ、Web URL フィルタを有効にする場合は URL フィルタが、それぞれ必要です。Web フィルタ プロファイルを編集する場合は、画面が [Edit Web Filter Profile] ページに移動します。

[名前]	Web フィルタ プロファイルの名前を入力します。
[コメント]	Webフィルタ プロファイルの説明を入力します (入力はオプションです)。
[Web Content Filter]	Web コンテンツ フィルタリングに適用するプロトコルを選択します。[Options] カラムで、ドロップダウン リストから Web コンテンツ フィルタ リストを選択します。 Web コンテンツ フィルタをログ記録するには、[Logging] カラムのチェック ボックスをオンにします。 しきい値を適用するには、[Threshold] フィールドに数値を入力します。
[Web URL Filter]	Web URL フィルタリングに適用するプロトコルを選択します。[Options] カラムで、ドロップダウン リストからURLフィルタ リストを選択します。 URLフィルタリングをログ記録するには、[Logging] カラムのチェック ボックスをオンにします。
[Safe Search]	有効に設定すると、サポートされる検索エンジンは、検索結果から攻撃的な情報を除外します。このオプションで有効に設定可能な検索エンジンは、Google、Yahoo!、および Bing です。
[Google]	[Options] カラムにあるこのチェック ボックスをオンにすると、Google 検索に適用されるセーフ サーチ保護の厳格なフィルタリング レベルを強制的に設定します。厳格なフィルタリングは、明示的なテキストおよび画像の双方をフィルタ処理します。
[Yahoo!]	[Options] カラムにあるこのチェック ボックスをオンにすると、Yahoo! 検索に適用されるセーフ サーチ保護の厳格なフィルタリング レベルを強制的に設定します。
[Bing]	[Options] カラムにあるこのチェック ボックスをオンにすると、Bing 検索に適用されるセーフ サーチ保護の厳格なフィルタリング レベルを強制的に設定します。
[FortiGuard Web Filtering]	FortiGuard Web フィルタリングのオプションを有効に設定し、プロファイルに適用します。 Web フィルタリングの設定を適用するプロトコルのチェック ボックスをオンにします。 FortiGuard カテゴリにより SSL Exempt のプロキシ除外を有効に設定するには、有効にするカテゴリ行の [SSL Exempt] チェック ボックスをオンにします。 FortiGuard Quota 設定を適用することもできます。[Classification] で、FortiGuard Quota 設定を適用できます。
[FortiGuard Web Filtering Override]	プロファイルで Web フィルタリング置き換えオプションを可能にするとき、有効に設定します。これらのオプションは、FortiGuard Web フィルタリングによりブロックされている Web サイトにアクセスする必要があるユーザのために提供されています。 Web フィルタリング置き換えを適用するプロトコルのチェック ボックスをオンにします。プロトコルは必ず選択します。選択しない場合は、オプションにアクセスできません。 各種 Web カテゴリをユーザがブラウズできる時間を指定する場合は、[FortiGuard Web Filtering Override] の [FortiGuard Web Quota] 領域で [有効] を選択します。時間の長さは、時間、分、または秒単位で指定できます。
[Override Scope]	ドロップダウン リストから、いずれかのオプションを選択します。
[Override Type]	ドロップダウン リストから、いずれかのオプションを選択します。

[Off-site URLs]	このオプションは、上書き Web ページが、ブロックされているオフサイト URL から画像などのコンテンツを表示するかどうかを定義します。 たとえば、すべての FortiGuard カテゴリがブロックされており、別のドメインから画像が提供されているサイトを閲覧するとします。そのサイトのディレクトリ上書きを作成し、そのページを表示できます。[Off-site URL] を [Deny] に設定する場合は、そのページの全画像は既存の上書きルールが適用されない別のドメインから転送されているので、画像は崩れて表示されます。[Off-site URL] を [Allow] に設定する場合は、そのページの画像は正常に表示されます。 そのページ上書きの対象に含まれるユーザのみが、一時的な上書きによる画像を表示できます。新しい上書きルールを作成する必要なく、ユーザは画像の元となるそのサイトのどのページも（ページが画像自体と同じディレクトリから提供されていない限り）表示できなくなります。
[Override Time]	上書きルールが終了する時点を指定します。
[User Group]	[Override Scope] で [User Group] を選択している場合は、[Available] カラムでそのユーザ グループ選択し、そのグループを [Selected] カラムに移動します。
[Advanced Filter]	利用可能な高度なフィルタ オプションを選択します。 これらのオプションをログ記録する場合は、[Logging] カラムのチェックボックスをオンにします。 [HTTP POST Action] 行では、[Option] ドロップダウン リストからアクションを選択します。

We コンテンツ フィルタ

Web コンテンツ フィルタにより、Web ページへのアクセスを制御する特定の語彙またはパターンのリストを設定できます。たとえば、Example という単語を含む Web ページには誰もアクセスできないように設定できます。また、ワイルドカードまたは Perl 正規表現を入力し、Web コンテンツをフィルタリングできます。

注記：Web コンテンツ フィルタでは、Perl 正規表現パターンの大文字と小文字は区別されます。単語または語句の大文字と小文字が区別されないようにするには、正規表現の `/i` を使用します。たとえば、
`/bad language/i` を指定すると、文字の大小にかかわらず、`bad language` というフレーズであればすべてブロックされます。ワイルドカード パターンでは、文字の大小は区別されません。詳細については、393 ページの「ワイルドカードおよび Perl 正規表現の使用」を参照してください。

Web コンテンツ フィルタが有効の場合、ファイアウォール ポリシーでは、要求されたすべての Web ページはコンテンツ フィルタ リストに対するチェックが行われます。ページに現れる各パターンのスコア値が加算され、その合計が、Web フィルタ プロファイルに設定されているしきい値を超えると、そのページはブロックされます。ある同じパターンが Web ページに繰り返し現れても、そのパターンにスコアが適用されるのは 1 回のみです。

パターンごとに、*[Block]* または *[Exempt]* を選択できます。[Block] は、パターンと一致する Web ページへのアクセスをブロックします。[Exempt] は、Web ページへのアクセスをブロックする他のエントリがリスト中にある場合でも、その Web ページへのアクセスを可能にします。Web コンテンツパターンには、1 単語または最大 80 文字のテキスト文字列が可能です。リスト中には、最大 5,000 のパターンを含むことができます。

Web コンテンツ フィルタを設定するには、*[UTM]*、*[Web Filter]*、*[Web Content Filter]* の順に選択します。

[Web Content Filter] ページ

このページには、作成済みの Web コンテンツ フィルタが一覧表示されます。このページでは、Web コンテンツ フィルタを編集、削除、または新規作成できます。

[Create New]	[Create New] を選択すると、[New List] ページの画面に自動的に移動します。[New List] ページには、[名前] フィールドおよび [コメント] フィールドがあり、[Web Content Filter List] ページを表示するにはリストの名前を入力する必要があります。
[名前]	Web コンテンツ フィルタ リストの名前。
[# Entries]	各 Web コンテンツ フィルタ リスト内のコンテンツ パターンの数。

[コメント]	オプションで記述される Web コンテンツ フィルタ リストの説明。説明テキストは、63 文字まで入力できます。超過した文字は、切り捨てられます。
削除アイコン	Web コンテンツ フィルタをこのページから削除します。
編集アイコン	Web コンテンツ フィルタを編集します。編集アイコンを選択すると、画面が [Web Content Filter Settings] ページに自動的に移動します。

[Web Content Filter Settings] ページ

このページでは、Web コンテンツ フィルタを構成する複数のパターンを設定できます。また、Web コンテンツ フィルタ用に作成したパターンが一覧表示されます。[New List] ページからこのページの画面に、自動的に移動します。Web コンテンツ フィルタを編集する場合は、このページの画面に移動します。

[名前]	既存の Web コンテンツ フィルタを編集しプロファイル名を変更する場合は、このフィールドに新しい名前を入力します。変更を保存するには、必ず [OK] を選択します。
[コメント]	既存の Web コンテンツ フィルタを編集し、説明内容を変更する場合は、このフィールドに新しい説明を入力します。説明を変更する場合は、変更をこのフィールドに入力します。変更を保存するには、必ず [OK] を選択します。
[OK]	[名前] フィールドで名前を変更した場合、または [コメント] フィールドに説明を加えた (または変更した) 場合のみ、[OK] を選択します。
[Create New]	Web コンテンツ フィルタの新しいパターンを設定するとき選択します。[Create New] を選択すると、画面が [New Pattern] ページに自動的に移動します。
[有効]	パターンが有効または無効のいずれかを示します。
[Pattern]	Web コンテンツ フィルタ用に作成したパターンの、現行のリスト。
[パターンタイプ]	パターン リスト内のそれぞれのエントリで使用されるパターンの種類。パターンの種類は、[Wildcard] または [Regular Expression] が表示されます。
[Language]	このパターンが属する文字セット。[Simplified Chinese]、[Traditional Chinese]、[Cyrillic]、[French]、[Japanese]、[Korean]、[Spanish]、[Thai]、または [Western] が表示されます。
[アクション]	[アクション] には、[Block] または [Exempt] が表示されます。
[Score]	このパターンに適用される重み付けのスコア値。あるページに現れるすべての一致パターンのスコア値が加算され、その合計が Web フィルタ プロファイルで設定されているしきい値を超えると、そのページはブロックされます。[アクション] を [Exempt] に設定している場合は、スコア値は適用されません。
ページ コントロール	ページ コントロールを使用し、[Web Content Filter Settings] ページに含まれる Web コンテンツ フィルタを表示します。
編集アイコン	リスト内のパターンを編集します。
削除アイコン	リスト内のパターンを削除します。
[有効]	パターンを有効に設定し、リスト内で使用します。
[無効]	パターンを無効に設定し、リスト内で使用しません。
[Remove All Entries]	リスト内からすべてのパターンを削除するとき選択します。

[New Pattern] ページ

[アクション]	次のいずれかを選択します。 **[Block]** – パターンが一致する場合は、その Web ページのスコアをすべて加算します。Web ページのスコア合計が、プロテクション プロファイルに定義されている Web コンテンツ ブロックのしきい値を超えると、その Web ページがブロックされます。 **[Exempt]** – パターンが一致する場合は、ブロックに一致するエントリがある場合でも、Web ページはブロックされません。
[Pattern]	コンテンツ パターンを入力します。Web コンテンツのパターンには、1 単語、または最大 80 文字のテキスト文字列が可能です。 1 単語の場合、すべての Web ページでその単語の有無が FortiGate ユニットによってチェックされます。語句の場合、すべての Web ページで語句に含まれるいずれかの単語の有無が FortiGate ユニットによってチェックされます。引用符で囲まれた語句の場合、すべての Web ページでその語句全体の有無が FortiGate ユニットによってチェックされます。

[パターンタイプ]	ドロップダウン リストから、パターンの種類 [Wildcard] または [Regular Expression] のいずれかを選択します。
[Language]	このパターンが属する文字セット。[Simplified Chinese]、[Traditional Chinese]、[Cyrillic]、[French]、[Japanese]、[Korean]、[Spanish]、[Thai]、または [Western] から選択します。
[Score]	このパターンのスコア値を入力します。 Web コンテンツ リストをプロテクション プロファイルに追加するとき、そのプロテクション プロファイルの Web コンテンツ フィルタのしきい値を設定します。Web ページがコンテンツ ブロック リストのエントリと一致する場合は、スコアが記録されます。Web ページが 2 つ以上のエントリと一致する場合は、Web ページのスコアは加算されます。Web ページのスコア合計がしきい値以上の場合は、その Web ページはブロックされます。コンテンツ リスト エントリのデフォルトのスコアは 10、およびデフォルトのしきい値は 10 です。したがって、デフォルトでは Web ページは 1 つの一致でブロックされます。複数の一致がある場合のみ Web ページがブロックされるように、スコアおよびしきい値を変更できます。
[有効]	このエントリを有効にする場合にオンにします。

HTTP および FTP クライアント コンフォーティング

注意: クライアント コンフォーティングでは、スキャンされていない、したがって感染の可能性があるコンテンツを、クライアントに送信する場合があります。クライアント コンフォーティングは、このリスクを受け入れた上で有効にしてください。クライアント コンフォーティングの [Interval] を高く、[Amount] を低く設定し、その状態を維持すると、感染の可能性があるデータをダウンロードする量を削減できます。

基本的に、クライアント コンフォーティングにより、Web ページのロードまたは HTTP あるいは FTP ファイルのダウンロード進行状況が視覚的に表示されます。この表示を行うために、クライアント コンフォーティングは、ダウンロードされているファイルまたは Web ページの最初のパケットの一部を、[Interval] の設定に基づいてクライアントに送信するので、クライアントはダウンロードの遅れを意識しません。クライアントは、Web ブラウザまたは FTP クライアントです。クライアント コンフォーティングを使用しない場合、FortiGate ユニットがダウンロード データのバッファおよびスキャンを完了するまで、クライアントのユーザにはダウンロード開始が示されません。ダウンロードが進行中であることがわからないため、ユーザはダウンロード失敗と考え、転送処理をキャンセルまたは何度も繰り返す可能性があります。

クライアント コンフォーティング メッセージの表示 (進捗バーなど) は、クライアントに応じて異なります。 クライアント コンフォーティングが、 視覚的に表示されない場合もあります。

クライアント コンフォーティングの最中に、ダウンロード中のファイルから感染が検出されると、FortiGate ユニットはその URL をキャッシュし、接続を破棄します。クライアントへのダウンロードはすでに開始されているので、クライアントには何が発生したかについて通知されずに、ダウンロードが停止し、ファイルの一部のみがダウンロードされたままの状態となります。

ユーザが短時間の内に同じファイルを再ダウンロードすると、キャッシュされた URL が照合されダウンロードはブロックされます。感染キャッシュ メッセージの差し替えメッセージにより、ダウンロードがブロックされた状況がクライアントに通知されます。キャッシュ内の URL 数は、キャッシュ サイズにより制限されます。

FTP および HTTP クライアント コンフォーティングの設定

以下のステップは、FTP または HTTP ダウンロードのクライアント コンフォーティングが機能する仕組みを示しています。ここでは、ダウンロード ファイルのサイズは 10 MB、クライアント コンフォーティングの [Interval] は 20 秒、[Amount] は 512 バイトです。

1 FTP または HTTP クライアントから、ファイルが要求されます。

2 FortiGate ユニットにより、サーバからのファイルがバッファされます。接続は低速なので、20 秒後にファイルの約半分がバッファされています。

3 FortiGate ユニットは、サーバからファイルを引き続きバッファ処理しながら、512 バイトをクライアントに送信します。

4 さらに 20 秒後、FortiGate ユニットはバッファ処理したファイルから次の 512 バイトをクライアントに送信します。

5 ファイルが完全にバッファ処理されると、クライアントには以下のデータ量が転送されます。
`ca * (T/ci) bytes == 512 * (40/20) == 512 * 2 == 1024 bytes`

ここでは、`ca` はクライアント コンフォーティングの [Amount]、`T` はバッファ時間、`ci` はクライアント コンフォーティングの [Interval] です。

6 **FTP クライアント。**ファイルにウイルスが含まれない場合は、FortiGate ユニットからファイルの残りがクライアントに送信されます。ファイルが感染している場合は、FortiGate ユニットによりデータ接続が遮断され、FTP ウイルス差し替えメッセージがクライアントに送信されます。

HTTP クライアント。ファイルにウイルスが含まれない場合は、FortiGate ユニットからファイルの残りがクライアントに送信されます。ファイルが感染している場合は、FortiGate ユニットによりデータ接続が遮断されますが、クライアントにメッセージは送信されません。

文字セットおよび Web コンテンツ フィルタリング、電子メール フィルタリングの禁止単語、および DLP スキャン

注意: 複数の文字セットを指定すると、Web フィルタリングおよび DLP のパフォーマンスが低下します。

FortiGate ユニットは、プロテクション プロファイルでの指定に応じた電子メール フィルタリング禁止単語チェック、Web フィルタリングおよび DLP コンテンツ スキャンを適用する前に、HTTP、HTTPS、および電子メールのコンテンツを、UTF-8 文字セットに変換します。

電子メール メッセージの場合、FortiGate ユニットは、MIME コンテンツの解析と並行して、電子メール フィルタリング禁止単語チェックおよび DLP スキャンを適用する前に、電子メール メッセージの文字セット フィールドに応じて、メールのコンテンツを UTF-8 エンコーディングに変換します。

HTTP get ページの場合、FortiGate ユニットは、Web コンテンツ フィルタリングおよび DLP スキャンを適用する前に、そのページに指定される文字セットに応じて、Web コンテンツを UTF-8 エンコーディングに変換します。

HTTP post ページの場合、HTTP post では文字セットが必ずしも正確に表示されないことから、以下の CLI コマンドを使用して 5 種類までの文字セット エンコーディングを指定できます。

```
config firewall profile
  edit <profile_name>
    set http-post-lang <charset1> [<charset2> ... <charset5>]
  end
```

FortiGate ユニットは、HTTP post ページを指定された文字セットごとに強制的に UTF-8 に変換します。各変換後に、FortiGate ユニットにより Web フィルタリングおよび DLP スキャンが、変換されたページのコンテンツに適用されます。

利用可能な文字セットを表示するには、プロテクション プロファイルの編集シェルから、`set http-post-lang ?` を入力します。複数の文字セット名は、スペースで区切ります。最大 5 種類の文字セット名まで追加できます。

URL フィルタ

特定の URL へのアクセスを許可またはブロックするには、それらの URL を URL フィルタ リストに追加します。URL を許可またはブロックするには、テキストや正規表現 (またはワイルドカード文字) を使用してパターンを追加します。FortiGate ユニットは、指定された任意の URL またはパターンに一致する Web ページを許可またはブロックし、差し替えメッセージを表示します。

複数の URL フィルタ リストを追加し、その中から各プロファイルに最適な URL フィルタ リストを選択できます。

以下を追加することにより、URL をブロックまたは除外できます。

- 完全な URL
- IP アドレス
- すべてのサブドメインを許可またはブロックするための部分的な URL

URL フィルタ リスト内のエントリの最大数は 5,000 です。

URL フィルタを設定するには、*[UTM]*、*[Web Filter]*、*[URL Filter]* の順に選択します。

注記: URL ブロッキングでは、ユーザが Web ブラウザを使用してアクセスできる他のサービスへのアクセスはブロックされません。たとえば、URL ブロッキングでは、`ftp://ftp.example.com` へのアクセスはブロックされません。FTP 接続を拒否するには、代わりにファイアウォール ポリシーを使用します。

[URL Filter] ページ

このページには、作成済みの URL フィルタが一覧表示されます。このページでは、URL フィルタを編集、削除、または新規作成できます。

[Create New]	[Create New] を選択すると、[New List] ページの画面に自動的に移動します。[New List] ページには、[名前] フィールドおよび [コメント] フィールドがあり、[URL Filter Settings] ページを表示するにはリストの名前を入力する必要があります。
[名前]	使用可能な URL フィルタ リスト。
[# Entries]	各 URL フィルタ リスト内の URL パターンの数。
[コメント]	オプションで記述される URL フィルタ リストの説明。
削除アイコン	カタログからこの URL フィルタ リストを削除する場合に選択します。削除アイコンは、この URL フィルタ リストがどのプロテクション プロファイルでも選択されていない場合にのみ使用できます。
編集アイコン	URL フィルタ リスト、リスト名、またはリストのコメントを編集する場合に選択します。

[URL Filter Settings] ページ

このページには、URL フィルタを構成する URL の設定が含まれており、作成済みの URL が一覧表示されます。[New List] ページからこのページの画面に、自動的に移動します。ファイル フィルタを編集する場合は、画面がこのページに自動的に移動します。

[名前]	既存の URL フィルタ設定を編集しフィルタ名を変更する場合は、このフィールドに新しい名前を入力します。変更を保存するには、必ず [OK] を選択します。
[コメント]	既存の URL フィルタ設定を編集し、説明内容を変更する場合は、このフィールドに変更を入力します。変更を保存するには、必ず [OK] を選択します。
[OK]	リストの変更内容を保存するとき選択します。
[Create New]	URL フィルタ リストに URL を追加する場合に選択します。[Create New] を選択すると、以下が表示されます。
編集アイコン	設定を変更するとき選択します。
削除アイコン	リストからこのエントリを削除する場合に選択します。
[有効]	リスト中のフィルタを有効にする場合に選択します。
[無効]	リスト中のフィルタを無効にする場合に選択します。
移動アイコン	[Move URL Filter] ダイアログ ボックスを開き、リスト中で URL が表示される位置を設定するとき選択します。

[Remove All Entries]	リストからすべてのフィルタ エントリを削除する場合に選択します。

[New URL Filter] ページ

[URL]	URL を入力します。http:// を含めないでください。URL 形式の詳細については、381 ページの「URL 形式」を参照してください。
[Type]	ドロップ ダウン リストから、フィルタの種類 [Simple]、[Regex] (正規表現)、または [Wildcard] のいずれかを選択します。
[アクション]	FortiGate ユニットが実行するアクションを、[Allow]、[Exempt]、または [Block] から選択します。 許可に一致すると、その URL フィルタ リストのチェックは終了し、他の Web フィルタがチェックされます。 除外に一致すると、AVスキャンを含むそれ以降のチェックはすべて実行されません。 ブロックに一致すると、その URL はブロックされ、それ以降のチェックは実行されません。
[有効]	この URL を有効にする場合にオンにします。

ヒント : トップレベルのドメイン サフィックス (たとえば、前にピリオドが付かない "com") を入力すると、このサフィックスを含むすべての URL へのアクセスがブロックされます。

URL 形式

URL を URL フィルタ リストに追加するときは (380 ページの「URL フィルタ」を参照)、以下のルールに従います。

HTTPS を使用する場合に URL 形式を検出する方法

ユニットが SSL コンテンツ スキャンおよびインスペクションをサポートしない、または、*[Protocol Recognition]* の *[HTTPS content filtering mode]* に、Web コンテンツ プロファイルで *[URL filtering]* オプションを選択している場合は、`www.example.com` などのトップレベル ドメイン名を入力することでHTTPSトラフィックをフィルタ処理します。暗号化されたセッションの HTTPS URL フィルタリングは、SSL ネゴシエーション中にサーバ証明書から CN を抽出することによって機能します。CN には、アクセス中のサイトのドメイン名のみが含まれるので、暗号化された HTTPS セッションの Web フィルタリングはドメイン名によるフィルタ処理のみが可能です。

FortiGate ユニットが SSL コンテンツ スキャンおよびインスペクションをサポートし、[Deep Scan] を選択している場合は、HTTP トラフィックと同じ方法で HTTPS トラフィックをフィルタ処理できます。SSL コンテンツ スキャンおよびインスペクションの詳細については、『*FortiOS ハンドブック*』の「*UTM* 」の章を参照してください。

HTTP を使用する場合に URL 形式を検出する方法

アクションが [Exempt] に設定された URL に対しては、ウイルス スキャンが実行されません。ネットワーク上のユーザが、信頼できる Web サイトから FortiGate ユニットを介してファイルをダウンロードする場合は、この Web サイトの URL を [Exempt] のアクションで URL フィルタ リストに追加しておくことで、このURLからダウンロードされたファイルに対してFortiGate ユニットがウイルス スキャンを実行しないようにします。

- Web サイト上のすべてのページへのアクセスを制御するには、トップレベルの URL または IP アドレスを入力します。たとえば、`www.example.com` または `192.168.144.155` を入力すると、この Web サイトにあるすべてのページへのアクセスが制御されます。
- Web サイト上の特定のページへのアクセスを制御するには、トップレベルの URL に続けてそのパスとファイル名を入力します。たとえば、`www.example.com/news.html` または `192.168.144.155/news.html` を入力すると、この Web サイト上のニュース ページが制御されます。
- `example.com` で終わる URL を含むすべてのページへのアクセスを制御するには、フィルタ リストに `example.com` を追加します。たとえば、`example.com` を追加すると、`www.example.com`、`mail.example.com`、`www.finance.example.com` などへのアクセスが制御されます。

- テキストと正規表現（またはワイルドカード文字）を使用して作成されたパターンに一致するすべての URL へのアクセスを制御します。たとえば、example.* は、example.com、example.org、example.net などに一致します。

  FortiGate URL フィルタリングは、標準の正規表現をサポートします。

上書き

FortiGuard Web フィルタリングによってブロックされている Web サイトにアクセスする必要のあるユーザのために、FortiGuard Web フィルタリングの上書きを編集できます。Web フィルタ上書きの詳しい設定方法については、461 ページの「ユーザ グループからの動的な VPN クライアント IP アドレス割り当て」を参照してください。

ブロックされているサイトにユーザがアクセスしようとしたとき、そのユーザのユーザ グループで上書きが有効になっていると、そのユーザを認証フォームに導くリンクがブロックされているページに表示されます。ユーザはユーザ名およびパスワードを入力し、その Web サイトの FortiGuard Web フィルタリングを解除できます。

上書きを編集するには、*[UTM]*、*[Web Filter]*、*[Override]* の順に選択します。

[Override] ページ

このページには、デフォルトの 2 種類の上書きである、「管理上書き」および「ユーザ上書き」が表示されます。このページでは、上書きの編集、およびデフォルトの上書きに新たな上書きを追加できます。上書きの新規作成には対応していません。

編集アイコン	上書きの設定を変更するとき選択します。
[名前]	上書き設定の名前。
[Administrative Overrides]	管理上書き。これらを編集するか、または管理上書きを追加できます。詳しくは、382 ページの「管理上書き」を参照してください。
[User Overrides]	ユーザ上書き。これらのユーザ上書きを編集できます。詳しくは、383 ページの「ユーザ上書き」を参照してください。

管理上書き

管理上書きルールを編集することにより、ディレクトリ、ドメイン名、またはカテゴリに基づいて、ブロックされている Web サイトへのアクセスを許可できます。また、[Administrative Overrides] グループ内に新しい上書きを作成できます。

管理上書きは、メインの設定によってバックアップされ、システムにより管理されます。管理上書きは有効期限を経過しても抹消されず、有効期限の日付を延長することで上書きのエントリを再利用できます。管理上書きを作成するには、CLI および Web ベース マネージャの双方を利用できます。

管理上書きにアクセスするには、*[UTM]*、*[Web Filter]*、*[Override]* の順に選択し、[Override] ページを表示します。管理上書きリストのルールを編集または新規ルールを作成する場合は、[Override] ページの [Administrative Overrides] にアクセスします。

[Administrative Overrides] ページ

このページには、管理上書きに作成されているルールが一覧表示されます。このページでは、上書きを編集、削除、または新規作成できます。リストでは、個別の上書きを無効にするか、またはリストの上書きすべてを削除できます。

[Create New]	このリストに新しい上書きルールを追加する場合に選択します。[User Overrides] では利用できません。
編集アイコン	管理上書きの設定を編集するとき選択します。
削除アイコン	管理上書きのルールを削除するとき選択します。
[有効]	管理上書きのルールを有効にするとき選択します。
[無効]	管理上書きのルールを無効にするとき選択します。
[Remove All Entries]	リストからすべての管理上書きエントリを削除する場合に選択します。
#	リスト中に表示される上書きの順序を示す番号。
[有効]	リスト中のルールの順序を示す番号。

[URL/Category]	このルールが適用される URL またはカテゴリ。
[Scope]	このルールを使用できるユーザまたはユーザ グループ。
[Off-site URLs]	緑色のチェック マークは [Off-site URL] オプションが [Allow] に設定されていることを示し、この場合、Web ページの上書きによりオフサイトのドメインからコンテンツが表示されます。灰色のクロス マークは [Off-site URL] オプションが [Block] に設定されていることを示し、この場合、Web ページの上書きによりオフサイトのドメインからコンテンツが表示されません。詳細については、382 ページの「管理上書き」を参照してください。
[Initiator]	この上書きルールの作成者。
[Expiry Date]	この上書きルールの有効期限日。
ページ コントロール	ページ コントロールを使用し、ページに含まれるリストを表示します。

[New Override Rule] ページ

[Type]	*[Directory]*、正確な *[Domain]*、または [Categories] を選択します。[Categories] を選択すると、Web フィルタリングのカテゴリ オプションが分類 (Classification) とともに表示されます。
[URL]	Web サイトの URL またはドメイン名を入力します。
[Scope]	*[User]*、*[User Group]*、*[IP]* または *[Profile]* のいずれかを選択します。選択したオプションに応じて、*[Scope]* の下に異なるオプションが表示されます。
[User Group]	ドロップダウン リストから、ユーザ グループを選択します。ユーザ グループは、FortiGuard Web フィルタリングを設定する前に必ず設定します。詳細については、457 ページの「ユーザ グループ」を参照してください。
[User]	*[Scope]* で選択したユーザの名前を入力します。
[IP]	このフィールドに IP アドレスを入力します。この設定は IPv4 アドレス用です。
[IPv6]	このフィールドに IPv6 アドレスを入力します。
[Off-site URLs]	このオプションは、上書き Web ページが、ブロックされているオフサイト URL から画像などのコンテンツを表示するかどうかを定義します。 たとえば、すべての FortiGuard カテゴリがブロックされており、別のドメインから画像が提供されているサイトを閲覧するとします。そのサイトのディレクトリ上書きを作成し、そのページを表示できます。[Off-site URL] を [Deny] に設定する場合は、そのページの全画像は既存の上書きルールが適用されない別のドメインから転送されているので、画像は崩れて表示されます。[Off-site URL] を [Allow] に設定する場合は、そのページの画像は正常に表示されます。 そのページ上書きの対象に含まれるユーザのみが、一時的な上書きによる画像を表示できます。新しい上書きルールを作成する必要なく、ユーザは画像の元となるそのサイトのどのページも (ページが画像自体と同じディレクトリから提供されていない限り) 表示できなくなります。
[Override End Time]	利用可能な時間オプションを使用し、上書きルールが終了する時点を指定します。

ユーザ上書き

ユーザ認証によりユーザ上書きが有効になると、ユーザ上書きリストにエントリが追加されます。ユーザ上書きは、FortiGate 設定の一部としてバックアップされません。また、有効期限が経過すると消去されます。管理者は、ユーザ上書きを表示および削除できます。

ユーザ上書きにアクセスするには、*[UTM]*、*[Web Filter]*、*[Override]* の順に選択し、[Override] ページを表示します。[Override] ページのリストに含まれるエントリは、編集できません。

[User Override] ページ

このページには、認証ユーザが一覧表示されます。リストに新規上書きを追加できません。

削除アイコン	ユーザ上書き設定を削除するとき選択します。
[有効]	ユーザ上書きを有効にするとき選択します。

[無効]	ユーザ上書きを無効にするとき選択します。
[Remove All Entries]	リストからすべてのユーザ上書きを削除する場合に選択します。
#	リスト中の項目の順序を示す番号。
[有効]	ユーザ上書きが有効の場合、緑色のチェック マークが表示されます。ユーザ上書きが無効の場合、灰色のクロス マークが表示されます。
[URL/Category]	この上書きが適用される URL またはカテゴリ。
[Scope]	この上書きを使用できるユーザまたはユーザ グループ。
[Off-site URLs]	緑色のチェック マークは [Off-site URL] オプションが [Allow] に設定されていることを示し、この場合、Web ページの上書きによりオフサイトのドメインによるコンテンツが表示されます。灰色のクロス マークは [Off-site URL] オプションが [Block] に設定されていることを示し、この場合、Web ページの上書きによりオフサイトのドメインによるコンテンツが表示されません。詳細については、382 ページの「管理上書き」を参照してください。
[Initiator]	この上書きルールの作成者。
[Expiry Date]	この上書きルールの有効期限日。

ローカル カテゴリ

ユーザがプロファイル単位に URL のグループをブロックできるようにするために、ユーザ定義のカテゴリを作成できます。ここで定義されたカテゴリは、プロテクション プロファイルの設定時にグローバル URL カテゴリ リストに表示されます。ユーザは URL を、これらのローカル カテゴリに基づいて評価できます。

ユーザは、ユーザ定義のカテゴリを作成した後、そのカテゴリに属する URL を指定できます。これにより、ユーザは Web サイトのグループをプロファイル単位でブロックできるようになります。グローバル URL リストの中には、評価が、関連するカテゴリとともに含まれており、URL ブロック リストの処理と同じ方法で照合されます。

これらのローカル評価は FortiGuard サーバの評価より優先され、レポート内では "Local Category" と表示されます。

ローカル カテゴリを設定するには、*[UTM]*、*[Web Filter]*、*[Local Categories]* の順に選択します。

[Local Cateogries] ページ

このページには、作成済みのローカル カテゴリが一覧表示されます。[Create New] フィールドにローカル カテゴリ名を入力すると、ローカル カテゴリが作成されます。ローカル カテゴリは編集できず、リストからの削除のみ可能です。

[Create New]	ローカル カテゴリの名前をこのフィールドに入力し、[Create New] を選択します。.
削除アイコン	リストからローカル カテゴリを削除する場合に選択します。
[Local categories]	この URL が属しているカテゴリまたは分類。この URL が複数のカテゴリまたは分類で評価されている場合は、後続のドットが表示されます。*[Category Filter]* ダイアログ ボックスを開くには、灰色のじょうごアイコンを選択します。リストがフィルタ処理されると、じょうごアイコンが緑色で表示されます。

注記：FortiGate ユニット上でバーチャル ドメインが有効に設定されている場合、Web フィルタリング機能はグローバルに設定されます。これらの機能にアクセスするには、メイン メニューから *[Global Configuration]* を選択します。

ローカル評価

ユーザ定義のカテゴリを設定し、そのカテゴリに属する URL を指定できます。これにより、ユーザは Web サイトのグループをプロファイル単位でブロックできるようになります。グローバル URL リストの中には、評価が、関連するカテゴリとともに含まれており、URL ブロック リストの処理と同じ方法で照合されます。

ローカル評価を設定するには、*[UTM]*、*[Web Filter]*、*[Local Ratings]* の順に選択します。

[Local Ratings] ページ
このページには、作成済みのローカル評価が一覧表示されます。このページでは、ローカル評価の編集、削除、または新規作成、ローカル評価の有効 / 無効の設定が可能です。また、ページからすべてのローカル評価を削除できます。

[Create New]	ローカル評価を新規作成するとき選択します。
[Search]	リストからローカル評価を検索するための語句または名前を入力します。[Go] を選択して、検索を開始します。
編集アイコン	ローカル評価の設定を変更するとき選択します。
削除アイコン	リストからローカル評価を削除する場合に選択します。
[有効]	ローカル評価を有効にするとき選択します。
[無効]	ローカル評価を無効にするとき選択します。
全エントリ削除アイコン	リストからすべてのローカル評価を削除する場合に選択します。
#	リスト中の項目の順序を示す番号。
[有効]	ローカル評価が有効の場合、緑色のチェック マークが表示されます。ローカル評価が無効の場合、灰色のクロス マークが表示されます。
[URL]	ローカル評価の URL アドレス。
[Category]	ローカル評価に選択されているカテゴリ。

[New Local Rating] ページ
このページでは、[Category Rating] および [Classification Rating] に属する URL アドレスを設定できます。ローカル評価を編集するとき、同じ設定を含む [Edit Local Rating] ページの画面に自動的に移動します。

[URL]	URL アドレスを入力します。
[Category Rating]	URL の評価を選択します。
[Classification Rating]	分類 (Classification) を追加するとき選択します。

レポート

[Reports] メニューは、ローカル ディスクを備える FortiGate モデルでのみ表示されます。[Reports] メニューを表示するには、*[UTM]*、*[Web Filtering]* の順に選択します。メニューから、Web フィルタリング プロファイルに基づくレポートを使用できます。情報は、テキストおよび円グラフの形式で生成されます。FortiGate ユニットには、Web ページの許可、ブロック、および監視に関する統計が、カテゴリごとに保持されています。所定の時間数または日数に応じたレポートの表示、またはアクティビティ全体の表示が可能です。

レポートを作成するには、*[UTM]*、*[Web Filtering]*、*[Reports]* の順に選択しますが、レポート作成の前に Web フィルタリング プロファイル (1 つまたは複数) を必ず設定しておきます。

[Reports] ページ
このページでは、作成したレポートの設定が可能です。レポートに含まれる情報は、Web フィルタ プロファイルから取得します。レポートを作成する前に、Web フィルタ プロファイルを設定する必要があります。

[Web Filter Profile]	レポートのベースとなる Web フィルタ プロファイルを選択して表示します。
[Clear report data]	現在表示されているレポートから、すべてのデータを削除します。
[Report Type]	レポートの期間を選択します。[Hour]、[Day]、または [All] から選択します。
[Report Range]	レポートの時間の範囲 (24 時間表示) または日にちの範囲 (6 日前から今日まで) を選択します。たとえば、[Hour] レポートの種類で範囲が 13 ～ 16 の場合は、今日の午後 1 時から午後 4 時までのカテゴリ ブロック レポートになります。[Day] レポートの種類で範囲が 0 ～ 3 の場合は、3 日前から今日までのカテゴリ ブロック レポートになります。
[Get Report]	レポートを生成する場合に選択します。

生成されるレポートには、[Reports] ページの円グラフの下に表示される、以下のカラムが含まれます。

[Category]	この統計が生成されたカテゴリ。
[Allowed]	選択された期間にアクセスされた、許可された Web アドレスの数。

[Blocked]	選択された期間にアクセスされた、ブロックされた Web アドレスの数。
[Monitored]	選択された期間にアクセスされた、監視された Web アドレスの数。

電子メール フィルタ

ここでは、IMAP、POP3、および SMTP 電子メールの FortiGate 電子メール フィルタリングについて説明します。FortiGate ユニットが SSL コンテンツ スキャンおよびインスペクションをサポートする場合は、IMAPS、POP3S、SMTPS 電子メール トラフィックの電子メール フィルタリングを設定できます。SSL コンテンツ スキャンおよびインスペクションの詳細については、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとに電子メール フィルタリングを個別に設定します。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

FortiGate ユニットの電子メール フィルタ機能を設定し、既知のスパム サーバまたは疑わしいスパム サーバからのスパム メッセージを特定することにより、迷惑メールに対処できます。

FortiGuard Antispam Service により、送信者 IP 評価データベースおよびスパム シグネチャ データベースの双方とともに、洗練されたスパム フィルタリング ツールを利用し、幅広いスパム メッセージを検出してブロックできます。FortiGuard 電子メール フィルタリング プロファイルの設定を使用することにより、IP アドレス チェック、URL チェック、電子メール チェックサム チェック、スパム提出を有効に設定できます。IP 評価およびスパム シグネチャの両データベースは、グローバルな FDN (FortiGuard Distribution Network) により、継続的にアップデートされます。

[FortiGuard Center] の [FortiGuard Antispam Service] ページから IP およびシグネチャ検索を使用し、IP アドレスが FortiGuard アンチスパム IP 評価データベースでブラックリストに登録されているかどうか、あるいは URL または電子メール アドレスがシグネチャ データベースにあるかどうかをチェックできます。

この項では、電子メール フィルタリング設定の基礎について説明します。詳細については、『*FortiGate UTM ユーザ ガイド*』を参照してください。

電子メール フィルタリングの順序

FortiGate 電子メール フィルタリングでは、各種のフィルタリング手法を使用しています。FortiGate ユニットがこれらのフィルタを使用する順序は、使用されるメール プロトコルに応じて異なります。

サーバへのクエリと応答が必要なフィルタ (FortiGuard Antispam サービスと DNSBL/ORDBL) は、同時に実行されます。遅延を回避するために、クエリは、他のフィルタが実行されている間に送信されます。スパム アクションをトリガする最初の応答は、その応答が受信されるとすぐに有効になります。

一致や問題が発見されない場合、各フィルタは電子メールを次のフィルタに渡します。フィルタ内のアクションが [Mark as Spam] である場合、FortiGate ユニットは、プロテクション プロファイル内の設定に従って、その電子メールにスパムのタグを付けます。

SMTP および SMTPS では、アクションが [Discard] である場合、電子メール メッセージは破棄または削除されます。

フィルタ内のアクションが [Mark as Clear] である場合、その電子メールは残りのすべてのフィルタから除外されます。フィルタ内のアクションが [Mark as Reject] である場合、その電子メール セッションは破棄されます。拒否された SMTP または SMTPS 電子メール メッセージは、設定可能な差し替えメッセージに置き換えられます。

SMTP および SMTPS 電子メール フィルタリングの順序

SMTPS 電子メール フィルタリングは、SSL コンテンツ スキャンおよびインスペクションをサポートする FortiGate ユニットのみで使用できます。SSL コンテンツ スキャンおよびインスペクションの詳細については、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。

1 ラスト ホップ IP に対する IP アドレス BWL チェック
2 ラスト ホップ IP に対する DNSBL/ORDBL チェック、ラスト ホップ IP に対する FortiGuard 電子メール フィルタリング IP アドレス チェック、HELO DNS 参照
3 MIME ヘッダ チェック、電子メール アドレス BWL チェック
4 電子メールの件名に対する禁止単語チェック
5 IP アドレス BWL チェック (″Received″ ヘッダから取得された IP に対して)
6 電子メールの本文に対する禁止単語チェック
7 返信電子メール DNS チェック、FortiGuard Antispam 電子メール チェックサム チェック、FortiGuard 電子メール フィルタリング URL チェック、ヘッダから取得されたパブリック IP に対する DNSBL/ORDBL チェック

IMAP、POP3、IMAPS、および POP3S 電子メール フィルタリングの順序

IMAPS および POP3S 電子メール フィルタリングは、SSL コンテンツ スキャンおよびインスペクションをサポートする FortiGate ユニットのみで使用できます。SSL コンテンツ スキャンおよびインスペクションの詳細については、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。

1 MIME ヘッダ チェック、電子メール アドレス BWL チェック
2 電子メールの件名に対する禁止単語チェック
3 IP BWL チェック
4 電子メールの本文に対する禁止単語チェック
5 返信電子メール DNS チェック、FortiGuard 電子メール フィルタリング電子メール チェックサム チェック、FortiGuard 電子メール フィルタリング URL チェック、DNSBL/ORDBL チェック

電子メール アドレス

プロファイル

[Profile] メニューでは、ファイアウォール ポリシーに適用するための電子メール フィルタ プロファイルを設定できます。プロファイルに含まれる特定の情報は、ポリシーに基づきトラフィックがどのように検証され、検証に基づいてどのようなアクションが実行されるかを定義します。

電子メール フィルタ プロファイルを設定するには、*[UTM]*、*[Email Filter]*、*[Profile]* の順に選択します。

[Profile] ページ

このページには、作成済みの電子メール フィルタ プロファイルが一覧表示されます。このページでは、電子メール フィルタ プロファイルを編集、削除、または新規作成できます。

[Create New]	新しい電子メール フィルタ プロファイルを作成するとき選択します。
編集アイコン	電子メール フィルタリング プロファイルの設定を編集するとき選択します。
削除アイコン	電子メール フィルタ プロファイルを削除するとき選択します。
[名前]	電子メール フィルタ プロファイルの名前。
[コメント]	電子メール フィルタ プロファイルの説明。この設定は、オプションです。

[New Email Filter Profile] ページ

このページでは、複数の電子メール フィルタ プロファイルを設定できます。電子メール フィルタ プロファイルを編集する場合は、[Edit Email Filter Profile] ページの画面に自動的に移動します。

[名前]	電子メール フィルタ プロファイルの名前を入力します。

[コメント]	電子メール フィルタ プロファイルの説明を入力します (入力はオプションです)。
[Enable logging]	電子メール フィルタ プロファイルのロギングを有効にするとき選択します。
[FortiGuard Email Filtering]	このオプションを利用するには、設定するプロトコル列名の横にあるチェック ボックスをオンにする必要があります。たとえば、IMAP の横にあるチェック ボックスをオンにすると、IMAP で利用可能なオプションにアクセスできます。
[IP Address Check]	FortiGuard IP アドレスのブラック リストのチェックを有効にするとき選択します。IP アドレス チェックが有効でない場合は、FortiGate ユニットはその種類のトラフィックを検証しません。 **注記**: チェック不要なトラフィックの種類を無効にすると、システムのリソースを節約できます。
[URL Check]	FortiGuard URLブラック リストのチェックを有効にするとき選択します。
[Email Checksum Check]	電子メール メッセージ チェックサム チェックを有効にするとき選択します。
[Spam submission]	FortiGuard 電子メール フィルタリングによってスパムとしてマークされたすべての電子メール メッセージの本文に、スパム提供メッセージとリンクを追加する場合に選択します。受信者が電子メール メッセージをスパムではないと判断した場合は、本文メッセージに含まれるリンクを使用して語検知であることを通知できます。スパム提供メッセージの内容を変更するには、[Replacement Messages] ページを表示し、メッセージ内容をカスタマイズします。詳細については、159 ページの「スパム差し替えメッセージ」を参照してください。
[IP address BWL check]	[Options] カラムで、ドロップダウン リストから IP アドレス ブラック / ホワイト リストを選択します。
[HELO DNS Lookup]	SMTP 電子メール メッセージの送信元ドメイン名を (SMTP HELO コマンドから) 検索するとき選択します。
[E-mail Address DNS Check]	電子メール アドレスの DNS を検索するとき選択します。
[Return E-mail DNS Check]	返信先または返信元のアドレスで指定されたドメインに A または MX レコードが含まれているかどうかをチェックする場合に選択します。
[Banned Word Check]	選択されている電子メール フィルタ禁止単語リストの単語または語句とメール メッセージ内容の照合に基づいて、電子メール メッセージをブロックする場合に選択します。
[Spam Action]	FortiGate ユニットによりスパムとして識別された電子メールにタグ付けするか、または電子メールを破棄するかを選択します。[Tagging] を選択すると、[Tag Format] フィールドのテキストを、スパムとして識別された電子メールの件名行またはヘッダに追加します。 **注記**: アンチウイルス プロファイルで SMTP および SMTPS のウイルス スキャンを有効にする場合、スプライス モード (別名ストリーミング モード) が自動的に有効に設定されます。スプライス モードでスキャンを行う場合、FortiGate ユニットによって、トラフィックのスキャンおよびトラフィックを送信先にストリーミングする処理が同時に行われ、ウイルスが検出されると送信先へのストリーミングが中止されます。スプライス設定の詳細については、『*FortiGate CLI リファレンス*』の、`config firewall profile` コマンドの各プロトコルのスプライス オプションを参照してください。 SMTP のスプライス動作の詳細については、Knowledge Base の、『*FortiGate プロキシ スプライスおよびクライアント コンフォーティング テクニカル ノート*』を参照してください。 SMTP のウイルス スキャンを有効にすると、FortiGate ユニットはウイルスが検出された場合にスパム メールの破棄のみを実行できます。[Discarding] を選択すると、接続をただちに中断します。ウイルス スキャンを有効に設定しない場合、SMTP スパムにタグ付けするかまたは破棄するかを選択できます。

[Tag Location]	スパムとして識別された電子メールの件名または MIME ヘッダにタグを追加する場合に選択します。 件名行へのタグ追加を選択すると、FortiGate ユニットにより、タグを含む件名行のすべてが UTF-8 形式に変換されます。これによって、複数のエンコーディングを用いる件名を正しく表示できない電子メール クライアントで、表示を改善することができます。件名行を UTF-8 に変換しない設定の詳細については、『*FortiGate CLI リファレンス*』の「システム設定」の章を参照してください。 MIME ヘッダにタグを追加するには、プロトコルごとに (IMAP、SMTP、および POP3) CLI から `spamhdrcheck` を有効にする必要があります。詳細については、『*FortiGate CLI リファレンス*』の `profile` を参照してください。
[Tag Format]	スパムとして識別された電子メールにタグとして付加する語句を入力します。タグを入力するとき、FortiGate ユニットの現在設定されている管理者言語と同じ言語を使用します。他のエンコーディングを使用するタグ テキストは、許可されない場合があります。たとえば、日本語の文字を使用してスパム タグを入力する場合、まず管理者言語が日本語に設定されていることを確認します。管理者言語が日本語以外の設定のままでは、FortiGate ユニットで日本語文字のスパム タグを設定できません。言語変更の詳しい方法については、27 ページの「Web ベース マネージャの言語の変更」を参照してください。 タグの長さは、64 バイトに限られます。64 バイトに含まれる文字数は、FortiGate の管理者言語の設定に応じたテキスト エンコーディングにより異なります。

禁止単語

特定の単語またはパターンを含む電子メール メッセージをブロックすることによって、スパムを制御します。単語、語句、ワイルドカード、Perl 正規表現を追加し、電子メール メッセージのコンテンツと照合できます。ワイルドカードおよび Perl 正規表現の詳細については、393 ページの「ワイルドカードおよび Perl 正規表現の使用」を参照してください。

FortiGate ユニットによって、禁止単語リストに対する電子メール メッセージのチェックが行われます。FortiGate ユニットでは、禁止単語を件名、本文、または双方に含む電子メール メッセージの分類が可能です。メッセージに現れる各禁止単語のスコア値が加算され、その合計がプロテクション プロファイルで設定されているしきい値を超えると、FortiGate ユニットはプロファイルの設定に基づいてメッセージを処理します。ある単語がメッセージに複数回現れた場合でも、そのパターンのスコアは 1 回だけ適用されます。

禁止単語を設定するには、*[UTM]*、*[Email Filter]*、*[Banned Word]* の順に選択します。

[Banned Word] ページ

このページには、作成済みの禁止単語リストが表示されます。このページでは、禁止単語を編集、削除、または新規作成できます。

[Create New]	[Create New] を選択すると、[New List] ページの画面に自動的に移動します。[New List] ページには、[名前] フィールドおよび [コメント] フィールドがあり、[Banned Word Settings] ページを表示するにはリストの名前を入力する必要があります。
[名前]	使用可能な電子メール フィルタ禁止単語リスト。
[# Entries]	各禁止単語リスト内のエントリの数。
[コメント]	オプションで記述される各禁止単語リストの説明。
削除アイコン	カタログから禁止単語リストを削除します。削除アイコンは、禁止単語リストがどの電子メール フィルタ プロファイルでも選択されていない場合のみ使用できます。
編集アイコン	禁止単語リスト、リスト名、またはリストのコメントを編集します。

[Banned Word Settings] ページ

このページでは、FortiGate ユニットにより禁止と判断される単語パターンまたは単語を設定できます。[Banned Word] ページに表示される禁止単語リストは、これらの単語および単語パターンにより構成されています。禁止単語を編集する場合は、[Banned Word Settings] ページの画面に自動的に移動します。

[名前]	既存の禁止単語リストを編集し、リスト名を変更する場合は、このフィールドに新しい名前を入力します。変更を保存するには、必ず [OK] を選択します。
[コメント]	既存の禁止単語リストを編集し、説明内容を変更する場合は、このフィールドに新たな説明を入力します。変更を保存するには、必ず [OK] を選択します。

[OK]	リストの変更を保存するために選択します。
[Create New]	禁止単語リストに単語または語句を追加する場合に選択します。[Create New] を選択すると、以下が表示されます。
[有効]	禁止単語が有効の場合、緑色のチェック マークが表示されます。
[Pattern]	禁止単語のリスト。リスト内のすべての禁止単語を有効にするには、このチェック ボックスをオンにします。
[パターンタイプ]	禁止単語リストの入力で使用されるパターンの種類。[Wildcard] または [Regular Expression] から選択します。詳細については、393 ページの「ワイルドカードおよび Perl 正規表現の使用」を参照してください。
[Language]	禁止単語が属する文字セット。
[Where]	FortiGate ユニットにより禁止単語が検索される、*[Subject]*、*[Body]*、または *[All]* のいずれかの場所。
[Score]	この禁止単語に適用される重み付けの数値。電子メール メッセージに現れるすべての一致単語のスコア値を加算し、その合計がプロテクション プロファイルに設定されている禁止単語チェック値を超える場合、そのメールは、電子メール フィルタ プロファイルの [Spam Action] の設定、*[Discard]* または *[Tagged]* に応じて処理されます。ある禁止単語が電子メールの Web ページに複数回現れた場合でも、その単語のスコアは 1 回だけカウントされます。
編集アイコン	禁止単語の設定を変更するとき選択します。
削除アイコン	リストから禁止単語を削除するとき選択します。
[有効]	禁止単語を有効にするときオンにします。
[無効]	禁止単語を無効にするときオンにします。
[Remove All Entries]	リストからすべての禁止単語エントリを削除するとき選択します。
ページ コントロール	ページ コントロールを使用し、[Banned Word] メニューに含まれる情報を表示します。

[Add Banned Word] ページ

[Pattern]	禁止単語パターンを入力します。 パターンは、単語の一部、単語全体、または語句が可能です。1 つのパターンとして複数の単語を入力すると、1 つの語句として扱われます。語句が一致するには、その語句が入力したとおりに現れる必要があります。ワイルドカードまたは正規表現を使用し、パターンを複数の単語または語句と一致させることもできます。
[パターンタイプ]	禁止単語のパターンの種類を選択します。[Wildcard] または [Regular Expression] から選択します。詳細については、393 ページの「ワイルドカードおよび Perl 正規表現の使用」を参照してください。
[Language]	禁止単語の文字セットを選択します。
[Where]	FortiGate ユニットが禁止単語を検索する場所を、[Subject]、[Body]、または [All] から選択します。
[Score]	このパターンのスコア値を入力します。 プロファイルに追加される禁止単語リストの各エントリには、スコアが含まれています。電子メール メッセージが禁止単語リストのエントリと一致する場合は、スコアが記録されます。電子メール メッセージが複数のエントリと一致する場合は、そのメール メッセージのスコアは増加します。電子メール メッセージのスコア合計が、しきい値以上の場合は、メッセージはスパムと判断され、プロファイルで設定される [Spam Action] の設定に応じて処理されます。

注記： 禁止単語では、Perl 正規表現パターンは大文字と小文字が区別されます。単語または語句の大文字と小文字が区別されないようにするには、正規表現の `/i` を使用します。たとえば、
`/bad language/i` を指定すると、文字の大小にかかわらず、`bad language` というフレーズであればすべてブロックされます。ワイルドカード パターンでは、文字の大小は区別されません。

IP アドレス

IP アドレス ブラック / ホワイト リストおよび電子メール アドレス ブラック / ホワイト リストを追加して、電子メールをフィルタ処理できます。IP アドレス リスト チェックを実行する場合、FortiGate ユニットは、メッセージの送信者の IP アドレスを IP アドレス リストに対して順番に比較します。電子メール リスト チェックを実行する場合、FortiGate ユニットは、メッセージの送信者の電子メール アドレスを電子メール アドレス リストに対して順番に比較します。一致が見つかった場合は、その IP アドレスまたは電子メール アドレスに関連付けられたアクションが実行されます。一致が見つからない場合、そのメッセージは次の有効な電子メール フィルタに渡されます。

複数の IP アドレス リストを追加し、後から電子メール フィルタ プロファイルごとに最適なリストを選択できます。

特定の IP アドレスからの電子メールをフィルタ処理するように、FortiGate ユニットを設定します。FortiGate ユニットは、送信者の IP アドレスをチェック リストに対して順番に比較します。各 IP アドレスを、[Mark as Clear]、[Mark as Spam]、または [Mark as Reject] としてマークします。単一の IP アドレスをフィルタ処理するか、またはアドレスとマスクを設定することでネットワーク レベルで複数のアドレスをフィルタ処理します。

IP アドレス リストを作成した後、IP アドレスをリストに追加できます。

IP アドレス、または IP アドレスとマスクのペアを、次の形式で入力します。

- x.x.x.x、たとえば 192.168.69.100
- x.x.x.x/x.x.x.x、たとえば 192.168.69.100/255.255.255.0
- x.x.x.x/x、たとえば 192.168.69.100/24

IP アドレス ブラック / ホワイト リストを設定するには、*[UTM]*、*[Email Filter]*、*[IP Address]* の順に選択します。

[IP Address] ページ

このページには、作成済みの IP アドレス リストが一覧表示されます。このページでは、IP アドレス リストを編集、削除、または新規作成できます。IP アドレス リストには複数の IP アドレスが含まれ、リストは [IP Address Settings] ページで設定します。

[Create New]	[Create New] を選択すると、[New List] ページの画面に自動的に移動します。[New List] ページには、[名前] フィールドおよび [コメント] フィールドがあり、[IPS Address Settings] ページを表示するにはリストの名前を入力する必要があります。
[名前]	IP アドレス リストの名前。
[# Entries]	各 IP アドレス リスト内のエントリの数。
[コメント]	オプションで記述される IP アドレス リストの説明。
削除アイコン	カタログから IP アドレス リストを削除します。削除アイコンは、IP アドレス リストがどのプロテクション プロファイルでも選択されていない場合にのみ使用できます。
編集アイコン	IP アドレス リスト、リスト名、またはリストのコメントを編集する場合に選択します。

[IP Address Settings] ページ

このページでは、複数の IP アドレスを設定し、それらをグループ化して IP アドレス リストを作成できます。作成したリストを、電子メール フィルタ プロファイルに適用します。[New List] ページからこのページの画面に、自動的に移動します。IP アドレスを編集する場合は、[IP Address Settings] ページの画面に自動的に移動します。

[名前]	既存の IP アドレス リストを編集し、リストの名前を変更する場合は、このフィールドに新しい名前を入力します。変更を保存するには、必ず [OK] を選択します。
[コメント]	既存の IP アドレス リストを編集し、説明内容を変更する場合は、このフィールドに新たな説明を入力します。変更を保存するには、必ず [OK] を選択します。
[OK]	リストの変更を保存するために選択します。
[Create New]	新規 IP アドレス リストを作成するとき選択します。
編集アイコン	アドレス情報を編集します。

削除アイコン	リストから IP アドレスを削除する場合に選択します。
[有効]	IP アドレスを有効にする場合に選択します。
[無効]	IP アドレスを無効にする場合に選択します。
移動アイコン	エントリをリスト内の別の位置に移動する場合に選択します。 ファイアウォール ポリシーは、リストを上から順に実行します。たとえば、Spam としての IP アドレス 192.168.100.1 および Clear としての IP アドレス 192.168.100.2 がリスト中にある場合、192.168.100.2 の上に 192.168.100.1 を置くことにより、192.168.100.1 を有効にする必要があります。
全エントリ削除アイコン	リストから IP アドレスをすべて削除する場合に選択します。

[Add IP Address] ページ

[IP/Netmask]	IP アドレスまたは IP アドレス / マスクのペアを入力します。
[アクション]	プロテクション プロファイルで設定されているスパム アクションを適用するための *[Mark as Spam]*、このフィルタと残りのスパム フィルタをバイパスするための *[Mark as Clear]*、またはこのセッションを破棄するための *[Mark as Reject]* (SMTP または SMTPS) のいずれかを選択します。
[有効]	アドレスを有効にするときオンにします。

電子メール アドレス

FortiGate ユニットによって、特定の送信者から送信される電子メール、またはドメイン (example.net など) から送信されるすべての電子メールを、フィルタ処理できます。電子メール アドレス リストを追加し、後からプロテクション プロファイルごとに最適なリストを選択できます。

電子メール アドレス リストを設定するには、*[UTM]*、*[Email Filter]*、*[Email アドレス]* の順に選択します。

[Email アドレス] ページ

このページには、作成済みの電子メール アドレス リストが一覧表示されます。このページでは、電子メール アドレス リストを編集、削除、または新規作成できます。

[Create New]	[Create New] を選択すると、[New List] ページの画面に自動的に移動します。[New List] ページには、[名前] フィールドおよび [コメント] フィールドがあり、[E-mail Address Settings] ページを表示するにはリストの名前を入力する必要があります。
[名前]	電子メール アドレス リストの名前。
[# Entries]	各電子メール アドレス リスト内のエントリの数。
[コメント]	オプションで記述される電子メール アドレス リストの説明。
削除アイコン	カタログから電子メール アドレス リストを削除します。削除アイコンは、電子メール アドレス リストがどのプロテクション プロファイルでも選択されていない場合にのみ使用できます。
編集アイコン	電子メール アドレス リスト、リスト名、またはリストのコメントを編集する場合に選択します。

[E-mail Address Settings] ページ

このページでは、複数の IP アドレスを設定し、それらをグループ化して IP アドレス リストを作成できます。作成したリストを、電子メール フィルタ プロファイルに適用します。[New List] ページからこのページの画面に、自動的に移動します。電子メール アドレスを編集する場合は、[E-mail Address Settings] ページの画面に自動的に移動します。

[名前]	既存の電子メール アドレス リストを編集し、リストの名前を変更する場合は、このフィールドに新しい名前を入力します。変更を保存するには、必ず [OK] を選択します。
[コメント]	既存の電子メール アドレス リストを編集し、説明内容を変更する場合は、このフィールドに新たな説明を入力します。変更を保存するには、必ず [OK] を選択します。
[OK]	リストの変更を保存するために選択します。
[Create New]	新しい電子メール アドレスを電子メール アドレス リストに追加します。[Create New] を選択すると、以下が表示されます。
編集アイコン	電子メール アドレスに変更を加えるとき選択します。

削除アイコン	電子メール アドレスを削除するとき選択します。
[有効]	電子メール アドレスを有効にするとき選択します。
[無効]	電子メール アドレスを無効にするとき選択します。
全エントリ削除アイコン	リストからすべてのエントリを削除します。
[有効]	電子メール アドレスが有効の場合、緑色のチェック マークが表示されます。電子メール アドレスが無効の場合、灰色のクロス マークが表示されます。
[Email-Address]	入力された電子メール アドレス。
[パターンタイプ]	その電子メール アドレスに対して選択されたパターンの種類。
[アクション]	その電子メール アドレスが検出されたとき実行されるアクション。
ページ コントロール	ページ コントロールを使用し、[E-mail Address Settings] ページのリストを表示します。
[Add E-Mail Address] ページ	
[Email アドレス]	電子メール アドレスを入力します。
[パターンタイプ]	パターンの種類として、*[Wildcard]* または *[Regular Expression]* のいずれかを選択します。詳細については、393 ページの「ワイルドカードおよび Perl 正規表現の使用」を参照してください。
[アクション]	プロテクション プロファイルで設定されているスパム アクションを適用するための *[Mark as Spam]*、またはこの電子メール フィルタと残りのフィルタをバイパスする *[Mark as Clear]* のいずれかを選択します。
[有効]	電子メール アドレスを有効にするときオンにします。

注記 : FortiGate ユニットでは、サーバのドメイン名に基づいて DNSBL または ORDBL サーバに接続するため、この名前を DNS サーバで検索できる必要があります。DNS 設定の詳細については、112 ページの「ネットワーク オプションの設定」を参照してください。

ワイルドカードおよび Perl 正規表現の使用

電子メール アドレス リスト、MIME ヘッダ リスト、および禁止単語リストのエントリには、ワイルドカードまたは Perl 正規表現を含めることができます。

Perl 正規表現の詳しい利用方法については、http://perldoc.perl.org/perlretut.html を参照してください。

正規表現とワイルドカードの一致パターンの比較

ワイルドカード文字は、1 つ以上の任意の文字を表す特殊文字です。最もよく使用されるワイルドカード文字には、一般に長さが文字数ゼロ以上の任意の文字列を表すアスタリスク (*) と、一般に任意の 1 文字を表す疑問符 (?) があります。

Perl 正規表現では、'.' の文字は任意の 1 文字を示します。ワイルドカードの一致パターンにある '?' の文字と同様です。そのため、次のようになります。

- fortinet.com は、fortinet.com だけでなく、fortinetacom、fortinetbcom、fortinetccom などにも一致します。

注記 : FortiGate CLI から疑問符 (?) 文字を正規表現に追加するには、Ctrl+V に続いて ? を入力します。、CLI からバックスラッシュ (\) 1 文字を正規表現に追加するには、それに先行するもう 1 つのバックスラッシュ文字を加える必要があります。たとえば、`fortinet\\.com` のように入力します。

'.' や '*' などの特殊文字に一致させるには、エスケープ文字の '¥' を使用します。たとえば、

- fortinet.com に一致させるには、正規表現を fortinet¥.com にする必要があります。

Perl 正規表現では、'*' は、任意の文字が 0 回以上一致するのではなく、その直前の文字が 0 回以上一致することを示します。たとえば、次のようになります。

- forti*.com は fortiiii.com に一致しますが、fortinet.com には一致しません。

任意の文字を 0 回以上一致させるには、'.*' を使用します。ここで、'.' は任意の文字を示し、'*' は 0 回以上一致することを示します。したがって、たとえば、ワイルドカードの一致パターン forti*.com は、fort.*¥.com にする必要があります。

単語境界

Perl 正規表現では、パターンに暗黙の単語境界は含まれていません。たとえば、正規表現の "test" は単語 "test" に一致するだけでなく、"atest"、"mytest"、"testimony"、"atestb" などの、"test" を含む任意の単語に一致します。"¥b" の表記は、単語境界を指定します。単語 "test" に正確に一致させるには、式を ¥btest¥b にする必要があります。

大文字と小文字の区別

Web フィルタや電子メール フィルタでは、正規表現のパターン一致は大文字と小文字が区別されます。単語または語句の大文字と小文字が区別されないようにするには、正規表現の /i を使用します。たとえば、/bad language/i を指定すると、文字の大小にかかわらず、"bad language" というフレーズであればすべてブロックされます。

Perl 正規表現形式

表 53 は、Perl 正規表現形式のいくつかの例を説明しています。

表 53: Perl 正規表現形式

表現	一致する文字列
abc	"abc" (文字シーケンスは正確に一致するが、文字列内のどの位置にあってもよい)
^abc	文字列の先頭にある "abc"
abc$	文字列の最後尾にある "abc"
a|b	"a" または "b" のどちらか
^abc|abc$	文字列の先頭または最後尾にある文字列 "abc"
ab{2,4}c	"a" の後に 2 ～ 4 個の "b"、その後に 1 個の "c"
ab{2,}c	"a" の後に少なくとも 2 個の "b"、その後に 1 個の "c"
ab*c	"a" の後に任意個数 (0 個以上) の "b"、その後に 1 個の "c"
ab+c	"a" の後に 1 個以上の "b"、その後に 1 個の "c"
ab?c	"a" の後にオプションの "b"、その後に 1 個の "c" (つまり、"abc" または "ac" のどちらか)
a.c	"a" の後に任意の 1 文字 (改行以外)、その後に 1 個の "c"
a¥.c	正確に "a.c"
[abc]	"a"、"b"、"c" のうちの任意の 1 つ
[Aa]bc	"Abc" または "abc" のどちらか
[abc]+	複数個の "a"、複数個の "b"、複数個の "c" から成る任意の (空以外の) 文字列 ("a"、"abba"、"acbabcacaa" など)
[^abc]+	"a"、"b"、"c" をまったく含まない任意の (空以外の) 文字列 ("defg" など)
\\d\d	任意の 2 桁 10 進数 (42 など)、¥d{2} と同じ
/i	パターンの大文字と小文字が区別されないようにします。たとえば、/bad language/i を指定すると、文字の大小にかかわらず、bad language というフレーズであればすべてブロックされます。
\w+	1 つの " 単語 ": 英数字とアンダーライン (アンダースコア) から記述される空以外のシーケンス (foo、12bar8、foo_1 など)
100¥s*mk	オプションで任意数の空白 (スペース、タブ、改行) によって分けられた文字列 "100" と "mk"
abc¥b	後に単語境界が存在する場合の "abc" (たとえば、"abc!" には含まれるが、"abcd" には含まれない)

表 53: Perl 正規表現形式 (続き)

perl¥B	後に単語境界が存在しない場合の "perl" (たとえば、"perlert" には含まれるが、"perl stuff" には含まれない)
¥x	正規表現パーサーに、直前にバックスラッシュ文字がなく、かつ文字クラスにも含まれていない空白を無視するように指示します。正規表現をいくつかの部分に分割して (若干) 読みやすくするために使用します。
/x	他のテキスト内に正規表現を追加するために使用されます。パターン内の最初の文字がフォワードスラッシュ '/' である場合、その '/' は区切り記号として処理されます。このパターンには、2 つ目の '/' が含まれている必要があります。'/' の間にあるパターンは正規表現と見なされ、2 つ目の '/' の後の任意の文字は正規表現のオプション ('i'、'x'、その他) のリストとして解析されます。2 つ目の '/' がないと、エラーが発生します。正規表現では、前や後に置かれているスペースは正規表現の一部として処理されます。

正規表現の例

語句に含まれている任意の単語をブロックする

```
/block|any|word/
```

意図的なスペル間違いの単語をブロックする

スパム発信者は多くの場合、スパム ブロッキング ソフトウェアを通り抜けるために、単語の文字の間に他の文字を挿入します。

```
/^.*v.*i.*a.*g.*r.*o.*$/i
/cr[eéèêë][\+\-\*=<>\.\,;!\?%&$@\^°\$£€\{\}()\[\]\|\\_01]dit/i
```

一般的なスパム語句をブロックする

次の語句は、スパム メッセージ内に見られる一般的な語句のいくつかの例です。

```
/try it for free/i
/student loans/i
/you're already approved/i
/special[\+\-\*=<>\.\,;!\?%&~#$@\^°\$£€\{\}()\[\]\|\\_1]offer/i
```

情報漏洩防止

FortiGate の情報漏洩防止 (DLP) システムを利用することにより、機密情報がネットワークを出入りすることを防止できます。機密情報のパターンを定義することで、そのパターンに一致する情報が FortiGate ユニットを通過するとき、その情報をブロック、ログ記録またはアーカイブできます。DLP システムを設定するには、ルールを個別に策定し、そのルールを DLP センサーに組み合わせ、DLP センサーをプロテクション プロファイルに割り当てます。

DLP 機能の主な目的は、機密情報をネットワークから漏出させないことですが、他にも、望ましくない情報がネットワークに入り込むことを防止し、FortiGate ユニットを通過するコンテンツの一部またはすべてをアーカイブするためにも利用できます。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとに情報漏洩防止を個別に設定します。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

このトピックには、以下の項目が含まれています。

センサー

注意：センサーを使用する前に、センサーおよびそこに含まれるルールを慎重に確認し、それらがネットワーク上のトラフィックに及ぼす影響について十分理解してください。

DLP センサーは、DLP ルールおよび DLP 複合ルールから構成されています。また DLP センサーには、[アクション]、[アーカイブ]、[重要度] など、ルールまたは複合ルールごとの設定も含まれています。設定を完了した DLP センサーは、プロテクション プロファイルで指定できます。プロテクション プロファイルが指定されているポリシーによって処理されるすべてのトラフィックには、強制的に DLP センサーの設定が適用されます。

新しい DLP センサーを作成し、ネットワークから送出されるトラフィックを保護するために必要な DLP ルールおよび DLP 複合ルールを含むように、センサーを設定できます。

DLP センサーを設定する前に、ルールおよび複合ルールを加えて DLP センサーを作成する必要があります。

DLP センサーを設定するには、*[UTM]*、*[データ漏えい防止]*、*[センサー]* の順に選択します。

[センサー] ページ

このページには、作成済みの DLP センサーおよびデフォルトの DLP センサーが一覧表示されます。このページでは、DLP センサーを編集 (デフォルトまたは作成済みのセンサー)、削除、または新規作成できます。

[Create New]
[Create New] を選択すると、[New DLP List] ページの画面に自動的に移動します。[New DLP List] ページには、[名前] フィールドおよび [コメント] フィールドがあり、[Sensor Settings] ページを表示するには DLP センサーの名前を入力する必要があります。

[名前]
DLP センサーの名前。デフォルトの DLP センサーには 6 種類があり、以下のデフォルト DLP センサーが FortiGate ユニットに含まれています。これらは、そのまま使用するか、または必要に応じて編集できます。

Content_Archive (デフォルト)
すべての電子メール (POP3、IMAP、および SMTP)、FTP、HTTP、および IM トラフィックをアーカイブする DLP。センサーに含まれる各ルールとも、*[アーカイブ]* は *[フル]* に設定されています。ブロックまたは隔離は実行されません。詳しくは、404 ページの「DLP アーカイブ」を参照してください。
[All-Session-Control] ルールを追加し、セッション制御コンテンツをアーカイブすることもできます。
SSL コンテンツ スキャンおよびインスペクションをサポートする FortiGate ユニットの場合、*[All-Email]* ルールを編集し、POP3S、IMAPS、および SMTPS トラフィックをアーカイブできます。SSL コンテンツ スキャンおよびインスペクションの詳細については、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。また、*[All-HTTP]* ルールを編集し、HTTPS トラフィックをアーカイブすることもできます。

Content_Summary (デフォルト)
すべての電子メール (POP3、IMAP、および SMTP)、FTP、HTTP、および IM トラフィックをアーカイブする DLP サマリ。センサーに含まれる各ルールとも、*[アーカイブ]* は *[Summary Only]* に設定されています。ブロックまたは隔離は実行されません。詳しくは、404 ページの「DLP アーカイブ」を参照してください。
[All-Session-Control] ルールを追加し、セッション制御コンテンツをアーカイブすることもできます。
SSL コンテンツ スキャンおよびインスペクションをサポートする FortiGate ユニットの場合、*[All-Email]* ルールを編集し、POP3S、IMAPS、および SMTPS トラフィックをアーカイブできます。また、*[All-HTTP]* ルールを編集し、HTTPS トラフィックをアーカイブすることもできます。
SSL コンテンツ スキャンおよびインスペクションの詳細については、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。

Credit-Card (デフォルト)
American Express、Visa、Mastercard のクレジット カードで使われる番号書式を、HTTP および電子メール トラフィックで検出します。
この DLP センサーは、デフォルトでは一致トラフィックをアーカイブせず、[アクション] は *[None]* に設定されています。[アクション] および [アーカイブ] オプションは、必要に応じて設定できます。

Large-File（デフォルト）	5MB を超えるファイルが電子メール メッセージに添付されているか、または HTTP あるいは FTP により送信される場合、そのファイルを検出します。 この DLP センサーは、デフォルトでは一致トラフィックをアーカイブせず、[アクション] は *[None]* に設定されています。[アクション] および [アーカイブ] オプションは、必要に応じて設定できます。
SSN-Sensor（デフォルト）	米国社会保障番号およびカナダ社会保険番号で使われる番号書式を、電子メールおよび HTTP トラフィックで検出します。 この DLP センサーは、デフォルトでは一致トラフィックをアーカイブせず、[アクション] は *[None]* に設定されています。[アクション] および [アーカイブ] オプションは、必要に応じて設定できます。
[コメント]	オプションで記述される DLP センサーの説明。
削除アイコン	リストから DLP センサーを削除する場合に選択します。
編集アイコン	DLP センサーに変更を加えるとき選択します。

[Sensor Settings] ページ

このページでは、DLP センサーに加えるルールを設定できます。[Create New] を選択し新しいセンサーを作成する場合は、[New DLP Sensor] ページの画面に自動的に移動します。[Sensor Settings] ページの画面に移動しセンサーを設定するには、[名前] フィールドにセンサーの名前を入力する必要があります。このページで [Create New] を選択すると、[New DLP Sensor Rule] ページの画面に移動します。

[名前]	既存の DLP センサーを編集しセンサー名を変更する場合は、このフィールドに新しい名前を入力します。変更を保存するには、必ず [OK] を選択します。
[コメント]	既存の DLP センサーを編集し説明内容を変更する場合は、このフィールドに変更を入力します。変更を保存するには、必ず [OK] を選択します。
[Create New]	[Create New] を選択すると、新しいルールまたは複合ルールをセンサーに加えます。メンバの種類を [コンパウンド ルール] または [ルール] に指定すると、異なるオプションが表示されます。
[有効]	このチェック ボックスをオフにすると、ルールまたは複合ルールを無効に設定できます。この項目はセンサーの一部として表示されますが、使用されません。
[ルール名]	センサーに含まれるルールおよび複合ルールの名前。
[アクション]	各ルールに設定されているアクション。*[None]* を選択している場合は、アクションは表示されません。 アクションの設定にかかわらずアーカイブは有効になりますが、選択されている [アクション] の内容とともに *[アーカイブ]* が表示されます。 たとえば、あるルールで、[アクション] を *[Block]* に設定し *[アーカイブ]* を *[フル]* に設定すると、センサー ルール リストに表示される [アクション] は、*[Block, Archive]* となります。
[コメント]	ルールまたは複合ルールの説明。説明はオプションです。
編集アイコン	ルールまたは複合ルールを編集するとき選択します。
削除アイコン	複合ルールまたはルールをリストから削除するとき選択します。
[有効]	ルールまたは複合ルールを有効にするとき選択します。
[無効]	ルールまたは複合ルールを無効にするとき選択します。

[New DLP Sensor Rule] ページ

[アクション]	特定のルールまたは複合ルールに対して、FortiGate ユニットが実行するアクションを選択します。 [Ban]、[Ban Sender]、[Quarantine IP address]、または [Quarantine Interface] を選択すると、[Expires] オプションが表示されます。
[アーカイブ]	そのセンサーでアーカイブされるロギングの種類を選択します。
[Expires]	[Quarantine Virus Sender (to Banned Users List)] を選択したとき表示されます。 攻撃者を無期限に禁止するか、または指定された日数、時間数、または分数に限り禁止するかを選択できます。

[重要度]	ルールまたは複合ルールに一致するコンテンツの重大度を入力します。FortiGate ユニットを通過するコンテンツが原因となり発生する問題の深刻さを、重大度によって示します。たとえば、DLP ルールが高度なセキュリティをともなうコンテンツと一致する場合、重大度は 5 に匹敵します。一方、DLP ルールがどのようなコンテンツとも一致する場合であれば、重大度は 1 でも妥当です。 ルールまたは複合ルールがコンテンツに一致するとき生成されるログメッセージの [重要度] フィールドに、DLP によって重大度が加えられます。数字が大きいほど、重大度は大きくなります。
[メンバータイプ]	*[ルール]* または *[コンパウンド ルール]* を選択します。選択した種類のルールが、その下の表に表示されます。

注記：DLP は、アクションの重複を避けます。1 つのセンサーに含まれている複数のルールがコンテンツに一致する場合でも、DLP は同じコンテンツからは DLP アーカイブ エントリ、隔離アイテム、または禁止エントリを、1 つしか作成しません。

複合ルール

DLP 複合ルールは、DLP ルールをグループ化したもので、DLP センサーに加わると動作の仕方が変わります。個別のルールは、1 つの属性のみによって設定できます。この属性がネットワーク トラフィックから発見されると、ルールの動作が始まります。

複合ルールにより、個別のルールをグループ化し、より詳しい動作の状態を指定できます。複合ルールに含まれる個々のルールには 1 つの属性 (または条件) が設定されますが、ルールが動作するにはその属性があらかじめトラフィックに存在する必要があります。

たとえば、以下の 2 つのルールを作成し、それらをセンサーに加えます。

- ルール 1 は、SMTP トラフィックの送信者アドレス spammer@example.com をチェック。
- ルール 2 は、SMTP トラフィックのメッセージ本文に含まれる sale という単語をチェック。

センサーを使用すると、いずれのルールも設定された条件が true であれば作動します。1 の条件のみ true の場合は、該当するルールのみが作動します。SMTP トラフィックのコンテンツ次第で、両ルールとも作動する、両ルールとも作動しない、または片方のみ作動します。

これらのルールをセンサーから削除する場合は、これらを複合ルールに加えて、その複合ルールをセンサーに加え、この複合ルールが作動するにはネットワーク トラフィックに両方のルールの条件が存在する必要があります。1 つの条件のみが存在する場合は、ルールまたは複合ルールが何も作動しないまま、メッセージは通過を許可されます。

複数のルールにともなう個別に設定可能な属性を組み合わせた複合ルールによって、ルールの動作をトリガする特定の条件をきめ細かく指定できます。

DLP センサーの複合ルールを設定するには、*[UTM]*、*[データ漏えい防止]*、*[Compund]* の順に選択します。

[コンパウンド] ページ

このページには、作成済みの複合ルールが一覧表示されます。このページでは、複合ルールを編集、削除、または新規作成できます。

[Create New]	新しい複合ルールを追加するには、*[Create New]* を選択します。
[名前]	複合ルールの名前。
[コメント]	オプションで記述される複合ルールの説明。
[DLP センサー]	複合ルールがいずれかの DLP センサーに使用される場合は、センサーの名前がここに表示されます。
編集アイコン	複合ルールを編集するとき選択します。
削除アイコン	[コンパウンド] ページから複合ルールを削除するとき選択します。DLP センサーで複合ルールが使用される場合は、削除アイコンは使用できません。DLP センサーから複合ルールを削除し、さらにこのページのリストから削除します。

[New/Edit Compound Rule] ページ

このページでは、複合ルールを設定できます。既存の複合ルールを編集する場合は、このページの画面に自動的に移動します。

[名前]	複合ルールの名前を入力します。

[コメント]	オプションで記述される複合ルールの説明。
[プロトコル]	DLP 複合ルールが適用されるコンテンツ トラフィックの種類を選択します。複合ルールに加えることができるルールは、選択するプロトコルに応じて異なります。プロトコルは、*[Email]*、*[HTTP]*、*[FTP]*、*[NNTP]*、および *[Instant Messaging]* から選択できます。
[AIM]、[ICQ]、[MSN]、[Yahoo!]	*[Instant Messaging]* プロトコルを選択すると、ルールが加えられるサポート対象の IM プロトコルを選択できます。選択したプロトコルすべてを含むルールのみを、複合ルールに加えることができます。
[HTTP POST]、[HTTP GET]	*[HTTP]* プロトコルを選択すると、HTTP post セッションまたは HTTP get セッションあるいは両方に適用する複合ルールを設定できます。選択したオプションすべてを含むルールのみを、複合ルールに加えることができます。
[HTTPS POST]、[HTTPS GET]	*[HTTP]* プロトコルを選択すると、FortiGate ユニットが SSL コンテンツ スキャンおよびインスペクションをサポートする場合は、HTTPS post セッションまたはHTTPS getセッションあるいは両方に適用する複合ルールを設定できます。選択したオプションすべてを含むルールのみを、複合ルールに加えることができます。 SSL コンテンツ スキャンおよびインスペクションの詳細については、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。 これらの暗号化されたトラフィックの種類をスキャンするには、プロテクション プロファイルの *[Protocol Recognition]* セクションで、*[HTTPS Content Filtering Mode]* を *[Deep Scan (Decrypt on SSL Traffic)]* に設定する必要があります。*[URL Filtering]* を選択している場合は、DLP センサーは HTTPS コンテンツをスキャンしません。
[FTP]、[PUT]、[GET]	*[FTP]* プロトコルを選択すると、FTP post セッションまたは FTP get セッションあるいは両方に適用する複合ルールを設定できます。選択したオプションすべてを含むルールのみを、複合ルールに加えることができます。
[SMTP]、[IMAP]、[POP3]	*[Email]* プロトコルを選択すると、ルールが加えられるサポート対象の電子メール プロトコルを選択できます。選択したプロトコルすべてを含むルールのみを、複合ルールに加えることができます。
[ルール]	複合ルールに加えるルールを選択します。選択したプロトコルすべてを含むルールのみを、複合ルールに加えることができます。
ルール追加 / ルール削除 (プラスおよびマイナス記号)	ルール追加およびルール削除アイコンを使用して、複合ルールにルールを追加または削除します。ルール追加アイコンを選択してから、リスト中のルールを選択します。

ルール

注意：ルールを使用する前に慎重に確認し、それらがネットワーク上のトラフィックに及ぼす影響について十分理解してください。

DLP ルールは、情報漏洩防止機能の中心的な要素です。これらのルールによって保護される情報を定義することで、FortiGate ユニットがその情報を識別できます。たとえば、含まれるルールは正規表現を使用し、社会保障番号を表します。

```
([0-6]\d{2}|7([0-6]\d|7[0-2]))[ \-]?\d{2}[ \-]\d{4}
```

この正規表現によって、可能な社会保障番号をすべて表示する変わりに、社会保障番号の構成が表されます。このパターンを、FortiGate ユニットにより容易に識別できます。

DLP ルールを、複合ルールに組み合わせ、それらの複合ルールを DLP センサーに加えることができます。DLP センサーの中でルールを直接指定する場合は、トラフィックがいずれか 1 つのルールに一致したとき、設定済みのアクションが発生します。まずルールを複合ルールにグループ化し、次に DLP センサーで指定する場合は、複合ルールに含まれるすべてのルールがトラフィックと一致しなければ、設定済みのアクションは発生しません。

DLP センサーに含まれる個別のルールは、暗示的 OR 条件と関連付けられており、一方で複合ルールに含まれるルールは暗示的 AND 条件と関連付けられています。

CLI から、SIP、SIMPLE、または SCCP を含むセッション制御 DLP ルールを作成し DLP アーカイブを行うこともできます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

ルールを設定するには、*[UTM]*、*[データ漏えい防止]*、*[ルール]* の順に選択します。

注記 : これらのルールは、暗号化されていないトラフィックの種類のみに有効です。FortiGate ユニットで、暗号化されたトラフィックを暗号化解除し検証できる場合は、必要に応じてこれらのルールでそのようなトラフィックの種類を有効に設定し、ルールの機能を拡張できます。

[ルール] ページ

このページには、作成済みのルールが一覧表示されます。このページでは、ルールを編集、削除、または新規作成できます。

[Create New]	新しいルールを追加するには、*[Create New]* を選択します。
編集アイコン	ルールを編集するとき選択します。
削除アイコン	このページのリストからルールを削除するとき選択します。複合ルールまたは DLP センサーで複合ルールが使用される場合は、削除アイコンは使用できません。複合ルールまたは DLP センサーから複合ルールを削除し、さらにこのページのリストから削除します。
[名前]	ルールの名前。FortiGate ユニットには、あらかじめ数種のデフォルト ルールが含まれており、そこから任意のルールを選択できます。必要に応じて、デフォルト ルールを編集できます。
All-Email、 All-FTP、 All-HTTP、 All-IM、 All-NNTP、 All-Session-Control	これらのルールにより、指定された種類のトラフィックすべてが検出されます。
Email-AmEx、 Email-Canada-SIN、 Email-US-SSN、 Email-Visa-Mastercard	これら 4 種類のルールは、SMTP、POP3、および IMAP 電子メール トラフィックのメッセージ本文から、American Express クレジット カード番号、カナダ社会保険番号、米国社会保障番号、または Visa および Mastercard クレジット カード番号を検出します。
HTTP-AmEx、 HTTP-Canada-SIN、 HTTP-US-SSN、 HTTP-Visa-Mastercard	これら 4 種類のルールは、HTTP トラフィックの POST コマンドから、American Express クレジット カード番号、カナダ社会保険番号、米国社会保障番号、または Visa および Mastercard クレジット カード番号を検出します。HTTP POST は、Web サーバに情報を送信するために使用されます。上述のように、これらのルールは、ユーザが Web サーバに送信する情報を検出するように設計されています。このルールは、Web ページを読み込み取得する HTTP GET コマンドにより得た情報は、検出しません。
[Email-Not-Webex]、 [HTTP-Post-Not-Webex]	これらのルールは、DLP が、*WebEx* という文字列を含む電子メールまたは HTTP ページと一致するのを阻止します。
[Large-Attachment]	このルールは、SMTP、POP3、IMAP 電子メール メッセージに添付されている、5 MB より大きなファイルを検出します。
[Large-FTP-Put]	このルールは、FTP PUT プロトコルにより送信される、5 MB より大きなファイルを検出します。FTP GET を使用して受信されるファイルは、検出されません。
[Large-HTTP-Post]	このルールは、FTP POST プロトコルにより送信される、5 MB より大きなファイルを検出します。HTTP GET を使用して受信されるファイルは、検出されません。
[コメント]	オプションで記述されるルールの説明。
[Compound Rules]	ルールがいずれかの複合ルールに含まれている場合は、その複合ルールがここに表示されます。
[DLP センサー]	ルールがいずれかの DLP センサーで使用されている場合は、そのセンサーの名前がここに表示されます。

[New/Edit Regular Rule]

ここでは、電子メールに適用されるルールなど、種類ごとにルールを設定できます。

[名前]	ルールの名前。
[コメント]	オプションで記述されるルールについての説明。
[プロトコル]	DLP ルールが適用されるコンテンツ トラフィックの種類を選択します。利用可能なルール オプションは、選択されるプロトコルに応じて異なります。プロトコルは、*[Email]*、*[HTTP]*、*[FTP]*、*[NNTP]*、*[Instant Messaging]*、および *[Session Control]* から選択できます。

[AIM]、[ICQ]、[MSN]、[Yahoo!]	*[Instant Messaging]* プロトコルを選択すると、サポートされる IM プロトコル (AIM、ICQ、MSN、および Yahoo!) のいずれかまたはすべてを使用するファイル転送に適用されるルールを設定できます。 IM プロトコルを使用するファイル転送のみが、DLP ルール適用の対象となります。IM メッセージは、スキャンされません。
[HTTP POST]、[HTTP GET]	*[HTTP]* プロトコルを選択すると、HTTP post トラフィックまたは HTTP get トラフィックあるいは両方に適用するルールを設定できます。
[HTTPS POST]、[HTTPS GET]	*[HTTP]* プロトコルを選択すると、FortiGate ユニットが SSL コンテンツ スキャンおよびインスペクションをサポートする場合は、HTTPS post セッションまたは HTTPS get セッションあるいは両方に適用する HTTP ルールを設定できます。SSL コンテンツ スキャンおよびインスペクションの詳細については、『*FortiOS ハンドブック*』の「*UTM* 」の章を参照してください。 これらの暗号化されたトラフィックの種類をスキャンするには、プロテクション プロファイルの *[Protocol Recognition]* セクションで、*[HTTPS Content Filtering Mode]* を *[Deep Scan (Decrypt on SSL Traffic)]* に設定する必要があります。*[URL Filtering]* を選択している場合は、DLP センサーは HTTPS コンテンツをスキャンしません。
[FTP]、[PUT]、[GET]	*[FTP]* プロトコルを選択すると、FTP put セッションまたは FTP get セッションあるいは両方に適用するルールを設定できます。
[SMTP]、[IMAP]、[POP3]	*[Email]* プロトコルを選択すると、サポート対象の電子メール プロトコル (SMTP、IMAP、および POP3) のいずれかまたはすべてに適用するルールを設定できます。
[SMTPS]、[IMAPS]、[POP3S]	*[Email]* プロトコルを選択すると、FortiGate ユニットが SSL コンテンツ スキャンおよびインスペクションをサポートする場合は、SMTPS、IMAPS、POP3S、またはこれらの組み合わせに適用するルールを設定できます。 SSL コンテンツ スキャンおよびインスペクションの詳細については、『*FortiOS ハンドブック*』の「*UTM* 」の章を参照してください。
[SIP]、[SIMPLE]、[SCCP]	*[Session Control]* プロトコルを選択すると、サポート対象のセッション制御プロトコル (SIP、SIMPLE、および SCCP) のいずれかまたはすべてに適用するルールを設定できます。セッション制御プロトコルの唯一のルール オプションは、*[Always]* です。このオプションは、すべてのセッション制御トラフィックと一致し、セッション制御 DLP アーカイブに使用されます。
[ルール]	*[ルール]* 設定を使用することにより、DLP ルールと一致するコンテンツを設定します。これらの設定は、選択しているプロトコルに応じて異なります。たとえば、[HTPS] プロトコルを選択している場合は、[ルール] 設定は表示されません。 **注記**：HTTPS の場合、設定は何もないので表示されません。

[プロトコル] でプロトコルの種類に [Email] を選択すると、以下が表示されます。

[Always]	どのコンテンツとも一致します。このオプションは、すべてのプロトコルで利用できます。
[Body]	メッセージまたはページの本文から、指定された文字列を検索します。
[Subject]	メッセージの件名から、指定された文字列を検索します。 このオプションは、すべての電子メールで利用できます。
[Sender]	メッセージ送信者ユーザ ID または電子メール アドレスから、指定された文字列を検索します。このオプションは、すべての電子メールおよび IM で利用できます。 電子メールの場合、メール ヘッダの From: アドレス から送信者を識別します。IM の場合、IM セッションの全メンバが送信者となり、セッションから IM ユーザ ID を見分けることで送信者を識別します。
[Receiver]	メッセージ受信者の電子メール アドレスから、指定された文字列を検索します。
[Attachment Size]	添付ファイルのサイズをチェックします。
[Attachment Type]	選択されたファイル フィルタの指定に応じて、電子メール メッセージからファイルの種類またはファイル パターンを検索します。
[Attachment Text]	場合によりワイルド カードまたは正規表現を含んでいる UTF-8 または ASCII 形式の添付ファイルから、テキストを検索します。
[Transfer Size]	転送される情報の合計サイズをチェックします。たとえば、電子メール トラフィックの場合は、転送サイズにはメッセージ ヘッダ、本文、エンコーディングされた添付データが含まれます。
[Binary file pattern (enter in base 64)]	ネットワーク トラフィックから、 指定されたバイナリ文字列を検索します。

[Authenticated User]	指定された認証ユーザから送信されたトラフィックを検索します。
[User group]	指定されたユーザ グループに含まれるユーザから送信されたトラフィックを検索します。
[File]	ファイルが暗号化されているか否かをチェックします。暗号化されているファイルとは、アーカイブされたファイルおよびパスワード保護付きの Microsoft Word ファイルを指します。これらはパスワードで保護されているので、FortiGate ユニットは暗号化されたファイルの中身をスキャンできません。

[プロトコル]でプロトコルの種類に[HTTP]を選択すると、以下が表示されます。

[Always]	どのコンテンツとも一致します。このオプションは、すべてのプロトコルで利用できます。
[Body]	メッセージまたはページの本文から、指定された文字列を検索します。
[URL]	HTTP トラフィックから、指定された URL を検索します。
[Transfer Size]	転送される情報の合計サイズをチェックします。たとえば、電子メール トラフィックの場合は、転送サイズにはメッセージ ヘッダ、本文、エンコーディングされた添付データが含まれます。
[Cookie]	Cookie のコンテンツから指定されたテキストを検索します。 このオプションは、HTTP で利用できます。
[CGI parameters]	CGI コードをともなうあらゆる Web ページから、指定された CGI パラメータを検索します。 このオプションは、HTTP で利用できます。
[HTTP header]	HTTP ヘッダから、指定された文字列を検索します。
[Hostname]	HTTP サーバに接続するとき、指定されたホスト名を検索します。
[File type]	指定されたファイル パターンおよびファイルの種類を検索します。ファイル フィルタ リストで設定されたファイル パターンおよび種類、およびリストが、DLP ルールで選択されます。
[Binary file pattern (enter in base 64)]	ネットワーク トラフィックから、 指定されたバイナリ文字列を検索します。
[Authenticated User]	指定された認証ユーザから送信されたトラフィックを検索します。
[User group]	指定されたユーザ グループに含まれるユーザから送信されたトラフィックを検索します。
[File]	ファイルが暗号化されているか否かをチェックします。暗号化されているファイルとは、アーカイブされたファイルおよびパスワード保護付きの Microsoft Word ファイルを指します。これらはパスワードで保護されているので、FortiGate ユニットは暗号化されたファイルの中身をスキャンできません。

[プロトコル]でプロトコルの種類に[FTP]を選択すると、以下が表示されます。

[Always]	どのコンテンツとも一致します。このオプションは、すべてのプロトコルで利用できます。
[Transfer Size]	転送される情報の合計サイズをチェックします。たとえば、電子メール トラフィックの場合は、転送サイズにはメッセージ ヘッダ、本文、エンコーディングされた添付データが含まれます。
[Server: Start/End]	指定されたアドレス範囲から、サーバの IP アドレスを検索します。
[File type]	指定されたファイル パターンおよびファイルの種類を検索します。ファイル フィルタ リストで設定されたファイル パターンおよび種類、およびリストが、DLP ルールで選択されます。
[File text]	転送されたテキスト ファイルから、指定されたテキストを検索します。
[Binary file pattern (enter in base 64)]	ネットワーク トラフィックから、 指定されたバイナリ文字列を検索します。
[Authenticated User]	指定された認証ユーザから送信されたトラフィックを検索します。
[User group]	指定されたユーザ グループに含まれるユーザから送信されたトラフィックを検索します。

[File]	ファイルが暗号化されているか否かをチェックします。暗号化されているファイルとは、アーカイブされたファイルおよびパスワード保護付きの Microsoft Word ファイルを指します。これらはパスワードで保護されているので、FortiGate ユニットは暗号化されたファイルの中身をスキャンできません。

[プロトコル]でプロトコルの種類に[NNTP]を選択すると、以下が表示されます。

[Always]	どのコンテンツとも一致します。このオプションは、すべてのプロトコルで利用できます。
[Body]	メッセージまたはページの本文から、指定された文字列を検索します。
[Transfer Size]	転送される情報の合計サイズをチェックします。たとえば、電子メール トラフィックの場合は、転送サイズにはメッセージ ヘッダ、本文、エンコーディングされた添付データが含まれます。
[Server: Start/End]	指定されたアドレス範囲から、サーバの IP アドレスを検索します。
[File type]	指定されたファイル パターンおよびファイルの種類を検索します。ファイル フィルタ リストで設定されたファイル パターンおよび種類、およびリストが、DLP ルールで選択されます。
[File text]	転送されたテキスト ファイルから、指定されたテキストを検索します。
[Binary file pattern (enter in base 64)]	ネットワーク トラフィックから、 指定されたバイナリ文字列を検索します。
[Authenticated User]	指定された認証ユーザから送信されたトラフィックを検索します。
[User group]	指定されたユーザ グループに含まれるユーザから送信されたトラフィックを検索します。
[File]	ファイルが暗号化されているか否かをチェックします。暗号化されているファイルとは、アーカイブされたファイルおよびパスワード保護付きの Microsoft Word ファイルを指します。これらはパスワードで保護されているので、FortiGate ユニットは暗号化されたファイルの中身をスキャンできません。

[プロトコル]でプロトコルの種類に[Instant Messaging]を選択すると、以下が表示されます。

[Always]	どのコンテンツとも一致します。このオプションは、すべてのプロトコルで利用できます。
[Sender]	メッセージ送信者ユーザ ID または電子メール アドレスから、指定された文字列を検索します。このオプションは、すべての電子メールおよび IM で利用できます。 電子メールの場合、メール ヘッダの From: アドレス から送信者を識別します。IM の場合、IM セッションの全メンバが送信者となり、セッションから IM ユーザ ID を見分けることで送信者を識別します。
[Transfer Size]	転送される情報の合計サイズをチェックします。たとえば、電子メール トラフィックの場合は、転送サイズにはメッセージ ヘッダ、本文、エンコーディングされた添付データが含まれます。
[File type]	指定されたファイル パターンおよびファイルの種類を検索します。ファイル フィルタ リストで設定されたファイル パターンおよび種類、およびリストが、DLP ルールで選択されます。
[File Text]	転送されたテキスト ファイルから、指定されたテキストを検索します。
[Binary file pattern (enter in base 64)]	ネットワーク トラフィックから、 指定されたバイナリ文字列を検索します。
[Authenticated User]	指定された認証ユーザから送信されたトラフィックを検索します。
[User group]	指定されたユーザ グループに含まれるユーザから送信されたトラフィックを検索します。
[File]	ファイルが暗号化されているか否かをチェックします。暗号化されているファイルとは、アーカイブされたファイルおよびパスワード保護付きの Microsoft Word ファイルを指します。これらはパスワードで保護されているので、FortiGate ユニットは暗号化されたファイルの中身をスキャンできません。

[New/Edit Regular Rule] ページには、以下のルール演算子が表示されます。

[matches] [does not match]	この演算子は、FortiGate ユニットが特定の文字列がある場合、または特定の文字列がない場合の、いずれを検索するかを指定します。 · [Matches] ネットワーク トラフィックから特定の文字列が発見されると、ルールがトリガされます。 · [Does not match] ネットワーク トラフィックから特定の文字列が発見されない場合に、ルールがトリガされます。
[ASCII] [UTF-8]	テキスト ファイルおよびメッセージに使用されているエンコーディングを選択します。
[Regular Expression] [Wildcard]	パターンを定義する方法を選択します。
[is] [is not]	この演算子は、ルールのアクションがトリガされるのは、条件に一致する場合か、または一致しない場合かを指定します。 · [is] ルール条件が一致すれば、ルールのアクションがトリガされます。 · [is not] ルール条件が一致しなければ、ルールのアクションがトリガされます。 たとえば、指定されたファイル タイプ リストにそのファイルの種類が含まれている、という条件をルールが指定する場合、ファイルが一致するたびにルールのアクションがトリガされます。反対に、指定されたファイル タイプ リストにそのファイルの種類が含まれない、という条件をルールが指定する場合、リストに含まれないファイルの種類によってのみルールのアクションがトリガされます。
==/>=/<=/!=	これらの演算子により、転送ファイルまたは添付ファイルのサイズを、指定された値と比較できます。 · == は、指定された値に等しいサイズ。 · >= は、指定された値以上のサイズ。 · <= は、指定された値以下のサイズ。 · !== は、指定された値と等しくないサイズ。

DLP アーカイブ

DLP アーカイブを使用することにより、FortiGuard Analysis and Management Service (FAMS) にアーカイブされている履歴ログを、収集および表示できます。DLP アーカイブは、FortiAnalyzer ユニットを FortiGate の構成に加える場合に利用可能になります (詳しくは 491 ページの「FortiAnalyzer ユニットへのリモート ロギング」を参照)。FortiGuard Analysis and Management サーバは、FortiGuard Analysis and Management Service (FAMS) に加入することで利用可能になります (詳しくは、*FortiGuard Analysis and Management Service 管理ガイド*を参照)。

完全な DLP アーカイブおよびサマリ DLP アーカイブを設定できます。完全な DLP アーカイブにはすべてのコンテンツが含まれており、たとえば、完全な電子メール DLP アーカイブには完全な電子メールメッセージおよび添付データが含まれます。サマリ DLP アーカイブにはコンテンツに関するメタデータのみが含まれており、たとえば、電子メール メッセージのサマリ レコードには、電子メール ヘッダのみが含まれます。

アーカイブできるのは、電子メール、FTP、HTTP、IM、およびセッション制御コンテンツです。

- 電子メール コンテンツには、IMAP、POP3、SMTP セッションが含まれます。また、FortiGate 電子メール フィルタリングによりスパムとしてタグ付けされる電子メール メッセージも、電子メール コンテンツに加えることができます。FortiGate ユニットが SSL コンテンツ スキャンおよびインスペクションをサポートする場合は、電子メール コンテンツに IMAPS、POP3S、および SMTPS のセッションも加えることができます。SSL コンテンツ スキャンおよびインスペクションの詳細については、『*FortiOS ハンドブック*』の「*UTM* 」の章を参照してください。
- HTTP コンテンツには、HTTP セッションが含まれます。FortiGate ユニットが SSL コンテンツ スキャンおよびインスペクションをサポートする場合は、HTTP コンテンツに HTTPS セッションも加えることができます。

  SSL コンテンツ スキャンおよびインスペクションの詳細については、『*FortiOS ハンドブック*』の「*UTM* 」の章を参照してください。
- IM コンテンツには、AIM、ICQ、MSN、および Yahoo! のセッションが含まれます。

- セッション制御コンテンツには、SIP、SIMPLE、および SCCP のセッションが含まれます。SIP および SCCP では、サマリ DLP アーカイブのみを利用できます。SIMPLE では、完全およびサマリの DLP アーカイブを利用できます。

DLP センサーを加えることにより、電子メール、Web、FTP、IM、およびセッション制御のコンテンツをアーカイブします。スパム電子メール メッセージのアーカイブは、プロテクション プロファイルで設定します。

DLP アーカイブは、DLP センサーの中で有効に設定します。DLP センサーを設定するには、*[UTM]*、*[データ漏えい防止]*、*[センサー]* の順に選択します。また、アーカイブのために新しい DLP センサーを作成する代わりに、Content_Archive または Content_Summary センサーのいずれかを使用し DLP ログをアーカイブできます。

CLI から、SIP、SIMPLE、または SCCP を含むセッション制御 DLP ルールを作成し DLP アーカイブを行うこともできます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

アプリケーション制御

この項では、ファイアウォール プロテクション プロファイルに関連するアプリケーション制御オプションを設定する方法について説明します。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとにアプリケーション制御を個別に設定します。たとえば、ある VDOM で作成されたアプリケーション ブラック / ホワイト リストは、他の VDOM では表示されません。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

アプリケーション制御 UTM 機能を使用する場合、FortiGate ユニットによりネットワーク トラフィックが検出され、トラフィックを生成したアプリケーションに応じて、そのトラフィックに対するアクションが実行されます。FortiGate 不正侵入防御プロトコル デコーダに基づくアプリケーション制御は、FortiGate ユニットを通過するアプリケーション トラフィックの動作をログ記録および管理するための、扱いやすく高機能な手法を提供します。アプリケーション制御で使用される IPS プロトコル デコーダは、ネットワーク トラフィックの分析により、標準以外のポートまたはプロトコルに基づくアプリケーション トラフィックであっても、トラフィックを検出できます。

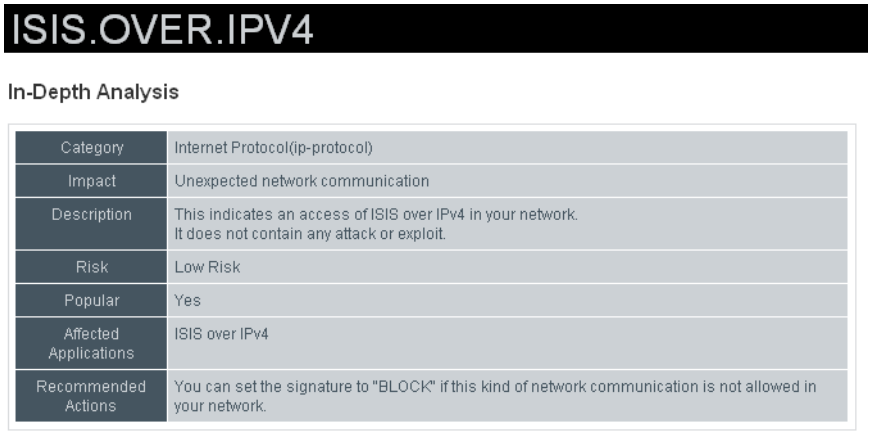
FortiGate ユニットにより、多数のアプリケーションから生成されたネットワーク トラフィックを識別できます。アプリケーション制御ブラック / ホワイト リストを作成し、管理する必要があるアプリケーション トラフィックおよびアプリケーション実行の土台となるネットワークに対して実行されるアクションを指定できます。監視の対象となるネットワーク トラフィックに適用されるプロテクション プロファイルに、アプリケーション制御ブラック / ホワイト リストを加えます。

フォーティネットは、FortiGuard アプリケーション制御データベースにアプリケーションを追加することにより、アプリケーション制御に基づいて検出されるアプリケーションのリストを継続的に更新し充実させています。アプリケーション制御では不正侵入防御プロトコル デコーダが利用されるので、アプリケーション制御データベースは FortiGuard 不正侵入防止システム データベースの一部となり、双方のデータベースのバージョン番号は同じになります。

FortiGate ユニットにインストールされているアプリケーション制御データベースのバージョンを確認するには、*[License Information]* ダッシュボード ウィジェットを表示し、IPS Definitions バージョンを確認します。

FortiGuard アプリケーション制御によりサポートされるアプリケーションの完全なリストをに表示するには、FortiGuard Application Control List にアクセスします。この Web ページには、サポートされるアプリケーションがすべて表示されます。任意のアプリケーション名を選択し、そのアプリケーションの詳細を確認できます。

図 26: ISIS.Over.IPv4 アプリケーション ページ



このトピックには、以下の項目が含まれています。

- ブラック / ホワイト リスト
- アプリケーション リスト

ブラック / ホワイト リスト

アプリケーション制御ブラック / ホワイト リストには、監視されるアプリケーション トラフィック、およびトラフィックが検出されたとき実行されるアクションについての、詳しい設定内容が含まれています。アプリケーション制御ブラック / ホワイト リストを有効にするには、ファイアウォール ポリシーでリストを選択する必要があります。

デフォルトのブラック / ホワイト リストはありません。

FortiGate ユニットは、リストの並び順に従い最上位から順次、一度に 1 つずつ、エントリされているアプリケーションのネットワーク トラフィックを検証します。トラフィックの一致が検出されると、一致ルールに指定されているアクションがそのトラフィックに適用され、エントリされているアプリケーションとの照合作業はその時点で停止します。このため、両方のアクション (許可およびブロック) に基づく複合的なルールを、少数のアプリケーション エントリをリストに加えることで作成できます。

たとえば、組織内の標準インスタント メッセージングに AIM を採用している場合、2 つのアプリケーションをエントリするだけで、AIM を許可し他の IM クライアントをすべてブロックできます。まず、[Application] に AIM を指定したアプリケーション エントリを作成します。このエントリの [アクション] を *[Pass]* に設定します。次に、*[Category]* を *[im]*、*[Application]* を *[all]*、および [アクション] を *[Block]* に設定したアプリケーション エントリを作成します。アプリケーション エントリは上位から下位の順にチェックされるので、AIM トラフィックにより最初のルール (AIM アプリケーション エントリ) がトリガされ、AIM トラフィックは許可されます。AIM 以外の IM トラフィックが検出される場合、2 番目のルール (All アプリケーション エントリ) がトリガされるので、FortiGateユニットによりそのトラフィックはブロックされます。

[Black/White List] メニューでは、監視を有効にすることにより、ネットワークを監視状態に設定できます。[Black/White Lists Setting] ページの *[Monitor]* 横にあるチェック ボックスをオンにすると、ネットワーク監視が有効に設定されます。

ブラック / ホワイト リストを設定するには、*[UTM]*、*[Application Control]*、*[Black/White List]* の順に選択します。

[Black/White Lists] ページ

このページには、作成済みのブラック / ホワイト リストが一覧表示されます。このページでは、ブラック / ホワイト リストを編集、削除、または新規作成できます。

[Create New] [Create New] を選択すると、[New Application Control Black/White List] ページの画面に自動的に移動します。このページには、[名前] フィールドおよび [コメント] フィールドがあり、[Black/White Lists Settings] ページを表示するには DLP センサーの名前を入力する必要があります。

[名前]	利用可能な、アプリケーション制御ブラック / ホワイト リスト。
[# of Entries]	各アプリケーション制御ブラック / ホワイト リストに含まれるアプリケーション ルールの数。
[Profiles]	各アプリケーション制御ブラック / ホワイト リストが適用されている、プロテクション プロファイル。ブラック / ホワイト リストがプロテクション プロファイルに提供されていない場合は、このフィールドは空白になります。
[コメント]	オプションで記述される、アプリケーション制御ブラック / ホワイト リストの説明。
削除アイコン	アプリケーション制御ブラック / ホワイト リストを削除するとき選択します。削除アイコンは、アプリケーション制御ブラック / ホワイト リストがどのプロテクション プロファイルでも選択されていない場合にのみ使用できます。
編集アイコン	アプリケーション制御ブラック / ホワイト リストを編集するとき選択します。

[Black/White Lists Settings] ページ

このページでは、ブラック / ホワイト リストのアプリケーションを設定できます。ブラック / ホワイト リストを編集する場合は、このページの画面に移動します。

[名前]	既存のブラック / ホワイト リストを編集し、リストの名前を変更する場合は、このフィールドに新しい名前を入力します。変更を保存するには、必ず [OK] を選択します。
[コメント]	既存のブラック / ホワイト リストを編集し、説明内容を変更する場合は、このフィールドに説明の変更を入力します。変更を保存するには、必ず [OK] を選択します。
[OK]	[名前] フィールドおよび [コメント] フィールドに加えた変更を保存するとき選択します。
[Monitor]	ネットワーク監視を有効にするときオンにします。
[Create New]	新しいアプリケーション エントリを作成するとき選択します。
[ID]	主にアプリケーション エントリを並べ替えるとき使用する、固有の番号。
[Category]	[Category] は、*[Application]* が *[all]* に設定されている場合、アプリケーション エントリに含まれているアプリケーションの対象範囲を示します。たとえば、*[Application]* が *[all]* に設定され、*[Category]* が *[toolbar]* に設定されているとき、個別のアプリケーションが指定されていない場合も、すべてのツールバー アプリケーションがアプリケーション エントリに含まれます。 *[Application]* が単一のアプリケーションの場合、*[Category]* はアプリケーション エントリの実行に何も影響しません。
[Application]	表示されているアプリケーションのネットワーク トラフィックが、FortiGate ユニットによって検証されます。*[Application]* を *[all]* に設定している場合は、選択されたカテゴリに該当するすべてのアプリケーションが含まれます。
[アクション]	FortiGate ユニットによって、指定のアプリケーションから生じたトラフィックが検出されると、選択されているアクションが実行されます。
[Logging]	指定のアプリケーションから生じたトラフィックが検出されると、FortiGate ユニットはその検出および実行されたアクションをログ記録します。
削除アイコン	アプリケーション エントリを削除するとき選択します。
編集アイコン	アプリケーション エントリを編集するとき選択します。
挿入アイコン	挿入アイコンを選択したアプリケーション エントリの上に、新しいアプリケーション エントリを作成するとき選択します。
移動アイコン	アプリケーション エントリをブラック / ホワイト リスト内の別の位置に移動する場合に選択します。

[New Application Entry] ページ

[Category]	アプリケーションは、種類に応じてカテゴリに分類されます。たとえば、IM アプリケーションを選択する場合は、*[im]* カテゴリを選択すると、アプリケーション ブラック / ホワイト リストの [Application] には *[im]* のみが表示されます。 また、*[Category]* を使用し、アプリケーションの包括的なカテゴリを指定できます。たとえば、すべての IM アプリケーションを選択するには、*[im]* カテゴリを選択し、[Application] に *[all]* を選択します。この設定により、1 つのアプリケーション制御ブラック / ホワイト リスト エントリのみで、すべての IM アプリケーションを指定できます。
[Application]	表示されているアプリケーションのネットワーク トラフィックが、FortiGate ユニットによって検証されます。*[Application]* を *[all]* に設定している場合は、選択されたカテゴリに該当するすべてのアプリケーションが含まれます。
[アクション]	FortiGate ユニットによって、指定のアプリケーションから生じたトラフィックが検出されると、選択されているアクションが実行されます。
[Options]	ブラック / ホワイト リストで選択可能なオプション。
[Session TTL]	アプリケーションのセッション TTL。このオプションを有効にしない場合は、TTL はデフォルトで CLI コマンド `config system session-ttl` の設定に従います。
[Enable Logging]	このオプションを有効にすると、指定されたアプリケーションのトラフィックが検出されとき、その検出および実行されたアクションが FortiGate ユニットによってログ記録されます。
[Enable Packet Logging]	

アプリケーション リスト

アプリケーション リストは、アプリケーションおよびその普及度とリスクを表示します。各アプリケーションの詳しい情報を表示するには、アプリケーションの名前を選択します。名前にリンクされている FortiGuard Application Control List が表示され、そのアプリケーションに関する詳細を確認できます。また、*[UTM]*、*[Application Control]*、*[Application List]* の順に選択して表示される情報をフィルタリングできます。情報をフィルタリングする詳しい方法については、を参照してください。

FortiGuard アプリケーション制御によりサポートされるアプリケーションの完全なリストを表示するには、FortiGuard Application Control List にアクセスします。この Web ページには、サポートされるアプリケーションがすべて表示されます。任意のアプリケーション名を選択し、そのアプリケーションの詳細を確認できます。

アプリケーション リストを設定するには、*[UTM]*、*[Application Control]*、*[Application List]* の順に選択します。

[Application List] ページ

このページには、ユニットで利用可能なアプリケーションが、カテゴリ (Category)、普及度 (Popularity)、およびリスク (Risk) とともに表示されます。

[Current Page]	表示されるリスト項目の現在のページ番号。左右の矢印を選択し、電子メール アドレス リストの最初、前、次、または最後のページを表示します。
[Total: 1083]	FortiGuard Application Control List に含まれるアプリケーションの最大数。
[Application Name]	アプリケーションの名前。
[Category]	アプリケーションと関連するカテゴリ。
[Popularity]	アプリケーションの普及度。[Popularity] には、[Low]、[Medium]、[High] の 3 段階があります。
[Risk]	アプリケーションに関連するリスクのレベル。[Risk] には、[Low]、[Medium]、[High] の 3 段階があります。

VoIP

FortiGate ユニットは、VoIP プロトコルをサポートしシグナリング層のステートをメディア層のパケット フローと関連付けることにより、VoIP ソリューションのセキュリティを効果的に実現できます。SIP ALG 制御を使用することで、FortiGate ユニットはネットワークで使用される VoIP シグナリング プロトコルを解釈し、特定の VoIP 通話ごとにポートをダイナミックに開閉 (ピンホール) してセキュリティを維持できます。

[UTM]、*[VoIP]*、*[Profile]* の順に選択して表示される画面では、VoIP プロトコルのみを対象とするファイアウォール ポリシーに適用するための、複数のプロファイルを設定できます。

プロファイル

[Profile] メニューでは、ファイアウォール ポリシーに適用するための VoIP プロファイルを設定できます。プロファイルに含まれる特定の情報は、ポリシーに基づきトラフィックがどのように検証され、検証に基づいてどのようなアクションが実行されるかを定義します。

VoIP プロファイルを設定するには、*[UTM]*、*[VoIP]*、*[Profile]* の順に選択します。

[Profile] ページ

このページには、SIP および SCCP プロトコル用に作成されたプロファイルが一覧表示されます。このページでは、VoIP プロトコル プロファイルを編集、削除、または新規作成できます。

[Create New]	新しい VoIP プロファイルを作成するとき選択します。
編集アイコン	プロファイルの設定を変更するとき選択します。
削除アイコン	プロファイルを削除するとき選択します。
[名前]	プロファイルの名前。
[コメント]	プロファイルの説明。この設定は、オプションです。

[New VoIP Profile] ページ

このページでは、プロファイルの SIP および SCCP オプションを設定できます。VoIP プロファイルを編集する場合は、[Edit VoIP Profile] ページに自動的に移動します。

[名前]	このプロファイルの名前を入力します。
[コメント]	プロファイルの説明を入力します (入力はオプションです)。
[SIP]	SIP プロトコルの設定。
[Limit REGISTER requests]	REGISTER 要求の帯域制限を設定する数値を入力します。
[Limit INVITE requests]	INVITE 要求の帯域制限を設定する数値を入力します。
[Enable Logging]	SIP 要求をログ記録するとき選択します。
[Enable Logging of Violations]	SIP 違反をログ記録するとき選択します。
[SCCP]	SCCP プロトコルの設定。
[Limit Call Setup]	コール セットアップに帯域制限を設定する数値を入力します。
[Enable Logging]	SCCP をログ記録するとき選択します。
[Enable Logging of Violations]	SCCP 違反をログ記録するとき選択します。

IPsec VPN

この項では、Web ベース マネージャからおこなえる IPsec (Internet Protocol Security) VPN の設定オプションの導入を説明します。FortiGate ユニットでは、ポリシーベース (トンネル モード) およびルートベース (インタフェース モード) VPN の両方をサポートします。IPsec VPN の設定方法およびその他の詳細については、『*FortiGate IPSec VPN ユーザ ガイド*』を参照してください。

FortiGate ユニットでバーチャルドメイン (VDOM) を有効にしているときは、それぞれのバーチャルドメインごとに VPN IPsec を個別に設定します。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には以下のトピックが含まれています。

注記: L2TP および IPSec は、Windows XP、Windows Vista、および Mac OSX のネイティブ VPN クライアントでサポートされます。

IPsec VPN の概要

[IPsec VPN] メニューには、IPsecVPN の設定項目およびオプションがあります。IPsec VPN は仮想プライベートネットワークであり、IPsec プロトコルスイートを用いてその仮想プライベートネットワークにセキュリティと保護を提供します。これはつまり、ネットワークへ入ってくるデータも、ネットワークから出ていくデータも暗号化されることを意味します。

FortiOS で設定される IPsec VPN は、以下の基本的な手順を使用して設定しなければなりません。

1 FortiGate がリモートピアまたはクライアントを認証し、セキュアなコネクションを確立するために必要なフェーズ 1 パラメータを定義します。詳しくは、413 ページの「フェーズ 1 の設定」を参照してください。

2 FortiGate ユニットがリモートピアまたはダイアルアップクライアントと VPN トンネルを張るために必要なフェーズ 2 パラメータを定義します。詳しくは、417 ページの「フェーズ 2 の設定」を参照してください。

注記: もし FortiGate ユニットがユニークな IPsec 暗号化キーと認証キーを自動的に生成させたいのであれば、ステップ 1 とステップ 2 を踏まなければなりません。もしリモート VPN ピアまたはクライアントが特定の IPsec 暗号化キーと認証キーを要求するのであれば、FortiGate ユニットがマニュアルキーを使うように設定しなければなりません。詳細については、419 ページの「手動キー」を参照してください。

3 あなたのプライベートネットワークと VPN 間での通信を許可するファイアウォールポリシーを作成してください。ポリシーベース VPN の場合は、ファイアウォール ポリシーの [Action] を [IPSEC] に設定します。インタフェースベース VPN の場合は、ファイアウォール ポリシーの [Action] を [ACCEPT] に設定します。詳しくは、268 ページの「ファイアウォール ポリシーの設定」を参照してください。

フェーズ 1 は IPsecVPN の最初のパートを構成する一連の設定です。これらの設定はリモートピアまたはクライアントを認証して、セキュアなコネクションを確立するために使われます。フェーズ 2 は IPsecVPN の 2 番目であり、かつ最後のパートを構成するの一連の設定であり、FortiGate ユニットがリモートピアまたはダイアルアップクライアントと VPN トンネルを作成するために必要な情報を提供します。

FortiGate ユニットは、ESP (Encapsulated Security Payload) プロトコルを実装しています。暗号化されたパケットは通常のパケットと同じように、IP ネットワークでルーティングされます。IKE (インターネット鍵交換) は、事前共有キーまたは X.509 デジタル証明書に基づいて自動的に実行されます。オプションで手動キーを指定できます。NAT/ ルート モードのみでサポートされるインタフェース モードでは、VPN トンネルのローカル エンドの仮想インタフェースが作成されます。

ポリシーベース VPN およびルートベース VPN の比較

FortiGate ユニットはポリシーベース VPN とルートベース VPN のどちらもサポートします。一般的には、ルートベース VPN のほうがポリシーベース VPN よりも容易に設定することができます。しかしながら、これら 2 種類の VPN には使用できる場所を制約する異なった要件があります (表 54 を参照)。

表 54: ポリシーベース VPN およびルートベース VPN の対比

ポリシーベース	ルートベース
NAT/ ルートまたはトランスペアレントモードで利用可能	NAT/ ルート モードでのみ使用可能
[Action] が [IPSEC] に設定された、VPN トンネルを指定するファイアウォール ポリシーが必要。1 つのポリシーで、両方向の接続を制御します。	[Action] が [ACCEPT] に指定された、簡潔なファイアウォール ポリシーのみが必要。各方向の接続に個別のポリシーが必要です。

ポリシーベースの VPN を作成するには、2 つのネットワークインタフェースの間に IPsec ファイアウォール ポリシーを定義して、それに VPN トンネル (フェーズ 1 またはマニュアルキー) の設定を関連付けます。作成した VPN のいずれの側からコネクションを開始しても、必要なファイアウォールポリシーはひとつだけです。

ルートベースの VPN を作成するには、VPN フェーズ 1 または手動キーの設定を作成するときに、IPsec インタフェースモードを有効にします。これにより、選択されたローカルインタフェースにバインドされた仮想 IPsec インタフェースが作成されます。次に、仮想 IPsec インタフェースともうひとつのネットワーク インタフェースの間にトラフィックが流れることを許可するために、[Action] が [ACCEPT] のファイアウォール ポリシーを定義します。VPN 両端のいずれからも接続を開始できるようにするには、各方向に 1 つずつ、合わせて 2 つのファイアウォール ポリシーが必要となります。

仮想 IPSec インタフェースのバインドはネットワークインタフェースページに表示されます (*[System]*、*[Network]*、*[Interface]* の順に選択して表示します)。物理インタフェース、アグリゲート インタフェース、VLAN インタフェース、VDOM 間リンク インタフェース、またはワイヤレス インタフェースにバインドされたすべてのトンネルの名前は関連付けられた物理インタフェースの名前カラムの下に表示されます。詳細については、89 ページの「インタフェースの設定」を参照してください。その他のインタフェースとともに、仮想 IPsec インタフェースをゾーンに加えることができます。

ハブアンドスポークの設定

ハブアンドスポーク VPN のハブとして機能するために、FortiGate ユニットにはコンセントレータ機能が含まれています。この機能はポリシーベース VPN のみで利用できますが、以下のいずれかの方法によって、ルートベース VPN でも同等の機能を実現できます。

- 集結させたい IPsec インタフェースの各ペア間で、ファイアウォール ポリシーを定義する。サイト間の接続数が多い場合、スポークの数が増加するにつれ、必要なポリシー数が急増するため、これを維持するには多くの時間がかかる場合があります。
- すべての IPsec インタフェースを 1 つのゾーンにまとめ、ひとつのゾーン間ポリシーを定義する。

- すべての IPsec インタフェースを 1 つのゾーンにまとめ、ゾーン内のトラフィックを有効にする。この場合、そのゾーン内に複数の IPsec インタフェースが必要となります。

冗長設定

ルートベース VPN を使って、VPN トンネルを冗長化させるための実装をシンプルにおこなえます。同じ宛先に異なる経路メトリックを持った複数の経路を設定することができます。また、VPN トンネルを通してダイナミックルーティング (RIP, OSPF や BGP) の経路情報の交換を設定することもできます。もし、プライマリーの VPN コネクションが切れたり、経路のプライオリティがダイナミック ルーティングにより変わると、冗長経路を使ってトラフィックを転送するために代替経路が選択されます。

単にフェイルオーバーの冗長性を提供する方法は、バックアップの IPsec インタフェースを作成することです。CLI からこの作業をおこなうことができます。設定例などの詳細については、『*FortiGate CLI リファレンス*』の、`ipsec vpn phase1-interface` コマンドの `monitor-phase1` キーワードを参照してください。

ルーティング

任意に CLI から仮想 IPsec インタフェースに特定のデフォルト ルートを定義することもできます。詳しくは、『*FortiGate CLI リファレンス*』の、`vpn ipsec phase1-interface` コマンドの `default-gw` 変数を参照してください。

自動キー (IKE)

2 つの VPN ピア (または FortiGate ダイヤルアップ サーバおよび VPN クライアント) を設定することにより、IPSec フェーズ 1 およびフェーズ 2 の交換の際に、固有の IKE (インターネット鍵交換) キーを自動的に生成できます。

フェーズ 2 パラメータを定義するとき、フェーズ 1 パラメータの任意のセットを選択することで、トンネルのセキュアな接続を確立し、リモート ピアを認証できます。

自動キーの設定は、トンネル モードとインタフェース モード双方の VPN に適用されます。

2 つの VPN ピアを設定するには、*[VPN]*、*[IPsec]*、*[Auto Key (IKE)]* の順に選択します。

[Auto Key (IKE)] ページ

このページには、IKEキーを構成する2つのVPNピアのフェーズ1およびフェーズ2の設定が表示されます。

[Create Phase 1]	新しいフェーズ 1 トンネル設定を作成します。詳細については、413 ページの「フェーズ 1 の設定」を参照してください。
[Create Phase 2]	新しいフェーズ 2 トンネル設定を作成します。詳細については、417 ページの「フェーズ 2 の設定」を参照してください。
[Phase 1]	既存のフェーズ 1 トンネル設定の名前。
[Phase 2]	既存のフェーズ 2 設定の名前。
[Interface Binding]	IPSec トンネルがバインドされるローカル インタフェースの名前。ローカル インタフェースには、物理インタフェース、アグリゲート インタフェース、VLAN インタフェース、VDOM 間インタフェース、またはワイヤレス インタフェースが該当します。
編集アイコン	交換の設定を変更するとき選択します。
削除アイコン	IKE キーを削除するとき選択します。

フェーズ 1 の設定

フェーズ 1 では、2 つの VPN ピア (または FortiGate ダイヤルアップ サーバと VPN クライアント) が相互に認証を行い、キーを交換して、双方間にセキュアな通信チャンネルを確立します。基本的なフェーズ 1 設定では、IPSec フェーズ 1 パラメータをリモート ゲートウェイに関連付け、以下を定義します。

- さまざまなフェーズ 1 パラメータが、暗号化された認証情報によって複数のラウンドで交換されるか (メイン モード)、または暗号化されていない認証情報によって単一のメッセージで交換されるか (アグレッシブ モード)。
- 2 つの VPN ピア (または VPN サーバとそのクライアント) の身元を認証するために、事前共有キーまたはデジタル証明が使用されるか。
- 接続が試みられた際、リモート VPN ピアまたはクライアントを識別するために、特別な識別子、証明書識別名、またはグループ名が使用されるか。

[New Phase 1] ページ

このページには、フェーズ 1 の設定項目が表示されます。[Auto Key (IKE)] ページで [Create Phase 1] を選択すると、画面が [New Phase 1] ページに自動的に移動します。

[Name]

フェーズ 1 の定義を表す名前を入力します。名前の長さは、インタフェース モード VPN では最大 15 文字、ポリシー ベース VPN では最大 35 文字です。[*Remote Gateway*] を [*Dialup User*] に設定する場合は、確立可能なダイヤルアップ トンネルの数に応じて、名前の最長文字数は減り、トンネル 9 個までは 2 文字、99 個までは 3 文字、999 個までは 4 文字減り、以下同様に最長文字数が短くなります。
トンネル モード VPN では、名前にリモート接続の起点を反映させる必要があります。ルート ベースのトンネルでは、FortiGate ユニットによって自動的に作成される仮想 IPSec インタフェースの名前が使用されます。

[Remote Gateway]

リモート接続のカテゴリを、以下から選択します。
[Static IP Address] – リモート ピアの IP アドレスがスタティック IP アドレスである場合に選択します。
[Dialup User] – ダイナミック IP アドレスを持つ 1 つ以上の FortiClient または FortiGate ダイヤルアップ クライアントが FortiGate ユニットに接続する場合に選択します。
[Dynamic DNS] – ドメイン名を持ちダイナミック DNS サービスに登録しているリモート ピアが、FortiGate ユニットに接続する場合に選択します。

[IP Address]

[Static IP Address] を選択した場合に、リモート ピアの IP アドレスを入力します。

[Dynamic DNS]

[Dynamic DNS] を選択した場合に、リモート ピアのドメイン名を入力します。

[Local Interface]

このオプションは、NAT/ ルート モードでのみ使用できます。リモート ピアまたはダイヤルアップ クライアントが FortiGate ユニットに接続するとき経由する、インタフェースの名前を選択します。
デフォルトでは、ローカル VPN ゲートウェイの IP アドレスは、選択したインタフェースの IP アドレスです。オプションで、VPN ゲートウェイの固有 IP アドレスを、*[Advanced]* 設定で指定できます。

[Mode]

[Main (ID Protection)] または *[Aggressive]* を選択します。
- [Main] モードでは、フェーズ 1 パラメータは暗号化された認証情報とともに複数のラウンドで交換されます。
- [Aggressive] モードでは、フェーズ 1 パラメータは暗号化されていない認証情報とともに単一のメッセージで交換されます。

VPN ピアが、ダイナミック IP アドレスを持ち、事前共有キーにより認証される場合は、インタフェース IP アドレスのダイヤルアップ フェーズ 1 設定が複数あれば、必ず [Aggressive] モードを選択します。
リモート VPN ピアが、ダイナミック IP アドレスを持ち、証明書により認証される場合は、インタフェース IP アドレスのダイヤルアップ フェーズ 1 設定が複数あり、これらのフェーズ 1 設定が異なるプロトコルを使用するのであれば、必ず [Aggressive] モードを選択します。
[Peer Options] 設定に特定のモードが必要になる場合があります。下記の [Peer Options] を参照してください。

[Authentication Method]

[Preshared Key] または *[RSA Signature]* を選択します。

[Pre-shared Key]

[Authentication Method] で *[Pre-shared Key]* を選択した場合は、事前共有キーを入力します。FortiGate ユニットは、フェーズ 1 のネゴシエーション中にこの事前共有キーを用いて、リモート ピアまたはダイヤルアップ クライアントに対してユニット自体の認証を行います。リモート ピアまたはクライアントでは、同じ値を定義する必要があります。この鍵には、印字可能な文字が 6 字以上含まれる必要があり、ネットワーク管理者以外にこの鍵を知られてはなりません。既知の攻撃に対して最大限の保護を実施するためには、鍵にはランダムに選択した 16 字以上の英数文字を使用してください。

[Certificate Name] [Authentication Method] で *[RSA Signature]* を選択した場合、サーバ証明書の名前を選択します。FortiGate ユニットは、フェーズ 1 のネゴシエーション中にそのサーバ証明書を用いて、リモート ピアまたはダイヤルアップ クライアントに対してユニット自体の認証を行います。必要なサーバ証明書を取得およびロードする方法については、『*FortiGate 証明書管理ユーザ ガイド*』を参照してください。

[Peer Options] *[Remote Gateway]* および *[Authentication Method]* の設定に応じて、VPN ピアまたはクライアントを認証するための、以下の1つまたは複数のオプションが表示されます。

[Accept any peer ID] 任意のリモート VPN ピアまたはクライアントのローカル ID を受け入れます。FortiGate ユニットでは識別子 (ローカル ID) の確認は行われません。*[Mode]* を、*[Aggressive]* または *[Main]* のどちらにも設定できます。
このオプションを、RSA シグネチャ認証で使用できます。ただし、最高レベルのセキュリティを確保するには、ピアの PKI ユーザ / グループを設定し、*[Peer Options]* を *[Accept this peer certificate only]* に設定してください。

[Accept this peer ID] このオプションは、リモート ピアにダイナミック IP アドレスが設定されている場合に限り使用できます。リモート ピアを認証するために使用する、識別子を入力します。この識別子は、リモート ピアの管理者が設定した識別子と一致する必要があります。
リモート ピアが FortiGate ユニットである場合、フェーズ 1 設定の *[Local ID]* フィールドに識別子を指定します。
リモート ピアが FortiClient ダイヤルアップ クライアントである場合は、VPN 接続の *[Advanced Settings]* の *[Policy]* セクションで *[Config]* を選択して表示される *[Local ID]* フィールドに、識別子を指定します。

[Accept peer ID in dialup group] 同じ VPN トンネルを経由して、固有の識別子および固有の PSK (または固有の PSK のみ) を使用する、複数の FortiGate または FortiClient ダイヤルアップ クライアントを認証します。
認証用としてダイヤルアップ ユーザ グループを必ず作成します (詳細については、457 ページの「ユーザ グループ」を参照してください)。*[Accept peer ID in dialup group]* オプションの横に表示されるリストから、グループを選択します。
FortiGate ダイヤルアップ クライアントの設定方法については、『FortiGate *IPSec VPN ユーザ ガイド*』を参照してください。FortiClient ダイヤルアップ クライアントの設定方法については、『*FortiClient ダイヤルアップ クライアント認証テクニカル ノート*』を参照してください。
ダイヤルアップ クライアントが固有の識別子および固有の PSK を使用する場合は、*[Mode]* を *[Aggressive]* に設定する必要があります。ダイヤルアップ クライアントが固有の PSK のみを使用する場合に、このインタフェース IP アドレスに対するダイヤルアップ フェーズ 1 設定が 1 つのみであれば、*[Mode]* を *[Main]* に設定できます。

[Advanced] フェーズ 1 の詳細パラメータを定義します。詳細については、415 ページの「フェーズ 1 の詳細設定」を参照してください。

フェーズ 1 の詳細設定

詳細設定に含まれている *[P1 Proposal]* のパラメータを設定することで、IKE 交換キーの生成時に FortiGate ユニットによって使用される、暗号化および認証アルゴリズムを選択します。また、この詳細設定を選択し、フェーズ 1 ネゴシエーションの円滑な実行を保証できます。

[New Phase 1] ページの [Advanced] セクション

[Enable IPsec Interface Mode] このオプションは、NAT/ ルート モードでのみ使用できます。
VPN トンネルのローカル エンドに仮想インタフェースを作成します。このチェック ボックスをオンにするとルートベース VPN を作成し、オフにするとポリシーベース VPN を作成します。

[IKE Version] 使用する IKE のバージョンとして、[1] または [2] を選択します。デフォルトは [1] です。このオプションは、*[Enable IPsec Interface Mode]* を有効に設定している場合のみ利用できます。IKE v2 の詳細については、RFC 4306 を参照してください。
[Mode] を *[Aggressive]* に設定している場合は、IKE v2 は利用できません。*[IKE Version]* が *[2]* の場合は、*[Mode]* および *[XAUTH]* は利用できません。

[IPv6 Version] リモート ゲートウェイおよびインタフェース IP アドレスに IPv6 を使用する場合に選択します。このオプションは、[Enable IPsec Interface Mode] を有効に設定し、管理設定で [IPv6 Support] を有効に設定している場合のみ利用できます。

[Local Gateway IP]

[Enable IPsec Interface Mode] をオンにした場合、VPN トンネルのローカル エンドの IP アドレスを指定します。次のいずれかを選択します。
[Main Interface IP] – FortiGate ユニットはインタフェースの IP アドレスをネットワーク インタフェース設定から取得します。詳細については、89 ページの「インタフェースの設定」を参照してください。
Specify – フェーズ 1 の *[Local Interface]* フィールドで選択したインタフェースの第 2 アドレスを指定できます。詳細については、414 ページの「[Local Interface]」を参照してください。
トランスペアレント モード VDOM では、インタフェース モードを設定できません。

[P1 Proposal]

ネゴシエーションを保護するためのキーの生成に使用する、暗号化および認証アルゴリズムを選択します。
必要に応じて、暗号化および認証アルゴリズムを追加または削除します。組み合わせを、3 つまで選択します。定義したプロポーザルを少なくとも 1 つは使用するように、リモート ピアまたはクライアントを設定する必要があります。

以下のいずれかの対称キー アルゴリズムを選択します。
DES — 56 ビット キーを使用する 64 ビット ブロック アルゴリズム。
3DES — プレーン テキストが 3 つのキーで 3 回暗号化されるトリプル DES。
AES128 – 128 ビット キーを使用する、128 ビット ブロック CBC (Cipher Block Chaining) アルゴリズム
AES192 – 192 ビット キーを使用する、128 ビット ブロック CBC (Cipher Block Chaining) アルゴリズム
AES256 – 256 ビット キーを使用する、128 ビット ブロック CBC (Cipher Block Chaining) アルゴリズム

次のメッセージ ダイジェストのいずれかを選択して、フェーズ 1 ネゴシエーション中のメッセージの信憑性を確認します。
MD5 (Message Digest 5) — RSA Data Security が開発したハッシュ アルゴリズム。
SHA1 — Secure Hash Algorithm 1。160 ビットのメッセージ ダイジェストを生成します。
SHA256 — Secure Hash Algorithm 2。256 ビットのメッセージ ダイジェストを生成します。
3つ目の組み合わせを指定するには、2つ目の組み合わせを設定するフィールドの横にある*追加*ボタンをクリックします。

[DH Group]

DH Group 1、2、5、および 14 の各チェック ボックスをオンにして、1 つまたは複数の Diffie-Hellman グループを選択します。リモート ピアまたはクライアントの *[DH Group]* 設定の 1 つ以上が、FortiGate ユニットの設定と一致する必要があります。

[Keylife]

IKE 暗号化キーが期限切れになるまでの時間 (秒) を入力します。キーが期限切れになると、サービスを中断させることなく、新しいキーが生成されます。[Keylife] は 120 ～ 172,800 秒に設定できます。

[Local ID]

FortiGate ユニットが VPN クライアントとして動作し、認証にピア ID を使用している場合は、フェーズ 1 交換中に FortiGate ユニットが VPN サーバに提供する識別子を入力します。
FortiGate ユニットが VPN クライアントとして動作し、認証にセキュリティ証明書を使用している場合は、FortiGate ユニットが認証に使用するローカル サーバ証明書の識別名 (DN) を選択します。
FortiGate ユニットがダイヤルアップ クライアントで、他のダイヤルアップ クライアントとトンネルを共有しない場合 (つまり、トンネルがこの FortiGate のダイヤルアップ クライアント専用となる場合)、*[Mode]* を *[Aggressive]* に設定します。

[XAuth]

このオプションは、ダイヤルアップ クライアントの認証をサポートし、IKE v1 のみで利用できます。

[Disable] – XAuth を使用しない場合に選択します。

[Enable as Client] – FortiGate ユニットがダイヤルアップ クライアントの場合は、FortiGate ユニットがリモートの XAuth サーバに対して自己認証するために必要なユーザ名とパスワードを入力します。

[Enable as Server] – このオプションは、*[Remote Gateway]* を *[Dialup User]* に設定した場合のみ利用できます。ダイヤルアップ クライアントは、ダイヤルアップ ユーザ グループのメンバとして認証を行います。最初に、FortiGate ユニット背後にあるネットワークにアクセスする必要があるダイヤルアップ クライアントのユーザ グループを、必ず作成します。詳細については、460 ページの「ユーザ グループの設定」を参照してください。

また、認証リクエストを外部の RADIUS または LDAP 認証サーバに転送するように、FortiGate ユニットを設定する必要があります。これらのトピックの詳細については、450 ページの「RADIUS サーバの設定」または 452 ページの「LDAP サーバの設定」を参照してください。

FortiGate ユニット、XAuth クライアント、および外部認証サーバの間で使用する暗号化の種類を決定するために、*[Server Type]* 設定を選択し、続いて [User Group] リストからユーザ グループを選択します。

[Username] 認証に使用するユーザ名を入力します。

[Password] 認証に使用するパスワードを入力します。

[NAT Traversal] ローカルの FortiGate ユニットと VPN ピアまたはクライアントとの間に NAT デバイスが存在する場合は、このチェック ボックスをオンにします。信頼性の高い接続を確立するには、ローカル FortiGate ユニットと VPN ピアまたはクライアントの NAT トラバーサル設定が同一である必要があります (両方を選択または解除)。

[Keepalive Frequency] *[NAT-traversal]* を有効に設定した場合は、[Keepalive Frequency] の設定を入力します。入力する数値は、10 ～ 900 秒の範囲で間隔を表します。

[Dead Peer Detection] このチェック ボックスをオンにすると、アイドル状態の接続においてVPN トンネルが回復するとともに、必要に応じて、切断された IKE ピアを除去します。このオプションを使用することで、トンネルの始動または停止時に通知を受け取るか、またはトンネル内でトラフィックが発生しない場合にトンネル接続を開いたままの状態にできます (たとえば、定期的に変化する IP アドレスからダイヤルアップ クライアントまたはダイナミック DNS ピアが接続する状況では、IP アドレスが変化する間にトラフィックが一時的に中断される場合があります)。
[Dead Peer Detection] オプションをオンにした状態では、CLI コマンド `config vpn ipsec phase1` (トンネル モード) または `config vpn ipsec phase1-interface` (インタフェース モード) を使用して、リトライの回数と間隔をオプションで指定できます。詳細については、『*FortiGateCLI リファレンス*』を参照してください。

フェーズ 2 の設定

IPsec フェーズ 1 のネゴシエーションが正しく終了した後、フェーズ 2 を開始します。フェーズ 2 パラメータを設定することで、以降のセッションで扱われるデータを暗号化および転送するために、FortiGate ユニットによって使用されるアルゴリズムを定義します。フェーズ 2 では、セキュリティ サービスを実装しトンネルを確立するために必要な、特定の IPSec セキュリティ アソシエーションを選択します。

フェーズ 2 の基本設定では、IPsec フェーズ 2 パラメータと、VPN トンネルのリモート エンドポイントを指定するフェーズ 1 設定を関連付けます。ほとんどの場合、設定する必要があるのは基本的なフェーズ 2 設定のみです。

[New Phase 2] ページ

このページには、フェーズ 2 の設定項目が表示されます。[Auto Key (IKE)] ページで [Create Phase 2] を選択すると、画面が [New Phase 2] ページに自動的に移動します。

[Name] フェーズ 2 の設定を識別する名前を入力します。

[Phase 1] フェーズ 1 トンネル設定を選択します。詳細については、413 ページの「フェーズ 1 の設定」を参照してください。フェーズ 1 設定では、リモート VPN ピアまたはクライアントがこのトンネルでどのように認証されるか、またリモート ピアまたはクライアントへの接続がどのように保護されるかを設定します。

[Advanced] フェーズ 2 詳細パラメータを定義します。詳細については、417 ページの「フェーズ 2 の詳細設定」を参照してください。

フェーズ 2 の詳細設定

フェーズ 2 では、FortiGate ユニットと VPN ピアまたはクライアントが再びキーを交換し合い、セキュアな通信チャンネルを確立します。セキュリティ アソシエーション (SA) の実装詳細を保護するために、キーの生成に必要な暗号化および認証アルゴリズムを選択します。これらは、P2 Proposal パラメータと呼ばれます。キーは、Diffie-Hellman のアルゴリズムを使用して、自動的に生成されます。

フェーズ 2 の各種の詳細設定を使用することで、トンネルの機能を強化できます。

[Advanced section of New Phase 2] ページ

[P2 Proposal] リモート VPN ピアに提案される、暗号化および認証アルゴリズムを選択します。このプロポーザルは、3 つまで指定できます。VPN 接続を確立するには、指定したプロポーザルの少なくとも 1 つが、リモート ピアの設定と一致する必要があります。
ページには、デフォルトで 2 つのプロポーザルが表示されます。2 番目の *[Authentication]* フィールドの横には、*追加*アイコンおよび*削除*アイコンが表示されます。プロポーザルを 1 つだけ指定する場合は、*削除*アイコンを使用して 2 番目のプロポーザルを削除します。3 番目のプロポーザルを指定するには、*追加*アイコンを選択します。
[Encryption] および *[Authentication]* の双方を [NULL] に設定するのは無効です。

[Encryption] 以下のいずれかの対称キー アルゴリズムを選択します。
NULL — 暗号化アルゴリズムを使用しません。
DES (Digital Encryption Standard) — 56 ビット キーを使用する 64 ビット ブロック アルゴリズム。
3DES — プレーン テキストが 3 つのキーで 3 回暗号化されるトリプル DES。
AES128 – 128 ビット キーを使用する、128 ビット ブロック CBC (Cipher Block Chaining) アルゴリズム
AES192 – 192 ビット キーを使用する、128 ビット ブロック CBC (Cipher Block Chaining) アルゴリズム
AES256 – 256 ビット キーを使用する、128 ビット ブロック CBC (Cipher Block Chaining) アルゴリズム

[Authentication] 次のメッセージ ダイジェストのいずれかを選択して、暗号化されたセッション中に、メッセージの信憑性を確認します。
NULL — メッセージ ダイジェストを使用しません。
MD5 (Message Digest 5) — RSA Data Security が開発したハッシュ アルゴリズム。
SHA1 — Secure Hash Algorithm 1。160 ビットのメッセージ ダイジェストを生成します。
SHA256 — Secure Hash Algorithm 2。256 ビットのメッセージ ダイジェストを生成します。

[Enable replay detection] オプションで、リプレイ攻撃の検知を有効または無効にします。リプレイ攻撃は、許可されていない相手が一連の IPsec パケットを傍受し、トンネルに向けてそれを再送信することで発生します。

[Enable perfect forward secrecy (PFS)] PFS を有効または無効にします。PFS (Perfect Forward Secrecy) は、キーの期限が切れるたびに新しいDiffie-Hellman交換を強制的に実行することにより、セキュリティを強化します。

[DH Group] Diffie-Hellman グループのオプションを、1 つ選択します (1、2、5、または 14)。この DH Group は、リモート ピアまたはダイヤルアップ クライアントが使用する DH Group と一致する必要があります。

[Keylife] フェーズ 2 キーの期限を定める方法を、*[Seconds]* (秒)、*[Kbytes]* (キロバイト)、または *[Both]* (両方)、から選択します。*[Both]* を選択した場合、指定の時間が経過するか、または指定のバイト数の処理が完了すると、キーは期限切れとなります。範囲は 120 ～ 172,800 秒、または 5120 ～ 2,147,483,648 KB です。

[Autokey Keep Alive] データが処理されていない間もトンネルを有効に維持する場合は、このチェック ボックスをオンにします。

[DHCP-IPSec] VPN クライアントに、ＩＰ アドレスを動的に付与します。このオプションは、ダイヤルアップのフェーズ 1 設定と関連するフェーズ 2 設定のみで使用できます。
また、DHCP サーバまたはプライベート ネットワーク インタフェース上のリレーを設定する必要があります。DHCP パラメータは、必ず別途設定します。詳細については、133 ページの「システム - DHCP サーバ」を参照してください。
RADIUS ユーザ グループの属性に基づき IP アドレスを割り当てるように、DHCP サーバを設定する場合は、フェーズ 1 の *[Peer Options]* を *[Accept peer ID in dialup group]* に設定し、適切なユーザ グループを選択します。詳しくは、413 ページの「フェーズ 1 の設定」を参照してください。
FortiGate ユニットがダイヤルアップ サーバとして機能し、ダイヤルアップ サーバの背後にあるネットワークと一致する FortiClient ダイヤルアップ クライアント VIP アドレスを手動で割り当てた場合は、このチェック ボックスをオンにすると、FortiGate ユニットはダイヤルアップ クライアントのプロキシとして機能します。

[Quick Mode Selector] オプションで、IKE ネゴシエーションのセレクタとして使用する、送信元および宛先 IP アドレスを指定します。FortiGate ユニットがダイヤルアップ サーバである場合、VPN を構成する 1 つ以上のプライベート ネットワーク間の IP アドレスが不明瞭なことによって生じる問題を防止する必要がある場合を除き、デフォルト値の 0.0.0.0/0 を変更しないでください。単一のホスト IP アドレス、IP アドレス範囲、またはネットワーク アドレスを指定できます。オプションで、送信元と宛先のポート番号およびプロトコル番号を指定できます。
既存のフェーズ 2 設定を編集する場合、ファイアウォールのアドレスをセレクタとして使用するようにトンネルが設定されていると、*[Source address]* および *[Destination address]* のフィールドは使用できません。このオプションは、CLI でのみ使用できます。詳しくは、『*FortiGate CLI リファレンス*』の、`vpn ipsec phase2` コマンドのキーワード、`dst-addr-type`、`dst-name`、`src-addr-type`、および `src-name` を参照してください。

[Source address] FortiGate ユニットがダイヤルアップ サーバである場合、ローカルの送信者、またはローカル VPN ピアの背後にあるネットワークに対応する、送信元 IP アドレスを入力します（たとえば、サブネットには `172.16.5.0/24` または `172.16.5.0/255.255.255.0`、サーバまたはホストには `172.16.5.1/32` または `172.16.5.1/255.255.255.255`、あるいはアドレス範囲には `192.168.10.[80-100]` または `192.168.10.80-192.168.10.100` など）。`0.0.0.0/0` の値は、ローカル VPN ピア背後のすべての IP アドレスを意味します。
FortiGate ユニットがダイヤルアップ クライアントである場合、送信元アドレスは、FortiGate ダイヤルアップ クライアントの背後にあるプライベート ネットワークを参照する必要があります。

[Source port] 指定されたサービス（プロトコル番号）に関係するトラフィックを伝送するために、ローカル VPN ピアによって使用されるポート番号を入力します。範囲は、0 ～ 65535 です。すべてのポートを指定するには、`0` を入力します。

[Destination address] リモート VPN ピアの背後にある受信者またはネットワークに対応する宛先 IP アドレスを入力します（たとえば、サブネットには `192.168.20.0/24`、サーバまたはホストには `172.16.5.1/32`、あるいはアドレス範囲には `192.168.10.[80-100]` など）。`0.0.0.0/0` の値は、リモート VPN ピアの背後にあるすべての IP アドレスを意味します。

[Destination port] 指定されたサービス（プロトコル番号）に関係するトラフィックを伝送するためにリモート VPN ピアが使用するポート番号を入力します。範囲は、0 ～ 65535 です。すべてのポートを指定するには、`0` を入力します。

[Protocol] サービスの IP プロトコル番号を入力します。範囲は、`0` ～ `255` です。すべてのサービスを指定するには、`0` を入力します。

注記：VPN ユーザが FortiGate ユニット経由でインターネットを閲覧できるように、各項目を設定できます。詳細については、421 ページの「インターネット ブラウジング」を参照してください。

手動キー

注意：手動キーは、やむを得ない場合のみ使用してください。キーの機密性を保持すること、およびリモート VPN ピアに変更キーを安全に伝えることは、困難な場合があります。

必要に応じて、IPSec VPN トンネルを確立するための暗号化キーを手動で定義できます。手動キーは、次のような状況で定義します。

- 暗号化キーまたは認証キーについての予備知識が必要な（いずれかの VPN ピアが特定の IPSec 暗号化キーまたは認証キーを必要とする）場合。
- 暗号化および認証を無効にする必要がある場合。

どちらの場合も、IPSec のフェーズ 1 およびフェーズ 2 のパラメータは指定せず、*[VPN]*、*[IPSEC]*、*[Manual Key]* の順に選択して表示されるページで、手動キーを定義します。

[Manual Key] ページ

このページには、IPsec VPN を確立するために作成した暗号化キーが一覧表示されます。

[Create New] 新しい手動キー設定を作成します。詳しくは、420 ページの「新しい手動キーの設定」を参照してください。

[Tunnel Name]	既存の手動キー設定の名前。
[Remote Gateway]	リモート ピアまたはダイヤルアップ クライアントの IP アドレス。
[Encryption Algorithm]	手動キー設定で指定された暗号化アルゴリズムの名前。
[Authentication Algorithm]	手動キー設定で指定された認証アルゴリズムの名前。
編集アイコン	暗号化キーの設定を編集するとき選択します。
削除アイコン	リストから暗号化キーを削除するとき選択します。

新しい手動キーの設定

注意：実際のシステム環境に適するセキュリティ ポリシー、SA、セレクタ、および SA データベースを扱い慣れていない場合は、必ず資格を持つ専門技術者の協力を得て、以下の手順を実施してください。

一方の VPN デバイスのキーを手動で設定する場合は、他方の VPN デバイスのキーも同一の認証キーおよび暗号化キーを用いて同様に手動で設定する必要があります。また、両方の VPN デバイスを相補的な SPI（セキュリティ パラメータ インデックス）で設定することが重要です。デバイスの管理者同士が連携しながら、これらの設定を行う必要があります。

各 SPI は、SA（セキュリティ アソシエーション）を識別します。値は、ESP データグラムを SA にリンクするために、そのデータグラムに配置されます。ESP データグラムを受信すると、受信者は SPI を参照して、データグラムに適用する SA を決定します。SPI は、SA ごとに必ず手動で指定します。通信の方向ごとに SA があるので、各 VPN にローカル SPI およびリモート SPI の 2 つの SPI を指定して、2 台の VPN デバイス間の双方向通信に対応する必要があります。

[New Manual Key] ページ

このページでは、IPsec VPN の暗号化キーを設定できます。

[Name]	VPN トンネルの名前を入力します。名前の長さは、インタフェース モード VPN では最大 15 文字、ポリシーベース VPN では最大 35 文字です。
[Local SPI]	ローカル FortiGate ユニットの送信トラフィックを処理する SA を表す、16 進数の値（最大 8 文字、0 ～ 9、a ～ f）を入力します。有効範囲は、`0x100` ～ `0xffffffff` です。この値は、リモート ピアにおける手動キー設定の [Remote SPI] の値と一致する必要があります。
[Remote SPI]	ローカル FortiGate ユニットの受信トラフィックを処理する SA を表す、16 進数の値（最大 8 文字、0 ～ 9、a ～ f）を入力します。有効範囲は、`0x100` ～ `0xffffffff` です。この値は、リモート ピアにおける手動キー設定の [Local SPI] の値と一致する必要があります。
[Remote Gateway]	リモート ピアへのパブリック インタフェースの IP アドレスを入力します。このアドレスは、ESP データグラムの受信者を識別します。
[Local Interface]	このオプションは、NAT/ ルート モードでのみ使用できます。IPsec トンネルが結合されるインタフェースの名前を選択します。FortiGate ユニットは、ネットワーク インタフェースの設定から、インタフェースの IP アドレスを取得します。詳細については、89 ページの「インタフェースの設定」を参照してください。
[Encryption Algorithm]	以下のいずれかの対称キー暗号化アルゴリズムを選択します。 **NULL** — 暗号化アルゴリズムを使用しません。 **DES (Digital Encryption Standard)** — 56 ビット キーを使用する 64 ビット ブロック アルゴリズム。 **3DES** — プレーン テキストが 3 つのキーで 3 回暗号化されるトリプル DES。 **AES128** – 128 ビット キーを使用する、128 ビット ブロック CBC (Cipher Block Chaining) アルゴリズム **AES192** – 192 ビット キーを使用する、128 ビット ブロック CBC (Cipher Block Chaining) アルゴリズム **AES256** – 256 ビット キーを使用する、128 ビット ブロック CBC (Cipher Block Chaining) アルゴリズム **注記**：暗号化および認証に使用されるアルゴリズムは、両方を NULL に設定することはできません。

[Encryption Key]	暗号化アルゴリズムに適する暗号化キーを入力します。 · DES を選択した場合は、16 字の 16 進数 (0 ～ 9、a ～ f) を入力します。 · 3DES を選択した場合は、48 字の 16 進数 (0 ～ 9、a ～ f) を、3 つの 16 文字セグメントに分けて入力します。 · AES128 を選択した場合は、32 字の 16 進数 (0 ～ 9、a ～ f) を、2 つの 16 文字セグメントに分けて入力します。 · AES192 を選択した場合は、48 字の 16 進数 (0 ～ 9、a ～ f) を、3 つの 16 文字セグメントに分けて入力します。 · AES256 を選択した場合は、64 字の 16 進数 (0 ～ 9、a ～ f) を、4 つの 16 文字セグメント分けて入力します。
[Authentication Algorithm]	以下のいずれかのメッセージ ダイジェストを選択します。 **NULL**— メッセージ ダイジェストを使用しません。 **MD5 (Message Digest 5)** — 128 ビットのメッセージ ダイジェストを生成するアルゴリズム。 **SHA1** — Secure Hash Algorithm 1。160 ビットのメッセージ ダイジェストを生成します。 **SHA256** — Secure Hash Algorithm 2。256 ビットのメッセージ ダイジェストを生成します。 **注記**：暗号化および認証に使用されるアルゴリズムは、両方を NULL に設定することはできません。
[Authentication Key]	認証アルゴリズムに適する認証キーを入力します。 · MD5 を選択した場合は、32 字の 16 進数 (0 ～ 9、a ～ f) を、2 つの 16 文字セグメントに分けて入力します。 · SHA1 を選択した場合は、40 字の 16 進数を、2 つの 16 文字セグメントおよび 1 つの 8 文字セグメントの、3 つのセグメントに分けて入力します。 · SHA256 を選択した場合は、64 字の 16 進数を、4 つの 16 文字セグメントに分けて入力します。 ダイジェストの入力範囲は、0 ～ 9、および a ～ f です。
[IPSec Interface Mode]	VPN トンネルのローカル エンドに仮想インタフェースを作成します。このチェック ボックスをオンにするとルートベース VPN を作成し、オフにするとポリシーベース VPN を作成します。 このオプションは、NAT/ ルート モードでのみ使用できます。

インターネット ブラウジング

適切なファイアウォールポリシーを使用することにより、VPN ユーザの FortiGate ユニット経由によるインターネット閲覧が可能になります。必要なポリシーは、ポリシーベース VPN とルートベース VPN で異なります。詳細については、268 ページの「ファイアウォール ポリシーの設定」を参照してください。

コンセントレータ

ハブアンドスポークの構成では、多数のリモート ピアへのポリシー ベース VPN 接続は、中央にある単一の FortiGate ユニットから放射状に広がります。リモート ピア同士のサイト間接続は存在しませんが、ハブ FortiGate ユニットを経由することで、任意の 2 つのリモート ピア間に VPN トンネルを確立できます。

ハブアンドスポーク ネットワークでは、VPN トンネルはすべてハブが終端となります。ハブに接続するピアは「スポーク」と呼ばれます。ハブは、ネットワークのコンセントレータとして機能し、スポーク間のすべての VPN 接続を管理します。VPN トラフィックは、ハブを介して 1 つのトンネルから別のトンネルへと進みます。

ハブアンドスポーク設定にスポークが含まれるように、コンセントレータを定義します。コンセントレータを作成するには、[VPN]、[IPSec]、[Concentrator] の順に選択します。コンセントレータの設定では、IPSec ハブアンドスポーク設定に加えるスポークを指定します。

[Concentrator] ページ

このページには、スポークから構成されるコンセントレータが一覧表示されます。このページでは、コンセントレータを編集、削除、または新規作成できます。

[Create New]	IPSec ハブアンドスポーク設定の新しいコンセントレータを定義します。詳細については、422 ページの「VPN のモニタ」を参照してください。

[Concentrator Name]	既存の IPsec VPN コンセントレータの名前。
[Members]	コンセントレータと関連付けられるトンネル。
削除アイコン	リストからコンセントレータを削除するとき選択します。
編集アイコン	コンセントレータの設定を編集するとき選択します。
[New VPN Concentrator]	ここでは、IPsec トンネル (メンバと呼ばれる) から構成されるコンセントレータを設定できます。
[Concentrator Name]	コンセントレータの名前を入力します。
[Available Tunnels]	定義済みの IPSec VPN トンネルのリスト。このリストからトンネルを選択し、右向きの矢印をクリックします。この手順を繰り返し、スポークに関連付けられるすべてのトンネルを、コンセントレータに加えます。
[Members]	コンセントレータのメンバであるトンネルのリスト。コンセントレータからトンネルを削除するには、トンネルを選択し左向きの矢印をクリックします。

VPN のモニタ

VDOM

IPSec モニタを使用することにより、IPSec VPN トンネルの活動を表示し、それらのトンネルを開始または停止できます。モニタ リストには、トンネル モードおよびルートベース (インタフェース モード) トンネルを含む、アクティブなすべてのトンネルの、アドレス、プロキシ ID、タイムアウトなどの情報が表示されます。

ダイヤルアップ VPN の場合、モニタ リストには、ダイヤルアップ クライアントにより確立された VPN トンネルについての、IP アドレスなどのステータス情報が表示されます。リストに表示されるトンネルの数は、ダイヤルアップ クライアントの接続および接続切断に応じて変わる可能性があります。

スタティック IP またはダイナミック DNS VPN の場合、モニタ リストには、IP アドレスまたはドメイン名を持つリモート ピアに対する VPN トンネルについての、ステータスおよび IP アドレッシング情報、アクティブまたは非アクティブの状態が表示されます。また、リストから個々のトンネルを開始または停止できます。

フィルタを使用することにより、リストにどの情報を表示するかを調整できます。詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。

[Monitor] ページ

このページには、現在モニタされている IPSec VPN が一覧表示されます。IPSec VPN の表示を、Dialup または Static or Dynamic DNS に切り替えることができます。

[Type]	リストに表示する VPN の種類を、[All]、[Dialup]、または [Static IP or Dynamic DNS] から選択します。
[Column Settings]	テーブルの表示をカスタマイズします。カラムの表示、非表示を選択し、テーブル内のカラムの表示順序を指定できます。詳細については、34 ページの「表示されるカラムのカラム設定を使用した制御」および 35 ページの「」を参照してください。
[Clear All Filters]	適用されているカラム表示フィルタをすべて解除するとき選択します。
ページ コントロール	表示されているリスト項目の現在のページ番号。左右の矢印を選択し、モニタされる VPN の最初、前、次、または最後のページを表示します。
フィルタ アイコン	指定した条件に応じて IPsec モニタ リストをフィルタ処理または並べ替えるための、カラムフィルタを編集します。詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。
[Name]	VPN のフェーズ 1 設定の名前。
[Type]	[Type] フィールドで [All] を選択したとき表示されます。
[Remote Gateway]	リモート ホスト デバイスのパブリック IP アドレス。または、リモート ホストの前に NAT デバイスがある場合は、NAT デバイスのパブリック IP アドレス。
[Remote Port]	リモート ホスト デバイスの UDP ポート。または、リモート ホストの前に NAT デバイスがある場合は、NAT デバイスの UDP ポート。ゼロ (0) は、どのポートも使用されることを示します。

[Proxy ID Source]	FortiGate ユニットの背後にあるホスト、サーバ、またはプライベート ネットワークの IP アドレス。ファイアウォール暗号化ポリシーの送信元アドレスが IP アドレスの範囲として表される場合は、ページにネットワーク範囲が表示されます。
[Proxy ID Destination]	FortiClient ダイヤルアップ クライアントによりトンネルが確立される場合、次の表示になります。 ・ VIP アドレスが使用されない場合、[Proxy ID Destination] フィールドには、リモート ホストのネットワーク インタフェース カード (NIC) のパブリック IP アドレスが表示されます。 ・ VIP アドレスを (手動または FortiGate の DHCP リレーにより) 設定した場合、[Proxy ID Destination] フィールドには、FortiClient ダイヤルアップ クライアントに属する VIP アドレス、または VIP アドレスが指定されたサブネット アドレスのいずれかが表示されます。 FortiGate のダイヤルアップ クライアントによりトンネルが確立される場合、[Proxy ID Destination] フィールドには、リモート プライベート ネットワークの IP アドレスが表示されます。
[Status]	緑の矢印は、現在トンネルがトラフィックを処理していることを意味します。これを選択すると、トンネルが停止します。 赤の矢印は、トンネルがトラフィックを処理していないことを意味します。これを選択すると、トンネルが開始します。
[Reset Statistics]	ページに表示されている現在の統計をリセットするとき選択します。

PPTP VPN

FortiGate ユニットでは、2 つの VPN ピア間で PPP トラフィックをトンネリングするための、PPTP がサポートされます。Windows または Linux の PPTP クライアントは、PPTP サーバとして機能するように設定された FortiGate ユニットとの間に、PPTP トンネルを確立できます。または、FortiGate ユニットの背後にあるネットワーク上の PPTP サーバに PPTP パケットを転送するように、FortiGate ユニットを設定することも可能です。

PPTP VPN は、NAT/ ルート モードでのみ使用できます。現時点では、PPTP セッションの最大数は 254 です。FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとに VPN PPTP を個別に設定する必要があります。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

FortiGate ユニットを PPTP ゲートウェイとして使用する場合は、ローカル アドレス範囲から PPTP クライアント IP を選択するか、または PPTP ユーザ グループで定義されたサーバを使用できます。IP アドレスを取得するために使用する方法を選択し、ユーザ グループ サーバの場合は、IP アドレスおよびユーザ グループを指定します。

この項では、PPTP クライアントの IP アドレス範囲を指定する方法、またはトンネルのセットアップで使用するクライアント側 IP アドレスを設定する方法について説明します。PPTP VPN をセットアップするための他の設定方法については、『*FortiGate PPTP VPN ユーザ ガイド*』を参照してください。

この項には以下のトピックが含まれています。

注記： FortiGate Web ベース マネージャでは、PPTP 機能はデフォルトで無効に設定されています。PPTP トンネルを設定するには、カスタムの FortiGate 画面を作成します。

FortiGate Web ベース マネージャによる PPTP 設定

PPTP トンネルを設定するには、Web ベース マネージャでカスタム画面を作成します。Web ベース マネージャの *[Categories]* 見出し下に表示される *[Additional]* カテゴリの 1 つに、*[PPTP Range]* タブがあります。

PPTP には、トンネルの各端に 1 つずつ、IP アドレスが必要です。PPTP アドレス範囲は、リモート PPTP クライアント用に予約されたアドレスの範囲です。リモート PPTP クライアントが接続を確立すると、FortiGate ユニットは、予約された IP アドレス範囲から IP アドレスをクライアント PPTP インタフェースに割り当てるか、または割り当てられた IP アドレスを PPTP ユーザ グループから取得します。PPTP ユーザ グループを使用する場合は、FortiGate ユニットの IP アドレスを *[Local IP]* (Web ベース マネージャ) *または* `local-ip` (CLI) に入力し、トンネルの FortiGate 側端を定義する必要があります。PPTP クライアントは接続中、割り当てられた IP アドレスを送信元アドレスとして使用します。

PPTP を有効にして、PPTP アドレス範囲を指定するか、または PPTP クライアント側でピアのリモート IP の IP アドレスを指定するには、Web ベース マネージャでカスタム画面を表示し、必要に応じてオプションを選択して、[Apply] を選択します。

注記： PPTP アドレス範囲での開始および終了 IP は、たとえば 192.168.1.1 ～ 192.168.1.254 のように、同じ 24 ビット サブネットに含まれる必要があります。

[Enable PPTP]	PPTP を有効にします。このオプションを選択する前に、ユーザ グループを追加する必要があります。詳しくは、457 ページの「ユーザ グループ」を参照してください。
[IP Mode]	PPTP ユーザに IP アドレスを割り当てる方法を選択します。
[Range]	ユーザの IP アドレスは、*[Starting IP]* および *[Ending IP]* のフィールドに指定される IP アドレス範囲から割り当てられます。
[User Group]	ユーザの IP アドレスは、ユーザの認証に使用されるユーザ グループによって割り当てられます。そのユーザ グループを選択します。詳しくは、461 ページの「ユーザ グループからの動的な VPN クライアント IP アドレス割り当て」を参照してください。
[Starting IP]	予約する IP アドレス範囲の開始アドレスを入力します。
[Ending IP]	予約する IP アドレス範囲の終了アドレスを入力します。
[Local IP]	PPTP クライアント側でピアのリモート IP に使用する IP アドレスを入力します。
[User Group]	リストから PPTP ユーザ グループを選択します。
[Disable PPTP]	PPTP サポートを無効にする場合に選択します。

CLI コマンドによる PPTP 設定

FortiGate Web ベース マネージャでカスタム画面を設定しないことが望ましい場合は、CLI を使用して PPTP トンネルを設定できます。

構文

```
config vpn pptp
  set eip <address_ipv4>
  set ip-mode {range | usrgrp}
  set local-ip <address_localip>
  set sip <address_ipv4>
  set status {disable | enable}
  set usrgrp <group_name>
end
```

変数	説明	デフォルト
`eip <address_ipv4>`	PPTP アドレス範囲の終了アドレス。	`0.0.0.0`
`ip-mode {range | usrgrp}`	次のいずれかを選択します。 `range` - `sip`および`eip`により設定されるIPアドレス範囲から、ユーザ IP アドレスを割り当てます。 `usrgrp` - ユーザの認証に使用するユーザ グループから IP アドレスを取得します。`usrgrp` で、ユーザ グループを選択します。	`range`
`local-ip <address_localip>`	PPTP クライアント側でピアのリモート IP に使用する IP アドレスを入力します。	`0.0.0.0`
`sip <address_ipv4>`	PPTP IP アドレス範囲の開始アドレス。	`0.0.0.0`
`status {disable | enable}`	PPTP VPN を有効または無効に設定します。	`disable`
`usrgrp <group_name>`	`ip-mode`を`usrgrp`に設定するとき、キーワードを利用できます。 PPTP クライアントを認証するためのユーザ グループ名を入力します。ここでユーザ グループを指定するには、事前にユーザ グループを FortiGate 設定に加える必要があります。	Null
`eip <address_ipv4>`	PPTP アドレス範囲の終了アドレス。	`0.0.0.0`

SSL VPN

この項では、[SSL VPN] メニューの基本的な設定について説明します。SSL VPN の詳しい設定方法、およびその他の一般的な情報については、『*FortiOS ハンドブック*』の「*FortiGate SSL VPN*」の章を参照してください。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとに VPN SSL を個別に設定します。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には以下のトピックが含まれています。

注記： iPhone または iPod touch 用の Fortinet SSL VPN App を使用すると、FortiGate ユニットの SSL VPN に直接接続できます。この App では、Web モードのアクセスのみがサポートされます。またこの App によって、ユーザ定義のブックマークを追加、編集、または削除できます。

SSL VPN の概要

SSL (Secure Sockets Layer) VPN は、標準の Web ブラウザとともに利用可能な VPN の一種です。SSL VPN では、エンド ユーザのコンピュータに専用のクライアント ソフトウェアをインストールする必要はなく、Web ベースの電子メール、企業および行政機関のディレクトリ、ファイル共有、リモート バックアップ、リモート システム管理、コンシューマ向け電子商取引などのアプリケーションに適しています。

SSL VPN には、以下の 2 種類の機能モードがあります (NAT/ ルート モードでのみサポート)。

- Web 専用モード。Web ブラウザのみをともなうリモートのシン クライアント向け。
- トンネル モード。各種のクライアント / サーバ アプリケーションを実行するリモート コンピュータ向け。

FortiGate ユニットが Web 専用モードでサービスを実行する場合は、FortiGate ユニットの SSL VPN セキュリティおよび Web ブラウザの SSL セキュリティにより、リモート クライアントおよび FortiGate ユニット間にセキュアな接続が確立されます。FortiGate ユニットとの接続が確立すると、Web ポータルから選択されたサービスおよびネットワーク リソースにアクセスできます。FortiGateSSL VPN Web ポータルには、表示形式のカスタマイズが可能なウィジェットが、所定のレイアウトで表示されます。各ウィジェットは、1 列または 2 列の配置で表示され、設定の変更、ウィジェット ウィンドウの最小化など、ウィジェットの表示内容に応じて設定および表示を調整できます。

ユーザが各自のコンピュータの完全な管理者権限を持ち、さまざまなアプリケーションを実行する場合、トンネル モードを使用することで、あたかもリモート クライアントが直接ネットワークに接続されているかのように、リモート クライアントからローカルの内部ネットワークへのアクセスが可能となります。

基本的な設定手順

FortiGate の SSL VPN テクノロジを最も効果的に設定するには、以下の基本的な設定手順に従います。以下の手順は、必ず記述されている順序で行ってください。手順の間に別の設定作業を行うと、設定結果が異なる原因になります。

1 SSL VPN 接続を有効にして、SSL VPN 構成をサポートするために必要な基本オプションを設定します。
2 Web ポータルを作成し、ネットワーク リソースへのユーザ アクセスを定義します。異なるユーザ グループへの異なる種類のアクセスを可能にする場合は、複数の Web ポータルを作成する必要があります。
3 リモート クライアントのユーザ アカウントを作成します。SSL VPN ユーザ グループを作成し、それらのグループを Web ポータルまたは作成したポータルと関連付けます。ユーザを、適切な SSL VPN ユーザ グループに割り当てます。
4 ファイアウォール ポリシー、および VPN モード機能のサポートに必要な残りのパラメータを設定します。
5 トンネルモードを使用する場合は、トンネルモードのクライアント パケットが SSL VPN インタフェースに確実に届くようにルーティングを加えます。
6 オプションで、SSL VPN イベントロギング パラメータを定義し、アクティブな SSL VPN セッションを監視します。

トラブルシューティングについては、『FortiOS ハンドブック』の「SSL VPN」の章を参照してください。

ssl.root

FortiGate ユニットには、ssl.<vdom 名 > で表される仮想 SSL VPN インタフェースがあります。ファイアウォール ポリシー インタフェース リストおよびスタティック ルート インタフェース リストには、ssl.root というルート VDOM が表示されます。ssl-root インタフェースを使用することで、他のネットワークへのアクセスが可能となり、ネットワークに接続したユーザが FortiGate ユニット経由で容易にインターネットを閲覧できるようになります。

SSL VPN トンネルモードのアクセスには、以下のファイアウォール ポリシーが必要です。

- External > Internal のファイアウォール ポリシー、[Action] を [SSL] に設定し、ユーザ グループを加えます。
- ssl.root > Internal のファイアウォール ポリシー、[Action] を [Accept] に設定します。
- Internal > ssl.root のファイアウォール ポリシー、[Action] を [Accept] に設定します。

また SSL VPN トンネル モードのアクセスには、新しいスタティック ルートとして、宛先ネットワーク・<sslトンネルモードにより割り当てられる範囲>インタフェースssl.rootが必要です。

SSL VPN トンネル経由でのインターネット アクセスを設定するには、[Action] を [Accept] および NAT を有効に設定した Internal > ssl.root のファイアウォール ポリシー設定を追加する必要があります。

Config

ここでは、タイムアウトの値および SSL 暗号化など、SSL VPN の基本的な設定について説明します。必要に応じて、デジタル証明書を使用してリモート クライアント認証を行うように設定できます。SSL VPN を設定するには、*[VPN]*、*[SSL]*、*[Config]* の順に選択します。

注記：必要に応じて、FortiGate の CLI コマンドから、SSL バージョン 2 暗号化を有効に（旧バージョンのブラウザとの互換性のため）設定できます。詳細については、『*FortiGate CLI リファレンス*』の `ssl settings` コマンドを参照してください。

[SSL-VPN Settings] ページ

このページには、SSL-VPN の設定が含まれています。また、DNS および WINS サーバの詳細な設定も行うことができます。

[Enable SSL VPN] このオプションをオンにすると、SSL VPN 接続を有効に設定します。

[IP Pools]	*[Edit]* を選択すると、トンネルモード SSL VPN クライアントに予約されている IP アドレス範囲を表す、範囲またはサブネット ファイアウォール アドレスを選択できます。適切なアドレスがない場合は、*[Firewall]*、*[Address]* の順に選択し、アドレスを作成します。すべての (*all*) ファイアウォール アドレスまたは FQDN ファイアウォール アドレスは、追加できません。また、すべての (*all*) ファイアウォール アドレスまたは FQDN アドレスを含むアドレス グループも、追加できません。
[Server Certificate]	認証に使用する署名済みサーバ証明書を選択します。デフォルトの設定 ([Self-Signed]) を使用する場合は、FortiGate ユニット出荷時に導入されているフォーティネットによる (自己署名済み) 証明書が、ネットワークに接続するリモート クライアントにユニットから提供されます。
[Require Client Certificate]	リモート クライアントの認証にグループ証明書を使用できるようにするには、このチェック ボックスをオンにします。設定以後、リモート クライアントが接続を開始すると、FortiGate ユニットはクライアントに対し、認証プロセスの一部としてクライアント側の証明書を要求します。
[Encryption Key Algorithm]	リモート クライアントの Web ブラウザと FortiGate ユニットとの間にセキュアな SSL コネクションを確立するためのアルゴリズムを選択します。
[Default - RC4(128 bits) and higher]	リモート クライアントの Web ブラウザが 128 ビット以上の暗号スイートに対応できる場合は、このオプションを選択します。
[High - AES(128/256 bits) and 3DES]	リモート クライアントの Web ブラウザが高度な SSL 暗号化に対応できる場合は、このオプションを選択して、128 ビットを超えるビット数でデータを暗号化する暗号スイートを有効にします。
[Low - RC4(64 bits), DES and higher]	リモート クライアントの Web ブラウザでサポートされる SSL 暗号化のレベルが分からない場合は、このオプションを選択して、64 ビット以上の暗号スイートを有効にします。
[Idle Timeout]	システムがユーザを強制的に再ログインさせる前に、コネクションがアイドル状態のままでいられる時間 (秒単位) を入力します。範囲は 10 ～ 28,800 秒です。アイドル接続のタイムアウトを設定しない場合は、値を 0 に設定できます。この設定は、SSL VPN セッションに適用されます。Web アプリケーションのセッションまたはトンネルが活動している場合、インタフェースはタイムアウトしません。
[Advanced (DNS and WINS Servers)]	
[DNS Server #1] **[DNS Server #2]**	クライアントが使用できる DNS サーバを 2 台まで入力します。
[WINS Server #1] **[WINS Server #2]**	クライアントが使用できる WINS サーバを 2 台まで入力します。

ポータル

SSL VPN Service ポータルを使用することにより、Web ブラウザからセキュアなチャネルを経由して、ネットワーク リソースにアクセスできます。FortiGate の管理者は、システム ユーザのログイン権限を設定し、さらに HTTP/HTTPS、telnet、FTP、SMB/CIFS、VNC、RDP、および SSH など、ユーザが利用可能なネットワーク リソースを指定できます。

システム ユーザが FortiGate にログインしたとき開く画面の内容は、Web ポータルの設定に応じて表示されます。システム管理者およびシステム ユーザの両者とも、SSL VPN ポータルをカスタマイズできます。

Web ポータルには、デフォルトで 3 種類の定義済みの設定があります。

- *[full-access]*。ユーザが利用可能な、*[Session Information]*、*[Connection Tool]*、*[Bookmarks]*、および *[Tunnel Mode]* の全ウィジェットが含まれます。
- *[tunnel-access]*。*[Session Information]* ウィジェットおよび *[Tunnel Mode]* ウィジェットが含まれます。
- *[web-access]*。*[Session Information]* ウィジェットおよび *[Bookmarks]* ウィジェットが含まれます。

また、[VPN]、[SSL]、[Portal] の順に選択し、独自の Web ポータルの作成も選択できます。

このトピックには、以下の項目が含まれています。

- ポータルの設定

- ポータル ウィジェット

[Portal] ページ

このページには、作成済みの Web ポータルおよびデフォルトの Web ポータルが一覧表示されます。このページでは、Web ポータルを編集、削除、または新規作成できます。必要に応じて、デフォルトの Web ポータルも編集できます。

[Create New]	[Create New] を選択すると、画面が [Portal Settings] ページに自動的に移動します。
編集アイコン	デフォルトまたは作成済みの Web ポータルを編集する場合に選択します。[Edit] を選択すると、画面が [Portal Settings] ページに自動的に移動します。
削除アイコン	[Portal] ページから Web ポータルを削除するとき選択します。
[Name]	Web ポータルの名前。

ポータル設定ページ

このページには、[SSL VPN Service] ページの設定が含まれています。

設定ウィンドウ	このウィンドウでは、[SSL VPN Service] ポータル ページの設定が、[General]、[Virtual Desktop]、および [Security Control] の各タブに含まれています。このウィンドウは、[Settings] を選択したとき表示されます。また、[Create New] を選択して [Portal Settings] ページの画面に自動的に移動する際にも表示されます。詳細については、430 ページの「ポータルの設定」を参照してください。
[OK]	設定を保存する場合に選択します。*[OK]* を選択すると、SSL VPN Web ポータル設定ウィンドウが閉じます。
[Cancel]	変更を保存せずに設定ウィンドウを閉じるとき選択します。
[Apply]	Web ポータル設定の変更を適用するとき選択します。*[Apply]* を選択した場合は、ポータル設定ウィンドウは閉じません。
[Settings]	SSL VPN Web ポータルの設定を編集するとき選択します。詳しくは、429 ページの「ポータル」を参照してください。
[Widgets]	[SSL VPN Service] ページに表示されるウィジェット。[Add Widgets] ドロップダウン リストからウィジェットを追加できます。詳細については、432 ページの「ポータル ウィジェット」を参照してください。
[Add Widget]	ページに新しいウィジェットを追加する場合に選択します。
[Session Information]	ユーザのログイン名、ユーザのログイン以降の経過時間、HTTP および HTTPS の送受信トラフィックを表示します。詳細については、432 ページの「Session Information」を参照してください。
[Bookmarks]	設定されているブックマークが表示されます。また、新しいブックマークの追加、および既存ブックマークの編集が可能です。詳細については、432 ページの「Bookmarks」を参照してください。
[Connection Tool]	接続ツール アプリケーション / サーバの URL または IP アドレスを入力します (*[Connection Tool]* の設定時に選択)。*[Type]* を [Ping] に設定することで、FortiGate ユニット背後にあるネットワーク上のホストまたはサーバとの接続をチェックできます。詳細については、433 ページの「Connection Tool」を参照してください。
[Tunnel Mode]	トンネル情報およびユーザ モードのアクションが表示されます。管理者は、スプリットトンネリング オプションを設定できます。詳細については、433 ページの「Tunnel Mode」を参照してください。

ポータルの設定

Web ポータルでは、SSL VPN ユーザによる、HTTP/HTTPS、telnet および SSH などのネットワーク リソースへのアクセスを定義します。SSL VPN ユーザが FortiGate にログインするときの画面の内容は、Web ポータルの設定に応じて表示されます。FortiGate 管理者および SSL VPN ユーザの両者とも、Web ポータルの設定をカスタマイズできます。ポータルを設定するには、*[VPN]*、*[SSL]*、*[Portal]* の順に選択します。

設定ウィンドウでは、Web ポータルの設定項目が、[General]、[Virtual Desktop]、[Security control] の各タブに含まれています。

Windows XP および Windows Vista クライアント PC で利用可能な [Virtual Desktop] オプションを設定することにより、SSL VPNセッションをクライアント コンピュータの通常のデスクトップ環境から完全に隔離できます。キャッシュされるユーザの認証情報、ブラウザ履歴、Cookie、一時ファイル、セッション中に作成されるユーザ ファイルなど、すべてのデータが暗号化されます。SSL VPN セッションが正常に終了すると、ファイルは削除されます。何らかの異常が原因でセッションが終了した場合は、ファイルは削除されない場合がありますが、それらは暗号化されており情報は保護されます。

仮想デスクトップが有効な状態でユーザが SSL VPN セッションを開始すると、ユーザの通常のデスクトップが仮想デスクトップに入れ替わります。仮想デスクトップが終了すると、ユーザの通常のデスクトップに戻ります。

仮想デスクトップには、フォーティネットのホスト チェック プラグインが必要です。プラグインがない場合は、クライアント コンピュータに自動的にダウンロードされます。

セキュリティ制御オプションにより、キャッシュの消去、および Web ポータルのクライアントに対するホスト チェックを実行できます。キャッシュ消去を実行すると、SSL VPN セッション終了の直前に、クライアントのブラウザ キャッシュ情報が消去されます。キャッシュが消去されるのは、セッションが正常に終了する場合に限られます。セッションが停電など何らかの異常が原因で終了する場合は、キャッシュは消去されません。

ホスト チェックを実行すると、アンチウイルスまたはファイアウォール ソフトウェアを、クライアントに強制的に使用させます。Windows Security Center によって認識されるセキュリティ ソフトウェアのチェックが、各クライアントに対して行われます。または、カスタムのホスト チェックを作成し、ホスト チェック リストで選択されている特定のセキュリティ ソフトウェアを検索することも可能です。ホスト チェック リストを表示するには、*[VPN]*、*[SSL]*、*[Host Check]* の順に選択します。詳しくは、434 ページの「ホスト チェック」を参照してください。

設定ウィンドウ

このウィンドウには、特定の設定項目を含む [General]、[Virtual desktop]、[Security control] タブが表示されます。[OK] を選択すると、これらの設定が [Portal Settings] ページの表示に反映されます。たとえば、通常のカラー スキームに [Orange] を指定し [OK] を選択すると、ウィジェットおよびページの表示にそのカラー スキームが適用されます。

[General] タブ	カラー スキームなど、ページの一般的な設定。
[Name]	Web ポータル設定の名前を入力します。
[Applications]	サーバ アプリケーションまたはクライアントが使用可能なネットワーク サービスの略称を選択します。
[Portal Message]	Web ポータル ホーム ページの上部に表示されるキャプションを入力します。
[Theme]	Webポータル ホーム ページのカラー スキームを、リストから選択します。
[Page Layout]	Web ポータル ホーム ページの表示レイアウトを、1 列または 2 列から選択します。
[Redirect URL]	Web ポータル ホーム ページを表示すると、ポップアップ ウィンドウに別の HTML ページが表示されるように設定できます。この HTML ページの URL を入力します。
[Virtual Desktop] タブ	このタブでは、仮想デスクトップと通常デスクトップの切り替えなど、ユーザが利用な仮想デスクトップのオプションを、有効または無効に設定できます。
[Enable Virtual Desktop]	このオプションをオンにすると、仮想デスクトップ機能を有効に設定します。
[Allow switching between virtual desktop and regular desktop]	このオプションをオンにすると、ユーザによる仮想デスクトップと通常デスクトップの切り替えが可能になります。
[Allow clipboard contents to be shared with regular desktop]	このオプションをオンにすると、通常デスクトップの使用中に、ユーザがクリップボード内のデータにアクセスできます。
[Allow use of removable media]	このオプションをオンにすると、ユーザがリムーバブル メディアを使用できます。

[Allow network share access]	このオプションをオンにすると、ユーザが共有ネットワークにアクセスできます。
[Allow printing]	このオプションをオンにすると、ユーザが仮想デスクトップから印刷を実行できます。
[Quit the virtual desktop and logout session when browser is closed]	このオプションをオンにすると、ブラウザの終了時に、仮想デスクトップを終了して実行中のセッションからユーザをログアウトします。
[Application Control List]	ドロップダウン リストから、仮想デスクトップ アプリケーション リストを選択します。
[Security Control] タブ	Web ポータルのセキュリティ設定が含まれています。
[Clean Cache]	このオプションを選択すると、SSL VPN セッション終了の直前に、リモート クライアント コンピュータに残る情報がFortiGateユニットによって削除されます。
[Host Check]	このオプションを選択すると、ホスト チェックを有効にします。
[Interval]	ホスト チェックを繰り返す頻度を入力します。
[Policy]	検索する特定のホスト チェック ソフトウェアを選択します。このオプションは、[Host Check] で [Custom] を選択した場合のみ表示されます。

ポータル ウィジェット

ユーザが Web ポータルを開くと、ポータル内に配置されているポータル ウィジェットに、様々な設定情報および選択項目が表示されます。これらの設定情報には、Web URL ブックマーク、またはネットワーク リソースへの接続などが含まれます。Web ポータルにトンネル アクセスが含まれる場合は、[Tunnel Mode] ウィジェットを利用して、IP アドレスが割り当てられるトンネル モード クライアントの数を設定し、スプリット トンネリングを有効に設定できます。

編集アイコン	ウィジェットに表示される情報を編集する場合に選択します。
[OK]	*[Session Information]* の設定を保存する場合に選択します。
[Cancel]	変更を保存せずに *[Session Information]* ウィジェットを閉じる場合に選択します。
[Name]	[Session Information] ウィジェットの名前をカスタマイズするとき、その名前を入力します。
ウィジェット削除アイコン (x マーク)	ウィジェットを閉じて、Web ポータル ホーム ページからそのウィジェット削除する場合に選択します。

Session Information

[Session Information] ウィジェットには、ユーザのログイン名、ユーザのログイン以降の経過時間、HTTP および HTTPS の送受信トラフィック統計が表示されます。

Bookmarks

[Bookmark] ウィジェットは、ネットワーク上の特定リソースへのリンクに使用します。ブックマーク リストからブックマークを選択すると、ポップアップ ウィンドウが開き、要求した Web ページが表示されます。Telnet、VNC、および RDP では、いずれもポップアップ ウィンドウが開きますが、これらのウィンドウにはブラウザ プラグインが必要です。FTP および Samba は、ブックマーク ページを HTML ファイルブラウザに置き換えます。

Web ブックマークには、SSL VPN ユーザを Web サイトに自動的にログインさせるための、ログイン認証情報を加えることができます。これにより、ユーザが SSL VPN に一度ログインした後は、そのユーザは認証情報を入力することなく、設定済みの Web サイトを閲覧できます。管理者がブックマークを設定するとき、Web サイトの認証情報はユーザの SSL VPN 認証情報と同一である必要があります。各自のブックマークを設定するユーザは、Web サイト用に別の認証情報を指定できます。

Connection Tool

[Connection Tool] ウィジェットを使用することで、ブックマーク リストにブックマークを加えることなく、ネットワーク リソースに接続できます。リソースの種類を選択し、ホスト コンピュータの URL または IP アドレスを指定します。

Tunnel Mode

Web ポータルからトンネル モードのアクセスを提供する場合は、必ず [Tunnel Mode] ウィジェットを設定します。この設定により、トンネル モード クライアントに IP アドレスがどのように割り当てられるかが指定されます。また、スプリット トンネリング設定を有効にすることで、FortiGate ユニット背後にあるネットワークのトラフィックのみが VPN によって転送されるように設定できます。ユーザが扱う他のトラフィックは、通常のルートで転送されます。

仮想デスクトップ アプリケーション制御

仮想デスクトップ上でユーザがどのアプリケーションを実行できるかを、制御することができます。この制御を行うために、許可またはブロックされるアプリケーションのリストを作成し、仮想デスクトップの設定時にリストからアプリケーションを選択します。この設定を行うには、*[VPN]*、*[SSL]*、*[Virtual Desktop Application Control]* の順に選択します。

[Virtual Desktop Application] ページ

このページには、作成済みの仮想デスクトップ アプリケーション リストが一覧表示されます。このページでは、仮想デスクトップ アプリケーション リストを編集、削除、または新規作成できます。

[Create New]	[Create New] を選択すると、画面が [Virtual Desktop Application Settings] ページに自動的に移動します。
[Name]	仮想デスクトップ アプリケーション制御リストの名前。
[Action]	仮想デスクトップ アプリケーション制御リストごとに設定されるアクション。 *[Block the applications on this list and allow all others]（このリストに含まれるアプリケーションをブロックし、他のアプリケーションをすべて許可する）* または、*[Allow the applications on this list and block all others]（このリストに含まれるアプリケーションを許可し、他のアプリケーションをすべてブロックする）*を選択します。
編集アイコン	編集アイコンを選択すると、画面が [Virtual Desktop Application Settings] ページに自動的に移動します。
削除アイコン	アプリケーション制御リストを削除します。
クローン アイコン	アプリケーション制御リストのコピーを作成します。コピーしたリストを編集し、新規のアプリケーション制御リストを作成できます。

[Virtual Desktop Application Settings] ページ

このページでは、複数のアプリケーションを含む仮想デスクトップ アプリケーション リストを設定できます。ブロックするアプリケーションまたは許可するアプリケーションの、いずれのリストも設定できます。

[Name]	仮想デスクトップ アプリケーション リストの名前を入力します。
[Allow the applications on the list and block all others]	このオプションを選択すると、このリストに含まれるアプリケーションを許可し、他のアプリケーションをすべてブロックします。
[Block the application on the list and allow all others]	このオプションを選択すると、このリストに含まれるアプリケーションをブロックし、他のアプリケーションをすべて許可します。

[Create New]	仮想デスクトップ アプリケーション リストにアプリケーションを加えるとき選択します。[Create New] を選択すると、[Application Signatures] ウィンドウが開きます。
編集アイコン	リスト内のアプリケーション設定を変更するとき選択します。
削除アイコン	リストからアプリケーションを削除するとき選択します。
[Applications]	アプリケーションの名前。

[Application Signatures] ページ

[Name]	アプリケーションの名前を入力します。この名前は、アプリケーションの正式名と一致する必要はありません。
[MD5 Signatures (one per line)]	アプリケーションの実行可能ファイルの MD5 シグネチャを入力します。複数のシグネチャを入力する場合は、必ずシグネチャごとに改行して入力します。サードパーティのユーティリティを使用し、ファイルの MD5 シグネチャまたは MD5 ハッシュを計算できます。 複数の MD5 シグネチャを入力することにより、アプリケーションの複数バージョンとの一致が容易になります。

ホスト チェック

Web ポータルの [Security Control] タブ設定で、[AV]、[FW]、または [AV-FW] ホスト チェックを有効にすると、Windows Security Center によって認識されるセキュリティ ソフトウェアのチェックがクライアントごとに行われます。あるいは、カスタムのホスト チェックを作成し、ホスト チェック リストで選択されているセキュリティ ソフトウェアを検索できます。詳細については、430 ページの「ポータルの設定」を参照してください。

ホスト チェック リストには、多数のセキュリティ ソフトウェア製品がデフォルトのエントリとして含まれています。

[Host Check] ページ

このページには、Web ポータルのホスト チェックのために作成したホスト チェック リストが一覧表示されます。このページでは、ホスト チェック リストを編集、削除、または新規作成できます。

[Create New]	新しいアプリケーションを、ホスト チェック リストに追加します。
[Name]	ホスト チェック リストに追加するアプリケーションの名前。名前は、実際のアプリケーション名と一致する必要はありません。
[Type]	ホスト チェックア プリケーションの種類。AV はアンチウイルス、FW はファイアウォールを表します。
[Version]	ホスト チェックア プリケーションのバージョン。
編集アイコン	既存のホスト チェック アプリケーション横にある *編集*アイコンを選択すると、ホスト チェック アプリケーションを編集できます。
削除アイコン	ホスト チェック アプリケーションを削除します。

[Host Check Software] ページ

このページには、アプリケーションとそれらのチェック方法を表示するホスト チェック リストを設定するための項目が含まれています。

[Name]	ホスト チェック リストの名前を入力します。
[Type]	ホスト チェックの種類を、[AV] または [FW] から選択します。
[GUID]	ホスト チェック アップリケーションの GUID (グローバルー意識別子) を入力します。GUID は通常、xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx の形式で使用され、x はいずれも 16 進数になります。Windows では GUID を使用して Windows レジストリ内のアプリケーションを識別します。
[Version]	ソフトウェアのバージョンを入力します。
[Create New]	新しいチェック アイテムを作成しリストに追加するとき選択します。[Create New] を選択すると、[Check Item] ウィンドウが開きます。
編集アイコン	ホスト チェックの設定を変更するとき選択します。
削除アイコン	リスト内のチェック アイテムを削除するとき選択します。
#	各アイテムが表示される順序。

[Target]	選択したターゲットの種類。
[Type]	選択したチェックの種類。
[Action]	選択したアクションの種類。

[Check Item] ページ

[Type]	アプリケーションのチェック方法を選択します。
[Action]	次のいずれかを選択します。 **[Require]** – チェック対象が検出される場合、クライアントはチェック アイテムの条件を満たしています。 **[Deny]** – チェック対象が検出される場合、クライアントはチェック アイテムの条件を満たさないと見なされます。特定のセキュリティ製品の使用を避ける必要がある場合は、このオプションを使用します。
[File/Path]	ファイル名およびパスを入力します。
[Process]	アプリケーションの実行可能ファイルの名前を入力します。[Process] を選択する場合は、1 つ以上の MD5 シグネチャを [MD5 Signatures] フィールドに入力する必要があります。サードパーティのユーティリティを使用し、ファイルの MD5 シグネチャまたは MD5 ハッシュを計算できます。
[Registery]	アプリケーションのレジストリ番号を入力します。
[Version]	アプリケーションのバージョンを入力します。
[MD5 Signatures (one per line)]	アプリケーションの実行可能ファイルの MD5 シグネチャを入力します。複数のシグネチャを入力する場合は、必ずシグネチャごとに改行して入力します。サードパーティのユーティリティを使用し、ファイルの MD5 シグネチャまたは MD5 ハッシュを計算できます。 複数の MD5 シグネチャを入力することにより、アプリケーションの複数バージョンとの一致が容易になります。

SSL VPN モニタ リスト

アクティブなすべての SSL VPN セッションのリストを表示できます。リストには、リモート ユーザのユーザ名、リモート クライアントの IP アドレス、接続が開始された時間が表示されます。また、提供されているサービスを表示し、アクティブな Web またはトンネルのセッションを FortiGate ユニットから削除できます。詳細については、427 ページの「SSL VPN」を参照してください。

[Monitor] ページ

このページには、現在モニタされている SSL VPN セッションが一覧表示されます。このページでは、現在モニタ中の SSL VPN セッションを削除できます。

[No.]	接続の識別番号。
[User]	接続されているすべてのリモート ユーザのユーザ名。
[Source IP]	FortiGate ユニットに接続されているホスト デバイスの IP アドレス。
[Begin Time]	各接続の開始時間。
[Description]	SSL VPN トンネル サブセッションの場合、クライアントに割り当てられたトンネル IP アドレスが表示されます。
[Action]	現在の SSL VPN トンネル セッションまたはサブセッションに適用するアクションを選択します。
削除アイコン	現在のセッションまたはサブセッションを削除します。

.

WAN 最適化および Web キャッシュ

FortiGate WAN 最適化および Web キャッシュを使用することにより、WAN (wide area network) 上のサイト同士、またはインターネットから Web サーバを通過するトラフィックのパフォーマンスおよびセキュリティを強化できます。この項では、FortiGate WAN 最適化および Web キャッシュの概要、およびこれらの設定方法について説明します。

WAN 最適化は、一部の FortiGate モデルでのみ利用できます。サポート対象のモデル、および FortiGate WAN 最適化、Web キャッシュの詳細な説明については、『*FortiGate WAN 最適化、Web キャッシュ、および Web プロキシ ユーザ ガイド*』を参照してください。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとに WAN 最適化を利用できます。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には以下のトピックが含まれています。

WAN 最適化の設定

WAN 最適化ルール リストには、WAN 最適化ルールが照合の優先順に表示されます。

FortiGate ユニットで、バーチャル ドメインが有効に設定されている場合は、各バーチャル ドメインごとに個別の WAN 最適化ルールを設定しますが、ルールを設定するにはまずバーチャル ドメインにアクセスする必要があります。バーチャル ドメインにアクセスするには、*[System]*、*[VDOM]* の順に選択し、ポリシーを設定するバーチャル ドメインに該当する行で、*[Enter]* を選択します。バーチャル ドメインを有効に設定する方法については、77 ページの「バーチャル ドメインの有効化」を参照してください。

ルール リストでは、ルールを追加、削除、編集し、さらに並べ替えることができます。WAN 最適化ルールの順序は、トラフィックとルールの照合に密接に関係しています。ルール リスト内でルールを並べ替える手順については、438 ページの「ルール リスト内のルール位置の移動」を参照してください。

WAN 最適化ルール リストを表示するには、*[WAN Opt. & Cache]*、*[Rule]*、*[Rule]* の順に選択します。

WAN 最適化ルールを追加する前に、最適化するトラフィックを許可するための、ファイアウォール ポリシーを追加する必要があります。さらに、以下のような WAN 最適化ルールを追加します。

- 最適化される WAN トラフィックと一致するルール。この WAN トラフィックは、送信元および宛先のアドレスおよびトラフィックの宛先ポートに基づき、ファイアウォール ポリシーで許可されるトラフィックです。
- トラフィックに適用される WAN 最適化テクニックを追加するルール。

[Rule] ページ

このページには、作成済みの WAN 最適化ルールが一覧表示されます。このページでは、WAN 最適化ルールを編集、削除、または新規作成できます。また、リスト中で WAN 最適化ルールを挿入または移動できます。

[Create New]	新しい WAN 最適化ルールを追加します。新しいルールは、リストの下部に追加されます。
[Status]	チェックボックスをオンにするとルールを有効に設定し、オフにするとルールを無効に設定します。無効に設定したルールは、適用されません。
[ID]	ルールの識別番号。ルールには、ルール リストに追加された順序で番号が付けられます。
[Source]	ルールに一致する発信元アドレスまたはアドレス範囲。詳しくは、441 ページの「WAN 最適化アドレスについて」を参照してください。
[Destination]	ルールに一致する宛先アドレスまたはアドレス範囲。詳しくは、441 ページの「WAN 最適化アドレスについて」を参照してください。
[Port]	ルールに一致する宛先ポート番号またはポート番号範囲。
[Method]	WAN 最適化ルールで、バイト キャッシュが選択されているかどうかを表示します。
[Auto-Detect]	ルールがアクティブ（クライアント）ルールまたはパッシブ（サーバ）ルールか、または Auto-Detect がオフかを表示します。Auto-Detect がオフの場合は、ルールはピアツーピア ルール、または Web Cache Only ルールのいずれかになります。
[Protocol]	ルールによって適用される、プロトコル最適化の WAN 最適化テクニック。詳しくは、『*FortiGateWAN 最適化、Web キャッシュ、および Web プロキシ ユーザ ガイド*』を参照してください。
[Peer]	ピアツーピア ルールでは、リンク別端ピアの WAN オプティマイザの名前。
[Mode]	ルールが、[Full Optimization] または [Web Cache Only] のいずれを適用するかを表示します。
[SSL]	ルールに SSL オフロードが設定されているかどうかを表示します。
[Secure Tunnel]	ルールが WAN 最適化トンネルを使用するように設定されているかどうかを表示します。
削除アイコン	リストからルールを削除します。
編集アイコン	ルールを編集します。
[Insert WAN Optimization Rule Before]	該当ルールの直前（上）の行に、新しいルールを追加します（[New rule] 画面が表示されます）。
移動アイコン	リスト内で、該当ルールを別のルールの前または後に移動します。詳しくは、438 ページの「ルール リスト内のルール位置の移動」を参照してください。

ルール リスト内のルール位置の移動

ルールと着信するトラフィックを照合する順序を、目的に応じて変更するために、WAN 最適化ルール リスト内のルールを並べ替えることができます。複数のルールが定義されている場合、最初に一致するルールがトラフィックのセッションに適用されます。

ルール リスト内でルールを移動しても、ルールが作成された順番を示すポリシーの ID は変わりません。

WAN 最適化ルール リストでルールを移動するには

1 *[WAN Opt & Cache]*、*[Rule]*、*[Rule]* の順に選択します。
2 ルール リストで、移動先として指定する前または後の基準となる ID を確認します。
3 移動するルールの行で、*移動*アイコンを選択します。
4 *[Before]* または *[After]* を選択し、基準となるルール ID を入力します。入力した ID の前 (before) または後 (after) が、移動先となります。この設定により、WAN 最適化ルール リスト内でルールの新しい位置が決まります。
5 *[OK]* を選択します。

WAN 最適化ルールの設定

この項では、WAN 最適化ルールのオプションについて説明します。WAN 最適化ルールに表示されるオプションは、ルールをどのように設定するかに応じて異なります。この項では、すべてのオプションについて説明します。

WAN 最適化ルールを追加するには、*[WAN Opt. & Cache]* > *[Rule]* > *[Rule]* の順に選択し、*[Create New]* を選択します。

***[New WAN Optimization Rule]* ページ**

このページで、WAN 最適化ルールを設定できます。

[Mode]

[Full Optimization] を選択すると、すべての WAN 最適化機能を適用可能なルールを追加します。

[Web Cache Only] を選択すると、Web キャッシュのみを適用するルールを追加します。*[Web Cache Only]* を選択する場合は、ルールの発信元および宛先アドレスおよびポートを指定できます。また、*[Transparent Mode]* および *[Enable SSL]* も選択できます。

[Source]

IP アドレスに続いてフォワード スラッシュ (/)、次にサブネット マスクを入力するか、または IP アドレス範囲をハイフンで区切って入力します。詳しくは、441 ページの「WAN 最適化アドレスについて」を参照してください。

この IP アドレスまたはアドレス範囲と一致する IP アドレスが発信元アドレスのヘッダに含まれるパケットのみが、このルールによって許可されルールの適用対象となります。

パッシブ ルールでは、サーバ (パッシブ) 発信元アドレス範囲が、一致するクライアント (アクティブ) ルールの発信元アドレスと互換性を持つ必要があります。1 つのパッシブ ルールが多数のアクティブ ルールと一致するには、パッシブ ルールの発信元アドレス範囲にすべてのアクティブ ルールの発信元アドレスが含まれる必要があります。

[Destination]

IP アドレスに続いてフォワード スラッシュ (/)、次にサブネット マスクを入力するか、または IP アドレス範囲をハイフンで区切って入力します。詳しくは、441 ページの「WAN 最適化アドレスについて」を参照してください。

この IP アドレスまたはアドレス範囲と一致する IP アドレスが宛先アドレスのヘッダに含まれるパケットのみが、このルールによって許可されルールの適用対象となります。

ヒント：[Web Cache Only] ルールでは、*[Destination]* を 0.0.0.0 に設定すると、インターネットまたは任意のネットワーク上の Web ページが、ルールによってキャッシュされます。

パッシブ ルールでは、サーバ (パッシブ) 宛先アドレス範囲が、一致するクライアント (アクティブ) ルールの宛先アドレスと互換性を持つ必要があります。1 つのパッシブ ルールが多数のアクティブ ルールと一致するには、パッシブ ルールの宛先アドレス範囲にすべてのアクティブ ルールの宛先アドレスが含まれる必要があります。

[Port]

単一のポート番号またはポート番号の範囲を入力します。このポート番号またはポート番号範囲と一致する宛先ポート番号のパケットのみが、このルールによって許可されルールの適用対象となります。

パッシブ ルールでは、サーバ (パッシブ) ポート範囲が、一致するクライアント (アクティブ) ルールのポート範囲と互換性を持つ必要があります。1 つのパッシブ ルールが多数のアクティブ ルールと一致するには、パッシブ ルールのポート範囲にすべてのアクティブ ルールのポート範囲が含まれる必要があります。

[Auto-Detect]

このオプションは、*[Mode]* を *[Full Optimization]* に設定した場合のみ利用できます。

ルールが、*[Active]* (クライアント) ルール、または *[Passive]* (サーバ) ルールか、または Auto-Detect が *[Off]* かを指定します。[Auto-Detect] がオフの場合は、ルールはピア ツーピア ルールです。

- *[Active]* (クライアント) ルールでは、このルールによって適用されるすべての WAN 最適化機能を選択する必要があります。最適化するプロトコル、トランスペアレント モード、バイト キャッシュ、SSL オフロード、セキュア トンネル、認証グループを選択できます。
- *[Passive]* (サーバ) ルールでは、クライアント FortiGate ユニット上のアクティブ ルールの設定を使用して、WAN 最適化設定を適用します。また、パッシブ ルールの Web キャッシュを選択できます。
- *[Auto-Detect]* が *[Off]* の場合は、必要なすべての WAN 最適化機能がルールに含まれる必要があり、ルールの *[Peer]* を必ず選択します。このオプションは、このルールによって WAN 最適化トンネルをこのピアのみから開始可能な、ピアツーピア WAN 最適化を設定する場合に選択します。

[Protocol] このオプションは、*[Mode]* を *[Full Optimization]* に、*[Auto-Detect]* を *[Off]* または *[Active]* に設定した場合のみ利用できます。
CIFS、FTP、HTTP、または MAPI のいずれかにプロトコル最適化を適用する場合は、これらのプロトコルのいずれかを選択します。プロトコル最適化の詳細については、『*FortiGateWAN 最適化、Web キャッシュ、および Web プロキシ ユーザ ガイド*』を参照してください。
WAN 最適化トンネルが、複数のプロトコルを使用するセッション、または CIFS、FTP、HTTP または MAPI プロトコルを使用しないセッションを許可する場合は、[TCP] を選択します。

[Peer] このオプションは、*[Mode]* を *[Full Optimization]* に、*[Auto-Detect]* を *[Off]* に設定した場合のみ利用できます。
このピアツーピア WAN 最適化ルールが WAN 最適化トンネルを開始する側のピアの、ピア ホスト ID を選択します。また、新しいピアを追加する場合は、*[Create New ...]* を選択します。

[Enable Web Cache] このオプションは、*[Mode]* を *[Full Optimization]* に、*[Auto-Detect]* を *[Off]* または *[Passive]* に設定した場合のみ利用できます。*[Auto-Detect]* を *[Off]* に設定した場合は、*[Protocol]* を必ず *[HTTP]* に設定します。
このオプションをオンにすると、このルールによって許可されたセッションに WAN 最適化 Web キャッシュを適用します。詳しくは、『*FortiGateWAN 最適化、Web キャッシュ、および Web プロキシ ユーザ ガイド*』を参照してください。

[Transparent Mode] WAN 最適化の適用後にパケットを受信するサーバは、*[Transparent Mode]* の設定に応じて、異なる発信元アドレスを認識します。このオプションを選択できるのは、*[Auto-Detect]* を *[Active]* または *[Off]* に設定している場合です。また、[Web Cache Only] ルールでもこのオプションを選択できます。
このオプションをオンにすると、パケットをサーバに送信するときパケットの元の発信元アドレスが維持されます。これによりサーバは、トラフィックを直接クライアントから受信するかたちで機能します。サーバ ネットワークを構成する際には、クライアント発信元 IP アドレスを持つトラフィックのルーティングを、サーバ側 FortiGate ユニットからサーバに、さらにサーバ側 FortiGate ユニットに戻るように、設定する必要があります。
このオプションをオンにしない場合、サーバ側 FortiGate ユニットは、サーバにより受信されるパケットの発信元アドレスを、パケットをサーバに送信する FortiGate ユニット インタフェースのアドレスに変更します。このためサーバは、パケットをサーバ側 FortiGate ユニットから受信するかたちで機能します。この場合、クライアントのアドレスは扱われないので、サーバ ネットワーク上のルーティングは比較的簡素になりますが、サーバはすべてのトラフィックを、個別のクライアントではなくサーバ側 FortiGate ユニットから送信されるものとして認識します。

[Enable Byte Caching] このオプションは、*[Mode]* を *[Full Optimization]* に、*[Auto-Detect]* を *[Off]* または *[Active]* に設定した場合のみ利用できます。
このオプションをオンにすると、このルールによって許可されたセッションに WAN 最適化バイト キャッシュを適用します。詳しくは、『*FortiGateWAN 最適化、Web キャッシュ、および Web プロキシ ユーザ ガイド*』を参照してください。

[Enable SSL] このオプションは、*[Auto-Detect]* を *[Active]* または *[Off]* に設定した場合のみ利用できます。
このオプションをオンにすると、HTTPS トラフィックの SSL オフロードを適用します。SSL オフロードを使用することで、SSL 暗号化および復号の負荷を、1 台以上の HTTP サーバから FortiGate ユニットに移すことができます。このオプションをオンにする場合は、SSL 暗号化トラフィックを許可するようにルールを設定する必要があり、たとえば、*[Port]* を 443 に設定することで HTTPS トラフィックを許可するようにルールを設定します。
SSL オフロードを有効に設定する場合は、さらに CLI コマンド `config wanopt ssl-server` を使用して、SSL 暗号化/復号の負荷を軽減する各 HTTP サーバの SSL サーバを追加する必要があります。詳しくは、『*FortiGateWAN 最適化、Web キャッシュ、および Web プロキシ ユーザ ガイド*』を参照してください。

[Enable Secure Tunnel] このオプションは、*[Mode]* を *[Full Optimization]* に、*[Auto-Detect]* を *[Active]* または *[Off]* に設定した場合のみ利用できます。
[Enable Secure Tunnel] オプションをオンにする場合は、SSL 暗号化によって WAN 最適化トンネルが暗号化されます。また、認証グループをルールに加える必要があります。詳しくは、『*FortiGateWAN 最適化、Web キャッシュ、および Web プロキシ ユーザ ガイド*』を参照してください。

[Authentication Group] このオプションは、*[Mode]* を *[Full Optimization]* に、*[Auto-Detect]* を *[Active]* または *[Off]* に設定した場合のみ利用できます。
WAN 最適化トンネルを開始する前に FortiGate ユニットのグループ同士が認証を行うようにする場合は、このオプションをオンにして、リストから認証グループを選択します。また、*[Enable Secure Tunnel]* オプションをオンにする場合も、認証グループを必ず選択します。
ルールによって開始される WAN 最適化トンネルに参加する両側の FortiGate ユニットに、同一の認証グループを追加する必要があります。詳細については、442 ページの「認証グループの設定」を参照してください。

WAN 最適化アドレスについて

WAN 最適化の発信元または宛先アドレスには、1 つ以上のネットワーク アドレスが含まれます。ネットワーク アドレスは、IP アドレスとネットマスク、または IP アドレス範囲によって表されます。

ネットマスクをともなう IP アドレスによりホストを表す場合、この IP アドレスで 1 つ以上のホストを表すことができます。たとえば、発信元または宛先アドレスは次のようになります。

- 192.45.46.45 などの、単一のコンピュータ
- クラス C サブネットの 192.168.1.0 などの、サブネットワーク
- 0.0.0.0、これはあらゆる IP アドレスに該当

ネットマスクは、追加されるアドレスのサブネット クラスに対応し、ドット区切り 10 進数または CIDR 形式のいずれかで表すことができます。FortiGate ユニットは、CIDR 形式のネットマスクをドット区切り 10 進数の形式に自動的に変換します。たとえば、次のような形式になります。

- 単一コンピュータのネットマスク：255.255.255.255、または /32
- クラス A サブネットのネットマスク：255.0.0.0、または /8
- クラス B サブネットのネットマスク：255.255.0.0、または /16
- クラス C サブネットのネットマスク：255.255.255.0、または /24
- すべての IP アドレスを含むネットマスク： 0.0.0.0

有効な IP アドレスおよびネットマスクの形式には、以下があります。

- x.x.x.x/x.x.x.x（192.168.1.0/255.255.255.0 など）
- x.x.x.x/x（192.168.1.0/24 など）

注記：ネットマスク 255.255.255.255 をともなう IP アドレス 0.0.0.0 は、有効な発信元または宛先アドレスではありません。

IP 範囲によりホストを表す場合、その範囲は、サブネット内の連続する IP アドレスを持つホストを示し、192.168.1.[2-10]、または 192.168.1.* のようになります。これにより、そのサブネット上のホストの完全な範囲を示します。有効な IP 範囲の形式には、次があります。

- x.x.x.x-x.x.x.x（192.168.110.100-192.168.110.120 など）
- x.x.x.[x-x]（192.168.110.[100-120] など）
- x.x.x.*（192.168.110.* など）

WAN 最適化 ピアの設定

WAN 最適化を使用する際に FortiGate ユニットを識別するためのローカル ホスト ID を追加し、さらに FortiGate ユニットによる WAN 最適化トンネル作成で使用される各 FortiGate ユニットのピア ホスト ID および IP アドレスを追加することができます。

WAN 最適化のピアを設定するには、*[WAN Opt & Cache]*、*[Peer]*、*[Peer]* の順に選択します。

[Peer] ページ

このページには、作成済みの WAN 最適化ピアが一覧表示されます。

[Create New]	新しいピアを追加します。[Create New] を選択すると、画面が [New WAN Optimization Peer] ページに自動的に移動します。
[Local Host ID]	このフィールドに、***この*** FortiGate ユニットのローカル ホスト ID を入力し、*[Apply]* を選択します。この FortiGate ユニットをピアとして別の FortiGate ユニットに追加する場合は、この ID をこのユニットのピア ホスト ID として使用します。
[Apply]	*[Local Host ID]* に加えた変更を、FortiGate 設定に保存します。
編集アイコン	既存のピアの横にある*編集*アイコンを選択すると、そのピアを編集できます。
削除アイコン	ピアを削除します。

[New WAN Optimization Peer] ページ

このページでは、ピア ホスト ID およびピアの IP アドレスを設定できます。

[Peer Host ID] ピア FortiGate ユニットのピア ホスト ID。これは、ピア FortiGate ユニットに追加されるローカル ホスト ID です。

[IP Address] FortiGate ユニットの IP アドレス。通常これは、WAN に接続される FortiGate インタフェースの IP アドレスです。

認証グループの設定

WAN 最適化ピア同士の認証およびセキュア トンネルをサポートするために、認証グループを加える必要があります。

認証を実行するために、WAN 最適化ピアでは、WAN 最適化トンネルの形成前に、認証グループに追加された証明書または事前共有キーに基づいて、ピア同士で相互の身元確認が行われます。双方のピアには、同じ名前と設定が含まれる認証グループが必要です。クライアント側 FortiGate ユニット上のピアツーピア ルールまたはアクティブ ルールに、認証グループを加えます。認証グループが追加されたクライアント側 FortiGate ユニットからトンネル開始が要求され、サーバ側 FortiGate ユニットでその要求が受信されると、サーバ側 FortiGate ユニットは同じ名前を持つ認証グループを同ユニットの設定から検索します。両方の認証グループに同じ証明書または事前共有キーがあれば、ピアは認証を行いトンネルを作成できます。

認証グループは、セキュア トンネルにも必要です。セキュア トンネルを設定するには、両方のピアに同じ名前と設定をともなう認証グループが必要です。クライアント側の FortiGate ユニットでは、セキュア トンネルを有効にするために、ピアツーピア ルールまたはアクティブ ルールの *[Enable Secure Tunnel]* オプションをオンにする必要があります。クライアント側およびサーバ側 FortiGate ユニット同士の認証後に、これらのユニットでは認証グループに含まれる事前共有キーまたは証明書に基づき、トンネル パケットが暗号化および復号化されます。トンネルの暗号化には、SSL 暗号化を使用します。

認証グループを追加するには、*[WAN Opt. & Cache]*、*[Peer]*、*[Authentication Group]* の順に選択します。

[Authentication Group] ページ

このページには、作成済みの認証グループが一覧表示されます。このページでは、認証グループを編集、削除、または新規作成できます。

[Create New] 新しい認証グループを追加します。

[Name] 認証グループの名前。

[Authentication Method] トンネルの認証に使用する方法として、[Certificate]（ および証明書名 ）または [Pre-shared key] が表示されます

[Peer(s)] 認証グループに追加されたピアのホスト ID。認証グループを WAN 最適化ルールに追加すると、これらの FortiGate ユニットに限り、この WAN 最適化ルールを使用するための認証が行われます。*[Peer(s)]* には、すべてのピア、FortiGate ユニットのピア リストに追加されたピア（定義済みピア）、または選択されたピアのいずれかが示されます。

[New Authentication Group] ページ

このページでは、認証グループを設定できます。

[Name] 認証グループの名前を入力または変更します。認証グループをルールに追加するときは、この名前を選択します。
この FortiGate ユニットとともに WAN 最適化トンネルに参加する他の FortiGate ユニットには、同じ名前の認証グループが必要です。

[Authentication Method] 使用する認証方法を選択します。
WAN 最適化トンネルの認証および暗号化に証明書を使用する場合は、*[Certificate]* を選択します。
WAN 最適化トンネルの認証および暗号化に事前共有キーまたはパスワードを使用する場合は、*[Pre-shared key]* を選択します。

[Certificate] (リスト)	このオプションは、*[Authentication Method]* で *[Certificate]* を選択した場合のみ利用できます。 この FortiGate ユニットに追加されているローカル証明書を選択します。この FortiGate ユニットとともに WAN 最適化トンネルに参加する他の FortiGate ユニットには、同じ名前の証明書をともなう認証グループが必要です。 ローカル証明書を FortiGate ユニットに追加するには、*[System]*、*[Certificates]*、*[Local Certificates]* の順に選択します。
[Password]	このオプションは、*[Authentication Method]* で *[Pre-shared key]* を選択した場合のみ利用できます。 認証グループによって使用されるパスワード (または事前共有キー) を追加します。このFortiGateユニットとともにWAN最適化トンネルに参加する他のFortiGate ユニットには、同じ名前のパスワードをともなう認証グループが必要です。 この鍵には、印字可能な文字が 6 字以上含まれる必要があり、ネットワーク管理者以外にこの鍵を知られてはなりません。既知の攻撃に対して最大限の保護を実施するためには、鍵にはランダムに選択した 16 字以上の英数文字を使用してください。
[Peer Acceptance]	WAN 最適化ピア認証のオプションとして、以下のうち 1 つまたは複数の項目が表示されます。
[Accept Any Peer]	どのピアとも認証を行います。この認証グループを使用するピアのピア ホスト ID または ID アドレスが不明の場合に、この設定を使用します。この設定は、FortiClient アプリケーションをともなう WAN 最適化で、最も頻繁に使用されます。
[Accept Defined Peers]	FortiGate ユニットのピア リストに含まれるどのピアとも認証を行います。
[Specify Peer]	選択されたピアのみと認証を行います。このオプションを選択する場合、さらにこの認証グループに追加するピアを選択します。

WAN 最適化のモニタリング

WAN 最適化モニタを使用することにより、WAN 最適化のパフォーマンスを表示し強化することができます。このモニタリング ツールは、パフォーマンスの問題の切り分けおよびトラブルシューティングに役立ち、ネットワーク最適化および能力計画 (キャパシティ プランニング) を支援します。

モニタ ユニットには、収集されたログ記録の情報に基づく統計が、グラフィカルな形式で表示され、ネットワーク トラフィックのサマリおよび帯域の最適化情報などが示されます。

WAN 最適化モニタを表示するには、*[WAN Opt. & Cache]*、*[Monitor]*、*[Monitor]* の順に選択します。

[Monitor] ページ

このページには、トラフィックおよび帯域最適化の情報を示す、2 つのウィジェットが表示されます。[Traffic Summary] ウィジェットには、プロトコル情報および円グラフが表示されます。[Bandwidth Optimization] ウィジェットには、帯域幅の最適化情報が棒グラフで示され、グラフの表示形式は変更できます。

[Monitor] ページの [Traffic Summary] ウィジェット

このセクションには、トラフィック最適化の情報が表示されます。円グラフには、*[Period]* フィールドで選択された期間に処理されたサポートされるアプリケーションのトラフィックの割合が示されます。表には、各プロトコルの LAN および WAN トラフィック量と比較した場合の、WAN 最適化によるトラフィック削減率が示されます。

更新アイコン	[Traffic Summary] の表示を更新します。
[Period]	表示する [Traffic Summary] 情報の期間を、以下の項目から選択します。 ・ [Last 10 Minutes] (直近 10 分間の統計) ・ [Last 1 Hour] (直近 1 時間の統計) ・ [Last 1 Day] (直近 1 日の統計) ・ [Last 1 Week] (直近 1 週間の統計) ・ [Last 1 Month] (直近 1 か月の統計)
[Reduction Rate]	アプリケーションごとの最適化率を表示します。たとえば、80% の最適化率は、そのアプリケーションにより処理されたデータ量が 20% 削減されていることを意味します。
[LAN]	アプリケーションごとの、LAN から受信されたデータ量 (MB 単位)。

[WAN]	アプリケーションごとの、WAN 経由で送信されたデータ量 (MB 単位)。LAN および WAN データの差が大きいほど、WAN 最適化のバイト キャッシュ、Web キャッシュ、およびプロトコル最適化によるデータ量の削減率が大きいことを意味します。

[Monitor] ページの [Bandwidth Optimization] ウィジェット

このセクションには、[Period] に指定される期間に応じて、ネットワーク帯域幅の最適化が示されます。折れ線グラフまたは棒グラフにより、アプリケーションの最適化前 (LAN データ) のサイズと、最適化後のサイズ (WAN データ) との比較が示されます。

更新アイコン	[Bandwidth Optimization] の表示を更新するとき選択します。
[Period]	表示する [Bandwidth Optimization] の期間を、以下の項目から選択します。 ・ [Last 10 Minutes] (直近 10 分間の統計) ・ [Last 1 Hour] (直近 1 時間の統計) ・ [Last 1 Day] (直近 1 日の統計) ・ [Last 1 Week] (直近 1 週間の統計) ・ [Last 1 Month] (直近 1 か月の統計)
[Protocol]	*[All]* を選択すると、すべてのアプリケーションの帯域幅最適化が表示されます。個別のプロトコルを選択すると、そのプロトコルの帯域幅最適化が示されます。
[Chart Type]	帯域幅最適化の表示形式を、折れ線グラフまたは棒グラフから選択します。

Web キャッシュ設定の変更

多くの場合、WAN 最適化 Web キャッシュの設定は、デフォルトのまま使用できます。一方、パフォーマンスの強化、キャッシュ可能なオブジェクトのサイズ調整、または実際の環境に合わせたキャッシュの最適化などが必要な場合は、デフォルトの設定を変更できます。Web キャッシュの設定を変更するには、*[WAN Opt. & Cache]*、*[Cache]*、*[Settings]* の順に選択します。

除外 URL をキャッシュしないようにするには、この設定を CLI から有効にして、キャッシュしない除外 URL の URL フィルタ リストを設定する必要があります。URL をキャッシュ対象から除外するコマンド構文は、以下のようになります。

```
config wanopt webcache
  set explicit enable
  set cache-exempt enable
end
```

Web キャッシュの各種設定の詳細については、RFC 2616 を参照してください。

[Settings] ページ

このページでは、WAN 最適化 Web キャッシュを設定できます。

[Always revalidate]	このオプションをオンにすると、サーバ上のコンテンツをともなうキャッシュされたオブジェクトが要求されたとき、そのオブジェクトをクライアントに提供する前に必ず検証します。
[Max Cache Object Size]	キャッシュされるオブジェクト (ファイル) の最大サイズを設定します。 デフォルトのサイズは 512000 KB です。この設定により、Web キャッシュに保存されるオブジェクトの上限サイズが決まります。このサイズを超えるオブジェクトは、 クライアントに提供されますが、 FortiGate の Web キャッシュには保存されません。
[Negative Response Duration]	ネガティブ レスポンス (否定的な応答) をキャッシュする時間の長さを、分単位で設定します。デフォルトの値は 0 ですが、この場合ネガティブ レスポンスをキャッシュしないことを意味します。コンテンツ サーバは、一部の要求に対して、クライアント エラー コード (HTTP レスポンス、4xx) またはサーバ エラー コード (HTTP レスポンス、5xx) の応答を返信する場合があります。このようなネガティブ レスポンスをキャッシュするように Web キャッシュを設定すると、以降にそのページまたは画像への要求が送信されたとき、指定された分単位の時間は Web キャッシュからそのレスポンスが返されます。
[Fresh Factor]	[Fresh Factor] には、 パーセントの数値を設定します。 デフォルト値は 100、 設定範囲は 1 ～ 100 です。有効期限を持たないキャッシュされたオブジェクトに対して、Web キャッシュはそのオブジェクトが期限切れかどうかを定期的にチェックします。 *[Fresh Factor]* の設定値が大きいほど、 チェックの頻度は低くなります。 たとえば、*[Max TTL]* の値および *[Default TTL]* を 7200 分 (5 日) に設定し、*[Fresh Factor]* を 20 に設定すると、キャッシュされたオブジェクトはその期限が切れる前に Web キャッシュによって 5 回チェックされます。*[Fresh Factor]* を 100 に設定すると、Web キャッシュのチェック回数は 1 回です。

[Max TTL] サーバ上で期限切れかどうかのキャッシュ チェックなしにオブジェクトが Web キャッシュに存在できる最長時間 (Time to Live)。デフォルトの値は、7200 分 (120 時間、または 5 日) です。

[Min TTL] サーバ上で期限切れかどうかの Web キャッシュ チェックが行われる前に、オブジェクトが Web キャッシュに存在できる最短時間。デフォルトの値は、5 分です。

[Default TTL] Web サーバにより設定される有効期間を持たないオブジェクトの、デフォルトの有効期間。デフォルトの有効期間は、1440 分 (24 時間) です。

[Explicit Proxy] FortiGate ユニットで [Explicit Web Proxy] が有効に設定されているかどうかを示します。詳しくは、117 ページの「Explicit Web プロキシの設定」を参照してください。

[Enable Cache Explicit Proxy] このオプションをオンにすると、WAN 最適化 Web キャッシュを使用して、Explicit Web Proxy により受信されたコンテンツをキャッシュします。

[Ignore]

[If-modified-since] デフォルトでは、クライアントの条件付き要求に含まれる if-modified-since (IMS) ヘッダによって指定される時刻が、キャッシュされているオブジェクトの最終更新時刻より遅い場合は、キャッシュされているコピーが陳腐化していることを強く示唆しています。その場合、キャッシュされているオブジェクトの最終更新時刻に基づいて、HTTP から OCS (Overlay Caching Scheme) に条件付き GET が送信されます。
このオプションをオンにして [Ignore] を有効にすると、この動作を無効にします。

[HTTP 1.1 Conditionals] HTTP 1.1 には他にも、陳腐化したオブジェクトを処理するキャッシュの動作をクライアント向けにコントロールする機能が含まれています。各種の cache-control ヘッダに応じて、キャッシュからオブジェクトを提供する前に、FortiGate ユニットに OCS への問い合わせを実行させることができます。cache-control ヘッダ値の詳しい動作については、RFC 2616 を参照してください。

[Pragma-no-cache] 通常は、クライアントから Pragma: no-cache (PNC) または Cache-Control: no-cache ヘッダをともなう HTTP GET 要求が送信されると、コンテンツが提供される前に、キャッシュから OCS への問い合わせが必ず行われます。したがって、FortiGate ユニットでは、キャッシュされているオブジェクトのコピーが最新の場合でも、OCS からオブジェクト全体が必ず新たにフェッチされます。
このような動作のために、PNC リクエストは、パフォーマンスを低下させ、サーバ側帯域幅の使用量を増大させる原因になります。しかし、このオプションをオンにして Pragma-no-cache の無視を有効にすると、クライアントからのリクエストに含まれる PNC ヘッダが無視されます。そのリクエストは、PNC ヘッダがないものとして FortiGate ユニットによって処理されます。

[IE Reload] Internet Explorer の一部バージョンでは、*[最新の情報に更新]* を選択すると、Pragma: no-cache ヘッダの代わりに Accept / ヘッダが発行されます。Accept ヘッダが / の値のみのとき、type-N オブジェクトの場合は FortiGate ユニットはそれを PNC ヘッダとして処理します。
このオプションをオンにして IE の再ロードを無視すると、FortiGate ユニットは Accept / ヘッダを PNC として解釈する処理を無視します。

[Cache Expired Objects] type-1 オブジェクトのみに適用されます。このオプションを選択すると、期限切れの type-1 オブジェクトがキャッシュされます (他の条件すべてによりオブジェクトがキャッシュ可能な場合)。

[Revalidated Pragma-no-cache] クライアントのリクエストに含まれる Pragma: no-cache (PNC) ヘッダは、FortiGate ユニットの効率的な帯域幅の利用に影響する場合があります。クライアントのリクエストに含まれる PNC を完全に無視 (上記 [Ignore] の [Pragma-no-cache] オプションをオンに設定) することが望ましくない場合は、*[Revalidate Pragma-no-cache]* オプションをオンにすることで、帯域幅利用への影響を緩和できます。
[Revalidate Pragma-no-cache] をオンにすると、オブジェクトがすでにキャッシュにある場合、クライアントの条件なし PNC-GET 要求は、条件付き GET 要求として OCS に送信されます。これにより、場合によっては OCS から 304 Not Modified のレスポンスが返される可能性があり、その場合 OCS からフル コンテンツが返される必要はないので、サーバ側帯域幅の使用量が節約される可能性があります。
[Revalidate Pragma-no-cache] オプションは、デフォルトではオフに設定されており、またトップレベル プロファイルの変更に影響されません。
大半のダウンロード マネージャは、PNC ヘッダをともなう byte-range リクエストを送信します。このようなリクエストにキャッシュから応えるには、*[Revalidate pragma-no-cache]* オプションを設定するとき byte-range のサポートも設定する必要があります。

ユーザ

この項では、ユーザ アカウント、ユーザ グループ、および外部の認証サーバを設定する方法について説明します。これらのユーザ認証のコンポーネントを使用することで、ネットワーク リソースへのアクセスを制御できます。

FortiGate ユニットでバーチャル ドメイン (VDOM) を有効にする場合は、バーチャル ドメインごとにユーザ認証を個別に設定します。詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には以下のトピックが含まれています。

ユーザ認証の設定

FortiGate の認証では、ユーザ グループごとにアクセスを制御しますが、ユーザ グループを作成する前に、以下のうち 1 つ以上の設定をしておく必要があります。

- ローカル ユーザ アカウントを設定します。各ユーザについて、FortiGate ユニット、RADIUS サーバ、LDAP サーバ、または TACACS+ サーバの、いずれによってパスワードを確認するかを選択できます。詳細については、448 ページの「ローカル ユーザ アカウント」を参照してください。
- IM ユーザ プロファイルを設定します。IM ユーザの場合、ネットワーク リソースの使用を許可またはブロックするためのユーザ リストを作成できます。FortiGate。詳細については、465 ページの「IM ユーザ モニタ リスト」を参照してください。
- RADIUS、LDAP、または TACACS+ サーバを使用してユーザ認証を行うように、FortiGate ユニットを設定します。詳細については、449 ページの「RADIUS」、451 ページの「LDAP」、および 453 ページの「TACACS+」を参照してください。
- 認証を行うためにディレクトリ サービス サーバを使用する場合は、FortiGate ユニットへのアクセスを設定します。詳細については、455 ページの「ディレクトリ サービス サーバの設定」を参照してください。
- 管理アクセス (HTTPS Web ベース マネージャ)、IPSec、SSL-VPN、および Web ベースのファイアウォール認証のための、証明書ベース認証を設定します。詳細については、456 ページの「PKI 認証」を参照してください。

システム管理者の認証を、FortiGate ユニットで RADIUS、LDAP、および TACACS+ サーバを使用して実行するように、および PKI を使用する証明書ベースの認証によって実行するように、FortiGate ユニットを設定できます。詳細については、169 ページの「システム – 管理者」を参照してください。また、認証のタイムアウト値を変更したり、またはファイアウォール認証でサポートされるプロトコルを選択できます。詳細については、463 ページの「認証」を参照してください。現在認証されているユーザ、認証されている IM ユーザ、および禁止ユーザのリストを表示できます。詳細については、464 ページの「モニタ」を参照してください。

認証が必要な各ネットワーク リソースについては、どのユーザ グループがネットワークへのアクセスを許可されるかを指定します。ユーザ グループには、ファイアウォール、ディレクトリ サービス、および SSL VPN の 3 種類があります。詳細については、459 ページの「ファイアウォール ユーザ グループ」、459 ページの「ディレクトリ サービス ユーザ グループ」、および 460 ページの「SSL VPN ユーザ グループ」を参照してください。

ローカル ユーザ アカウント

ローカル ユーザは、FortiGate ユニットで設定されるユーザです。ローカル ユーザの認証は、FortiGate ユニットに保存されているパスワードを使用するか (ユーザ名およびパスワードが FortiGate ユニットに保存されているユーザ アカウントと一致する必要があります)、または認証サーバに保存されているパスワードを使用して (ユーザ名が FortiGate ユニットに保存されているユーザ アカウントと一致し、ユーザ名およびパスワードがユーザと関連付けられている認証サーバに保存されているユーザ アカウントと一致する必要があります) 実行できます。

IM (Instant Messenger) プロトコルは、2 名以上の個人がリアルタイムに通信する主な手法として普及しつつあります。企業によっては、顧客サポートまたはテクニカル サポートなど重要な業務アプリケーションの運用に、IM プロトコルを採用している場合もあります。

現在、IM プロトコルによる代表的なサービスには、AOL Instant Messenger、Yahoo Instant Messenger、MSN messenger、および ICQ などがあります。FortiGate ユニットでは、アプリケーションの利用を許可またはブロックするように IM ユーザを設定し、どのアプリケーションの使用を許可するかを指定できます。

ローカル ユーザ アカウントの設定

有効なローカル ユーザ アカウントを持つユーザの認証実行を完全にブロックするか、または FortiGate ユニットを設定することにより、FortiGate ユニットに保存済みのユーザ名およびパスワードあるいは特定サーバ (LDAP、RADIUS、または TACACS+) に保存済みのアカウントを使用するユーザ認証の実行を許可できます。

既存のローカル ユーザのリストを表示するには、*[User]*、*[User]*、*[User]* の順に選択します。

[User] ページ

このページには、作成済みのローカル ユーザのリストが一覧表示されます。このページでは、ローカル ユーザ リストを編集、削除、または新規作成できます。

[Create New]	新しいローカル ユーザ アカウントを追加します。
[User Name]	ローカル ユーザ名。
[Type]	このユーザに対して使用する認証の種類。認証の種類は、Local (ユーザおよびパスワードが FortiGate ユニットに保存されている)、LDAP、RADIUS、および TACACS+ (ユーザおよびパスワードが認証サーバに保存されているユーザ アカウントと一致する) です。
削除アイコン	ユーザを削除します。 削除アイコンは、ユーザがユーザ グループに属している場合は使用できません。
編集アイコン	ユーザ アカウントを編集します。

注記: ユーザ名を削除すると、そのユーザに設定されている認証が削除されます。

Local ユーザを追加するには、*[User]*、*[User]*、*[User]* の順に選択し、*[Create New]* を選択して、以下の項目を入力または選択します。

[New User] ページ

このページでは、ローカル ユーザの認証実行を許可またはブロックするように設定できます。

[User Name]	ユーザを識別する名前。
[Disable]	このユーザに認証を実行させない場合にオンにします。
[Password]	FortiGate ユニットに保存されているパスワードを使用してこのユーザを認証する場合に選択し、フィールドにパスワードを入力します。パスワードには、必ず 6 文字以上を使用します。
[LDAP]	LDAPサーバに保存されているパスワードを使用してこのユーザを認証する場合に選択します。リストから LDAP サーバを選択します。 FortiGate の LDAP 設定に追加されている LDAP サーバのみを選択できます。詳細については、451 ページの「LDAP」を参照してください。
[RADIUS]	RADIUSサーバに保存されているパスワードを使用してこのユーザを認証する場合に選択します。リストから RADIUS サーバを選択します。 FortiGate の RADIUS 設定に追加されている RADIUS サーバのみを選択できます。詳細については、449 ページの「RADIUS」を参照してください。
[TACACS+]	TACACS サーバに保存されているパスワードを使用してこのユーザを認証する場合に選択します。リストから TACACS+ サーバを選択します。 FortiGate の TACACS 設定に追加されている TACACS サーバのみを選択できます。詳細については、453 ページの「TACACS+」を参照してください。

リモート認証

リモート認証の最も一般的な目的は、外出先で勤務する従業員が、適切なセキュリティ対策とともに企業ネットワークにリモート アクセスできるようにすることです。認証は基本的に、通信を行うとき、ログイン要求などを送付する送信者の (デジタルの) 身元を確認するためのプロセスです。送信者には、コンピュータの利用者、コンピュータ自体、またはコンピュータ プログラムなどが該当します。コンピュータ システムは、使用を許可されたユーザのみによって使用される必要があるので、未承認の使用を検出しそれを排除するための手段が必要となります。

FortiGate ユニットでは、ユーザ グループと呼ばれる、認証されたユーザのリストを定義することにより、ネットワーク リソースへのアクセスを制御できます。ネットワークまたは VPN トンネルなど、特定のリソースを使用するために、ユーザには以下が要求されます。

- アクセスを許可された、いずれかのユーザ グループに属すること。
- 要求に応じて、自身の身元を提示するユーザ名およびパスワードを正しく入力すること。

RADIUS

RADIUS (Remote Authentication and Dial-in User Service) サーバには、認証 (authentication)、使用権の付与 (authorization)、およびアカウンティング (accounting) の各機能が含まれています。FortiGate ユニットでは、RADIUS サーバの認証機能を使用します。認証のために RADIUS サーバを使用するには、そのサーバを必要とする FortiGate ユーザまたはユーザ グループを設定する前に、サーバを設定する必要があります。

RADIUS サポートが設定済みで、ユーザに RADIUS サーバによる認証を要求する場合は、そのユーザの資格情報が FortiGate ユニットから RADIUS サーバに認証のために送信されます。RADIUS サーバによってそのユーザが認証されれば、FortiGate ユニットでのユーザ認証が成功します。RADIUS サーバによってそのユーザを認証できない場合、その接続は FortiGate ユニットによって拒否されます。特定の認証プロトコルを選択するか、または RADIUS トラフィックのデフォルト ポートを変更することにより、デフォルトの認証方式を変更できます。

注記： RADIUS トラフィックのデフォルト ポートは、1812 です。RADIUS サーバがポート 1645 を使用している場合は、CLI を使用してデフォルトの RADIUS ポートを変更します。詳細については、『*FortiGateCLI リファレンス*』の `config system global` コマンドを参照してください。

UTF-8 エンコーディングを設定するには、CLI からこれを有効にする必要があります。UTF-8 エンコーディングを有効にするには、以下のコマンド構文を使用します。

```
config vpn ssl settings
  set force-utf8-login enable
end
```

RADIUS サーバのリストを表示するには、*[User]*、*[Remote]*、*[RADIUS]* の順に選択します。

[RADIUS] ページ

このページには、作成済みの RADIUS サーバが一覧表示されます。このページでは、RADIUS サーバを編集、削除、または新規作成できます。

[Create New]	新しい RADIUS サーバを追加します。最大数は、10 です。
[Name]	FortiGate ユニット上の RADIUS サーバを識別する名前。
[Server Name/IP]	RADIUS サーバのドメイン名または IP アドレス。
削除アイコン	RADIUS サーバの設定を削除します。 ユーザ グループに追加されている RADIUS サーバを削除することはできません。
編集アイコン	RADIUS サーバの設定を編集します。

RADIUS サーバの設定

RADIUS サーバは、共有鍵を使用することで、サーバ自体と FortiGate ユニットなどのクライアントとの間でやり取りされる情報を暗号化します。RADIUS サーバの設定では、さらに予備の RADIUS サーバを設定できます。FortiGate ユニットは、最初にメインの RADIUS サーバと認証を試み、応答がない場合は予備のサーバと認証を行います。RADIUS サーバをユーザ グループの設定に特別に加えることなく、すべてのユーザ グループに RADIUS サーバを加えることができます。

注記： サーバの共有鍵に使用する文字数は、16 文字までです。

RADIUS サーバでは、認証プロセスの際に数種類の異なる認証プロトコルを使用できます。

- MS-CHAP-V2 は、Microsoft チャレンジ ハンドシェイク認証プロトコル v2 です。
- MS-CHAP は、Microsoft チャレンジ ハンドシェイク認証プロトコル v1 です。
- CHAP（チャレンジ ハンドシェイク認証プロトコル）は、PAP と同様に機能しますが、パスワードなどのユーザ情報を、ネットワークを経由してセキュリティ サーバに送信しません。
- PAP (password authentication protocol) は、PPP 接続の認証に使用します。PAP では、パスワードなどのユーザ情報がクリア テキストで（暗号化されずに）送信されます。

プロトコルを選択していない場合は、デフォルトのプロトコル設定では PAP、MS-CHAPv2、および CHAP が、この順序で使用されます。

RADIUS サーバを追加するには、*[User]*、*[Remote]*、*[RADIUS]* の順に選択し、*[Create New]* を選択して、以下の項目を入力または選択します。

[New RADIUS Server] ページ

このページでは、RADIUS サーバを設定できます。

[Name]	FortiGate ユニットで RADIUS サーバを識別するために使用する名前を入力します。
[Primary Server Name/IP]	メインの RADIUS サーバのドメイン名または IP アドレスを入力します。

[Primary Server Secret]	メインの RADIUS サーバに使用する、RADIUS サーバ共有鍵を入力します。サーバの共有鍵に使用可能な文字数は、16 文字までです。
[Secondary Server Name/IP]	予備の RADIUS サーバがある場合は、そのドメイン名または IP アドレスを入力します。
[Secondary Server Secret]	予備の RADIUS サーバに使用する、RADIUS サーバ共有鍵を入力します。予備サーバの共有鍵に使用可能な文字数は、16 文字までです。
[Authentication Scheme]	デフォルトの方法で認証を行う場合は、[Use Default Authentication Scheme] を選択します。デフォルトの認証方法では、PAP、MS-CHAP-V2、および CHAP が、この順序で使用されます。 デフォルトの認証方法を無効にするには、[Specify Authentication Protocol] を選択し、リストから MS-CHAP-V2、MS-CHAP、CHAP、または PAP のプロトコルを、RADIUS サーバの要件に合わせて選択します。
[NAS IP/Called Station ID]	NAS IP アドレスおよび Called Station ID を入力します (RADIUS 属性 31 の詳細については、RFC 2548 Microsoft Vendor-specific RADIUS Attributes を参照してください)。IP アドレスを入力しない場合は、FortiGate インタフェースによって RADIUS サーバとの通信のために使用される IP アドレスが適用されます。
[Include in every User Group]	RADIUS サーバがすべてのユーザ グループに自動的に含まれるようにする場合に、このオプションをオンにします。

LDAP

LDAP (Lightweight Directory Access Protocol) は、部門、複数の個人、個人同士のグループ、パスワード、電子メール アドレス、プリンタなどが含まれる認証データを管理するために使用される、インターネット プロトコルです。LDAP は、データ表現スキーム、定義済み機能のセット、およびリクエスト / レスポンス型ネットワークから構成されます。

LDAP サポートが設定済みで、ユーザに LDAP サーバによる認証を行うように要求する場合は、認証のために FortiGate ユニットから LDAP サーバへの通信が行われます。FortiGate ユニットで認証を行う際には、ユーザはユーザ名とパスワードを入力します。入力されたユーザ名とパスワードは、FortiGate ユニットから LDAP サーバに送信されます。LDAP サーバによってそのユーザが認証される場合は、FortiGate ユニットにおけるユーザ認証も正しく行われます。LDAP サーバによってそのユーザを認証できない場合、その接続は FortiGate ユニットによって拒否されます。

FortiGate ユニットでは、RFC 2251: Lightweight Directory Access Protocol v3 で規定されている LDAP プロトコル機能がサポートされており、これによりユーザ名とパスワードが検索および検証されます。FortiGate の LDAP は、LDAP v3 に準拠するすべての LDAP サーバをサポートします。さらに、FortiGate の LDAP は、LDAP over SSL/TLS もサポートします。SSL/TLS 認証の設定については、『*FortiGate CLI リファレンス*』を参照してください。

FortiGate の LDAP はパスワード更新をサポートしており、これらの設定は CLI から行います。このとき行う設定には、パスワードの失効を知らせる警告、および失効のしきい値の設定が含まれます。LDAP のパスワード更新を設定するには、以下のコマンドを使用します。

```
config user ldap
  edit <name>
    set password-expiry-warning {enable | disable}
    set password-expiry-threshold <number_of_days>
    set password-renewal {enable | disable}
  end
```

LDAP サーバのリストを表示するには、*[User]*、*[Remote]*、*[LDAP]* の順に選択します。

[LDAP] ページ

このページには、作成済みの LDAP サーバが一覧表示されます。このページでは、LDAP サーバの編集、削除、または新規作成が可能です。

[Create New]	新しい LDAP サーバを追加します。最大数は、10 です。
[Name]	FortiGate ユニット上の LDAP サーバを識別する名前。
[Server Name/IP]	LDAP サーバのドメイン名または IP アドレス。

[Port]	LDAP サーバとの通信に使用される TCP ポート。
[Common Name identifier]	LDAP サーバの共通名識別子。ほとんどの LDAP サーバは、cn を使用します。ただし、一部のサーバは、uid など他の共通名識別子を使用する場合もあります。
[Distinguished Name]	LDAP サーバ上のエントリの検索に使用される識別名。この識別名には、共通名識別子より上にある LDAP データベース オブジェクト クラスの階層が反映されています。
削除アイコン	LDAP サーバの設定を削除します。
編集アイコン	LDAP サーバの設定を編集します。

LDAP サーバの設定

ディレクトリには、類似の属性を持つオブジェクトが、論理的、階層的に整理され置かれています。一般的に、LDAP ディレクトリ ツリーは地理的または組織的な境界を表し、階層の最上位には DNS (Domain Name System) 名があります。多くの LDAP サーバでは、共通名識別子は cn ですが、一部のサーバでは uid など他の共通名識別子が使用されます。

たとえば、次の基本識別名を使用できます。

```
ou=marketing,dc=fortinet,dc=com
```

ここで、ou は組織単位であり、dc はドメイン コンポーネントです。

また、識別名に同じフィールドの複数のインスタンスを指定することもできます。たとえば、複数の組織単位を指定するには次のようにします。

```
ou=accounts,ou=marketing,dc=fortinet,dc=com
```

LDAP サーバによってユーザが正しく認証され、そのユーザの権限に基づいて LDAP サーバへのユーザ アクセスが許可されると、バインドが発生します。

以下の 3 種類のバインドからいずれかを使用するように、FortiGate ユニットを設定できます。

- Anonymous・匿名ユーザ検索を用いるバインド
- Regular・ユーザ名 / パスワード、さらに検索を用いるバインド
- Simple・簡易パスワード認証を用い検索なしのバインド

ユーザの記録がすべて 1 つの dn に当てはまる場合は、簡易 (simple) 認証を使用できます。ユーザが複数の dn に当てはまる場合は、匿名 (Anonymous) または通常 (Regular) 認証を使用します。この場合、LDAP データベース全体で要求されたユーザ名を検索できます。

LDAP サーバから、検索を実行するための認証が要求される場合は、通常 (regular) 認証を使用し、ユーザ名およびパスワードの値を入力します。

LDAP サーバを追加するには、*[User]*、*[Remote]*、*[LDAP]* の順に選択し、*[Create New]* を選択します。以下の情報を入力し、[OK] を選択します。

[New LDAP Server] ページ

このページでは、LDAP サーバを設定できます。

[Name]	FortiGate ユニット上の LDAP サーバを識別する名前を入力します。
[Server Name/IP]	LDAP サーバのドメイン名または IP アドレスを入力します。
[Server Port]	LDAP サーバとの通信に使用される TCP ポートを入力します。 デフォルトでは、LDAP はポート 389 を使用します。 セキュア LDAP サーバを使用する場合は、[Secure Connection] をオンにするとデフォルト ポートが変更されます。
[Common Name identifier]	LDAP サーバの共通名識別子を入力します。使用可能な最大文字数は、20 文字です。
[Distinguished Name]	正しい X.500 または LDAP 形式を使用するサーバの基本識別名を入力します。FortiGate ユニットは、この識別名を、変更せずにそのままサーバに渡します。使用可能な最大文字数は、512 文字です。
クエリ アイコン	識別名を相互参照できるように、設定する LDAP サーバの LDAP サーバ識別名クエリ ツリーを表示します。 詳細については、「クエリの使用」を参照してください。
[Bind Type]	LDAP 認証のバインドの種類を選択します。

[Regular]	ユーザ名 / パスワードを使用して直接 LDAP サーに接続し、入力された値の検索結果に応じて許可または拒否を受け取ります。
[Anonymous]	匿名ユーザとして LDAP サーバに接続し、ユーザ名 / パスワードを取得して、それらを入力された値と比較します。
[Simple]	ユーザ名 / パスワードの認証により、直接 LDAP サーバに接続します。
[Filter]	グループ検索に使用するフィルタを入力します。このオプションは、*[Bind Type]* を *[Regular]* または *[Anonymous]* に設定する場合に*利用*できます。
[User DN]	認証するユーザの識別名を入力します。このオプションは、*[Bind Type]* を *[Regular]* に設定する場合に利用できます。
[Password]	認証するユーザのパスワードを入力します。このオプションは、*[Bind Type]* を *[Regular]* に設定する場合に利用できます。
[Secure Connection]	認証にセキュア LDAP サーバ接続を使用する場合にオンにします。
[Protocol]	認証に使用するセキュア LDAP プロトコルを選択します。このオプション指定に応じて、*[Server Port]* の値が、指定したプロトコルのデフォルトポートに変更されます。このオプションは、[Secure Connection] をオンにした場合に利用できます。 **[LDAPS]** の場合は、ポート 636。 **[STARTTLS]** の場合は、ポート 389。
[Certificate]	認証に使用する証明書を、リストから選択します。証明書リストは、CA 証明書 (*[System]*、*[Certificates]*、*[CA Certificates]* の順に選択) に基づいています。

クエリの使用

[LDAP Distinguished Name Query] リストには、*[LDAP Server]* の IP アドレス、および LDAP サーバの共通名識別子に関連付けられているすべての識別名 (DN) が表示されます。このツリーによって、[Distinguished Name] フィールドに正しい内容を容易に入力できます。共通名 (CN) 識別子に関連付けられた識別名 (DN) を表示するには、CN 識別子の横にある*展開矢印*を選択し、リストから DN を選択します。選択した DN が、*[Distinguished Name]* フィールドに表示されます。[OK] を選択して、LDAP サーバ設定の *[Distinguished Name]* フィールドの選択を保存します。

選択した *[Distinguished Name]* の LDAP サーバ ユーザ グループに含まれるユーザを表示するには、*[LDAP Distinguished Name Query]* ツリーの *[Distinguished Name]* の横にある展開矢印を選択します。

TACACS+

近年、リモート ネットワーク アクセスは、端末アクセスから LAN アクセスに移行しています。ユーザは、ノートブック PC またはホーム PC を使用して企業ネットワークにアクセスするとき、勤務オフィス内での接続と変わりない完全なネットワーク接続を行い、実際にオフィスでアクセスするとの同じレベルで、企業ネットワークのリソースにアクセスできます。このような接続は、リモート アクセス サーバを経由して行います。リモート アクセス テクノロジの発達にともない、ネットワーク アクセスのセキュリティは一段と重要になっています。

TACACS+ (Terminal Access Controller Access-Control System) は、リモート認証プロトコルです。TACACS+ では、ルータ、ネットワーク アクセス サーバなど、ネットワーク上のコンピューティング機器のアクセス制御が、1 台または複数の集中型サーバによって可能になります。また TACACS+ によって、クライアントは、ユーザ名およびパスワードを受け付け、TACACS+ 認証サーバにクエリを送信することが可能になります。サーバ ホストは要求を受け付けるか拒否するかを判断し、ネットワーク アクセスを許可または拒否する応答をユーザに返信します。TACACS+ サーバのデフォルトの TCP ポートは、49 です。

TACACS+ サーバのリストを表示するには、*[User]*、*[Remote]*、*[TACACS+]* の順に選択します。

[TACACS+] ページ

このページには、作成済みの TACACS+ サーバが一覧表示されます。このページでは、TACACS+ サーバの編集、削除、または新規作成が可能です。

[Create New]	新しい TACACS+ サーバを追加します。最大数は、10 です。

[Server]	TACACS+ サーバのドメイン名または IP アドレス。
[Authentication Type]	サポートされる認証方法。TACACS+ の認証方法には、Auto、ASCII、PAP、CHAP、および MSCHAP が含まれます。
削除アイコン	TACACS+ サーバを削除します。
編集アイコン	TACACS+ サーバを編集します。

TACACS+ サーバの設定

認証プロセスの際に TACACS+ による使用が可能な認証プロトコルには、数種類の異なるプロトコルがあります。

- ASCII

  英文字による記述を使用し、マシンに依存しない方式です。ユーザが入力するユーザ名およびパスワードが、クリア テキストで (暗号化なしに) 送信され、ユーザ データベースに ASCII 形式で保存されているエントリと照合されます。
- PAP (パスワード認証プロトコル)

  PPP 接続の認証に使用されます。PAP では、パスワードなどのユーザ情報がクリア テキストで送信されます
- CHAP (チャレンジ ハンドシェイク認証プロトコル)

  PAP と同様に機能しますが、パスワードなどのユーザ情報をネットワーク経由でセキュリティ サーバに送信しないので、高いセキュリティをともないます。
- MS-CHAP (Microsoft チャレンジ ハンドシェイク認証プロトコル v1)

  Microsoft 社バージョンの CHAP です。

デフォルトのプロトコル設定の [Auto] では、PAP、MS-CHAP、および CHAP が、この順序で使用されます。

TACACS+ サーバを追加するには、*[User]*、*[Remote]*、*[TACACS+]* の順に選択し、*[Create New]* を選択して、以下の項目を入力または選択します。

[New TACACS+ Server] ページ

このページでは、TACACS+ サーバを設定できます。

[Name]	TACACS+ サーバの名前を入力します。
[Server Name/IP]	TACACS+ サーバのドメイン名または IP アドレスを入力します。
[Server Key]	TACACS+ サーバにアクセスするためのキーを入力します。このサーバ キーに使用可能な最大文字数は、16 文字です。
[Authentication Type]	TACACS+ サーバで使用する認証の種類を選択します。選択可能な認証の種類には、Auto、ASCII、PAP、CHAP、および MSCHAP が含まれます。[Auto] を選択すると、認証に PAP、MSCHAP、および CHAP が (この順序で) 使用されます。

ディレクトリ サービス

Windows Active Directory (AD) および Novell eDirectory では、ドメイン (あるオペレーティング システムの異なるバージョンを実行する複数コンピュータの論理的なグループ) 上にあるネットワーク リソースに関する情報を、中央のディレクトリ データベースに保存することにより、集中管理型の認証サービスが可能になります。ドメイン内でコンピュータを使用する個人は、自分の固有アカウント / ユーザ名を受け取ります。このアカウントには、ドメイン内にあるリソースへのアクセスを割り当てることができます。ドメインでは、ドメイン コントローラとして設定されるコンピュータ上にディレクトリが置かれます。ドメイン コントローラは、セキュリティに関連する機能全般を運用するサーバとして稼働します。これらセキュリティ関連機能の対象には、ユーザ / ドメインの関連付け、セキュリティの一元化、および管理機能が含まれます。

FortiGate ユニットでは、ファイアウォール ポリシーを利用し、ポリシーに設定されたユーザ グループに基づいてリソースへのアクセスを制御します。FortiGate ユーザ グループは、グループごとに 1 つ以上のディレクトリ サービス ユーザ グループと関連付けられています。ユーザが Windows または Novell ドメインにログインすると、FSAE (Fortinet Server Authentication Extension) から、ユーザの IP アドレスおよびユーザが属するディレクトリ サービス ユーザ グループの名前が、FortiGate ユニットに送信されます。

FSAE には、ネットワークへの導入が必要な 2 種類のコンポーネントがあります。

- ドメイン コントローラ (DC) エージェント。すべてのドメイン コントローラに必ず導入することで、ユーザのログインを監視し、ユーザの情報をコレクタ エージェントに送信するために利用します。
- コレクタ エージェント。1 台以上のドメイン コントローラに必ず導入することにより、DC エージェントから受け取った情報を FortiGate ユニットに送信するために利用します。

FortiGate ユニットでは、この情報に基づく、ドメイン コントローラのユーザ グループ データベースが保守管理されます。ドメインコン トローラによってユーザ認証が行われるので、FortiGate ユニットによるユーザ認証は実行されません。ユニットでは、IP アドレスに基づいてグループのメンバが識別されます。

ネットワーク上に FSAE (Fortinet Server Authentication Extensions) を導入し、ディレクトリ サービス サーバから情報を取得するように FortiGate ユニットを設定する必要があります。FSAE の詳細については、『*Fortinet Server Authentication Extension 管理ガイド*』を参照してください。.

ディレクトリ サービス サーバのリストを表示するには、*[User]*、*[Directory Service]*、*[Directory Service]* の順に選択します。

[Directory Service] ページ

このページには、ディレクトリ サービス サーバが一覧表示され、個々のサーバに設定されているすべての FSAE コレクタ エージェントが含まれています。このページでは、ディレクトリ サービスを編集、削除、または新規作成できます。

[Create New]	新しいディレクトリ サービス サーバを追加します。[Create New] を選択すると、画面が [New] ページに自動的に移動します。
[Name]	サーバ / ドメイン / グループ名の横にある展開矢印を選択し、ディレクトリ サービス ドメインおよびグループ情報を表示します。
AD サーバ	ディレクトリ サービス サーバに定義されている名前。
ドメイン	ディレクトリ サービス サーバからインポートされるドメイン名。
グループ	ディレクトリ サービス サーバからインポートされるグループ名。
[FSAE Collector IP]	ディレクトリ サービス サーバのログオン情報を FortiGate ユニットに送信する最大 5 つの FSAE コレクタ エージェントの、IP アドレスおよび TCP ポート。
削除アイコン	このディレクトリ サービス サーバを削除します。
編集アイコン	このディレクトリ サービス サーバを編集します。
ユーザ / グループ追加アイコン	ユーザまたはサーバをリストに追加します。ユーザまたはグループの識別名を知っている必要があります。
更新アイコン	ページに表示されている現在の情報を更新するとき選択します。
ユーザ / グループ編集アイコン	リストに追加するユーザおよびグループを選択します。

ディレクトリ サービス サーバの設定

1 つ以上の FSAE コレクタ エージェントにアクセスが行われるように、FortiGate ユニットを設定する必要があります。コレクタ エージェントを導入したディレクトリ サービス サーバを、5 台まで指定できます。FSAE コレクタ エージェントからアクセスのための認証が要求される場合は、サーバのパスワードを入力します。サーバ名は、ユーザ グループの作成時にディレクトリ サービス サーバのリストに表示されます。また、ディレクトリ サービス情報を、FSAE エージェントからではなく直接 LDAP サーバから取得できます。

最大 5 つのコレクタ エージェントの情報を入力できます。

注記： 複数台のドメイン コントローラにコレクタ エージェントを導入する場合は、FortiGate ユニットに冗長性を設定できます。この場合、現行（ または最初 ）のコレクタ エージェントに不具合が生じても、FortiGate ユニットでは、最大 5 つのコレクタ エージェントを含むリスト中の次のエージェントに切り替わります。

新しいディレクトリ サービス サーバを追加するには、*[User]*、*[Directory Service]*、*[Directory Service]* の順に選択し、*[Create New]* を選択して、サーバに必要な情報を入力します。

[New] ページ

このページでは、複数の FSAE コレクタ エージェントを含むディレクトリ サービス サーバを設定できます。[Directory Service] ページで [Create New] を選択すると、画面が [New] ページに自動的に移動します。

[Name]	ディレクトリ サービス サーバの名前を入力します。この名前は、ユーザ グループの作成時にディレクトリ サービス サーバのリストに表示されます。
[FSAE Collector IP/Name]	このコレクタ エージェントが導入されているディレクトリ サービス サーバの IP アドレスまたは名前を入力します。使用可能な最大文字数は、63 文字です。
[Port]	ディレクトリ サービスに使用する TCP ポートを入力します。このポートは、FSAE コレクタ エージェントの設定で指定されたFortiGateのリスニング ポートと必ず同じにします。
[Password]	コレクタ エージェントのパスワードを入力します。このパスワードは、アクセスに認証を必要とするように FSAE コレクタ エージェントを設定した場合のみ必要となります。
[LDAP Server]	ディレクトリ サービスにアクセスするには、このチェック ボックスをオンにして、LDAP サーバを選択します。

PKI 認証

PKI (Public Key Infrastructure) 認証では、証明書認証ライブラリが利用されます。このライブラリは、ピア、ピア グループ、ユーザ グループのリストを取得し、認証成功または認証拒否の通知を返します。ユーザは、正しく認証を行うために証明書のみを必要とします。ユーザ名またはパスワードは必要ありません。ファイアウォールおよび SSL VPN は、PKI 認証を使用可能な唯一のユーザ グループです。

証明書認証の詳細については、『*FortiGate 証明書管理ユーザ ガイド*』を参照してください。CLI からのみ設定可能な PKI 設定の詳細については、『*FortiGate CLI リファレンス*』を参照してください。

PKI ユーザのリストを表示するには、*[User]*、*[PKI]*、*[PKI]* の順に選択します。

[PKI] ページ

このページには、作成済みの PKI ユーザが一覧表示されます。このページでは、PKI ユーザを編集、削除、または新規作成できます。

[Create New]	新しい PKI ユーザを追加します。[Create New] を選択すると、画面が [New PKI User] ページに自動的に移動します。
[Name]	PKI ユーザの名前。
[Subject]	認証しているユーザの証明書の [Subject] フィールドに表示されるテキスト文字列。
[CA]	このユーザの認証に使用される CA 証明書。
削除アイコン	この PKI ユーザを削除します。 削除アイコンは、ピア ユーザがユーザ グループに属している場合は使用できません。最初にそのユーザをユーザ グループから削除してください。
編集アイコン	この PKI ユーザを編集します。

ピア ユーザおよびピア グループの設定

注意：CLI を使用してピア ユーザを作成する場合、フォーティネットは、[Subject] または [CA] いずれかの値を入力することをお勧めします。入力せずに、ユーザ レコードを Web ベース マネージャで開くと、[Subject] または [CA] いずれかの値を入力するように促すメッセージが表示されます。

一部の VPN 設定における認証、およびファイアウォール ポリシーにおける PKI 証明書認証で使用される、ピア ユーザおよびピア グループを定義できます。

ピア ユーザは、PKI 認証を利用できるデジタル証明書の所持者です。PKI 認証を使用する前に、ファイアウォール認証ポリシーに組み入れられるユーザ グループに追加する、ピア ユーザを定義する必要があります。

ピア ユーザを定義するには、以下が必要です。

- ピア ユーザの名前
- 認証を行うピア ユーザの証明書の Subject フィールドに表示されるテキスト、またはピア ユーザを認証するために使用する CA 証明書

PKI 認証の他の設定を、追加または変更できます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

PKI 認証のピア ユーザを作成するには、*[User]*、*[PKI]*、*[PKI]* の順に選択し、*[Create New]* を選択して、ピア ユーザの情報を入力します。

注記：[Subject] または [CA] あるいは双方の値を、必ず入力します。

[New PKI User] ページ

このページでは、新しい PKI ユーザを設定できます。

[Name]	PKI ユーザの名前を入力します。
[Subject]	認証を行うユーザの証明書の [Subject] フィールドに表示されるテキスト文字列を入力します。このフィールドは、オプションです。
[CA]	このユーザを認証するために必ず使用する、CA 証明書を入力します。このフィールドは、オプションです。

[Two-factor authentication] セクション

[Require two-factor authentication]	この PKI ユーザに、証明書による認証に加えて、パスワードによって認証を行うように要求します。*[Password]* フィールドにパスワードを入力します。
[Password]	この PKI ユーザによって必ず入力されるパスワードを、このフィールドに入力します。

ピア ユーザ グループの設定は、CLI のみから実行できます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。

ユーザ グループ

ユーザ グループは、ユーザ ID のリストです。ユーザ ID には、以下があります。

- FortiGate ユニットに保存されているローカル ユーザ アカウント（ユーザ名とパスワード）
- パスワードが RADIUS、LDAP、または TACACS+ サーバに保存されているローカル ユーザ アカウント
- RADIUS、LDAP、または TACACS+ サーバ（このサーバ上の ID はすべて認証可能）
- ディレクトリ サービス サーバで定義されているユーザまたはユーザ グループ

各ユーザ グループは、ファイアウォール、ディレクトリ サービス、または SSL VPN の 3 種類のいずれかに属します。これら 3 種類の詳細については、459 ページの「ファイアウォール ユーザ グループ」, 459 ページの「ディレクトリ サービス ユーザ グループ」および 460 ページの「SSL VPN ユーザ グループ」を参照してください。各種ユーザ グループの設定については、460 ページの「ユーザ グループの設定」を参照してください。

FortiGate ユニットのユーザ認証は、多くの場合、ユーザ名およびパスワード入力を要求することで行われます。FortiGate ユニットでは、まずローカル ユーザ アカウントがチェックされます。一致が検出されない場合は、そのユーザ グループに属する RADIUS、LDAP、または TACACS+ サーバがチェックされます。FortiGate ユニットによりユーザ名およびパスワードの一致が確認されれば、認証が正しく行われます。

ディレクトリ サービス ユーザ グループの場合、ユーザがネットワークにログオンするとき、ディレクトリ サービス サーバによってユーザ認証が行われます。FortiGate ユニットでは、FSAE コレクタ エージェントから、そのユーザの名前と IP アドレスが受信されます。FSAE の詳細については、『*Fortinet Server Authentication Extension 管理ガイド*』を参照してください。.

以下の項目に認証アクセスできるように、ユーザ グループを設定できます。

- 認証が必要なファイアウォール ポリシー

  詳しくは、273 ページの「ファイアウォール ポリシーへの認証の追加」を参照してください。

  これらのポリシーに基づいて認証を実行できるユーザ グループを選択できます。
- FortiGate ユニット上の SSL VPN

  詳しくは、275 ページの「SSL VPN の ID ベース ファイアウォール ポリシーの設定」を参照してください。
- ダイヤルアップ ユーザの IPSec VPN フェーズ 1 設定

  詳しくは、413 ページの「フェーズ 1 の設定」を参照してください。

  認証を実行して VPN トンネルを使用できるユーザは、選択されたユーザ グループ内のユーザに限られます。
- IPSec VPN フェーズ 1 設定の XAuth

  詳しくは、415 ページの「フェーズ 1 の詳細設定」の [XAuth] を参照してください。

  XAuth を使用して認証されるユーザ グループは、選択されたユーザ グループ内のユーザ グループに限られます。
- FortiGate PPTP 設定

  詳しくは、425 ページの「FortiGate Web ベース マネージャによる PPTP 設定」を参照してください。

  PPTP を使用できるユーザは、選択されたユーザ グループ内のユーザに限られます。
- FortiGate L2TP 設定

  L2TP は、`config vpn l2tp` CLI コマンドでのみ設定できます。詳しくは、『*FortiGate CLI リファレンス*』を参照してください。

  L2TP を使用できるユーザは、選択されたユーザ グループ内のユーザに限られます。
- RADIUS 認証による管理者ログイン

  詳しくは、173 ページの「管理者に対する RADIUS 認証の設定」を参照してください。

  RADIUS サーバにアカウントを持つ管理者のみがログインできます。
- FortiGuard Web フィルタリングの置き換えグループ

  FortiGuard Web フィルタリングが Web ページをブロックする場合は、承認されたユーザが、Web ページへのアクセス、または別のグループのメンバに Web ページへのアクセスを許可するために、認証を実行できます。

認証が必要なリソースごとに、どのユーザ グループがアクセスを許可されるかを指定します。認証の需要に応じたユーザ グループの数とメンバシップを決定する必要があります。

このトピックには、以下の項目が含まれています。

- ファイアウォール ユーザ グループ

- ディレクトリ サービス ユーザ グループ
- SSL VPN ユーザ グループ
- ユーザ グループ リストの表示
- ユーザ グループの設定

ファイアウォール ユーザ グループ

ファイアウォール ユーザ グループでは、そのユーザ グループを許可グループの 1 つとして含み認証を求めるファイアウォール ポリシーに、アクセスすることができます。ユーザが、そのポリシーによって保護されているリソースにアクセスしようとすると、FortiGate ユニットから、グループ メンバのユーザ名およびパスワードを入力するように求められます。

証明書による認証方法を選択している場合は、証明書によるユーザ認証を実行できます。詳細については、273 ページの「ファイアウォール ポリシーへの認証の追加」を参照してください。

またファイアウォール ユーザ グループによって、ダイヤルアップ ユーザの IPSec VPN へのアクセスが可能となります。この場合、IPSec VPN フェーズ 1 設定では [Accept peer ID in dialup group peer] オプションが使用されます。ユーザの VPN クライアントは、ユーザ名がピア ID に、パスワードが PSK (pre-shared key) に設定されます。このユーザが IPSec VPN に正常に接続できるのは、ユーザ名が許可ユーザ グループのメンバであり、パスワードが FortiGate ユニットに保存されているパスワードと一致する場合のみです。

注記: いずれかのメンバが RADIUS または LDAP サーバを使用して認証されると、そのユーザ グループはダイヤルアップ グループになれません。

詳細については、413 ページの「フェーズ 1 の設定」を参照してください。

ファイアウォール ユーザ グループの設定については、460 ページの「ユーザ グループの設定」を参照してください。

また、ファイアウォール ユーザ グループを使用して、FortiGuardWeb フィルタリングの置き換え権限を提供できます。詳細については、461 ページの「ユーザ グループからの動的な VPN クライアント IP アドレス割り当て」を参照してください。

ディレクトリ サービス ユーザ グループ

ネットワーク上では、そのネットワークで既に認証されたディレクトリ サービス サーバ ユーザ グループのメンバにアクセスできるように、FortiGate ユニットを設定できます。ネットワーク ドメイン コントローラには、FSAE (Fortinet Server Authentication Extensions) を導入する必要があります。

ディレクトリ サービス ユーザ グループでは、そのユーザ グループを許可グループの 1 つとして含みディレクトリ サービス タイプの認証を求めるファイアウォール ポリシーに、アクセスすることができます。ディレクトリ サービス ユーザ グループのメンバは、設定したディレクトリ サービス サーバから FortiGate ユニットで受信されるリストに基づいて選択する、ディレクトリ サービス ユーザまたはグループです。詳細については、454 ページの「ディレクトリ サービス」を参照してください。

注記: ディレクトリ サービス ユーザ グループは、SSL VPN アクセスはできません。

ディレクトリ サービス ユーザ グループを、直接 FortiGate ファイアウォール ポリシーで使用することはできません。ディレクトリ サービス グループを、必ず FortiGate ユーザ グループに加えます。ディレクトリ サービス グループは、1 つの FortiGate ユーザ グループのみに属する必要があります。ディレクトリ サービス グループを、複数の FortiGate ユーザ グループに割り当てると、FortiGate ユニットは最後に割り当てられたユーザ グループのみを認識します。

また、ディレクトリ サービス ユーザ グループを使用することで、FortiGuardWeb フィルタリングの置き換え権限を提供できます。詳細については、461 ページの「ユーザ グループからの動的な VPN クライアント IP アドレス割り当て」を参照してください。

ユーザ グループの詳しい設定方法については、460 ページの「ユーザ グループの設定」を参照してください。

SSL VPN ユーザ グループ

SSL VPN ユーザ グループでは、そのユーザ グループを許可グループの 1 つとして含み SSL VPN タイプの認証を求めるファイアウォール ポリシーに、アクセスすることができます。ローカル ユーザ アカウント、LDAP サーバ、および RADIUS サーバは、いずれも SSL VPN ユーザ グループのメンバとなり得ます。ユーザが SSL VPN Web ポータルにアクセスするとき、FortiGate ユニットからユーザ名およびパスワードが要求されます。ユーザ グループの設定には、SSL VPN 機能のオプションが含まれます。

また SSL VPN ユーザ グループでは、ダイヤルアップ ユーザの IPSec VPN へのアクセスが可能です。この場合、IPSec VPN フェーズ 1 設定では [Accept peer ID in dialup group peer] オプションが使用されます。ユーザの VPN クライアント設定では、ユーザ名をピア ID に、パスワードを PSK (pre-shared key) に設定します。このユーザが IPSec VPN に正しく接続できるのは、ユーザ名が許可ユーザ グループのメンバであり、パスワードが FortiGate ユニットに保存されているパスワードと一致する場合のみです。IPSec VPN のユーザ グループの設定については、413 ページの「フェーズ 1 の設定」を参照してください。

注記： いずれかのメンバが RADIUS または LDAP サーバを使用して認証される場合は、そのユーザ グループは IPSec ダイヤルアップ グループになることはできません。

ユーザ グループの設定については、460 ページの「ユーザ グループの設定」を参照してください。SSL VPN ユーザ グループ オプションの設定については、275 ページの「SSL VPN の ID ベース ファイアウォール ポリシーの設定」を参照してください。

ユーザ グループ リストの表示

ユーザ グループ リストを表示するには、*[User]*、*[User Group]*、*[User Group]* の順に選択します。

[User Group] ページ

このページには、グループの種類別に、ユーザ グループ リストが表示されます。このページでは、ユーザ グループ リストを編集、削除、または新規作成できます。

[Create New]	新しいユーザ グループを追加します。
[Group Name]	ユーザ グループの名前。ユーザ グループ名には、ユーザ グループの種類別に、[Firewall]、[Directory Service]、および [SSL VPN] が表示されます。詳細については、459 ページの「ファイアウォール ユーザ グループ」、459 ページの「ディレクトリ サービス ユーザ グループ」、および 460 ページの「SSL VPN ユーザ グループ」を参照してください。
[Members]	そのユーザ グループに含まれる、ローカル ユーザ、RADIUS サーバ、LDAP サーバ、TACACS+ サーバ、ディレクトリ サービス ユーザ / ユーザ グループ、または PKI ユーザ。
削除アイコン	ユーザ グループを削除します。 ファイアウォール ポリシー、ダイヤルアップ ユーザ フェーズ 1 設定、PPTP または L2TP 設定に含まれているユーザ グループを削除することはできません。
編集アイコン	グループのメンバシップおよびオプションを編集します。

ユーザ グループの設定

新しいユーザ グループを追加するには、*[User]*、*[User Group]*、*[User Group]* の順に選択し、*[Create New]* を選択して、ユーザ グループの種類別に以下を入力または選択します。

注記：デフォルトでは、FortiGate Web ベース マネージャはファイアウォール オプションを表示します。以下の図では、[Firewall]、[Directory Service]、および [SSL VPN] のユーザ グループの種類別に、異なる表示内容が示されます。
管理者の認証に使用されるグループには、ローカル ユーザを追加できません。

[New User Group] ページ
このページでは、ユーザまたはグループあるいは双方を設定できます。

[Name]	ユーザ グループ名を入力します。
[Type]	ユーザ グループの種類を選択します。
[Firewall]	このグループは、ファイアウォール認証を要求するファイアウォール ポリシーの場合に選択します。詳しくは、273 ページの「ファイアウォール ポリシーへの認証の追加」および 461 ページの「ユーザ グループからの動的な VPN クライアント IP アドレス割り当て」を参照してください。
[Directory Service]	このグループは、ディレクトリ サービス認証を要求するファイアウォール ポリシーの場合に選択します。詳しくは、273 ページの「ファイアウォール ポリシーへの認証の追加」を参照してください。
[SSL VPN]	このグループは、[Action] を [SSL VPN] に設定しているファイアウォール ポリシーの場合に選択します。 トランスペアレント モードでは使用できません。 詳しくは、275 ページの「SSL VPN の ID ベース ファイアウォール ポリシーの設定」を参照してください。
[Portal]	このユーザ グループで使用する SSL VPN Web ポータル設定を選択します。詳細については、429 ページの「ポータル」を参照してください。
[Available Users/Groups] または **[Available Members]***	このユーザ グループに追加可能な、ローカル ユーザ、RADIUS サーバ、LDAP サーバ、TACACS+ サーバ、ディレクトリ サービス ユーザ / ユーザ グループ、または PKI ユーザのリスト。このリストにメンバを追加するには、名前を選択して右向き矢印を選択します。 * ユーザ グループの [Type] が [Directory Service] の場合は、[Available Members] が表示されます。
[Members]	このユーザ グループに属する、ローカル ユーザ、RADIUS サーバ、LDAP サーバ、TACACS+ サーバ、ディレクトリ サービス ユーザ / ユーザ グループ、または PKI ユーザのリスト。メンバを削除するには、名前を選択して左向き矢印を選択します。
[FortiGuard Web Filtering Override]	[Type] を [Firewall] または [Directory Service] に設定する場合のみ使用できます。 このグループの Web フィルタリングの上書き機能を設定します。 詳しくは、461 ページの「ユーザ グループからの動的な VPN クライアント IP アドレス割り当て」を参照してください。

ユーザ グループからの動的な VPN クライアント IP アドレス割り当て

SSL VPN トンネル モード、ダイヤルアップ IPSec、および PPTP VPN セッションでは、リモート ユーザに IP アドレスを割り当てることができます。ユーザに割り当てる IP アドレスは、RADIUS サーバによるユーザ認証成功の確認と同時に受け取る RADIUS レコードの Framed-IP-Address フィールドからから取得します。RADIUS フィールドの詳細については、RFC 2865 および RFC 2866 を参照してください。

FortiGate ユニットによって IP アドレスを動的に割り当てるには、RADIUS 認証を行うように VPN ユーザを設定する必要があり、ユーザに割り当てる IP アドレスを RADIUS サーバの Framed-IP-Address RADIUS フィールドに加える必要があります。VPN の設定は、種類ごとに区別して行います。それぞれの設定ごとに、IP アドレスをユーザに割り当てる設定を、ユーザ グループと関連付けます。

RADIUS レコードからの IP アドレスの割り当ては、アドレス範囲からの動的な IP アドレス割り当ての代わりに行われます。IP アドレス範囲と、RADIUS レコードからの IP アドレス割り当てを、同じ設定に含めることはできません。

IP アドレスを割り当てる RADIUS サーバを加えるには

1 *[User]*、*[Remote]*、*[RADIUS]* の順に選択し、*[Create New]* を選択して RADIUS サーバを追加します。

2 必要に応じて、RADIUS サーバを設定します。

特別な FortiGate の設定は必要ありません。

3 *[OK]* を選択して、RADIUS サーバを保存します。

SSL VPN トンネル モード ユーザの IP アドレスを動的に割り当てるには

RADIUS サーバを利用して SSL VPN トンネル モード ユーザの IP アドレスを割り当てるには、SSL VP ポータルに [Tunnel Mode] ウィジェットを追加することで、ポータルのトンネル モードを有効にします。[Tunnel Mode] ウィジェットでは、*[IP Mode]* を *[User Group]* に設定します。また、ポータルと、IP アドレスを割り当てる RADIUS サーバを、同じ SSL VPN ユーザ グループに追加します。さらに、SSL VPN ファイアウォール ポリシーで そのユーザ グループを選択します。

1 *[VPN]*、*[SSL]*、*[Portal]* の順に選択します。

2 SSL VPN ポータルを新規作成するか、または編集します。

3 [Tunnel Mode] ウィジェットをポータルに追加するか、またはウィジェットをポータルに追加済みの場合はウィジェットを編集します。

4 *[IP Mode]* を *[User Group]* に設定し、ポータルに加えた変更を保存します。

5 *[User]*、*[User Group]*、*[User Group]* の順に選択し、ユーザ グループを新規作成するかまたは SSL VPN ユーザ グループを編集します。

6 *[Type]* を *[SSL VPN]* に設定します。

7 [Tunnel Mode] ウィジェットを含む *ポータル* の名前を選択します。

8 IP アドレスを割り当てる RADIUS サーバを *[Members]* リストに追加し、SSL VPN ユーザ グループを保存します。

9 *[Firewall]*、*[Policy]*、*[Policy]* の順に選択し、*[Create New]* を選択します。

10 *[Action]* を *[SSL VPN]* に設定します。

11 ID ベース ポリシー、および RADIUS サーバを含む SSL VPN ユーザ グループ、およびポータルを、*[Selected User Groups]* リストに追加します。

12 必要に応じて、残りのファイアウォール ポリシー設定を行います。

RADIUS サーバを利用してダイヤルアップ IPSec VPN ユーザの IP アドレスを割り当てるには、IPSec VPN 設定に合わせて IPSec DHCP サーバを設定し、[Advanced] の設定で *[IP Assignment Mode]* を *[User-group defined method]* に設定します。また、RADIUS サーバをファイアウォール ユーザ グループに追加します。次に、ダイヤルアップ VPN のフェーズ 1 設定で、[Advanced] 設定の XAuth をサーバ モードに設定し、RADIUS サーバを追加したファイアウォール ユーザ グループを選択します。

ダイヤルアップ IPSec VPN の IP アドレスを動的に割り当てるには

1 *[System]*、*[DHCP Server]*、*[Service]* の順に選択し、IPSec VPN 設定で使用する IPSec DHCP サーバを追加または編集します。

2 [Advanced] を選択し、*[IP Assignment Mode]* を *[User-group defined method]* に設定して、DHCP サーバに加えた変更を保存します。

3 *[User]*、*[User Group]*、*[User Group]* の順に選択し、ユーザ グループを新規作成するかまたはファイアウォール ユーザ グループを編集します。

4 *[Type]* を *[Firewall]* に設定します。

5 IP アドレスを割り当てる RADIUS サーバを *[Members]* リストに追加し、ファイアウォール ユーザ グループを保存します。

6 *[VPN]*、*[IPSec]*、*[Auto Key (IKE)]* の順に選択し、ユーザ フェーズ 1 を作成または編集して、*[Remote Gateway]* を *[Dialup User]* に設定します。

7 [Advanced] を選択します。

8 *[XAUTH]* を *[Enable as Server]* に設定します。

9 *[User Group]* を、RADIUS サーバを含むファイアウォール ユーザ グループに設定します。

10 必要に応じて、残りの IPSec VPN 設定を行います。

PPTP VPN の場合、IP アドレスを割り当て可能な RADIUS サーバをファイアウォール ユーザ グループに追加することにより、RADIUS サーバを利用して PPTP ユーザの IP アドレスを割り当てることができます。次に、このユーザ グループを使用するように PPTP VPN を設定します。

PPTP VPN ユーザの IP アドレスを動的に割り当てるには

1 *[User]*、*[User Group]*、*[User Group]* の順に選択し、ユーザ グループを新規作成するかまたはファイアウォール ユーザ グループを編集します。

2 *[Type]* を *[Firewall]* に設定します。

3 IP アドレスを割り当てる RADIUS サーバを *[Members]* リストに追加し、ファイアウォール ユーザ グループを保存します。

4 FortiGate CLI に接続し、以下のコマンドを入力して PPTP を有効に設定し、割り当てる IP アドレスをユーザ グループとともに設定し、RADIUS サーバを含むユーザ グループを PPTP VPN 設定に追加します。

```
config vpn pptp
  set status enable
  set ip-mode usrgrp
  set usrgrp <user_group>
  set sip <address>
  set eip <address>
end
```

認証

ユーザ認証の設定では、認証タイムアウト、サポート対象のプロトコル、認証証明書などのオプションを定義できます。

認証タイムアウトは、認証接続されたファイアウォールが、ユーザの再認証が必要になるまでアイドル状態を維持できる期間として設定されます。

ファイアウォール ポリシーでユーザ認証が有効な場合、認証チャレンジは通常、4 種類のプロトコルのいずれかに対して (接続プロトコルに応じて) 発行されます。

- HTTP (HTTPS へのリダイレクトを行う設定も可能)
- HTTPS
- FTP
- Telnet

[Authentication Settings] 画面の [Protocol Support] リストからプロトコルを選択し、これによりどのプロトコルが認証チャレンジをサポートするかを制御できます。ユーザは、最初にサポートされるプロトコルによって接続を行う必要があり、以降は他のプロトコルによる接続が可能です。プロトコル サポートのメソッドとして HTTPS を選択する場合は、ユーザはカスタムのローカル証明書を使用して認証を実行できます。

ファイアウォール ポリシーでユーザ認証を有効に設定すると、ファイアウォール ポリシー ユーザはチャレンジ認証を行います。ユーザ ID およびパスワードによる認証では、ユーザは各自のユーザ名およびパスワードを入力する必要があります。証明書による認証では (HTTPS または HTTPS にリダイレクトされる HTTP のみ)、カスタムの証明書を FortiGate ユニットに導入できる一方、ユーザもカスタム証明書を各自のブラウザに導入できます。カスタムの証明書を使用しない場合は、ユーザは警告メッセージの表示に従い、デフォルトの FortiGate 証明書を受け入れる必要があります。

認証オプションを設定するには、*[User]*、*[User]*、*[Authentication]* の順に選択します。

[Authentication Settings] 画面

ここでは、ユーザのセッションで認証がどのように行われるかを設定できます。たとえば、認証タイムアウトを 10 分に設定すると、ユーザのセッションでアイドル状態が 10 分間続くと、ユーザはセッションから自動的にログアウトされます。

[Authentication Timeout]	分単位の時間を、1 ～ 480 の範囲で入力します。認証タイムアウトは、認証接続されたファイアウォールが、ユーザの再認証が必要になるまでアイドル状態を維持できる期間として設定されます。デフォルト値は 30 です。
[Protocol Support]	ファイアウォールのユーザ認証の際に、チャレンジ認証を実行するプロトコルを選択します。
[Certificate]	HTTPS プロトコル サポートを使用する場合は、認証に使用するローカル証明書を選択します。このオプションは、HTTPS プロトコル サポートを選択した場合のみ使用できます。
[Apply]	[Authentication Settings] に指定したユーザ認証設定を適用します。

注記：証明書による認証を利用するとき、ファイアウォール ポリシー作成時に証明書を何も指定しないと、グローバル設定が使用されます。証明書を指定する場合は、グローバル設定からポリシーごとの設定に置き換えられます。証明書認証の詳しい使用方法については、『*FortiGate 証明書管理ユーザ ガイド*』を参照してください。

モニタ

現在認証されているユーザ、認証されている IM ユーザ、および禁止ユーザのリストを表示できます。これらの情報を表示するには、*[User]*、*[Monitor]* の順に選択します。このリストでは、認証されているユーザごとに、ユーザ名、ユーザ グループ、認証の経過時間 (*[Duration]*)、ユーザ セッションのタイムアウトまでの残り時間 (*[Time left]*)、および使用された認証メソッドが示されます。[IM] ユーザのリストには、発信元 IP アドレス、プロトコル、および前回プロトコル使用された時刻が含まれます。[Banned User] のリストには、管理者により設定されたユーザ、および AV、IPS、または DLP ルールに基づき隔離されたユーザが含まれます。

リストには、以下が含まれます。

- ファイアウォール ユーザ モニタ リスト
- IM ユーザ モニタ リスト
- NAC 隔離および禁止ユーザ リスト

ファイアウォール ユーザ モニタ リスト

ネットワーク環境によっては、どのユーザが FortiGate ユニットによって認証されるかを指定でき、システム管理者がユーザの認証を解除 (進行中のセッションを停止) できると、便利な場合があります。ファイアウォール モニタでは、現在認証されている全ユーザの認証を解除するか、またはユーザごとに認証を解除することができます。あるユーザの再認証を永続的に停止するには、FortiGate の設定を変更し (ユーザ アカウントを無効にする)、ユーザ モニタを使用してそのユーザの現行セッションを直ちに終了します。

認証されているユーザ (Firewall) のリストを表示するには、*[User]*、*[Monitor]*、*[Firewall]* の順に選択します。

[Firewall] ページ

このページには、現在 FortiGate ユニットで認証されておりアクティブなファイアウォール ユーザが一覧表示されます。また、ページ情報を更新し、表示をフィルタリングできます。

更新アイコン	[Firewall] ユーザ モニタ リストを更新します。
ページ コントロール	表示されているリスト項目の現在のページ番号。左右の矢印を選択し、ログインユーザの最初、前、次、または最後のページを表示します。
[Column Settings]	テーブルの表示をカスタマイズします。カラムの表示または非表示を選択し、テーブル内のカラムの表示順序を指定できます。詳細については、34 ページの「表示されるカラムのカラム設定を使用した制御」を参照してください。
[Clear All Filters]	[Firewall] ユーザ モニタ リストに適用されているすべてのフィルタを削除します。

[De-authenticate All Users]	[Firewall] ユーザ モニタ リストに含まれる全ユーザの認証セッションを停止します。ユーザが通信セッションを再開するには、ファイアウォールの認証を再度行う必要があります。
フィルタ アイコン	指定した条件に応じてファイアウォール ユーザ モニタ リストをフィルタ処理または並べ替えるための、カラム フィルタを編集します。詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。
[User Name]	接続されているすべてのリモート ユーザのユーザ名。
[User Group]	リモート ユーザが属するユーザ グループ。
[Duration]	ユーザ認証後の経過時間。
[Time-left]	ユーザのセッションがタイムアウトするまでの、残り時間。セッションの認証時間が自動的に延長される場合のみ使用できます (authentication keepalive が有効)。authentication keepalive が有効でない場合は、[Time-left] カラムに [N/A] が表示されます。詳細については、『*FortiGate CLI リファレンス*』を参照してください。
[IP Address]	ユーザの発信元 IP アドレス。
[Traffic Volume]	ユーザから発信され FortiGate ユニットを通過するトラフィックの量。
[Method]	FortiGate ユニットによってユーザに適用される認証メソッド (認証メソッドは FSAE、ファイアウォール認証、または NTLM となります)。

IM ユーザ モニタ リスト

ユーザ リストを使用して、特定のユーザを許可またはブロックできます。各ユーザにポリシーを割り当て、IM プロトコルごとに動作を許可またはブロックできます。IM 機能を個別に許可またはブロックできることにより、管理者は、音声チャットなど帯域幅を消費しやすい機能をブロックする一方で、テキスト メッセージングなどの機能を許可するなど、きめ細かく調整できます。IM ユーザ モニタ リストには、接続中の IM ユーザに関する情報が表示されます。このリストでは、プロトコルごとに表示をフィルタ処理できます。IM ユーザがファイアウォール経由で接続すると、接続中のユーザが FortiGate ユニットによって表示されます。このリストを解析することで、どのユーザを許可またはブロックするかを選択できます。

アクティブな IM ユーザのリストを表示するには、*[User]*、*[Monitor]*、*[IM]* の順に選択します。

[IM] ページ

このページには、現在アクティブな IM ユーザが一覧表示されます。このページでは、ブロックされているユーザ、および MSN など特定の IM を使用中のユーザを確認できます。

[Protocol]	どのプロトコルを使用するユーザをリストに表示するかを、[AIM]、[ICQ]、[MSN]、または [Yahoo] から選択します。また、[All] を選択すると、現在のユーザをすべて表示できます。
#	リスト中の IM ユーザの順位番号。
[Protocol]	使用されているプロトコル。
[User Name]	IM プロトコルへの登録時にこのユーザによって選択された名前。複数の IM プロトコルに対して同じユーザ名を使用できます。ユーザ名 / プロトコルの各ペアが、リスト内で個別に表示されます。
[Source IP]	このユーザが IM セッションを開始したアドレス。
[Last Login]	現在のユーザがこのプロトコルを最後に使用した時刻。
ブロック アイコン	このユーザ名を永続的なブラック リストに追加する場合に選択します。ユーザ名 / プロトコルの各ペアが、管理者によって明示的にブロックされる必要があります。

NAC 隔離および禁止ユーザ リスト

注意 : IP アドレスをブロックするように NAC 隔離を設定しており、FortiGate ユニットで NAT デバイス経由のセッションを受信する場合は、個人ユーザだけでなくすべてのトラフィックがその NAT デバイスからブロックされます。

NAC (ネットワーク アクセス制御) 隔離を使用することで、ウイルス スキャンによりウイルスが検出される場合、または IPS センサーまたは DoS センサーにより攻撃が検出される場合に、FortiGate ユニットを通過するアクセスをブロックできます。IPS センサーのフィルタおよび上書きに合わせて、NAC 隔離を設定できます。NAC 隔離は、ウイルスまたは攻撃を送信した IP アドレスのアクセスをブロックし、また、ウイルスまたは攻撃を受けた FortiGate インタフェースに接続するすべてのトラフィックをブロックします。さらに、攻撃を送信した IP アドレスと攻撃の標的または受信者 (被害者) 間の通信をブロックするように、IPS センサーおよび DoS センサーを設定できます。NAC 隔離のブロック機能では、ブロックされたパケットは、ファイアウォール ポリシーによって許可される前に、ネットワーク層で破棄されます。

NAC 隔離では、ブロックされた IP アドレスまたはインタフェースが、禁止ユーザ リストに追加されます。禁止ユーザ リストを表示するには、*[User]*、*[Monitor]*、*[Banned User]* の順に選択します。NAC 隔離を設定するとき、IP アドレスまたはインタフェースをブロックする期間を指定できます。FortiGate 管理者は、禁止ユーザ リストから IP アドレスまたはインタフェースを削除することによって、再びアクセス可能な状態に手動で設定できます。禁止ユーザ リストから IP アドレスを削除すると、ユーザは FortiGate ユニット経由でネットワーク サービスへのアクセスを再開できます。禁止ユーザ リストからインタフェースを削除すると、そのインタフェースは通信セッションの受信機能および処理機能を通常どおりに再開できます。詳細については、467 ページの「禁止ユーザ リスト」を参照してください。

NAC 隔離および DLP

DLP (情報漏洩防止) センサーを使用する場合でも、アクセスをブロックし、ユーザを禁止ユーザ リストに加えることができます。ただし、NAC 隔離ではネットワーク層でパケットが破棄されますが、DLP ではパケットがファイアウォール ポリシーにより許可された***後に***、アプリケーション層でブロックされます。この違いにより、DLP ではどのパケットをブロックするか否かを、より細かく制御できます。たとえば、DLP センサーが SMTP 電子メール メッセージの内容を照合する場合、メール メッセージの "From:" フィールドで識別される特定の送信者からの SMTP メールをすべてブロックしながら、Web を閲覧するユーザはブロックしないように、DLP を設定できます。さらに DLP では、送信者の名前が禁止ユーザ リストに追加されます。

NAC 隔離および DLP 差し替えメッセージ

NAC 隔離、または [Action] を *[Quarantine IP address]* に設定した DLP センサーによってブロックされたユーザは、通常、TCP ポート 80 を使用して FortiGate ユニットで HTTP セッションを開始しようとします。これが行われると、FortiGate ユニットは、アクセスがブロックされたことを示すメッセージを表示する、4 つの NAC 隔離 Web ページのいずれかにユーザを接続します。これらの Web ページをカスタマイズするには、*[System]*、*[Config]*、*[Replacement Message]* の順に選択し、NAC 隔離差し替えメッセージを編集します。詳細については、163 ページの「NAC 隔離差し替えメッセージ」を参照してください。

NAC 隔離、または [Action] を *[Quarantine Interface]* に設定した DLP センサーによってインタフェースがブロックされると、TCP ポート 80 を使用してこのインタフェースから HTTP セッションを開始しようとするユーザも、FortiGate ユニットによって 4 つの NAC 隔離 Web ページのいずれかに接続されます。

DLP の *[Ban]* および *[Ban Sender]* オプションも、ブロックされたユーザにメッセージを送信します。

NAC 隔離の設定

プロテクション プロファイルのアンチウイルス プロテクション、IPS センサーおよび DoS センサーで、NAC 隔離を設定できます。

- アンチウイルス プロテクションで NAC 隔離を設定するには、*[Firewall]*、*[Protection Profile]* の順に選択します。プロテクション プロファイルを追加または編集し、*[Anti-Virus]* を設定します。*[Quarantine Virus Sender (to Banned Users List)]* をオン (Enabled) にして、*[Method]* を選択し、*[Expires]* を設定します。
- IPS センサーで NAC 隔離を設定するには、*[UTM]*、*[Intrusion Protection]*、*[IPS Sensor]* の順に選択します。IPS センサーを追加または編集します。NAC 隔離をフィルタに追加するには、*[Add Filter]* を選択し、*[Quarantine Attackers (to Banned Users List)]* をオンにして、*[Method]* を選択し、*[Expires]* を設定します。また IPS センサーで、NAC 隔離を定義済みおよびカスタムの上書きに追加することもできます。
- DoS センサーで NAC 隔離を設定するには、DoS センサーを作成または編集し、CLI を使用して、12 種類のアノマリのうち 1 つ以上のアノマリに NAC 隔離を設定します。アノマリに NAC 隔離を設定する場合、`quarantine` を `attacker` に設定すると攻撃をブロックし、`both` に設定すると攻撃および標的の双方をブロックし、または `interface` に設定すると攻撃を受信したインタフェースをブロックします。

  DoS センサーの追加は、Web ベース マネージャまたは CLI の双方から可能ですが、NAC 隔離の設定は CLI からのみ実行できます。以下の例では、`QDoS_sensor` という名前の DoS センサーを編集し、`udp_dst_session` の隔離を `attacker` に設定し、隔離の期限を 30 分に設定する方法が示されています。また、`icmp_flood` アノマリで隔離を `both` に設定する方法も示されています。

```
config ips DoS
  edit QDoS_sensor
    config anomaly
      edit udp_dst_session
        set quarantine attacker
        set quarantine-expiry 30
      next
      edit icmp_flood
        set quarantine both
      end
end
```

詳細については、『*FortiGate CLI リファレンス*』を参照してください。

禁止ユーザ リスト

禁止ユーザ (Banned User) リストには、NAC 隔離によってブロックされたすべての IP アドレスとインタフェースが表示されます。また、DLP (情報漏洩防止) によってブロックされたすべての IP アドレス、認証ユーザ、送信者、インタフェースも表示されます。システム管理者は、特定のユーザまたはインタフェースを隔離から解放するか、または指定期間が過ぎると隔離が期限切れになるように隔離を設定できます。

禁止ユーザ リスト上のユーザまたは IP アドレスによって開始されるすべてのセッションは、そのユーザまたは IP アドレスがリストから削除されるまでブロックされます。また、リスト上のインタフェースに対するすべてのセッションは、そのインタフェースがリストから削除されるまでブロックされます。

以下の条件に該当するユーザまたは IP アドレスを、禁止ユーザ リストに加えるように、NAC 隔離を設定できます。

- **IPS により検出された攻撃の発信源であるユーザまたは IP アドレス** – 攻撃の発信源であるユーザまたは IP アドレスを隔離するには、IPS Sensor Filter で *[Quarantine Attackers]* をオンにしてオプションの詳細を設定します。
- **ウイルス　スキャンにより検出されたウイルスの送信元である IP アドレスまたはインタフェース** – ウイルスの送信元である IP アドレス、またはウイルスをともなうトラフィックを受け取ったインタフェースを隔離するには、プロテクション プロファイルで *[Quarantine Virus Sender]* をオンにします。

- **DLP（情報漏洩防止）により禁止または隔離されるユーザまたはIPアドレス** – DLP センサーで各種のオプションを設定することで、ユーザまたは IP アドレスを禁止ユーザ リストに加えます。

禁止ユーザ（Banned User）リストを表示するには、*[User]*、*[Monitor]*、*[Banned User]* の順に選択します。

[Banned User] ページ

このページには、すべての禁止ユーザが表示されます。

ページ コントロール	表示されているリスト項目の現在のページ番号。左右の矢印を選択し、禁止されているユーザまたは IP アドレスの最初、前、次、または最後のページを表示します。
全エントリ削除アイコン	禁止ユーザリストから、すべてのユーザおよび IP アドレスを削除します。
#	リスト中のユーザまたは IP アドレスの順位番号。
[Application Protocol]	禁止ユーザリストに追加されたユーザまたは IP アドレスが使用していたプロトコル。
[Cause or rule]	ユーザまたは IP アドレスを禁止ユーザ リストに追加した FortiGate ユニットの機能。*[Cause or rule]* には、[IPS]、[Antivirus]、または [Data Leak Prevention] が表示されます。
[Created]	ユーザまたは IP アドレスが禁止ユーザ リストに追加された日時。
[Expires]	ユーザまたは IP アドレスが禁止ユーザ リストから自動的に削除される日時。*[Expires]* に *[Indefinite]* が表示される場合は、ユーザまたはホストをリストから手動で削除する必要があります。
削除アイコン	選択したユーザまたは IP アドレスを禁止ユーザ リストから削除します。

エンドポイント

エンドポイント NAC を利用する場合、ネットワーク上で FortiClient End Point Security（エンタープライズ エディション）アプリケーションを使用することが必須条件となります。エンドポイント NAC により、エンドポイントにインストールされているアプリケーションに応じて、エンドポイントからネットワークへのアクセスを許可または拒否できます。

FortiClient にはユーザのコンプライアンス遵守を促す機能が含まれており、エンドポイントで実行中の FortiClient アプリケーションは最新バージョンか、アンチウイルス シグネチャは最新版か、およびファイアウォールは有効かがチェックされます。エンドポイントとして最も一般的なのは、単体の PC です。この PC には、FortiGate ユニット経由でネットワーク サービスにアクセスするための単一 IP アドレスが割り当てられます。

エンドポイント NAC を有効に設定するには、ファイアウォール ポリシーを使用します。トラフィックがファイアウォール ポリシーを通過するとき、発信元インタフェース上の発信源であるホストで FortiGate ユニットによるコンプライアンス チェック（FortiClient 導入状況のチェック）が実行されます。コンプライアンス不遵守のエンドポイントは、ブロックされます。そのようなエンドポイントは、Web を閲覧しようとすると、コンプライアンス不遵守の説明および FortiClient アプリケーション インストーラのダウンロード先リンクを表示する、Web ポータルにリダイレクトされます。

エンドポイント NAC をネットワークに導入しやすいように、FortiGate ユニットではオプションで、不遵守ユーザに FortiClient ソフトウェアのインストールを推奨しながらも、ユーザが FortiClient ソフトウェアをインストールせずにネットワークにアクセスすることを許容できます。

エンドポイント NAC の対象となるエンドポイントを監視するために、コンピュータ、コンピュータのオペレーティング システム、検出されたアプリケーションの情報を表示できます。

この項には、以下のトピックが含まれています。

注記：負荷分散 VIP をともなうファイアウォール ポリシーでエンドポイント NAC を有効に設定しても、エンドポイント NAC は機能しません。

エンドポイント NAC 設定の概要

エンドポイント NAC を活用するには、ファイアウォール ポリシーを使用するすべてのホストに FortiClient Endpoint Security アプリケーションがインストールされている必要があります。このポリシーの適用対象となるすべてのホストに、このアプリケーションをインストールできることを確認してください。現在、FortiClient Endpoint Security は、Microsoft Windows 2000 以降バージョンのみを対象に提供されています。

エンドポイント NAC をセットアップするには、以下を設定する必要があります。

- FortiGuard サービスを使用して FortiClient アプリケーションまたはアンチウイルス シグネチャを更新するには、FortiGuard Analysis & Management Service で Central Management（集中管理）機能を有効にします。アカウント情報を入力する必要はありません。詳しくは、183 ページの「集中管理」を参照してください。
- コンプライアンス不遵守のエンドポイントを対象に、FortiClient の必須バージョンおよび FortiClient インストーラのダウンロード先を設定します。詳しくは、473 ページの「FortiClient インストーラ ダウンロードおよび必須バージョンの設定」を参照してください。

- アプリケーション検出リストを定義し、どのアプリケーションを許可するか否かを指定します。オプションで、検出リストにないアプリケーションをインストールしているエンドポイントへのアクセスを拒否できます。詳しくは、471 ページの「Configuring アプリケーション センサーの設定」を参照してください。
- エンドポイント NAC プロファイルを作成し、FortiClient の不遵守ユーザへの対応および使用するアプリケーション検出リストを設定できます。ファイアウォール ポリシーでエンドポイント NAC を有効にするとき、使用するエンドポイント NAC プロファイルを選択します。
- ファイアウォール ポリシーで、エンドポイント NAC を有効に設定します。

注記: *[User]*、*[Options]*、*[Authentication]* の順に選択したとき、*[Redirect HTTP Challenge to a Secure Channel (HTTPS)]* が有効に設定されている場合、ファイアウォール ポリシーでエンドポイント NAC を有効にできません。

- オプションで、エンドポイントが活動停止している状態のタイムアウトを編集できます。デフォルトの値は、5 分です。この期間が過ぎると、FortiGate ユニットはエンドポイント NAC の遵守要件をエンドポイントで再度チェックします。タイムアウト値を変更するには、`config endpoint-control settings` CLI コマンドで、`compliance-timeout` の値を調整します。

また、*Endpoint Download Portal* および *Endpoint Recommendation Portal* の表示内容を編集できます。これらは差し替えメッセージです。詳細については、162 ページの「エンドポイント NAC 差し替えメッセージ」を参照してください。

NAC メニュー

[NAC] メニューでは、プロファイル、アプリケーション センサ、データベース、およびネットワークの監視などを設定できます。

このトピックには、以下の項目が含まれています。

エンドポイント プロファイルの設定

エンドポイント NAC プロファイルには、FortiClient コンプライアンス遵守チェックの設定、およびアプリケーション検出リストを指定する設定が含まれています。ファイアウォール ポリシーにより、エンドポイント NAC プロファイルを、ポリシー適用対象のトラフィックに使用できます。

エンドポイント NAC プロファイルを作成するには、*[Endpoint]*、*[NAC]*、*[Profile]* の順に選択し、*[Create New]* を選択します。

[Profile] ページ

このページには、作成済みのエンドポイント NAC プロファイルが一覧表示されます。このページでは、プロファイルを編集、削除、または新規作成できます。

[Create New]	新しいエンドポイント NAC プロファイルを作成するとき選択します。
編集アイコン	エンドポイント NAC プロファイルの設定を編集するとき選択します。
削除アイコン	リストからエンドポイント NAC プロファイルを削除する場合に選択します。
[Name]	エンドポイント NAC プロファイルの名前。
[Action]	FortiGate ユニットによって実行されるアクションの種類。
[Additional Client Options]	緑のチェック マーク アイコンは、オプションが有効であることを示します。 灰色の X アイコンは、オプションが有効でないことを示します。

[Application Detection List]	このプロファイルで指定されるアプリケーション検出リスト。

[New Endpoint NAC Profile] ページ

このページでは、エンドポイント NAC プロファイルを設定できます。既存のエンドポイント NAC プロファイルを編集する場合は、画面が [Edit Endpoint NAC Profile] ページに自動的に移動します。

[Name]	エンドポイント NAC プロファイルの名前を入力します。
[Endpoint NAC checks for ・	コンプライアンス不遵守のホストがあるとき、FortiGate ユニットが実行するアクションを選択します。
[Notify Hosts to Install FortiClient (Warn only)]	ユーザは FortiClient Endpoint Security をインストールせずに、引き続きブラウジングを実行できます。
[Quarantine Hosts to User Portal (Enforce compliance)]	ユーザが FortiClient Endpoint Security をインストールするまで、エンドポイントを隔離されたままにします。
[Endpoint NAC can also ・	エンドポイント NAC により以下のいずれかを強制的に設定することを可能にします。
[Additional Client Options]	このチェック ボックスをオンにして、設定可能なオプションを有効にします。デフォルトでは各オプションが灰色に表示されており、[Additional Client Options] チェック ボックスをオンにすることでこれらが選択可能になります。
[Antivirus Enabled]	アンチウイルス機能が有効に設定されている必要があります。
[Antivirus Up-to-Date]	アンチウイルス シグネチャが最新版に更新されている必要があります。
[Firewall Enabled]	ファイアウォール機能が有効に設定されている必要があります。
[Enable Application Detection]	このオプションをオンにすると、エンドポイントにインストールされているアプリケーションを、アプリケーション検出リストと比較チェックします。
[Application Detection List]	使用するアプリケーション センサーを選択します。デフォルトでは灰色に表示されており、[Enable Application Detection] をオンにすると選択可能になります。

Configuring アプリケーション センサーの設定

アプリケーション センサーによって、どのアプリケーションがネットワーク エンドポイントで許可されるか否かを決めることができます。アプリケーション センサーは、ファイアウォール ポリシーで適用可能なエンドポイント NAC プロファイルの一部でもあります。複数のセンサーを作成できます。

アプリケーション センサーは、FortiGuard サービスにより提供されるアプリケーション シグネチャに基づきます。アプリケーション検出リストのエントリを作成するには、FortiGuard から提供されるカテゴリ、ベンダ、アプリケーション名のリストからアプリケーションを選択します。FortiGuard サービスによるアプリケーション情報を表示するには、*[Endpoint]*、*[NAC]*、*[Application Database]* の順に選択します。

アプリケーション センサーは、アプリケーションをデータベースと比較して、一致が検出されるまで上から順に照合し続けます。ある単一のアプリケーションをリストに含むような特別なエントリは、特定カテゴリのすべてのアプリケーションと一致するような、より一般的なエントリに先行する必要があります。

アプリケーション センサーを作成するには、*[Endpoint]*、*[NAC]*、*[Application Sensor]* の順に選択し、*[Create New]* を選択します。

[Application Sensor] ページ

このページには、作成済みのセンサーが一覧表示されます。このページでは、センサーを編集、削除、または新規作成できます。

[Create New]	[Create New] を選択すると、画面が [New Detection List] ページに自動的に移動します。[Application Sensor Settings] ページの設定を続けるには、必ず名前を入力します。
編集アイコン	アプリケーション センサーの設定を変更するとき選択します。
削除アイコン	リストからアプリケーション センサーを削除するとき選択します。
[Name]	アプリケーション センサーの名前。

[# of Entries]	リストに含まれるアプリケーション エントリの数。
[Profiles]	このアプリケーション検出リストを使用する、エンドポイント NAC プロファイル。
[Comments]	アプリケーション センサーの説明 (入力されている場合)。

[Application Sensor Settings] ページ

このページでは、アプリケーションを含むセンサを設定できます。

[Name]	アプリケーション センサーの名前を入力します。
[Comments]	アプリケーション センサーの説明を入力します (入力はオプションです)。
[Other Applications (not specified below)]	このリストにないアプリケーションがエンドポイントにインストールされている場合の対応を、以下から選択します。 · **Allow** – エンドポイントの接続を許可します。 · **Deny** – エンドポイントを隔離します。 · **Monitor** – このエンドポイントの情報を、統計およびログに加えます。
[OK]	選択すると、[Application Sensor configuration settings] ページに加えた変更を保存します。
[Create New]	[Application Sensor configuration settings] ページに加えられる新しいアプリケーション センサーを作成するとき選択します。
[Category]	ドロップダウン リストから、カテゴリを選択します。
[Vendor]	ドロップダウン リストから、ベンダを選択します。ベンダは、アプリケーション ソフトウェアの開発元です。たとえば、Adobe を選択すると、Adobe Systems Incorporated がそのベンダです。
[Application]	ドロップダウン リストから、アプリケーションを選択します。
[Status]	アプリケーションの状態として、インストール済みか、インストールされていないか、実行中か、実行中でないかを選択します。
[Action]	FortiGate ユニットが実行するアクションを選択します。
[ID]	リスト中のセンサーの識別番号。この番号によって、リスト中でのセンサーの位置付けを識別します。
[Category]	このアプリケーションに指定されるカテゴリ。
[Vendor]	このアプリケーションに指定されるベンダ。
[Application]	アプリケーションの名前。
[Status]	FortiGate ユニットが実行するアクション。
編集アイコン	アプリケーションの設定を変更する場合に選択します。
削除アイコン	ページのリストからアプリケーションを削除するとき選択します。
挿入アイコン	ページのリストに新しいアプリケーションを挿入するとき選択します。
移動アイコン	リスト中で別のアプリケーションの上または下にアプリケーションを移動するとき選択します。

アプリケーションデータベースの表示

FortiGuard サービスによって提供されるアプリケーション リストを表示できます。リストを表示するには、*[Endpoint]*、*[NAC]*、*[Application Database]* の順に選択します。

[Application Database] ページ

このページには、FortiGuard サービスによって提供されるアプリケーションが一覧表示されます。

ページ コントロール	リストの現在のページ番号が表示されます。左右の矢印を選択し、既知のエンドポイントの最初、前、次、または最後のページを表示します。
[Total Signatures:〈 数字 〉]	現在あるシグネチャの総数を表示します。
[Column Settings]	このリスト内で表示するカラムを選択します。カラムを表示する順番も指定できます。詳細については、34 ページの「表示されるカラムのカラム設定を使用した制御」および 35 ページの「」を参照してください。
[Clear All Filters]	カラムに適用されている表示フィルタをすべて解除します。

フィルタ アイコン	指定条件に応じてエンドポイント リストの表示をフィルタ処理または並べ替えるように、カラム フィルタを編集します。たとえば、BitTorrent ソフトウェアを実行しているすべてのエンドポイントを表示するように、[Detected Software] カラムにフィルタを追加できます。詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。
[Category]	アプリケーションに関連付けられるカテゴリ。
[Name]	アプリケーションの名前。
[Vendor]	アプリケーションに関連付けられるベンダ。たとえば、Adobe Reader に関連付けられるベンダは、Adobe Systems Incorporated です。

FortiClient インストーラ ダウンロードおよび必須バージョンの設定

エンドポイントでの実行が義務づけられる FortiClient の必須バージョン、および FortiClient インストーラのダウンロード先を設定するには、*[Endpoint]*、*[NAC]*、*[FortiClient]* の順に選択します。

[FortiClient Endpoint Security] ページ

このページでは、FortiClient のインストールを設定および管理できます。

[Information] セクション

このセクションには、FortiGuard の利用可能、さらにアンチウイルスおよびアプリケーション シグネチャ パッケージの現行バージョンが示されます。また、アンチウイルスおよびアプリケーション シグネチャ パッケージの更新、および Windows Installer のダウンロードが可能です。

[FortiGuard Availability]	インジケータが緑の場合、FortiGuard サービスを利用できます。
[FortiClient Endpoint Versions]	FortiGuard サービスから提供される FortiClient ソフトウェアのバージョンが表示されます。インストーラをダウンロードするには、*[Download]* リンクを選択します。
[AV Signature Package]	FortiGuard サービスから提供される最新の AV シグネチャ パッケージ。
[Application Signature Package]	FortiGuard サービスから提供される、最新のアプリケーション シグネチャ パッケージ。
[FortiClient Downloads]	このFortiGateユニットによってダウンロードされたFortiClientソフトウェアの数。
[Update Now]	FortiGuard サービスから最新の情報を取得します。

[FortiClient Installer Download Location] セクション

以下のオプションのいずれかを選択し、FortiClient ダウンロード ポータルからコンプライアンス不遵守ユーザに提供される、FortiClient インストーラをダウンロードするためのリンクを指定します。

[FortiGuard Distribution Network]	FortiClient アプリケーションは、FortiGuard Distribution Network によって提供されます。FortiGate ユニットから FortiGuard Distribution Network にアクセス可能であることが必要となります。詳しくは、205 ページの「FortiGate ユニットでの FDN および FortiGuard サブスクリプション サービスの設定」を参照してください。 FortiGate ユニットにハード ディスク ドライブが含まれる場合は、FortiGuard サービスからのファイルがキャッシュされ、多数のエンドポイントにダウンロード データを効率的に提供できます。
[This FortiGate]	ユーザは、FortiClient インストーラをこの FortiGate ユニットからダウンロードします。 このオプションは、FortiClient インストーラ ファイルのアップロードをサポートする FortiGate モデルに限り利用できます。`execute restore forticlient`CLIコマンドを使用して、FortiClientインストーラ ファイルをアップロードします詳細については、『*FortiGate CLI リファレンス*』を参照してください。

[Custom URL]	FortiClient インストーラのダウンロード先となる URL を指定します。このオプションを使用することで、FortiGate ユニットにカスタム インストーラ ファイル保存用のストレージ空間がない場合でも、そのようなインストーラ ファイルを提供できます。
[Enforce Minimum Version]	エンドポイントで使用される FortiClient 必須バージョンとして、リストから *[Latest Available]* を選択するか、または特定の FortiClient バージョンを指定します。 リストには、選択された *[FortiClient Installer Download Location]* から提供される FortiClient のバージョンが含まれています。 フォーティネットが FortiClient バージョンのアップデート方法として推奨するのは、管理者がアップデートをユーザに展開する、あるいは管理者がユーザに、アップデートをインストールし必須バージョンから最新バージョンへのアップデート前にアップデートのインストールを一定期間待つよう指示することです。

注記： カスタムの FortiClient アプリケーションを提供する場合は、*[This FortiGate]* または *[Custom URL]* を選択します。FortiManager ユニットによって FortiClient アプリケーションが集中的に管理される場合、この設定が必要となります。FortiClient アプリケーションのカスタマイズについては、『*FortiClient 管理ガイド*』を参照してください。

ネットワーク脆弱性スキャン

[Network Scan] メニューを使用することで、ネットワークのスキャンを設定できます。この機能は、これまで FortiAnalyzer または FortiScan にのみ含まれていました。

このトピックには、以下の項目が含まれています。

アセットの設定

[the Network Vulnerability Scan] メニューでは、複数のアセットを設定できます。

アセットを作成するには、*[Endpoint]*、*[Network Vulnerability Scan]*、*[Asset]* の順に選択し、[Create New] を選択します。

[Asset] ページ

このページには、作成済みのアセットが一覧表示されます。このページでは、アセットを編集、削除、または新規作成できます。

[Create New]	新しいアセットを作成するとき選択します。
編集アイコン	アセットを編集するとき選択します。
削除アイコン	このページでリストからアセットを削除するとき選択します。
[Name]	アセットの名前。
[IP Address/Range]	アセットの種類に [Host] が選択されている場合は、ホストの IP アドレスが表示されます。アセットの種類に [Range] が選択されている場合は、IP アドレス範囲が表示されます。
[Enable Scan]	アセットのスキャンが有効かどうかを表示します。
[Last Discovery]	アセットによる最後の発見。

[Asset Settings] ページ

このページでは、アセットを設定できます。

[Name]	作成するアセットの名前を入力します。
[Type]	ホストの IP アドレスを設定するには、[Host] を選択します。IP アドレス範囲を設定するには、[Range] を選択します。
[IP Address]	ホストの IP アドレスまたは IP アドレス範囲を、[Type] の設定に応じて入力します。
[Scan Type]	スキャンにアセットのみを使用する場合は、[Asset Discovery Only] を選択します。さまざまな脆弱性をスキャンする場合は、[Vulnerability Scan] を選択します。

[Windows Authentication]	Windows オペレーティング システム上で認証を使用する場合に選択します。ユーザ名およびパスワードを、フィールドに入力します。フィールドは、[Windows Authentication] を選択すると表示されます。
[Unix Authentication]	UNIX オペレーティング システム上で認証を使用する場合に選択します。ユーザ名およびパスワードを、フィールドに入力します。フィールドは、[Unix Authentication] を選択すると表示されます。

スキャンの設定

ネットワーク スキャンを監視のために設定できます。スキャンを作成するには、*[Endpoint]*、*[Network Vulnerability Scan]*、*[Scan]* の順に選択します。

[Network Scan] ページ

このページでは、スキャンのスケジュール、および FortiGate ユニットで実行するスキャンの種類を設定できます。

[Scan Mode]	FortiGate ユニットによって脆弱性スキャンに使用されるモードを選択します。 [Quick]・最小限のスキャンを実行します。 [Standard] – [Full]・完全なスキャンを実行します。
[Schedule]	脆弱性スキャン開始、終了のスケジュールを選択します。 [Manually]・スケジュールのオプションを設定します。 [Schedule]・デフォルトのスケジュールを使用します。
[Recurrence]	スケジュールを、毎日、毎週、または毎月の周期から選択します。[Weekly] を選択すると、[Day of Week] ドロップダウン リストが表示されます。[Monthly] を選択すると、[Day of Month] ドロップダウン リストが表示されます。
[Time]	スキャン スケジュールの開始時刻を、HH:MM (時、分) の形式で選択します。
[Day of Week]	毎週スキャンを行うスケジュールの場合、ドロップダウン リストから曜日を選択します。
[Day of Month]	毎月スキャンを行うスケジュールの場合、ドロップダウン リストから月の日付を選択します。

エンドポイントの監視

既知のエンドポイントを表示するには、*[Endpoint]*、*[Monitor]*、*[Endpoint Monitor]* の順に選択します。エンドポイントは、*[Endpoint NAC]* が有効に設定されたファイウォール ポリシーをそのエンドポイントが使用するとき、リストに加えられます。

エンドポイントがリストに追加されると、それを手動で削除するか、または FortiGate ユニットを再起動するまで、そのエンドポイントはリストに加えられたままとなります。エンドポイントから FortiGate ユニット経由でネットワーク サービスにアクセス (が試行) されるたびに、エンドポイントのエントリが更新されます。

エンドポイント リストは、ネットワーク上にあるエンドポイントのインベントリの役割を果たします。FortiClient アプリケーションを実行していないエンドポイントのエントリには、IP アドレス、前回のアップデート時刻、トラフィックの量 / 接続試行回数が含まれます。塔 R ンプライアンス不遵守・のステータスは、エンドポイントが FortiClient アプリケーションを実行していないことを示します。

FortiClient アプリケーションを実行しているエンドポイントのエントリでは、FortiClient アプリケーションでどのような情報を収集可能かに応じて、より多くの情報が示されます。表示される詳細情報には、エンドポイント ハードウェア (CPU およびモデル名) およびエンドポイントで実行されるソフトウェアなどが含まれます。表示カラムの設定および表示フィルタを調整することで、これらの情報をさまざまな形式で表示できます。

エンドポイント リストでは、各エンドポイントに関する情報を表示し、エンドポイントをエンドポイント NAC から一時的に除外し、さらに除外されたエンドポイントを再度ブロックするように設定できます。

[Endpoint Monitor] ページ

このページには、FortiGate ユニットにより監視中のエンドポイントが一覧表示されます。

更新アイコン	リストを更新します。
[View]	コンプライアンスを遵守している *[Compliant]* エンドポイント、遵守していない *[Non-compliant]* エンドポイント、または *[Both]*（両方）のエンドポイントを表示します。遵守エンドポイントは、必須バージョン以降の FortiClient を実行しています。FortiClient の必須バージョンを設定する方法については、473 ページの「FortiClient インストーラ ダウンロードおよび必須バージョンの設定」を参照してください。 エンドポイントがコンプライアンス不遵守の場合は、[Status] カラムに灰色アイコン、遵守の場合は緑アイコンが表示されます。不遵守のエンドポイントが一時的に除外されている場合は、[Status] カラムに砂時計付きの緑アイコンが表示されます。
ページ コントロール	リストの現在のページ番号が表示されます。左右の矢印を選択し、既知のエンドポイントの最初、前、次、または最後のページを表示します。
[Column Settings]	このリスト内で表示するカラムを選択します。カラムの表示順序も指定できます。詳細については、34 ページの「表示されるカラムのカラム設定を使用した制御」および 35 ページの「」を参照してください。
[Clear All Filters]	カラムに適用されている表示フィルタをすべて解除します。
フィルタ アイコン	指定条件に応じてエンドポイント リストの表示をフィルタ処理または並べ替えるように、カラム フィルタを編集します。たとえば、BitTorrent ソフトウェアを実行しているすべてのエンドポイントを表示するように、[Detected Software] カラムにフィルタを追加できます。詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。
表示アイコン	選択したエンドポイントの詳細を表示します。このアイコンを選択すると、FortiClient アプリケーションによって検出されたエンドポイントについての情報が表示されます。
一時除外アイコン	選択したエンドポイントを、エンドポイント NAC から除外します。この場合、ブロックされエンドポイント リストに加えられたエンドポイントが、FortiGateユニット経由でネットワーク サービスに一時的にアクセスできます。このアイコンを選択すると、そのエンドポイントをエンドポイント NAC から除外する期間を指定できます。デフォルトの除外期間は 600 秒です。
ブロック状態回復アイコン	一時的にエンドポイント NAC を除外されたエンドポイントのアクセス ブロックを回復します。
[Column Settings]	*[Column Settings]* を選択して、以下のどのカラムを表示するかを指定します。カラムに表示されるすべての情報は、特別な注がない限り、エンドポイント上で実行する FortiClient アプリケーションによって報告される情報です。
[AV signature]	エンドポイントにインストールされている FortiClient アンチウイルス シグネチャのバージョン。
[Computer Manufacturer]	エンドポイントのメーカー名。
[Computer Model]	エンドポイントのモデル名。
[CPU Model]	エンドポイントで実行している CPU。
[Compliant]	コンプライアンス遵守シグネチャの名前。
[Detected Applications]	このエンドポイントで検出されたソフトウェア アプリケーション。詳しくは、471 ページの「Configuring アプリケーション センサーの設定」を参照してください。 *[Detected Software]* フィルタを編集することで、[Detected Software] カラムに表示されるアプリケーションを設定できます。詳しくは、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。
[FortiClient Version]	エンドポイント上で実行している FortiClient アプリケーションのバージョン。
[Host Name]	エンドポイントのホスト名。
[Installed FCT Features]	エンドポイント上で有効な FortiClient 機能。
[IP Address]	通信セッションで検出されるエンドポイントの IP アドレス。この情報を取得する際に、FortiClient アプリケーションは必要ありません。
[Last Update]	エンドポイントのステータスが FortiGate ユニットによって最後に確認された時刻。この情報を取得する際に、FortiClient アプリケーションは必要ありません。

[Memory Size]	エンドポイントに取り付けられているメモリのサイズ。
[OS Version]	エンドポイント上で実行しているオペレーティング システムのバージョン。
[System Uptime]	エンドポイントのシステム アップタイム。
[Traffic Volume/Attempts]	エンドポイントがコンプライアンス遵守の場合、このカラムには、エンドポイントから発信された通信セッションによってFortiGateユニットを通過したデータ量が表示されます。エンドポイントがコンプライアンス不遵守の場合、このカラムには、エンドポイントからFortiGateユニットへの接続試行の回数が示されます。この情報を取得する際に、FortiClientアプリケーションは必要ありません。
[User]	エンドポイントのアクティブなユーザ アカウントの名前。

無線コントローラ

大半の FortiGate ユニットは、FortiWiFi モデルを除き、無線ネットワーク コントローラとして機能し、FortiWiFi ユニットの無線アクセス ポイント (AP) 機能を管理できます。すべてのユニットが、最新の FortiOS ファームウェアを実行する必要があります。

仮想アクセス ポイントを作成し、それらを複数の物理的なアクセス ポイントと連携させることができます。クライアントは物理的なアクセス ポイントでローミングを行い、無線ネットワークの範囲を拡大させることができます。

この項には以下のトピックが含まれています。

設定の概要

無線コントローラ機能を使用して無線ネットワークを構築するには、以下の設定が必要です。

- 無線コントローラが有効でない場合、有効に設定します。
- 無線コントローラによって管理される FortiWiFi ユニットを設定します。
- 仮想アクセス ポイント (VAP) を個別に設定します。VAP には、無線アクセス ポイント デバイスにあるような、SSID およびセキュリティ設定が含まれています。またオプションで、この VAP を同時に使用できる無線クライアントの数を制限できます。
- 物理的なアクセス ポイント (AP) を個別に設定します。AP 設定には、無線の設定および不正 AP をスキャンする設定が含まれています。物理的なアクセス ポイントで運用される VAP を選択します。オプションで、この AP で許容される同時クライアントの数を制限できます。
- 無線クライアントにアドレスを提供する DHCP サービスを設定します。
- 無線 LAN と他のネットワーク間の通信を可能にするように、ファイアウォール ポリシーを設定します。

無線コントローラの有効化

一部の FortiGate モデルでは、無線コントローラの機能はデフォルトで隠されています。

無線コントローラを有効にするには

1 *[System]*、*[Admin]*、*[Settings]* の順に選択します。
2 *[Enable Wireless Controller]* を選択します。
3 *[Apply]* を選択します。

無線コントローラ機能を無効にすると、関連する設定がすべて破棄されます。

マネージド アクセス ポイントとしての FortiWiFi ユニットの設定

FortiWiFi ユニットが物理的なマネージド アクセス ポイントとして機能するように、ユニットごとに設定する必要があります。この設定は、各ユニットで CLI から以下のように行います。

```
config system global
  set wireless-terminal enable
end
```

FortiWiFi ユニットの無線機能は、無線端末モードではユニット自体から制御できません。

無線コントローラの FortiGate ユニットとマネージド アクセス ポイントの FortiWiFi ユニットの間にファイアウォール デバイスがある場合は、ポート 5246 およびポート 5247 がオープンであることを確認してください。これらのポートはそれぞれ、暗号化された制御チャネル データ、および無線ネットワーク データの伝送に使用されます。必要に応じて、これらのポートを CLI から変更できます。

```
config system global
  set wireless-controller-port <port_int> (ÉAÉNÉZÉX ÉRÉìÉgÉçÅ[Éâ)
  set wireless-controller-port <port_int> (ÉAÉNÉZÉX É|ÉCÉìÉg)
end
```

これらのコマンドにより、制御チャネル ポートを設定できます。データ チャネル ポートは、制御ポートより必ず 1 多い数値になります。ポート設定は、アクセス コントローラおよびすべてのアクセス ポイントで一致する必要があります。

仮想無線アクセス ポイントの設定

仮想アクセスポイント (VAP) では、無線 LAN の SSID およびセキュリティ設定が定義されます。FortiGate ユニットでは、VAP ごとに、仮想ネットワーク インタフェースが作成されます。VAP インタフェースと他のネットワーク間のトラフィックを制御するように、ファイアウォール ポリシーを作成します。ユーザは、アクセス ポイントに接続するための正しいセキュリティ設定を必要とし、さらにファイアウォール ポリシーを使用する際に認証が要求される場合があります。

VAP を作成するには、*[Wireless Controller]*、*[Virtual AP]*、*[Virtual AP]* の順に選択し、さらに *[Create New]*、*[OK]* の順に選択します。

[Virtual AP] ページ

このページには、作成済みの仮想 AP が一覧表示されます。このページでは、仮想 AP を編集、削除、または新規作成できます。

[Create New]	[Create New] を選択すると、画面が [New Virtual AP] ページに自動的に移動します。
編集アイコン	仮想 AP の設定を編集するとき選択します。
削除アイコン	リストから仮想 AP を削除するとき選択します。
[Name]	仮想 AP の名前。
[SSID]	無線インタフェースの SSID またはネットワーク名。
[SSID Broadcast]	クライアントが無線ネットワークに接続するために使用する SSID ブロードキャスト。
[Security mode]	無線インタフェースのセキュリティの種類。
[Data Encryption]	無線インタフェースの暗号化の種類。
[Authentication]	クライアントが使用する認証の種類。
[Clients]	同時接続が許容されるクライアント数の上限。

[New Virtual AP] ページ

このページでは、仮想 AP を設定し、無線 LAN の SSID およびセキュリティ設定を定義できます。

[Name]	VAP を識別する名前を入力します。これは、ファイアウォール ポリシーで使用する仮想ネットワーク インタフェースの名前でもあります。

[SSID]	この無線インタフェースの無線 SSID (service set identifier) またはネットワーク名を入力します。無線ネットワークを使用するユーザは、このネットワーク名に基づいて各自のコンピュータを設定する必要があります。
[SSID Broadcast]	SSID をブロードキャストする場合にオンにします。SSID のブロードキャストにより、クライアントはあらかじめ SSID について知ることなく無線ネットワークに接続できます。セキュリティを万全にするには、SSID のブロードキャストを行わないでください。
[Security Mode]	無線インタフェースのセキュリティ モードを選択します。無線ユーザは、この無線インタフェースに接続できるように、必ず同じセキュリティ モードを使用します。 **None** – セキュリティはありません。無線ユーザは、誰でも無線ネットワークに接続できます。 **WEP64** – 64 ビット WEP (Web Equivalent Privacy)。WEP64 を使用するには、10 桁の 16 進数 (0 ～ 9、a ～ f) のキーを入力し、無線ユーザにこのキーを通知する必要があります。 **WEP128** – 128 ビット WEP。WEP128 を使用するには、26 桁の 16 進数 (0 ～ 9、a ～ f) のキーを入力し、無線ユーザにこのキーを通知する必要があります。 **WPA** – WPA (Wi-Fi protected access) セキュリティ。WPA を使用するには、データ暗号化の手法を選択する必要があります。また、8 文字以上の PSK (pre-shared key) を入力するか、または RADIUS サーバを選択する必要があります。RADIUS サーバを選択する場合は、無線クライアントに RADIUS サーバのアカウントが必要です。 **WPA2** – セキュリティ機能を強化した WPA。WPA2 を使用するには、データ暗号化の手法を選択し、8 文字以上の PSK (事前共有キー) を入力するか、または RADIUS サーバを選択する必要があります。RADIUS サーバを選択する場合は、無線クライアントに RADIUS サーバのアカウントが必要です。 **WPA2 Auto** – WPA2 と同じセキュリティ機能を持ちながら、WPA セキュリティを使用する無線クライアントも許可します。WPA2 Auto を使用するには、データ暗号化の手法を選択し、8 文字以上の PSK (pre-shared key) を入力するか、または RADIUS サーバを選択する必要があります。RADIUS サーバを選択する場合は、無線クライアントに RADIUS サーバのアカウントが必要です。
[Data Encryption]	無線クライアントの機能仕様に応じて、*[TKIP]* または *[AES]* の暗号化を選択します。このオプションは、WPA セキュリティ モードで使用できます。
[Key Index]	多くの無線クライアントは、最大 4 つの WEP キーを設定できます。クライアントがこのアクセス ポイントで必ず使用するキーを選択します。このオプションは、*[Security Mode]* で WEP を選択したとき利用できます。
[Key]	クライアントによって必ず使用される暗号化キーを入力します。このオプションは、WEP *[Security Mode]* を選択したとき利用できます。
[Authentication]	次のいずれかを選択します。 **[Pre-shared key]** – クライアントによって必ず使用される PSK (事前共有キー) を入力します。 **[RADIUS Server]** – クライアントの認証を行う RADIUS サーバを選択します。 これらの設定は、*[Security Mode]* で WEP を選択したとき利用できます。
[Maximum Clients]	同時接続が許容されるクライアント数の上限を入力します。 制限しない場合は、0 (ゼロ) を入力します。

物理アクセス ポイントの設定

物理的なアクセス ポイントの役割を果たし無線 LAN のおよび無線設定が可能な FortiWiFi ユニットを識別できるように、アクセス コントローラを設定する必要があります。

物理的なアクセス ポイントを設定するには、*[Wireless Controller]*、*[Physical AP]*、*[Managed Physical AP]* の順に選択し、*[Create New]* を選択して、必要な情報を入力し、*[OK]* を選択します。

[Managed Physical AP] ページ

このページには、作成済みの物理 AP が一覧表示されます。このページでは、物理 AP を編集、削除、または新規作成できます。

[Create New]	[Create New] を選択すると、画面が [New Managed Access Point] ページに自動的に移動します。
編集アイコン	物理的なマネージド AP の設定を編集するとき選択します。
削除アイコン	リストから物理的なマネージド AP を削除するとき選択します。
更新アイコン	ページに表示されている現在の情報を更新するとき選択します。
[Admin]	仮想 AP のアクセスの種類。[Disabled] は、AP がマネージされていないことを意味します。
[Name]	物理 AP の名前。
[Virtual AP]	物理 AP で運用される仮想 AP。
[Band/Channel]	その物理 AP に使用されている周波数帯またはチャネル。
[Clients]	同時接続が許容されるクライアント数の上限。
[Rogue-AP Scan]	[Wireless Controller]、[Rogue AP]、[Rogue AP] の順に選択したとき、他の AP を検出しそれらの AP をレポートするために使用されるスキャンの種類。
[Join Time]	仮想 AP が物理 AP に接続した時刻。

[New Managed Access Point] ページ

このページでは、物理アクセス ポイントを設定できます。

[Serial Number]	FortiWiFi ユニットのシリアル番号を入力します。AP がこの AC を発見し自動登録する場合は、このフィールドは自動的に入力されます。
[Name]	物理 AP の名前を入力します。
[Admin]	次のいずれかを選択します。 **[Discovery]** – この AC を発見し自動登録する AP のための設定。このような AP を使用するには、*[Enabled]* を選択します。 **[Disabled]** – この AP をマネージしません。 **Enabled** – この AP をマネージします。
[Last Error]	この AP の最後のエラー メッセージ (メッセージがある場合)。
[Rogue AP Scan]	不正 AP スキャンは、他の AP を検出し、それらの AP をレポートします。このレポート ページを表示するには、*[Wireless Controller]*、*[Rogue AP]* の順に選択します。 次のいずれかを選択します。 **[Dedicated]** – AP はスキャン機能のみを実行し、サービスを提供しません。 **[Background]** – AP は AP として動作中のアイドル時に、スキャンを実行します。 **[Disabled]** – スキャンを実行しません。スキャンを実行すると、パフォーマンスが低下する場合があります。
[Radio]	無線周波数帯を選択します。ユーザの無線カードまたはデバイスの機能仕様に合わせて選択してください。
[Geography]	国または地域を選択します。これにより、使用可能なチャネルが決まります。
[Channel]	無線ネットワークのチャネルを選択するか、または [Auto] を選択します。選択できるチャネルは、[Geography] の設定によって異なります。
[TX Power]	送信機の出力レベルを設定します。数値が高いほど、AP のカバー領域が広くなります。
[Maximum Clients]	この物理 AP への同時接続が許容されるクライアント数の上限を入力します。制限しない場合は、0 (ゼロ) を入力します。
[Virtual AP]	*[Available]* リストから、この物理 AP で運用する仮想 AP を選択し、次に右向き矢印を選択してその仮想 AP を *[Selected]* リストに移動します。

無線 LAN の DHCP の設定

無線クライアントにIPアドレスを割り当てるようにDHCPサービスを設定するには、*[System]*、*[DHCP Server]*、*[Service]* の順に選択します。仮想アクセス ポイントが、インタフェースとしてリストに表示されます。詳しくは、134ページの「DHCPサービスの設定」を参照してください。

無線 LAN のファイアウォール ポリシーの設定

仮想アクセス ポイントのクライアントが他の無線 LAN などのネットワークと通信するためには、適切なファイアウォール ポリシーが必要です。仮想 AP には同名の仮想インタフェースがあり、そのインタフェースをファイアウォール ポリシーで発信元または宛先インタフェースとして選択できます。

無線クライアントの監視

マネージド アクセス ポイントの無線クライアントに関する情報を表示するには、*[Wireless Controller]*、*[Wireless Client]*、*[Wireless Client]* の順に選択します。

[Wireless Client] ページ

このページには、マネージド アクセス ポイントと連携している無線クライアント、およびそれらの帯域幅と信号強度が表示されます。

更新アイコン	表示される情報を更新します。
ページ コントロール	リストの現在のページ番号が表示されます。左右の矢印を選択し、既知のエンドポイントの最初、前、次、または最後のページを表示します。
[Column Settings]	このリスト内で表示するカラムを選択します。カラムの表示順序も指定できます。詳細については、34 ページの「表示されるカラムのカラム設定を使用した制御」を参照してください。
[Clear All Filters]	カラムに適用されている表示フィルタをすべて解除します。
フィルタ アイコン	指定条件に応じてエンドポイント リストの表示をフィルタ処理または並べ替えるように、カラム フィルタを編集します。たとえば、BitTorrent ソフトウェアを実行しているすべてのエンドポイントを表示するように、[Detected Software] カラムにフィルタを追加できます。詳細については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。

情報表示のカラム

実際に表示されるカラムは、*[Column Settings]* に応じてことなります。

[Association Time]	このアクセスポイントにクライアントが接続している時間。
[Bandwidth Rx]	クライアントによって使用される受信帯域幅 (Kbps 単位)
[Bandwidth Tx]	クライアントによって使用される送信帯域幅 (Kbps 単位)
[Bandwidth Tx/Rx]	*[Bandwidth Rx]* + *[Bandwidth Tx]*.
[Idle Time]	このセッションでクライアントがアイドル状態の時間総計。
[IP]	無線クライアントに割り当てられた IP アドレス。
[MAC]	無線クライアントの MAC アドレス。
[Physical AP]	クライアントが連携している物理アクセス ポイントの名前。
[Signal Strength/Noise]	信号強度とノイズ レベルから計算された信号対雑音比 (デシベル値)。
[Virtual AP]	クライアントが連携している仮想アクセス ポイントの名前。

不正 AP の監視

検出された AP に関する情報を表示するには、*[Wireless Controller]*、*[Rogue AP]* の順に選択します。このリストは、以下の各セクションに区分されます。

- 未知のアクセス ポイント

- 不正アクセス ポイント
- 許可されたアクセス ポイント

未知のアクセス ポイントは、不正または許可のいずれにも指定されずに検出されるアクセス ポイントです。

[Rogue AP] ページ

このページには、検出された AP に関するすべての情報が表示されます。情報は、Unknown Access Points (未知のアクセス ポイント)、Rogue Access Points (不正アクセス ポイント)、Accepted Access Points (許可されたアクセス ポイント) の各セクションに区分され、見やすく表示されます。

[Refresh interval]	情報を更新する間隔を設定します。*[none]* に設定すると、更新を行いません。
[Refresh]	現在表示されている情報を更新します。
[Inactive Access Points]	表示するアクティブでないアクセス ポイントを、すべて表示、表示なし、1 時間以内に検出された AP、1 日以内に検出された AP から選択します。
[Online]	緑のチェックマークは、アクセス ポイントがアクティブであることを示します。灰色の X は、アクセス ポイントがアクティブでないことを示します。
[SSID]	無線インタフェースの、無線 SSID (service set identifier) またはネットワーク名。
[MAC Address]	無線インタフェースの MAC アドレス。
[Signal Strength/Noise]	信号強度およびノイズ レベル。
[Channel]	アクセス ポイントによって使用される無線チャネル。
[Rate]	アクセス ポイントのデータ速度。
[First Seen]	FortiWifi ユニットによってアクセス ポイントが初回検出された日付および時刻。
[Last Seen]	FortiWifi ユニットによってアクセス ポイントが前回検出された日付および時刻。
許可 AP マーク アイコン	このアイコンを選択すると、このエントリを *[Accepted Access Points]* リストに移動します。
不正 AP マーク アイコン	このアイコンを選択すると、このエントリを *[Rogue Access Points]* リストに移動します。
[Forget AP]	*[Accepted Access Points]* リストまたは *[Rogue Access Points]* リストからエントリを *[Unknown Access Points]* リストに戻します。

ログおよびレポート

この項では、FortiGate のログおよびレポート機能の基礎について説明します。FortiGate ユニットのログおよびレポート機能およびその他の詳細情報については、『*FortiOS 4.0 のログおよびレポート* ガイド』を参照してください。

FortiGate には、トラフィック、システム、およびネットワーク保護機能を対象とする幅広いロギング機能が含まれています。このロギング機能では、収集される詳細なログ記録情報から、レポートを作成することもできます。レポートに基づいて過去および現在のネットワーク活動を分析することにより、セキュリティの問題を容易に特定し、ネットワークの悪用および濫用を軽減あるいは防止できます。

VDOM を有効に設定している場合の詳細については、73 ページの「バーチャル ドメインの使用」を参照してください。

この項には以下のトピックが含まれています。

注記： FortiGate ユニットがトランスペアレント モードの場合、一部機能はログをサポートしないか、あるいはトランスペアレント モードで利用できないことがあるため、一部のロギング設定およびオプションが使用できない場合があります。たとえば、SSL VPN イベントはトランスペアレント モードには対応しません。

ログおよびレポートの概要

[Log&Report] メニューには、リモートまたはローカルのロギングを設定するための項目が含まれており、このメニューから FortiGate ユニットによって記録されるあらゆる種類のログ メッセージを表示できます。

さらにこのメニューを使用し、アラート メール メッセージも設定できます。アラート メール メッセージは、所定の電子メール アドレスに送信され、管理者のログアウトまたは不正侵入の検出など、特定の活動が発生したことを受信者に知らせるメッセージです。さらにアラート メール メッセージにより、FortiGuard ライセンス失効までの残り日数の通知を受けることもできます。

[Log&Report] メニューには、レポートの設定も含まれています。レポートには、さまざまなログの情報がテキスト、グラフおよび表の形式で表示されます。このレポートによって、長大なログ メッセージを手作業で確認することなく、ネットワーク活動の概要を簡潔、明瞭に把握できます。

SQL データベースを使用しておりログ ファイルを SQL データベースに送信している場合は、SQL レポートを設定できます。SQL レポートでは、情報がウィジェットに表示されます (*[Log&Report]*、*[Report Access]*、*[Executive Summary]* の順に選択)。このウィジェットは、[Dashboard] ページに表示されるウィジェットに似ていますが、カスタマイズできません。ウィジェットには、収集されたログ情報が、棒グラフまたは円グラフの形式で表示されます。

[Log&Report] メニューからは、隔離されたファイルおよびアーカイブを表示できます。隔離ファイルの詳細を確認するには、*[Log&Report]*、*[Quarantine Files]* の順に選択し、ファイルが疑わしい理由をこの詳細情報から確認できます。また、ファイルをフィルタ処理し、[Quarantine Files] ページに表示される情報をカスタマイズできます。

アーカイブには、DLP および IPS の 2 種類があります。DLP アーカイブには、電子メールおよび IM などの DLP ログに関する情報を含むログがアーカイブされています。IPS アーカイブは、過去の IPS パケット ログです。管理者は、このアーカイブからパケットを解析し、フォレンジック分析および誤検知の検出に利用できます。アーカイブ機能は、FortiAnalyzer ユニットまたは FortiGuard Analysis and Management サービスに登録している場合、FortiGuard Analysis サーバで利用できます。

ログについて

ログは、ネットワークの悪用または誤用の兆候を把握するための有用な情報です。ログに含まれる情報を詳細に検証することによって、不正侵入およびネットワークの悪用、誤用を高い精度で特定できます。

ログは、ログ ファイルとも呼ばれます。ログ、またはログファイルには、ログ メッセージが含まれています。ログ メッセージは、*[Log&Report]*、*[Log Access]* の順に選択し、所定のタブにアクセスことで表示できます。各ログ メッセージは、ログ ヘッダおよびログ本文から構成されます。ヘッダおよび本文にはそれぞれのフィールドがあり、フィールドごとにそのログ メッセージに関連する特定情報が含まれています。

ログ ヘッダには、ログが記録された日時などの一般情報が含まれています。ログ本文には、ヘッダ情報以外のメッセージを含む情報全般が含まれています。メッセージ (メッセージ フィールドに表示される) には、ログが記録された理由が説明されています。以下に示されるログ メッセージの例では、太字がヘッダ部分です。

2009-06-22 09:24:55 devname=FGT50B3G06500085 device_id=FGT50B3G06500085 log_id=0021010001 type=traffic subtype=allowed pri=notice vd=root fwver=041000 SN=613874 duration=120 carrier_ep=N/A user=admin1 group=admingroup policyid=1 proto=6 service=80/tcp app_type=N/A status=accept src=172.16.135.25 srcname=172.16.135.25 dst=172.16.25.125 dstname=172.16.25.125 src_int="internal" dst_int="wan1" sent=825 rcvd=4451 sent_pkt=8 rcvd_pkt=6 src_port=2504 dst_port=80 vpn="N/A" tran_ip=0.0.0.0 tran_port=0 dir_disp=org tran_disp=noop

ログのタイプおよびサブタイプ

ログ メッセージには、タイプ フィールドおよびサブタイプ フィールドがあります。これらのフィールド、および log_id フィールドに表示される識別番号により、ログを容易に識別できます。タイプ フィールドでは、ログ メッセージが、9 種類あるログ タイプ (traffic ログなど) のうちどの種類かを識別できます。サブタイプ フィールドでは、そのログ タイプに下位タイプ (allowed または admin など) が含まれるかどうかを識別できます。1 つのタイプには、複数のサブタイプが包含されることも可能です。

ログのタイプおよびサブタイプの名前のように、ログ メッセージを識別するための番号があります。この番号は、log_id フィールドに 10 桁の数字で表示されます。最初の 2 桁はログのタイプを表し、次の 2 桁はログのサブタイプを表します。最後の 5 桁は、メッセージ ID です。

以下の表には、ログのタイプとサブタイプ、および各タイプとサブタイプのログ識別番号が示されています。

表 55: ログのタイプおよびサブタイプ

ログのタイプ	カテゴリ番号	サブタイプ	サブタイプ番号
traffic（トラフィック ログ）	00	allowed – ポリシーにより許可されるトラフィック violation – ポリシー違反のトラフィック その他	21 22 38
event（イベント ログ）	01	system – システム活動イベント ipsec – IPSec ネゴシエーション イベント dhcp – DHCP サービス イベント ppp – L2TP/PPTP/PPPoE サービス イベント admin – admin イベント ha – 高可用性活動イベント auth – ファイアウォール認証イベント pattern – パターン更新イベント alertemail – アラート電子メール通知 chassis – FortiGate-5000 シリーズ シャーシ イベント sslvpn-user – SSL VPN ユーザ イベント sslvpn-admin – SSL VPN 管理イベント sslvpn-session – SSL VPN セッション イベント his-performance – パフォーマンス統計 vipssl – VIP SSL イベント ldb-monitor – LDB モニタ イベント	00 01 02 03 04 05 06 07 23 29 32 33 34 43 45 46
dlp（情報漏洩防止）	09	dlp – 情報漏洩防止	54
app-crtl （アプリケーション制御ログ）	10	app-crtl-all – すべてのアプリケーション制御	59
DLP archive (DLP アーカイブ ログ)	06	HTTP – ウイルスに感染 FTP – FTP コンテンツ メタデータ SMTP – SMTP コンテンツ メタデータ POP3 – POP3 コンテンツ メタデータ IMAP – IMAP コンテンツ メタデータ	24 25 26 27 28
virus（アンチウイルス ログ）	02	infected – ウイルスに感染 filename – ブロックされたファイル名 oversize – サイズ超過ファイル	11 12 13
webfilter (Web フィルタ ログ)	03	content – コンテンツ ブロック urlfilter – URL フィルタ FortiGuard ブロック FortiGuard 許可 FortiGuard エラー ActiveX スクリプト フィルタ Cookie スクリプト フィルタ アプレット スクリプト フィルタ	14 15 16 17 18 35 36 37
ips（攻撃ログ）	04	signature – 攻撃シグネチャ anomaly – 攻撃アノマリ	19 20
emailfilter （スパム フィルタ ログ）	05	SMTP POP3 IMAP	08 09 10

ログの重大度

pri ログ フィールドにはログの優先度が含まれており、通常ログの重大度と呼ばれます。この情報から、講じるべき対策、または FortiGate の動作が不安定かどうかを判断できます。

重大度は、ログ デバイスの設定時に定義されます。FortiGate ユニットは、選択されたロギング重大度以上のすべてのメッセージをログ記録します。たとえば、[Error] が選択されている場合、ユニットは重大度が [Error]、[Critical]、[Alert]、および [Emergency] のメッセージを記録します。

表 56: ログの重大度

レベル	説明	ログのタイプ
0 – Emergency（緊急）	システムが不安定になっています。	重大度が緊急となるのは、イベント ログ、特に管理イベントのログです。
1 – Alert（警告）	早急な対策が求められます。	重大度が警告となるのは、攻撃ログのみです。
2 – Critical（重大）	機能性に影響があります。	イベント、アンチウイルス、およびメール フィルタのログ。
3 – Error（エラー）	エラー状態が存在し、機能性に影響が及んでいる可能性があります。	イベントおよびメール フィルタのログ。
4 – Warning（注意）	機能性に影響が及んでいる可能性があります。	イベントおよびアンチウイルスのログ。
5 – Notification（通知）	通常のイベントに関する情報です。	トラフィックおよび Web フィルタのログ。
6 – Information（情報）	システムの動作に関する一般情報です。	DLP アーカイブ、イベント、およびメール フィルタのログ。
6 – Debug（デバッグ）	デバッグ メッセージを表示します。	デバッグの重大度は、ほとんど使用されません。ログ重大度としては最も低く、通常は何らかのファームウェア ステータス情報を含んでおり、FortiGate ユニットが正しく機能しないとき役立ちます。デバッグ重大度をともなうログ メッセージは、FortiGate 機能の全タイプによって生成されます。

ログの例

以下の 2 つの例では、ログ メッセージの例、およびトラフィック ロギングの設定方法の例が示されています。ログ メッセージの例では、例に含まれるフィールドについて説明しています。

ログ メッセージ

この例では、イベント ログ メッセージの各フィールドについて説明します。イベント ログ メッセージは、*[Log&Report]*、*[Log Configuration]*、*[Event]* の順に選択して表示する画面から、1 つ以上のイベントを有効に設定すると記録されます。

```
2009-06-30 04:15:22 devname=devname=FGT50B3G06500085
device_id=FGT50B3G06500085 log_id=0104032120 type=event subtype=admin
pri=notice vd=root fwver=041000 user=admin ui=GUI(172.16.24.144)
name="admin" msg="Administrator admin edited the settings of
administrator admin from GUI(172.16.24.144)"
```

日付 =(2009-06-30)	イベント発生時の年月日（yyyy-mm-dd 形式）。
時刻 =(04:15:22)	イベント発生時の時、分、秒の時刻（hh:mm:ss 形式）。
devname= (FGT50B3G06500085)	FortiGate ユニットの名前。名前は、デフォルトの名前（FGT<serial_number>）または管理者が名付ける名前です。このフィールドに表示される名前は、*[System]*、*[Status]* の順に選択して表示される [System Information] ウィジェットの [Host Name] の名前です。
device_id= (FGT50B3G06500085)	FortiGate ユニットのシリアル番号。
log_id=(0104032120)	10 桁の数字。最初の 2 桁はログのタイプを表し、次の 2 桁はログのサブタイプを表します。最後の 5 桁は、メッセージ ID です。
type=(event)	イベントの発生場所であるシステムのセクション。
subtype=(admin)	ログ メッセージのサブタイプ。これは、ファイアウォール ポリシーで FortiGate 機能に適用されるポリシーを表します。

pri=(notice)	このイベントの重大度。指定可能な重大度には、6 つのレベルがあります。
vd=(root)	トラフィックがログ記録されたバーチャル ドメイン。
fwver=(041000)	ログ メッセージの記録時に実行していたファームウェア バージョン。
user=("admin")	ユーザの admin プロファイル。通常は管理ユーザです。この例では、管理者が禁止単語を変更しています。
ui=[GUI (172.16.34.144)]	このイベントが発生したインタフェース、およびそのインタフェースの IP アドレス。ui フィールドには、GUI、CLI、コンソール、および LCD が含まれます。
name=("admin")	トラフィックを生成したユーザ。
msg=("Administrator admin edited the settings of administrator admin from GUI (172.16.24.144)")	FortiGate ユニットによって記録された活動またはイベントについての説明。この例では、管理者が管理者の設定を Web ベース マネージャから編集しています。

FortiGate の全トラフィックのロギング

以下の手順に従い、すべてのトラフィックについてトラフィック ログ メッセージを記録するように、FortiGate ユニットを設定できます。この手順により、トラフィックを受信するすべての FortiGate インタフェースでトラフィック ロギングを行うことができます。ただし、トラフィック ロギングでは、FortiGate ユニットによって破棄されてしまうトラフィックについてはログ記録しない場合があります。このようなトラフィックのログ メッセージを記録するために、定義済み IPS シグネチャを含む IPS センサーを追加し、このシグネチャによって、本来 FortiGate ユニットが破棄してしまうトラフィックを検出しログ記録できます。

FortiGate ユニットによって受信される全トラフィックをログ記録するには

1 以下の CLI コマンドを入力し、管理アクセス用に設定された TCP/IP ポート以外の TCP/IP ポートによる FortiGate ユニットへの接続に失敗した接続処理のロギングを有効にします。

```
config system global
  set localdeny enable
end
```

2 以下の CLI コマンドを入力して、グローバル ヘッダのチェックを strict に設定します。

```
config system global
  set check-protocol-header strict
end
```

strict ヘッダ チェックにより、パケットのチェックサムを検証することで無効な未加工 IP パケットを検出し、さらにヘッダが現行の標準に準拠することを確認するために IP ヘッダをチェックできます。デフォルトの設定は loose で、通常この設定は大半の環境に適しています。loose ヘッダ チェックは、パフォーマンスを低下させずに、ほとんどの環境で要件を満たすことができます。

3 以下の CLI コマンドを入力して、トラフィックを受信するすべての FortiGate インタフェースのトラフィック ロギングを有効に設定します。以下のコマンドでは、ポート 1 およびポート 2 でのトラフィックのロギングが有効に設定されます。これらのコマンドを、トラフィックを受信する他の全 FortiGate ユニット インタフェースで繰り返します。

```
config system interface
  edit port1
    set log enable
next
  edit port2
    set log enable
end
```

4 以下のコマンドを使用して、他のトラフィックのロギングを有効に設定します。このオプションは、外部 syslog サーバにロギングするときに限り利用できます。RP: この文言が必要なのは、4.0 MR1 で、other-traffic オプションが syslog に加えて、fortianalyzer、fortiguard、メモリ、および、および webtrends で利用可能であるため。

```
config log syslogd filter
  set other-traffic enable
end
```

5 *[UTM]*、*[Intrusion Protection]*、*[IPS Sensor]* の順に選択し、*[Create New]* を選択して IPS センサーを追加します。

IPS センサーを編集し、*[Add Pre-defined Override]* を選択して以下の定義済み IPS シグネチャをセンサーに追加します。

- Invalid.Protocol.Header
- TCP.Bad.Flags
- TCP.Invalid.Packet.Size

各シグネチャを有効に設定し、*[Action]* を *[Block]* に設定して *[Logging]* を有効にします。

6 以下の CLI コマンドを入力して、IPS センサーを含む DoS ポリシー (CLI では interface policy と表記される) を追加します。

```
config firewall interface-policy
  edit 1
    set interface <interface_name>
    set srcaddr all
    set dstaddr all
    set service ANY
    set ips-sensor-status enable
    set ips-sensor <sensor_name>
  end
```

ここでは、<sensor_name> は上記で追加された IPS センサーの名前です。

FortiGate ユニットでのログの保存方法

どの種類のログ メッセージをどの程度の頻度で保存するかにより、ログ保存に使用するストレージの種類が決まります。たとえば、トラフィックおよびコンテンツのログをログ記録する場合、FortiAnalyzer ユニットまたは syslog サーバにログ記録するように、FortiGate ユニットを設定する必要があります。トラフィックおよびコンテンツのログは、頻繁に記録されファイルサイズも大きいために、FortiGate のシステム メモリにこれらのログを記録することはできません。

ログ メッセージを、FortiAnalyzer ユニットまたは Syslog サーバなどの 1 か所または数か所に保存することは、FortiGate のシステム メモリへの記録に比べて、ロギング要件に適する保存方法と考えられます。FortiAnalyzer ユニットを使用せずにレポートを作成する場合は、FortiGuard Analysis サーバにログ記録するように FortiGate ユニットを設定するのも、適切なログ保存方法です。

このトピックには、以下の項目が含まれています。

FortiAnalyzer ユニットへのリモート ロギング

FortiAnalyzer ユニットは、ログ収集、分析ツール、およびデータ保存機能を統合したネットワーク デバイスです。詳細なログ レポートに基づいて過去および現在のネットワーク活動を分析することにより、セキュリティの問題を容易に特定し、ネットワークの悪用や濫用を削減できます。

FortiGate ユニットには、最大 3 台までの FortiAnalyzer ユニットへログ記録を行うように設定できます。FortiGate ユニットから、3 台すべての FortiAnalyzer ユニットにログが送信され、FortiAnalyzer ユニットごとに同じ情報が保存されます。複数の FortiAnalyzer ユニットにロギングを行うことで、FortiAnalyzer ユニットの 1 台に障害が発生した場合、リアルタイムのバックアップによってデータを保護できます。複数台の FortiAnalyzer ユニットは、CLI からのみ設定できます。

FortiGate ユニットでのログ設定を完了した後、FortiGate ユニットからログを受信するように、FortiAnalyzer ユニットを設定する必要があります。完全な設定を行うために、FortiAnalyzer 管理者までご連絡ください。

[Log Settings] ページの [Remote Logging & Archiving] セクション

[FortiAnalyzer]	FortiAnalyzer の設定を有効にします。
[IP Address]	ログ記録先となる FortiAnalyzer ユニットの内部 IP アドレス。FortiAnalyzer ユニットの IP アドレスをフィールドに入力します。IP アドレスを入力すると、[Test Connectivity] を使用して FortiAnalyzer ユニットと FortiGate ユニット間の通信をテストできます。
[Test Connectivity]	2 台のユニット間の通信をテストします。[IP Address] フィールドに IP アドレスを入力するまでは、使用できません。[Test Connectivity] を選択すると、両ユニットが正しく接続されていることを確認できます。 **注記**：[Test Connectivity] では、FortiGate ユニットにハイエンドの FortiAnalyzer ユニットが必要な場合、または FortiAnalyzer ユニットで VDOM/FortiGate ユニットの台数が上限に達している場合に、警告が表示されます。
[Minimum log level]	ログが記録される最も低いログの重大度。

注記：FortiAnalyzer ユニットのロギングを設定する際に、自己生成 (self-originated) トラフィックの発信元 IP を指定できますが、この設定は CLI からのみ行うことができます。

FortiAnalyzer 設定のテスト

FortiAnalyzer の設定完了後に、FortiGate ユニットおよび FortiAnalyzer ユニット間の接続をテストし、両デバイス間の正しい通信を確認できます。テストの際に、ログ、レポート、DLP アーカイブ、隔離ファイルを送受信するための特定の設定に関する情報が、FortiGate ユニットから表示されます。

テストを行う前に、FortiAnalyzer ユニットの IP アドレスを FortiGate ユニットに学習させる必要があります。FortiAnalyzer ユニットの IP アドレスを FortiGate ユニットに学習させる前に接続テストを実行すると、不正テスト レポートが生成される原因になります。

FortiGate ユニットと FortiAnalyzer ユニット間の接続状況は、次の CLI コマンドを使用してテストできます。

```
execute log fortianalyzer test-connectivity
```

このコマンドを実行すると、接続の状況およびディスク使用量のパーセンテージが表示されます。詳細については、『*FortiGateCLI リファレンス*』を参照してください。

[FortiAnalyzer (Hostname)]	FortiAnalyzer ユニットの名前。FortiAnalyzer ユニットのデフォルトの名前は、たとえば FortiAnalyzer-400 のように、その製品名となります。
[FortiGate (Device ID)]	FortiGate ユニットのシリアル番号。
[Registration Status]	FortiGate ユニットの FortiAnalyzer ユニットへの登録状況。FortiGate ユニットが未登録の場合は、ユニットに完全な権限がない場合があります。詳細については、『*FortiAnalyzer 管理ガイド*』を参照してください。

[Connection Status]	FortiGate と FortiAnalyzer の両ユニット間の接続状況。緑のチェック マークは接続があることを示し、灰色の X は接続がないことを示します。
[Disk Space (MB)]	FortiAnalyzer ユニットでログに使用可能なディスク容量 (MB 単位)。
	[Allocated Space] 隔離ファイルおよび DLP アーカイブを含むログに割り当てられている、FortiAnalyzer ユニットのハード ドライブ容量。
	[Used Space] 使用済みの領域の量。
	[Total Space] Free 未使用の領域の量。
[Privileges]	デバイスで許可される、ログ、レポート、DLPアーカイブ、隔離ログの送信および表示。 ・ *Tx* は、FortiGate ユニットから FortiAnalyzer ユニットにログ パケットを送信する許可を示します。 ・ *Rx* は、FortiAnalyzer ユニットに保存されているレポートおよびログを FortiGate ユニットで表示する許可を示します。 チェックマークは、FortiGate ユニットが、ログ情報およびレポートの送信または表示を許可されていることを示します。X は、FortiGate ユニットが、ログ情報の送信または表示を許可されていないことを示します。

注記 : [Test Connectivity] では、FortiGate ユニットにハイエンドの FortiAnalyzer ユニットが必要な場合、または FortiAnalyzer ユニットで VDOM/FortiGate ユニットの台数が上限に達している場合に、警告が表示されます。

FortiGuard 分析および管理サービスへのリモート ロギング

フォーティネットのサポート Web サイトで FortiGuard 分析および管理サービスの登録を済ませた後、FortiGuard Analysis サーバへのロギングを設定できます。なお、サーバへのロギング機能を設定する前に、接続が正常に機能するかどうか検証することをお勧めします。

FortiGuard Analysis サーバへのリモート ロギングは、ログのアーカイブを有効に設定できる点で、FortiAnalyzer ユニットへのロギングと共通性があります。またウィジェットを使用し、ログから収集された情報を絞り込むことができます。

syslog サーバへのリモート ロギング

syslog サーバは、syslog ソフトウェアを実行するリモート コンピュータです。また syslog サーバは、ロギングの業界標準でもあります。Syslog を使用して、ネットワーク デバイスによって提供されるログ情報を収集します。syslog ソフトウェアの実行には、Linux、Unix、および Intel ベースの Windows など、ほぼあらゆるコンピュータ システムを使用できるので、syslog サーバは利便性および柔軟性を兼ね備えるロギング デバイスといえます。

syslog サーバへのロギングを設定するとき、Facility、およびログ ファイルの形式を設定する必要があり、ファイル形式は通常形式または CSV (Comma Separated Values) 形式のいずれかを設定します。CSV 形式に含まれるコンマは、通常形式のスペースに相当します。CSV ファイル形式で保存されるログは、スプレッドシート アプリケーションを使用して表示し、通常形式で保存されるログはプレーン テキスト ファイルとして保存されるので、テキスト エディタ (Notepad など) を使用して表示できます

Facility を設定すると、ログ ファイルを記録したデバイスを容易に特定できます。facility 識別子は、daemon または local7 など、さまざまな種類から選択できます。

複数の Syslog サーバを設定する場合は、CLI のみから設定できます。また、Syslog ログ メッセージの信頼性の高い配信オプションを、CLI から有効に設定できます。

FortiGate CLI から、`config log {syslog | syslog2 | syslog3} settings` コマンドの `reliable` オプションを使用して、syslog メッセージの 信頼性の高い配信を有効に設定できます。FortiGate ユニットには、ログ メッセージの信頼性の高い配信に対応するために、RFC 3195 の RAW プロファイルが実装されています。信頼性の高い syslog の場合、認証およびデータ暗号化によってログ情報が保護され、正しい順序によるログ メッセージの信頼性の高い配信が保証されます。この機能は、デフォルトで無効に設定されています。

[Log Settings] ページの [Remote Logging & Archiving] セクション

[IP/FQDN]	Syslog サーバの IP アドレスまたは完全修飾ドメイン名。たとえば、完全修飾ドメイン名であれば log.example.com などとなります。

[Port]	Syslog サーバとの通信で使用するポート番号。通常はポート 514 です。
[Minimum log level]	FortiGate ユニットは、選択されたロギング重大度以上のすべてのメッセージをログ記録します。ロギング重大度の詳細については、487 ページの「ログの重大度」を参照してください。
[Facility]	*[Facility]* は、ログ メッセージの送信元を Syslog サーバに示します。デフォルトでは、local7 の Facility が FortiGate からレポートされます。*[Facility]* を変更して、異なる FortiGate ユニットからのログ メッセージを区別できます。
[Enable CSV Format]	CSV 形式を有効にすると、FortiGate ユニットは CSV (Comma Separated Value) 形式でログを生成します。CSV 形式を有効にしない場合、FortiGate ユニットはプレーン テキスト ファイルを生成します。

注記： Syslog サーバが複数設定されている場合は、[Log Settings] ページに Syslog サーバとそれらの設定が表示されます。CLIから `config log {syslog | syslog2 | syslog3} settings` CLI コマンドを使用して、複数の syslog サーバを設定できます。詳細については、『*FortiGateCLI リファレンス*』を参照してください。

注記： Syslog サーバを設定する際に、自己生成 (self-originated) トラフィックの発信元 IP を指定できますが、この設定は CLI からのみ行うことができます。

メモリへのローカル ロギング

FortiGate のシステム メモリには、ログ メッセージ用の限定的な容量が用意されています。FortiGate のシステム メモリは、最新のログ エントリのみを表示します。メモリに空きがなくなると、FortiGate ユニットは最も古いメッセージから上書きしていきます。FortiGate ユニットが再起動すると、ログ エントリはすべて消去されます。

[Log Settings] ページの [Local Logging & Archiving] セクション

[Memory]	FortiGate ユニットのシステム メモリにログを保存します。
[Minimum log level]	FortiGate ユニットは、選択されたロギング重大度以上のすべてのメッセージをログ記録します。ロギング重大度の詳細については、487 ページの「ログの重大度」を参照してください。
[Enable IPS Packet Archive]	IPS パケット ログのアーカイブを有効にします。IPS パケット ログをアーカイブするとき選択します。

ディスクへのローカル ロギング

FortiGate ユニットにハード ディスクが含まれる場合は、ディスクへのロギングを設定できます。記録する最も低いログの重大度、およびハード ディスクに空き容量がない場合の FortiGate ユニットのローカル ロギング対処方法を指定できます。

ローカル ログの場合、SQL ログ ストレージ形式が、コンテンツ アーカイブおよびトラフィック ログ以外のすべてのログ種類でデフォルト形式となります。これは、レポートを生成できる唯一の形式です。アーカイブ ログは、SQL 形式には対応しません。トラフィック ログでは SQL 形式のロギングを有効に設定できますが、SLQ 形式の書き込みは圧縮形式よりも低速です。このため、SLQ 形式のロギングでは、ログの一部損失が生じる場合があります。

[Log Settings] ページの [Local Logging & Archiving] セクション

[Disk]	ローカル ログを、FortiGateユニットのハード ディスクに保存します。
[Minimum log level]	FortiGate ユニットは、選択されたロギング重大度以上のすべてのメッセージをログ記録します。ロギング重大度の詳細については、487 ページの「ログの重大度」を参照してください。
[When log disk is full]	ディスクがログ保存の最大容量に達したとき、FortiGate ユニットでは、最も古いログから上書きするか、またはロギングをすべて停止するか、いずれかの対応が実行されます。 次のいずれかを選択します。 [Overwrite oldest logs]・最も古いログ メッセージを上書きしてロギングを続行します。 [Stop logging]・ディスクに空き容量がなくなると、すべてのロギングを停止します。

[Log rolling settings]	ログ ファイルの設定。
[Enable SQL Logging]	SQL データベースを FortiGate ユニット上に構成している場合は、この機能を有効に設定し、SQL データベースにログを保存できます。SQL データベースに記録するログの種類を選択します。 **注記**: SQL データベースにログを記録するとき、ログ情報を収集しその情報をレポート ウィジェットに表示できます（[Log&Report]、[Report]、[Executive Summary] の順に選択）。

ローカル アーカイブ

DLP および IPS パケット ログを、FortiAnalyzer ユニット、ローカル ハード ディスク（該当する場合）、および FortiGuard Analysis and Management Services（登録している場合）にアーカイブできます。アーカイブは、過去ログの保存データであり、データの古さに関わらずいつでもアクセスできます。アーカイブされたログは、*[Log&Report]*、*[Archive Access]* の順に選択する場所に保存されています。

これらのログのアーカイブを有効にする設定は、これら自体の設定の中で行います。たとえば、DLP ルールまたは複合ルールをセンサーで設定するとき、そのルールの中には [Archive] オプションがあり、[Full] または [Summary] のいずれのアーカイブの種類をともなうかを選択できます。アーカイブの種類は重要です。というのも、[Full] アーカイブではログ メッセージに含まれる全情報がアーカイブされ、メールのアーカイブであれば添付データも含めてアーカイブされるのに対し、[Summary] アーカイブでは基本情報のみがアーカイブされるからです。

ローカル ディスクにアーカイブする場合は、アーカイブを順次作成するオプションを設定できますが、これらのオプションは CLI のみから設定でき、さらに以下の FortiGate ユニットに限られます。

- 新世代の HDD
- ASM-S08 または ASM-SAS
- FMC または FSM モジュール ストレージ

ハード ディスクにアーカイブする CLI コマンドは、以下のようになります。

```
config log disk filter
  set dlp-archive {enable | disable}
end
```

イベント ログ

[Event Log] メニューでは、ログを行うイベントの種類を有効に設定できます。これらのイベント ログは、*[Log&Report]*、*[Log Config]*、*[Event Log]* の順に選択して表示できます。イベントのロギングの詳細については、『*FortiOS 4.0 のロギングおよびレポート ガイド*』を参照してください。

[Event Log] ページ

このページには、ロギングを有効に設定できるすべてのイベントが表示されます。このリストは、FortiGate ユニットに応じて異なり、また FortiGate ユニットの動作モードの種類によっても異なります。

[System Activity event]	ping サーバの障害やゲートウェイのステータスなど、システム関連のすべてのイベント。
[IPSec negotiation event]	進捗レポートやエラー レポートなど、すべての IPSec ネゴシエーション イベント。
[Admin event]	ユーザ ログイン、リセット、設定更新など、すべての管理イベント。
[HA activity event]	リンク、メンバ、ステータス情報など、すべての高可用性イベント。
[Firewall authentication event]	ユーザ認証など、ファイウォール関連のすべてのイベント。
[Pattern update event]	アンチウイルス、IPS パターンの更新、更新の失敗など、すべてのパターン更新イベント。

[Wireless activity event]	ワイヤレス コントローラのすべての活動。
[CPU & memory usage (every 5 minutes)]	CPU およびメモリの、5 分間ごとの全リアルタイム イベント。
[VoIP event]	SIP および SCCP 違反など、すべての VoIP 活動。
[NAC Quarantine event]	エンドポイント NAC によるホストのチェック中にホストを隔離したすべてのエンドポイント活動。
[Wireless activity event]	不正 AP など、ワイヤレス コントローラのすべての活動。
[AMC interface bypass mode event]	AMC インタフェース バイパス モードのすべての発生イベント。
[SSL VPN user authentication event]	ログイン、ログアウト、活動停止によるタイムアウトなど、SSL VPN 接続のすべてのユーザ認証イベント。
[SSL VPN administration event]	SSL 設定や CA 証明書のロードおよび削除など、SSL VPN に関連したすべての管理イベント。
[SSL VPN session event]	アプリケーション起動およびブロック、タイムアウト、検証など、すべてのセッション活動。
[VIP ssl event]	SSL セッション中に発生するサーバ負荷分散のすべてのイベント、特にハンドシェークに関する詳細。
[VIP server health monitor event]	VIPヘルス モニタが構成されている場合に発生する、nanインタフェース障害などの、VIP サーバ ヘルス モニタ関連のすべてのイベント。

アラート メール

アラート メール機能を使用して、ログ メッセージのログを監視し、ログ記録される特定の活動またはイベントについての通知をメールで送信できます。たとえば、管理者のログインおよびログアウトに関する通知が必要な場合、管理者がログインおよびログアウトするたびにアラート メールを送信するように設定できます。

また、ログの重大度に基づいてアラート メール メッセージを送信することもできます。このようなアラート メール メッセージは、指定の重大度に達した場合のみ送信されます。

アラート メールを設定するには、*[Log&Report]*、*[Log Config]*、*[Alert E-mail]* の順に選択します。

[Alert E-mail] ページ

このページでは、どのような種類のアラート メール通知を送信するかを設定できます。

[SMTP Server]	SMTP メール サーバの名前とアドレス。
[Email from]	アラート メッセージ送信元のメール アドレス。
[Email to]	アラート メール メッセージの受信アドレスを 3 か所まで入力します。
[Authentication]	SMTP 認証を有効にするには、[Authentication] の *[Enable]* チェック ボックスをオンにします。
[SMTP user]	アラート メール メッセージを送信するために SMTP サーバにログオンする際の、ユーザ名を入力します。この設定は、SMTP 認証を有効にした場合のみ行う必要があります。
[Password]	アラート メールを送信するために SMTP サーバにログオンする際のパスワードを入力します。この設定は、SMTP 認証を選択にした場合のみ行う必要があります。
[Send alert email for the following]	管理者のログインおよびログアウトなど、1 つまたは複数イベントの発生に合わせてアラート メールを送信する場合に選択します。
[Interval Time (1-9999 minutes)]	連続するアラート メールの最小間隔を入力します。このオプションを使用し、アラート メールの量を制限します。
[Intrusion detected]	不正侵入の検知に基づくアラート メール メッセージが必要な場合にオンにします。
[Virus detected]	ウイルス検知に基づくアラート メール メッセージが必要な場合にオンにします。

[Web access blocked]	アクセスされた Web サイトのブロックに基づくアラート メール メッセージが必要な場合にオンにします。
[HA status changes]	高可用性ステータスの変化に基づくアラート メール メッセージが必要な場合にオンにします。
[Violation traffic detected]	FortiGate ユニットによって検知された違反トラフィックに基づくアラート メール メッセージが必要な場合にオンにします。
[Firewall authentication failure]	ファイアウォール認証失敗に基づくアラート メール メッセージが必要な場合にオンにします。
[SSL VPN login failure]	SSL VPN ログイン失敗のたびに、その失敗に基づくアラート メール メッセージが必要な場合にオンにします。
[Administrator login/logout]	管理者のログインまたはログアウトに基づくアラート メール メッセージが必要な場合にオンにします。
[IPSec tunnel errors]	IPSec トンネル設定のエラーに基づくアラート メール メッセージが必要な場合にオンにします。
[L2TP/PPTP/PPPoE errors]	L2TP、PPTP、または PPPoE で生じたエラーに基づくアラート メール メッセージが必要な場合にオンにします。
[Configuration changes]	FortiGate の設定変更に基づくアラート メール メッセージが必要な場合にオンにします。
[FortiGuard license expiry time (1-100 days)]	FortiGuard ライセンス失効通知が送信される*前*の日数を入力します。詳しくは、Knowledge Base の「FortiGuard license is expired log messages」という記述を参照してください。
[FortiGuard log quota usage]	FortiGuard Analysis サーバ ログ ディスクの割り当てに基づくアラート メール メッセージが必要な場合にオンにします。
[Disk Usage]	内蔵ハード ディスクまたは AMC ディスクがディスク使用割合に達したとき、アラート メールが必要な場合に選択します。アラート メールが送信されるディスク使用割合を設定できます。
[Send alert email for logs based on severity]	警告 (Warning) など指定のログ重大度に基づいてアラート メールを送信する場合に選択します。
[Minimum log level]	リストからログの重大度を選択します。ログ重大度の詳細については、487 ページの「ログの重大度」を参照してください。

注記: アラート メール メッセージの自己生成 (self-originated) トラフィックの発信元 IP を指定できますが、この設定は CLI からのみ行うことができます。

ログ メッセージへのアクセスおよび表示

[Log Access] メニューには、リモート (FortiAnalyzer など) またはディスクへのローカル ロギング (Disk) など、指定に応じたロギング場所のログを表示するためのタブが含まれています。各タブには、検索およびフィルタ処理オプションなどのログ メッセージ表示オプション、およびログの種類を選択するオプションがあります。[Remote] タブには、ロギングに設定されている FortiGuard Analysis サーバまたは FortiAnalyzer ユニットのいずれかに保存されるログが表示されます。

FortiGuard Analysis and Management Service に登録している場合は、FortiGate Web ベース マネージャから FortiGuard Analysis サーバに保存されているログ ファイルにアクセスできます。FortiGuard Analysisサーバへのロギングを有効に設定すると、[Log Access] メニューに [Remote] タブが表示されます。リアルタイムおよび過去のログ ファイルを表示する詳しい方法については、『*FortiGuard Analysis and Management Service ガイド*』を参照してください。

ログ情報を表示するには、ページの横に表示される表で行を選択し、そのログ メッセージの情報を表示できます。表では、そのログ メッセージに含まれる各フィールドを明瞭に確認できます。この表は、ログを Format で表示する場合のみ使用できます。

表示されるカラムには、ログ ファイルに含まれる内容が反映されます。[Log Access] ページの最上部にはナビゲーション機能が表示され、ログ メッセージ間を移動しながら必要な情報を容易に特定できます。また特定の情報を表示するように、カラムをカスタマイズできます。たとえば、ログメッセージは、[Formatted] または [Raw] のビューで表示できます。[Formatted] ビューでは、カラムをカスタマイズするか、またはログ メッセージ表示をフィルタ処理できます。[Raw] ビューでは、ログ メッセージはログ ファイルと同じように表示されます。ログ メッセージ表示をフィルタ処理する方法については、32 ページの「Web ベース マネージャ リストへのフィルタの追加」を参照してください。カラムをカスタマイズする方法については、34 ページの「表示されるカラムのカラム設定を使用した制御」を参照してください。

フィルタ処理は、ログ メッセージの表示をカスタマイズするもう 1 つの方法です。フィルタ アイコンを使用することで、ログ メッセージの特定の情報を表示できます。たとえば、ログ重大度が [Alert] (警告) のイベント ログ メッセージのみを表示できます。

[Log&Report]、*[Log Access]* の順に選択すると、ログ デバイスの構成に応じて、以下のタブが表示されます。

- *[Remote]* タブでは、FortiAnalyzerユニットまたはFortiGuard Analysis and Management Service に保存されているログ メッセージを表示できます。
- *[Memory]* タブでは、FortiGate ユニットのシステム メモリに保存されているログ メッセージを表示できます。
- *[Disk]* タブでは、内蔵ハード ディスクまたは AMC ハード ディスクなどのハード ディスクに保存されているログ メッセージ、および SQL ログを表示できます。

以下の設定オプションは、ログの種類に応じたログ メッセージを表示するとき、[Archive Access] および [Log Access] のページに表示されます。

[Log Type]	表示するログの種類を選択します。
[Page Controls]	デフォルトでは、各項目を含むリストの最初ページが表示されます。現在のページ番号の後に、総ページ数が表示されます。たとえば、3/54 が表示される場合は、現在、全 54 ページ中 3 ページ目を表示しています。 左右の矢印を選択し、最初、前、次、または最後のページを表示します。 特定のページを表示するには、ページ番号をフィールドに入力し Enter キーを押します。 詳細については、34 ページの「Web ベース マネージャ リストに対するページ コントロールの使用」を参照してください。
[Column Settings]	カラムを追加または削除する場合に選択します。この設定により、[Log Access] ページに表示されるログ情報が変わります。
[Raw or **Formatted]**	デフォルトでは、ログ メッセージは [Formatted] モードで表示されます。*[Formatted]* を選択すると、ログ メッセージがカラムなしの *[Raw]* モードで表示されます。*[Raw]* モードのとき、*[Formatted]* を選択するとログ メッセージが再びカラムに配置されて表示されます。 ログ メッセージを [Formatted] ビューで表示する場合は、カラムをカスタマイズするか、またはログ メッセージ表示をフィルタ処理できます。
[Clear All Filters]	フィルタ設定をすべて消去します。

注記： FortiGate ユニットのログを表示するには、FortiAnalyzer ユニットがバージョン 3.0 以上のファームウェアで動作している必要があります。

アーカイブ ログ

FortiGate ユニットでは、DLP アーカイブまたは IPS パケット アーカイブなど、各種のアーカイブ ログを表示できます。アーカイブは、アーカイブ作成に対応するログ デバイス、たとえば FortiAnalyzer ユニットなどに保存されている、過去のログです。

これらのログにアクセスするには、*[Log&Report]*、*[Archive Access]* の順に選択します。また FortiGuard Analysis and Management Serviceに登録している場合は、同サービスからもログ アーカイブを表示できます。

[DLP Archive] メニューは、以下の場合に限り表示されます。

- FortiAnalyzer ユニットにリモート ロギングおよびアーカイブを行うように、FortiGate ユニットを設定している。詳しくは、491 ページの「FortiAnalyzer ユニットへのリモート ロギング」を参照してください。
- FortiGuard Analysis and Management Service に登録している。詳細については、『*FortiGuard Analysis and Management Service 管理ガイド*』を参照してください。

以下のいずれかのプロトコルの DLP アーカイブを表示する場合、 次のメニューが表示されます。

- *[E-mail]* では、POP3、IMAP、SMTP、POP3S、IMAPS、SMTPS およびスパム メールのアーカイブが表示されます。
- *[Web]* では、HTTP および HTTPS のアーカイブが表示されます。
- *[FTP]* では、FTP のアーカイブが表示されます。
- *[IM]* では、AIM、ICQ、MSN、および Yahoo! のアーカイブが表示されます。
- *[VoIP]* では、セッション制御 (SIP、SIMPLE、および SCCP) アーカイブが表示されます。

ログ アーカイブを [Raw] 形式で表示する場合は、*[Formatted]* の横にある *[Raw]* を選択します。

隔離

[Log Access] メニューでは、隔離されたファイルごとの詳細情報を表示できます。表示する内容に応じて、表示情報を並べ替えまたはフィルタ処理できます。

ファイルを並べ替える場合は、ファイル名、日付、サービス、状態、重複カウント (DC)、または TTL (Time to Live) を基準にします。またリストのフィルタ処理により、特定ステータスの隔離ファイルまたは特定サービスの隔離ファイルのみを表示できます。

[Log&Report]、*[Archive Access]*、*[Quarantine]* の順に選択すると、隔離ファイルごとの以下の情報がファイル隔離リストに表示されます。

[Quarantine] ページ

このページには、FortiGate ユニットにより感染ファイルと判断されたファイルが一覧表示されます。このページでは、特定ファイルのみをページに表示するように、表示情報をフィルタ処理できます。

[Source]	隔離ファイルの保存場所の設定に応じて、*[FortiAnalyzer]* または *[Local disk]* が表示されます。
[Sort by]	リストを並べ替えます。並べ替えの基準を、*[Status]*、*[Service]*、*[File Name]*、*[Date]*、*[TTL]*、または *[Duplicate Count]* から選択します。並べ替えを完了するには、*[Apply]* を選択します。
[Filter]	リストをフィルタ処理します。*[Status]* (infected、blocked、または heuristics) または *[Service]* (IMAP、POP3、SMTP、FTP、HTTP、IM、または NNTP) のいずれかを選択します。フィルタ処理を完了するには、*[Apply]* を選択します。ヒューリスティック モードは、CLI を使用してのみ設定できます。 FortiGate ユニットが SSL コンテンツ スキャンおよびインスペクションをサポートする場合、[Service] は IMAPS、POP3S、および SMTPS にも対応します。詳しくは、『*FortiOS ハンドブック*』の「*UTM*」の章を参照してください。
[Apply]	選択すると、並べ替えおよびフィルタ処理の設定を、隔離ファイル リストに適用します。
[Delete]	選択したファイルを削除するとき選択します。
ページ コントロール	コントロールを使用して、リスト内を移動します。詳細については、34 ページの「Web ベース マネージャ リストに対するページ コントロールの使用」を参照してください。
全エントリ削除アイコン	すべての隔離ファイルを、ローカル ハード ディスクから削除します。 このアイコンは、ファイルがハード ディスクに隔離されている場合のみ表示されます。
[File Name]	隔離ファイルのファイル名。
[Date]	ファイルが隔離された日時。dd/mm/yyyy hh:mm の形式で表示されます。同じファイルの隔離が重なる場合、この値は最初のファイルが隔離された時刻を示します。
[Service]	隔離されたファイルのサービスの種類 (HTTP、FTP、IMAP、POP3、SMTP、IM、NNTP、IMAPS、POP3S、SMTPS、または HTTPS)。
[Status]	ファイルが隔離された理由。*[infected]*、*[heuristics]*、または *[blocked]* が表示されます。

[Status Description]	[Status] の具体的な情報。たとえば、"File is infected with "W32/Klez.h"" (ファイルが "W32/Klez.h" に感染) または "File was stopped by file block pattern." (ファイル ブロック パターンがファイルを停止) などが表示されます。
[DC]	重複カウント。同じファイルが重複して隔離された回数を示します。この数が急速に増えているときは、ウイルスが発生し急拡大している可能性があります。
[TTL]	Time to Live。時、分 (hh:mm) の形式で表示されます。この TTL が経過すると、FortiGate ユニットによって、このファイルの [TTL] の見出しの下に [EXP] というラベルが表示されます。同じファイルの感染が重なる場合、重複が検出されるたびに TTL が更新されます。 ファイルが FortiAnalyzer ユニット上で隔離される場合は、 TTL 情報は表示されません。
[Upload Status]	*[Y]* は、このファイルが解析のためにフォーティネットにアップロード されたことを示し、*[N]* は、ファイルがアップロード されていないことを示します。 このオプションは、FortiGate ユニットがローカル ハード ディスクを備える場合のみ表示されます。
ダウンロード アイコン	該当するファイルを元の形式でダウンロードする場合に選択します。 このオプションは、FortiGate ユニットがローカル ハード ディスクを備える場合のみ表示されます。
送信アイコン	疑わしいファイルを解析のためにフォーティネットにアップロードする場合に選択します。 このオプションは、FortiGate ユニットがローカル ハード ディスクを備える場合のみ表示されます。

注記 : 隔離が重複するファイル (チェックサムに基づく) は保存されず、カウントされるだけです。TTL 値と DC (重複カウント) は、ファイルの重複が見つかるたびに更新されます。

レポート

レポート機能によって、ログの情報を容易に分析および表示できます。レポートには、さまざまなログの情報が集められ、テキスト、グラフおよび表の形式で表示されます。次のレポートを設定できます。

- FortiGate レポート ・レポート スケジュールおよび複製レポートの設定が含まれています。
- Executive Summary レポート ・ SQL データベースから収集したログ情報を表示するウィジェット。設定には制限があります。
- ベーシック トラフィック レポート ・FortiGate ユニットのシステム メモリから収集したログ情報。棒グラフで表示されます。

FortiOS レポートは、ローカル ハード ドライブを備える FortiGate ユニットのみで使用できます。また、[Report] メニューを Web ベース マネージャでも表示するように、CLI を使用して以下を有効に設定する必要があります。

```
config log fortianalyzer setting
  set gui-display enable
end
```

このトピックには、以下の項目が含まれています。

- FortiOS レポート
- SQL ログによるエグゼクティブ サマリ レポート

FortiOS レポート

FortiOS レポートは、FortiGate ユニットのハード ドライブに保存されているログから構成され、FortiGate ユニットによって生成されます。これまでこの機能は FortiAnalyzer ユニットのみで使用可能でしたが、FortiOS レポートにより、ログ ファイルから生成されるレポートを一元的に作成、保存できるようになります。

FortiOS レポートを設定するには、*[Log&Report]*、*[Report Config]* の順に選択します。

注記： FortiOS レポートは、ローカル ハード ドライブを備える FortiGate ユニットのみで使用できます。FortiOS 4.0 MR1 以前のバージョンからアップグレードする場合は、FortiAnalyzer レポートは FortiAnalyzer ユニットのみで使用でき、また FortiOS 4.0 MR2 では FortiAnalyzer レポートの設定には対応しません。

レポート メニューを有効にするまでは、レポートを設定できません。[Report Config] および [Report Access] を有効に設定するには、CLI を使用します。Web ベース マネージャの [Report Config] および [Report Access] メニューを有効にするには、必ず以下のコマンドを使用します。

```
config log fortianalyzer setting
  set gui-display enable
end
```

レポートのテーマ

テーマでは、フォントの種類、ページの向き、複数のカラムの使用など、情報をページに表示するスタイルを設定できます。

[Add Report Layout] ページには、必要に応じて利用可能な 2 種類のデフォルトのテーマが用意されています。

`theme` コマンドの詳細については、『FortiGate CLI リファレンス』を参照してください。

レポートのテーマを設定するには、CLI にログインし以下のコマンドを入力します。

```
config report theme
  edit <theme_name>
    set column-count [ 1 | 2 | 3]
    set default-html-style <string>
    set default-pdf-style <string>
    set graph-chart-style <string>
    set heading1-style <string>
    set heading2-style <string>
    set heading3-style <string>
    set heading4-style <string>
    set hline-style <string>
    set image-style
    set normal-text-style
    set page-footer-style
    set page-header-style
    set page-orient {landscape | portrait}
    set page-style
    set report-subtitle-style
    set report-title-style
    set table-chart-caption-style
    set table-chart-even-row-style
    set table-chart-head-style
    set table-chart-odd-row-style
    set table-chart-style
    set toc-heading1-style
    set toc-heading2-style
    set toc-heading3-style
    set toc-heading4-style
    set toc-title-style
end
```

レイアウト

レポート レイアウトには、FortiAnalyzer レポートに必ず設定するレイアウトと同様に、チャート、セクション、画像の追加、レイアウト生成時のスケジュール作成などの設定が含まれています。

[Add Report Layout] ページの [Report Components] セクションには、レポート表示用に選択されているチャート、セクション、画像を表示するための領域があります。このセクションでは、チャートなどの表示パーツをレポートの任意の場所に移動できます。

レポート レイアウトを設定するには、*[Log&Report]*、*[Report Config]*、*[Layout]* の順に選択します。

[Layout] ページ

このページには、設定済みのレポート レイアウトおよびデフォルトのレイアウトが一覧表示されます。このページでは、レポートの編集、削除、複製、または新規作成が可能です。

[Create New]	[Create New] を選択すると、画面が [Add Report Layout] ページに自動的に移動します。
編集アイコン	レポート レイアウトの設定を編集するとき選択します。
削除アイコン	リストからレポート レイアウトを削除するとき選択します。
クローン アイコン	既存のレポートをベースに新規レポートを作成するとき使用します。
[Run]	レポートを直ぐに生成します。
[Report Layout]	レポート レイアウトの名前。
[Title]	生成したレポートに表示される題名。
[Format]	レポートの形式の種類。PDF または HTML 形式です。
[Schedule]	レポートが生成される時刻。
[Description]	レポートの説明。

[Add Report Layout] ページ

このページでは、レポート レイアウトを設定できます。

[Name]	レポート レイアウトの名前を入力します。レポートのタイトルとなる名前ではありません。
[Report Theme]	ドロップダウン リストから、テーマを選択します。
[Description]	必要に応じて、レポート内容の説明を入力します。この説明は、レポート内には表示されません。
[Output Format]	レポートが生成される形式の種類。PDF を選択すると、レポートを PDF として生成できます。
[Schedule]	レポートを生成するためのスケジュールの種類を選択します。スケジュールの種類には、毎日、毎週、任意 (必要に応じた日付)、または 1 回のみがあります。[On Demand] (任意) を選択すると、必要に応じた日付でレポートを生成できます。[Once] (1 回のみ) を選択すると、レポートを保存した直後に生成されます。
[Title]	レポートの題名を入力します。
[Sub Title]	レポートの副題となる名前を入力します。
[Option]	以下のレポート オプションの一部またはすべてを加えるように選択します。 [Table of Contents]・レポートに目次を加えます。 [Auto Heading Number]・見出しごとに数字の見出し番号を自動的に表示します。 [HTML navigation bar]・HTML 形式のレポートを容易に閲覧するためのナビゲーション バーを表示します。 [Chart Name as Heading]・チャートの名前を見出しとして表示します。
[Report Components]	[Add] を選択して、レポートに表示する情報の種類を加えます。 これらのコンポーネントを必ず追加することで、レポートに必要なログ情報を、レポートの中でどの形式を使用しどのように表示するかを指定します。 このセクションでは、レポートのプレビューを使用して、レポート表示をチャートや画像などのパーツごとに編集できます。生成されるレポートの中で、各パーツを移動し表示順に並べ替えることができます。

[Add Component] ページ

[Text]	見出しに使用する形式の種類を選択します。とたえば、[Heading 1] を選択すると、レポートに含まれる各見出しが [Heading 1] の形式で表示されます。 [Normal] を選択すると、レポートに含まれるセクションへのコメントを追加します。

[Chart]	[Categories] ドロップダウン リストから、カテゴリを選択します。各カテゴリには、そのカテゴリ特有の異なるチャートが含まれています。
[Image]	レポートに表示する画像を選択します。
[Misc]	レポートに含まれる、改ページ、段区切り、または横線を選択します。

チャート

レポートを作成するとき、デフォルトのチャートを利用できる他に、レポート レイアウトに合わせて独自のチャートを作成できます。チャートの作成時には、SQL データベースから特定のデータを収集するために使用するデータセットを設定する必要があります。最初に、レポート レイアウトに必要なデータセットを設定し、次にチャートを作成します。

データセットには、SQL ステートメントが必要です。このため、データセットを設定する際にはあらかじめ SQL に関する知識が必要となります。データセットは、CLI からのみ設定できます。

チャートを設定するには、*[Log&Report]*、*[Report Config]*、*[Chart]* の順に選択します。

[Chart] ページ

このページには、デフォルトおよび作成済みチャートの双方が一覧表示されます。このページでは、チャートを編集、削除、または新規作成できます。

[Create New]	新しいチャートを作成する際には、画面が [Add Graph Report Chart] ページに自動的に移動します。
編集アイコン	既存のチャートの設定を編集するとき選択します。
削除アイコン	リストからチャートを削除するとき選択します。
[Name]	チャートの名前。
[Type]	チャートに表示する情報の種類。たとえば、棒グラフを使用して、Attacks_February チャートに攻撃ログ情報を表示します。
[Dataset]	チャートに使用するデータセット。
[Comments]	チャートの説明。

[Add Graph Report Chart] ページ

このページでは、レポート レイアウトのチャートを設定できます。

[Name]	チャートの名前を入力します。
[Dataset]	チャートに使用する設定済みのデータセットを選択します。
[Category]	チャートのログ カテゴリを選択します。
[Comments]	チャート説明のコメントを入力します (入力はオプションです)。
[Graph Type]	チャート内に情報を表示するグラフの種類を選択します。[Pie] を選択する場合は、[Category Series] および [Value Series] のみが表示されます。
[Category Series]	[Databind] フィールドにカテゴリのフィールドを入力します。 データバインドは、SQL ステートメントから派生するフィールドまたは CLI の名前付きフィールドの組み合わせです。たとえば、field(3) などです。
[Value Series]	[Databind] フィールドに value のフィールドを入力します。 データバインドは、SQL ステートメントから派生するフィールドまたは CLI の名前付きフィールドの組み合わせです。たとえば、field(3) などです。
[X-series]	線グラフ、棒グラフまたはフロー チャートの X 軸の設定。
[Databind]	設定されている series にデータをバインドするための、SQL データバインドの値式を入力します。たとえば、field(3) などです。
[Category Axis]	軸がログ カテゴリの種類を示すように設定するとき選択します。デフォルトでは、軸上にログ カテゴリは示されません。
[Scale]	x 軸に表示される日時の形式を設定します。
[Format]	x 軸に表示される時刻の形式を選択します。
[Number of Step]	グラフの横軸の目盛り数を選択します。
[Step]	x 軸の目盛りごとに目盛り単位の数を入力します。
[Unit]	x 軸の目盛りの単位を選択します。

[Y-series]	線グラフ、棒グラフ、またはフロー チャートの y 軸を構成する、Y-series の設定。
[Databind]	x-series のフィールドを入力します。 データバインドは、SQL ステートメントから派生するフィールドまたは CLI の名前付きフィールドの組み合わせです。たとえば、field(3) などです。
[Group]	フィールドにグループを入力します。

画像

レポートに使用するための画像をインポートできます。サポートされる画像の形式は、JPEG、JPG、および PNG です。

画像をインポートするには、*[Log&Report]*、*[Report Config]*、*[Image]* の順に選択します。

[Image] ページ

このページには、インポートした画像が一覧表示されます。このページでは、画像を削除、ローカル PC からインポート、または表示できます。

削除アイコン	このページのリストから画像を削除します。
[インポート]	ローカル PC から画像をインポートします。
表示アイコン	画像を表示します。表示アイコンを選択すると、画像が表示される [View Image] ページに画面が自動的に移動します。[Image] ページに戻るには、[Return] を選択します。
[Image Name]	画像のファイル名。
[Thumbnail]	インポートした画像のサムネイル画像。

[Import Image File] ページ

このページでは、画像のインポートを設定できます。

[File to Import]	ローカル PC 上の画像の場所を入力するか、または [Browse] を選択して画像ファイルを指定します。[OK] を選択して、画像ファイルのインポートを開始します。

作成した FortiOS レポートの表示

レポート レイアウトを作成した後、*[Report Access]*、*[Disk]* の順に選択して、生成したレポートを表示できます。1 回のみのレポート作成を選択している場合は、レポートは直ちに生成されます。

[Disk] ページ

このページには、FortiGate ユニットによって生成されたレポートが一覧表示されます。ここでは、リストからレポートを削除できます。

削除アイコン	リストからレポートを削除する場合に選択します。
[Report File]	レポート名。FortiGate ユニットからレポートに割り当てられます。この名前は、<scheduletype>-<report_title>-<yyyy-mm-dd>-<start_time> の形式で表示されます。たとえば、Once-examplereport_1-2010-02-12-083054 という名前の場合、examplereport_1 という表題のレポートが 2010 年 2 月 12 日午前 8:30 に 1 回のみ生成されるようにスケジュールされたことを示します。
[Started]	レポート生成開始の時刻。yyyy-mm-dd hh:mm:ss の形式で表示されます。
[Finished]	レポート生成終了の時刻。yyyy-mm-dd hh:mm:ss の形式で表示されます。
[Size]	生成されたレポートのサイズ。バイト単位で示されます。
[Other Formats]	改めて選択するレポートの形式種類。たとえば、PDF などです。ここで PDF を選択すると、[Disk] ページでその PDF が開きます。[Disk] ページで開いた PDF は、ローカル PC に保存できます。

SQL ログによるエグゼクティブ サマリ レポート

ハード ドライブを備える FortiGate ユニットでは、SQL データベースに保存されているログに基づくエグゼクティブ サマリ レポートを表示できます。SQL データベースには、ログ メッセージがテキスト形式で保存されています。

デフォルトで各種のレポートが用意されており、それらを Web ベース マネージャで選択しカスタマイズできます。レポートをカスタマイズするには、[Executive Summary] でレポート更新のスケジュールおよび場所を選択します。

エグゼクティブ サマリ レポートを設定するには、*[Log&Report]*、*[Report]*、*[Access]*、*[Executive Summary]* の順に選択します。

FortiAnalyzer レポート スケジュール

FortiAnalyzer のレポート スケジュールは、FortiAnalyzer ユニットにロギングが設定されている場合のみ利用できます。レポート スケジュールを設定する前に、レポート レイアウトが必要です。このため、FortiGate ユニットからレポート スケジュールを設定する前に FortiAnalyzer 管理者まで連絡し、適切なレポート レイアウトが設定されていることを確認してください。レポート レイアウトは、FortiAnalyzer ユニットからのみ設定できます。

レポート レイアウトの詳しい設定方法については、*『FortiAnalyzer 管理ガイド』を参照してください。*

レポートを設定する前に、必ずレポート メニューを有効に設定します。[Report Config] および [Report Access] は、CLI から有効に設定します。Web ベース マネージャの [Report Config] および [Report Access] メニューを有効にするには、必ず以下のコマンドを使用します。

```
config log fortianalyzer setting
  set gui-display enable
end
```

FortiAnalyzer のレポート スケジュールを設定するには、*[Log&Report]*、*[Report Config]*、*[FortiAnalyzer]* の順に選択します。

[FortiAnalyzer] ページ

このページには、作成済みのレポート スケジュールが一覧表示されます。このページでは、レポート スケジュールの編集、削除、または新規作成が可能です。

[Create New]	新しいレポート スケジュールを作成します。
[Name]	レポート スケジュールの名前。
[Description]	レポート スケジュールが作成されたとき加えられるコメント。
[Report Layout]	レポート スケジュールに使用されるレポート レイアウトの名前。
[Schedule]	レポート スケジュールが生成される日時。表示される日時は、レポート スケジュール作成時に選択された、1 回のみ、毎日、指定の曜日の周期に応じて異なります。 たとえば、毎月を選択すると、月の各日付および時刻 (hh:mm) が Monthly 2, 10, 21, 12:00 の形式で表示されます。
削除および編集アイコン	リストのレポート スケジュールを削除または編集します。
複製アイコン	レポート スケジュールを複製し、それをベースに新規レポート スケジュールを作成します。

[Create Schedule Settings] ページ

このページでは、レポート スケジュールを設定できます。レポート スケジュールを設定する際には、レポート レイアウトが必要です。

[Name]	スケジュールの名前を入力します。
[Description]	スケジュールの説明を入力します (入力はオプションです)。
[Report Layout]	リストから設定済みのレポート レイアウトを選択します。レポート レイアウトを、レポート スケジュールに必ず適用します。詳細については、*『FortiAnalyzer 管理ガイド』* を参照してください。
[Language]	レポート スケジュールに使用する言語を、リストから選択します。
[Schedule]	以下のいずれかを選択し、1 回のみ、毎日、毎週、または毎月指定の日付または時刻の周期でレポートを生成します。
[Once]	レポートを 1 回のみ生成する場合に選択します。
[Daily]	毎日同じ時刻にレポートを生成する場合に選択します。レポート生成時刻の時、分を、hh:mm の形式で入力します。

[These Days]	特定の曜日にレポートを生成する場合に選択します。曜日チェック ボックスをオンにします。
[These Dates]	月の特定の日付にレポートを生成する場合に選択します。日付を入力し、日付同士はコンマで区切ります。たとえば、月の 1 日、21 日、30 日にレポートを生成する場合は、`1, 21, 30` と入力します。
[Log Data Filtering]	レポートの以下の変数を指定できます。
[Virtual Domain]	バーチャル ドメインに基づくレポートを作成する場合に選択します。レポートに含めるバーチャル ドメインを入力します。
[User]	ネットワーク ユーザに基づくレポートを作成する場合に選択します。1 名または数名のユーザをフィールドに入力し、ユーザ同士はスペースで区切ります。名前またはグループの名前にスペースが含まれる場合は、“user 1” のように引用符で囲みます。
[Group]	ローカルに定義されるネットワーク ユーザのグループに基づくレポートを作成する場合に選択します。1 つまたは複数のグループ名を、フィールドに入力します。
[LDAP Query]	[LDAP Query] チェック ボックスをオンにして、リストから LDAP ディレクトリまたは Windows Active Directory グループを選択します。
[Time Period]	レポートに含めるログの期間を加える場合に選択します。
[Relative to Report Runtime]	リストから期間を選択します。たとえば、[this year] などを設定します。
[Specify]	レポートを実行する日付、年、時間を指定する場合に選択します。 **[From]** – ログ時間範囲の開始日時を選択します。 **[To]** – ログ時間範囲の終了日時を選択します。
[Output]	レポートを出力する形式を選択し、必要に応じて出力テンプレートの適用を指定できます。
[Output Types]	生成されるレポートのファイル形式を、PDF、MS Word、Text、および MHT から選択します。
[Email/Upload]	リストからレポート出力テンプレートを適用する場合に、このチェック ボックスをオンにします。 レポート出力テンプレートがない場合は、このリストは空です。詳細については、『*FortiAnalyzer 管理ガイド*』を参照してください。

注記：バーチャル ドメイン (VDOM) を有効に設定している場合、FortiAnalyzer レポートへのアクセスは VDOM ごとに限られます。グローバル VDOM ではレポートにアクセスできません。

FortiGate ユニットが FortiAnalyzer ユニットに接続されていない場合、あるいは FortiAnalyzer ユニットで 3.0 以上のファームウェアを実行していない場合、FortiAnalyzer レポートは表示されません。

索引

記号

数字

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

ひ

ふ

へ

ほ

ま

む

め

も

ゆ

よ

ら

り

る

れ

ろ

わ

www.fortinet.com

www.fortinet.com