使用する前に

次のトピックでは、Firepower Threat Defense（FTD）の設定を開始する方法について説明します。

このガイドの対象読者

このマニュアルでは、Firepower Threat Defense デバイスに組み込まれたFirepower Device Manager（FDM）の Web ベース設定インターフェイスを使用して Firepower Threat Defense を設定する方法について説明します。

FDM では、小規模または中規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Firepower Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

多数のデバイスを管理している場合、または Firepower Threat Defense で許可される、より複雑な機能や設定を使用したい場合は、組み込みの FDM の代わりに Firepower Management Center（FMC）を使用してデバイスを設定します。

FDM は次のデバイスで使用できます。

表 *1 : FDM*サポート対象モデル

デバイス モデル	FTD ソフトウェアの最小バージョン
Firepower 1010、1120、1140	6.4

デバイス モデル	FTD ソフトウェアの最小バージョン
Firepower 1150	6.5
Firepower 2110、2120、2130、2140	6.2.1
Firepower 4110、4115、4120、4125、4140、4145、4150	6.5
Firepower 4112	6.6
Firepower 9300	6.5
FTDv （FTDv）VMware 用	6.2.2
FTDv カーネルベース仮想マシン（KVM）ハイパーバイザ用	6.2.3
FTDv Microsoft Azure クラウド用	6.5
FTDv Amazon Web Services（AWS）クラウド用	6.6
ASA 5508-X、5516-X	6.1
ISA 3000（Cisco 3000 シリーズ産業用セキュリティアプライアンス）	6.2.3

FDM/FTD バージョン 7.0.0 の新機能

リリース日：2021 年 5 月 26 日

次の表に、FDM を使用して設定された場合に Firepower Threat Defense 7.0.0 で使用できる新機能を示します。

機能	説明
プラットフォーム機能	
HyperFlex および Nutanix 向け FTDv。	Cisco HyperFlex および Nutanix Enterprise Cloud に FTDv が導入されました。
VMware vSphere/VMware ESXi 7.0 向け FTDv。	VMware vSphere/VMware ESXi 7.0 に FTDv を展開できるようになりました。 バージョン 7.0 でも VMware 6.0 のサポートは終了します。FTD をアップグレードする前に、ホスティング環境をサポートされているバージョンにアップグレードします。

機能	説明
AWS における FTDv の新しいデフォルトパスワード	AWS では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[Advanced Details]** > **[User Data]**）していなければ、FTDv のデフォルトの管理者パスワードは AWS のインスタンス ID です。
ISA 3000 によるシャットダウンのサポート。	バージョン 7.0.2 以降では、ISA 3000 をシャットダウンできるようになりました。以前は、デバイスを再起動することしかできませんでした。 バージョン 7.0.5 以降では、ISA 3000 をシャットダウンすると、システム LED が消灯します。その後、少なくとも 10 秒間待ってからデバイスの電源を切ってください。 バージョンの制限：バージョン 7.1 では、この機能のサポートが一時的に廃止されます。サポートは、バージョン 7.2 で再開されています。
ファイアウォールと IPS の機能	
システム定義の NAT ルールの新しいセクション 0。	新しいセクション 0 が NAT ルールテーブルに追加されました。このセクションは、システムの使用に限定されます。システムが正常に機能するために必要なすべての NAT ルールがこのセクションに追加され、これらのルールは作成したルールよりも優先されます。以前は、システム定義のルールがセクション 1 に追加され、ユーザー定義のルールがシステムの適切な機能を妨げる可能性がありました。セクション 0 のルールを追加、編集、または削除することはできませんが、**show nat detail** コマンド出力に表示されます。
Snort 3 のカスタム侵入ルール。	オフラインツールを使用して、Snort 3 で使用するカスタム侵入ルールを作成し、侵入ポリシーにアップロードできます。独自のカスタムルールグループにカスタムルールを編成して、必要に応じて簡単に更新できます。FDM で直接ルールを作成することもできますが、ルールの形式はアップロードされたルールと同じです。FDM には、ルール作成のガイダンスはありません。新しい侵入ルールの基礎として、システム定義のルールを含む既存のルールを複製できます。 侵入ポリシーの編集時に、**[Policies]** > **[Intrusion]** ページにカスタムグループとルールのサポートが追加されました。

機能	説明
FDM管理対象システムのSnort 3 の新機能	FDM 管理対象システムで Snort 3 を検査エンジンとして使用する場合、次の追加機能を設定できるようになりました。 • 時間ベースのアクセス制御ルール（FTD API のみ）。 • 複数の仮想ルータ。 • SSL復号ポリシーを使用したTLS 1.1以下の接続の復号。 • SSL復号ポリシーを使用したプロトコルFTPS、SMTPS、IMAPS、POP3S の復号。
URL カテゴリとレピュテーションに基づく DNS 要求のフィルタリング。	URL フィルタリングカテゴリとレピュテーションルールを DNS ルックアップ要求に適用できます。ルックアップ要求の完全修飾ドメイン名（FQDN）にブロックしているカテゴリやレピュテーションがある場合、システムはDNS応答をブロックします。ユーザーはDNS解決を受信しないため、ユーザーは接続を完了できません。非 Web トラフィックに URL カテゴリおよびレピュテーション フィルタリングを適用するには、このオプションを使用します。この機能を使用するには、URL フィルタリングライセンスが必要です。 アクセス コントロール ポリシーの設定に [Reputation Enforcement on DNS Traffic] オプションが追加されました。
Snort 2 を搭載したメモリが少ないデバイス用の小規模 VDB。	**アップグレードの影響。 メモリが少ないデバイスのアプリケーション ID が影響を受けます。** Snort 2 を搭載したバージョン 7.0.6 以降のデバイスの場合、VDB 363 以降では、Snort 2 搭載のメモリが少ないデバイスに小規模 VDB（別称：VDB lite）がインストールされるようになりました。この小規模VDBには同じアプリケーションが搭載されていますが、検出パターンは少なくなっています。小規模 VDB を使用しているデバイスでは、フルサイズの VDB を使用しているデバイスと比較して、一部のアプリケーションが識別されない場合があります。 メモリが少ないデバイス：ASA-5508-X、ASA-5516-X バージョンの制限：小規模VDBは、すべてのバージョンでサポートされているわけではありません。サポート対象のバージョンからサポート対象外のバージョンにアップグレードする場合、Snort 2 を実行しているメモリの少ないデバイスにVDB 363以降をインストールできません。影響を受けるリリースのリストについては、CSCwd88641 を参照してください。
VPN 機能	

機能	説明
リモートアクセス VPN の FDM SSL 暗号設定	FDM でリモートアクセス VPN 接続に使用する TLS バージョンと暗号化の暗号を定義できます。以前は、Firepower Threat Defense API を使用して SSL を設定する必要がありました。 次のページが追加されました：**[Objects]** > **[SSL Ciphers]**、**[Device]** > **[System Settings]** > **[SSL Settings]**。
Diffie-Hellman グループ 31 のサポート。	IKEv2 プロポーザルおよびポリシーで Diffie-Hellman（DH）グループ 31 を使用できるようになりました。
デバイス上の仮想トンネルインターフェイスの最大数は 1024 です。	作成できる仮想トンネルインターフェイス（VTI）の最大数は 1024 です。以前のバージョンでは、送信元インターフェイスあたりの最大数は 100 でした。
サイト間 VPN セキュリティアソシエーションの IPsec ライフタイム設定。	セキュリティ アソシエーションが再ネゴシエートされるまでに維持する期間のデフォルト設定を変更できます。 サイト間 VPN ウィザードに [Lifetime Duration] オプションと [Lifetime Size] オプションが追加されました。
ルーティング機能	
ISA 3000 の仮想ルータサポート。	ISA 3000 デバイスには最大 10 の仮想ルータを設定できます。
等コストマルチパス（ECMP）ルーティング。	複数のインターフェイスを含むように ECMP トラフィックゾーンを設定できます。これにより、ゾーン内の任意のインターフェイスで、既存の接続のトラフィックが Firepower Threat Defense デバイスに出入りできるようになります。この機能により、Firepower Threat Defense デバイス上での等コストマルチパス（ECMP）のルーティングや、Firepower Threat Defense デバイスへのトラフィックの複数のインターフェイスにわたる外部ロードバランシングが可能になります。 ECMP トラフィックゾーンはルーティングにのみ使用されます。これらはセキュリティゾーンとは異なります。 [ルーティング（Routing）] ページに [ECMP トラフィックゾーン（ECMP Traffic Zones）] タブが追加されました。Firepower Threat Defense API に ECMPZones リソースが追加されました。
インターフェイス機能	
新しいデフォルトの内部 IP アドレス。	192.168.1.0/24 のアドレスが DHCP を使用して外部インターフェイスに割り当てられている場合、IP アドレスの競合を避けるために、内部インターフェイスのデフォルト IP アドレスが 192.168.1.1 から **192.168.95.1** に変更されています。

機能	説明
デフォルトの外部 IP アドレスで IPv6 自動設定が有効になりました。管理用の新しいデフォルト IPv6 DNS サーバー。	外部インターフェイスのデフォルト設定には、IPv4 DHCP クライアントに加えて、IPv6 自動設定が含まれています。デフォルトの管理 DNS サーバーには、IPv6 サーバー：2620:119:35::35 も含まれるようになりました。
ISA 3000 の EtherChannel サポート。	FDM を使用して ISA 3000 で EtherChannel を設定できるようになりました。 新しい/変更された画面：**[デバイス（Devices）]** > **[インターフェイス（Interfaces）]** > **[EtherChannel]**
ライセンシング機能	
FTDv のパフォーマンス階層型ライセンス。	FTDv は、スループット要件と RA VPN セッションの制限に基づいて、パフォーマンス階層型のスマートライセンスをサポートするようになりました。使用可能なパフォーマンスライセンスのいずれかで FTDv のライセンスを取得すると、2 つのことが発生します。まず、デバイスのスループットを指定されたレベルに制限するレートリミッタがインストールされます。次に、VPN セッションの数は、ライセンスで指定されたレベルに制限されます。
管理およびトラブルシューティングの機能	
Firepower Threat Defense API を使用した DHCP リレー設定。	**アップグレードの影響。 アップグレード後の展開ができない場合があります。** Firepower Threat Defense API を使用して DHCP リレーを設定できます。インターフェイスで DHCP リレーを使用すると、他のインターフェイスを介してアクセス可能な DHCP サーバーに DHCP 要求を送信できます。物理インターフェイス、サブインターフェイス、EtherChannel、および VLAN インターフェイスで DHCP リレーを設定できます。いずれかのインターフェイス上に DHCP サーバーを設定している場合、DHCP リレーは設定できません。 以前のリリースで FlexConfig を使用して DHCP リレーを設定した場合は（**dhcprelay** コマンド）、アップグレード後に API を使用して設定を再実行し、FlexConfig オブジェクトを削除する必要があります。 Firepower Threat Defense API に次のモデルを追加しました：dhcprelayservices

機能	説明
ブートストラップ処理の高速化と FDM への早期ログイン	FDM 管理対象システムを最初にブートストラップするプロセスが改善され、より高速になりました。したがって、デバイスを起動してからFDMにログインするまで待機する必要はありません。また、ブートストラップの進行中にログインできるようになりました。ブートストラップが完了していない場合は、プロセスのステータス情報が表示されるため、デバイスで何が発生しているかがわかります。
多対 1 および 1 対多接続の CPU 使用率とパフォーマンスが向上しました。	ダイナミック NAT / PAT およびスキャン脅威検出とホスト統計情報を含む接続を除き、システムは接続の作成時に、ローカルホストオブジェクトを作成せず、ロックすることもなくなりました。これにより、多数の接続を同じサーバー（ロードバランサや Web サーバーなど）に対して確立する場合や、1 つのエンドポイントが多数のリモートホストに接続する場合に、パフォーマンスと CPU 使用率が向上します。 次のコマンドが変更されました：**clear local-host**（廃止）、**show local-host**
FDM 管理対象デバイスのアップグレード準備状況チェック。	アップロードした Firepower Threat Defense アップグレードパッケージをインストールする前に、アップグレード準備状況チェックを実行できます。準備状況チェックでは、システムに対してアップグレードが有効であり、システムがパッケージのインストールに必要な他の要件を満たしていることを確認します。アップグレードの準備状況チェックを実行すると、インストールの失敗を回避できます。 **[Device]** > **[Updates]**ページの **[System Upgrade]** セクションに、アップグレードの準備状況チェックを実行するリンクが追加されました。

機能	説明
CA バンドルの自動更新。	**アップグレードの影響。システムは、何か新しいことを求めてシスコに接続します。** ローカル CA バンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。システムは、毎日のシステム定義の時刻に、新しい CA 証明書についてシスコに自動的にクエリを実行するようになりました。以前は、CA 証明書を更新するにはソフトウェアをアップグレードする必要がありました。CLI を使用して、この機能を無効にすることができます。 新しいリソース：https://cisco.com/security/pki/ 新規/変更された CLI コマンド：**configure cert-update auto-update**、**configure cert-update run-now**、**configure cert-update test**、**show cert-update** バージョンの制限：バージョン 7.0.5、7.1.0.3、または 7.2.4 以降が必要です。バージョン 7.0.0 ～ 7.0.4、7.1.0 ～ 7.1.0.2、または 7.2.0 ～ 7.2.3 ではサポートされていません。 参照：*Cisco Secure Firewall Threat Defense コマンドリファレンス*
すべての RADIUS 応答に Message-Authenticator 属性が必要です。	**アップグレードの影響。アップグレード後、既存のサーバーに対して有効にします。** すべての RADIUS 応答で Message-Authenticator 属性を要求できるようになりました。これにより、Threat Defense VPN ゲートウェイで、RA VPN 用でもデバイス自体へのアクセス用でも、RADIUS サーバーからのすべての応答を安全に検証できるようになります。 新しい RADIUS サーバーでは、[すべてのRADIUS応答にメッセージオーセンティケータを要求（Require Message-Authenticator for all RADIUS Responses）] オプションがデフォルトで有効になっています。既存のサーバーでも有効にすることを推奨します。無効にすると、ファイアウォールが攻撃にさらされる可能性があります。 新しい CLI コマンド：**message-authenticator-required** バージョンの制限：バージョン 7.0.7 以降/7.7.0 以降が必要です。

機能	説明
FTD REST API バージョン 6.1（v6）。	ソフトウェアバージョン 7.0 の Firepower Threat Defense REST API はバージョン 6.1 です。API URL の v6 を使用するか、優先的に /latest/ を使用して、デバイスでサポートされている最新の API バージョンを使用していることを示せます。6.1 の URL バージョンパス要素は、6.0：v6 と同じであることに注意してください。 使用しているリソースモデルに変更が加えられている可能性があるため、既存のすべての呼び出しを再評価してください。リソースを表示できる API エクスプローラを開くには、FDM にログインして、[More options] ボタン（⋮）をクリックし、[API Explorer] を選択します。

デフォルト設定

デバイスのデフォルト設定は、初期セットアップを完了しているかどうかによって異なります。

初期設定前のデフォルト設定

ローカルマネージャ（FDM）を使用して Firepower Threat Defense デバイスの初期設定を行う前、デバイスには次のデフォルト設定が含まれています。

多数のモデルにおいて、この設定では、デバイスマネージャを内部インターフェイス経由で開き（通常、コンピュータをインターフェイスに直接接続する）、内部インターフェイス上に定義された DHCP サーバを使用してコンピュータに IP アドレスを提供することを前提としています。または、コンピュータを管理インターフェイスに接続し、DHCP を使用してアドレスを取得できます。ただし、一部のモデルではデフォルト設定や管理要件が異なります。詳細については、次の表を参照してください。

（注） ウィザードを使用してセットアップを実行する前に、CLI セットアップ（（任意）CLI での管理ネットワーク設定の変更 （23 ページ））を使用してこれらの設定の多くを事前に設定できます。

デフォルト設定

設定	デフォルト	初期設定時に変更できるか
管理者ユーザのパスワード	Admin123 Firepower 4100/9300：論理デバイスを展開するときのパスワードを設定します。 AWS：初期展開時にユーザデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）]** > **[ユーザデータ（User Data）]**）していなければ、デフォルトは AWS のインスタンス ID です。	可。デフォルトパスワードを変更する必要があります。
管理 IP アドレス	DHCP 経由で取得。 FTDv192.168.45.45 Firepower 4100/9300：論理デバイスの展開時に管理 IP アドレスを設定します。	番号 Firepower 4100/9300の場合：可。
管理ゲートウェイ	デバイスのデータインターフェイス。通常、外部インターフェイスがインターネットへのルートになります。このゲートウェイは、from-the-device（デバイスからの出力）トラフィックのみで機能します。デバイスがDHCPサーバからデフォルトゲートウェイを受信した場合は、そのゲートウェイが使用されます。 Firepower 4100/9300：論理デバイスの展開時にゲートウェイIPアドレスを設定します。 ISA 3000：192.168.45.1。 FTDv192.168.45.1	番号 Firepower 4100/9300の場合：可。
管理インターフェイスの DNS サーバ	OpenDNS パブリック DNS サーバ、IPv4：208.67.220.220 と 208.67.222.222、IPv6：2620:119:35::35。DHCP から取得した DNS サーバは使用されません。 Firepower 4100/9300：論理デバイスの展開時に DNS サーバを設定します。	可

設定	デフォルト	初期設定時に変更できるか
内部インターフェイスの IP アドレス	192.168.95.1/24 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：BVI1 IP アドレスは事前に設定されていません。BVI1 にはすべての内部インターフェイスと外部インターフェイスが含まれます。 FTDv192.168.45.1/24	不可。
内部クライアントの DHCP サーバ	内部インターフェイス上で実行されており、アドレスプールは 192.168.95.5 ～ 192.168.95.254 です。 Firepower 4100/9300: No DHCP server enabled. ISA 3000: DHCP サーバが有効になっていません。 FTDv：内部インターフェイスのアドレスプールは 192.168.45.46 ～ 192.168.45.254 です。	不可。
内部クライアントに対する DHCP 自動設定（自動設定では、WINS サーバおよび DNS サーバ用のアドレスがクライアントに提供）	外部インターフェイスで有効です。	可（ただし間接的）。外部インターフェイスにスタティック IPv4 アドレスを設定した場合、DHCP サーバの自動設定が無効になります。
外部インターフェイスの IP アドレス	IPv4：インターネットサービスプロバイダー（ISP）またはアップストリームルータから DHCP を通して取得されます。 IPv6：自動設定。 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：BVI1 IP アドレスは事前に設定されていません。BVI1 にはすべての内部インターフェイスと外部インターフェイスが含まれます。	可

デバイスモデル別のデフォルトインターフェイス

初期設定時に異なる内部および外部インターフェイスを選択することはできません。設定後にインターフェイスの割り当てを変更するには、インターフェイス設定とDHCP設定を編集します。非交換インターフェイスとして設定するには、ブリッジグループからインターフェイスを削除する必要があります。

FTD デバイス	外部インターフェイス	内部インターフェイス
ASA 5508-X ASA 5516-X	GigabitEthernet 1/1	GigabitEthernet 1/2
Firepower 1010	Ethernet1/1	VLAN1 には、物理ファイアウォールインターフェイスである外部インターフェイスを除く他のすべてのスイッチポートが含まれます。
Firepower 1120、1140、1150	Ethernet1/1	Ethernet1/2
Firepower 2100	Ethernet1/1	Ethernet1/2
Firepower 4100	データインターフェイスが事前設定されていません。	データインターフェイスが事前設定されていません。
Firepower 9300	データインターフェイスが事前設定されていません。	データインターフェイスが事前設定されていません。
FTDv	GigabitEthernet 0/0	GigabitEthernet 0/1
ISA 3000	GigabitEthernet1/1 および GigabitEthernet1/3 GigabitEthernet1/1（outside1）と 1/2（inside1）、および GigabitEthernet1/3（outside2）と 1/4（inside2）（非光ファイバモデルのみ）は、ハードウェアバイパスペアとして設定されます。 すべての内部および外部インターフェイスは、BVI1 の一部です。	GigabitEthernet1/2 および GigabitEthernet1/4

初期セットアップ後の設定

セットアップ ウィザードを完了すると、デバイス設定は次のようになります。この表では、個々の設定項目の値が、ユーザーが明示的に選択したものとなるのか、または他の項目の設定に基づき自動的に定義されたものかを示します。「暗黙的」な設定を検証し、ニーズに合わない場合は編集します。

（注） Firepower 4100/9300 と ISA 3000 は、セットアップ ウィザードをサポートしていません。Firepower 4100/9300 の場合、シャーシから論理デバイスを展開するときにすべての初期設定が行われます。ISA 3000 の場合、出荷前に特殊なデフォルト設定が適用されます。

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
管理者ユーザーのパスワード	任意の入力値	明示的
管理 IP アドレス	DHCP 経由で取得。 FTDv：192.168.45.45 Firepower 4100/9300：論理デバイスの展開時に設定した管理 IP アドレス	デフォルト
管理ゲートウェイ	デバイスのデータインターフェイス。通常、外部インターフェイスがインターネットへのルートになります。管理ゲートウェイは、from-the-device（デバイスからの出力）トラフィックのみで機能します。デバイスが DHCP サーバからデフォルトゲートウェイを受信した場合は、そのゲートウェイが使用されます。 Firepower 4100/9300：論理デバイスの展開時に設定したゲートウェイ IP アドレス ISA 3000：192.168.45.1 FTDv：192.168.45.1	デフォルト
管理インターフェイスの DNS サーバー	OpenDNS パブリック DNS サーバー、IPv4：208.67.220.220、208.67.222.222、IPv6：2620:119:35::35、またはユーザーの入力値。DHCP から取得した DNS サーバーは使用されません。 Firepower 4100/9300：論理デバイスの展開時に設定した DNS サーバー	明示的
管理ホスト名	**firepower** または任意の入力値 Firepower 4100/9300：論理デバイスの展開時に設定したホスト名。	明示的

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
データ インターフェイスを通過する管理アクセス	データ インターフェイスの管理アクセス リスト ルールにより、内部インターフェイスを通過する HTTPS アクセスが許可されます。SSH 接続は許可されません。IPv4 および IPv6 接続はいずれも許可されます。 Firepower 4100/9300: デフォルトの管理アクセス ルールを持つデータ インターフェイスはありません。 ISA 3000：デフォルトの管理アクセスルールを持つデータインターフェイスはありません。 FTDv: デフォルトの管理アクセス ルールを持つデータ インターフェイスはありません。	暗黙的
システム時間	選択したタイム ゾーンおよび NTP サーバー。 Firepower 4100/9300：システム時刻はシャーシから継承されます。 ISA 3000：Cisco NTP サーバー：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org。	明示的
スマート ライセンス	基本ライセンスとともに登録したか、または評価期間を開始したか、いずれか選択した方法。 サブスクリプション ライセンスは有効化されていません。スマート ライセンスのページに移動して、スマート ライセンスを有効化してください。	明示的
内部インターフェイスの IP アドレス	192.168.95.1/24 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：なし。BVI1 の IP アドレスは手動で設定する必要があります。 FTDv192.168.45.1/24	デフォルト
内部クライアントの DHCP サーバ	内部インターフェイス上で実行されており、アドレスプールは 192.168.95.5 ～ 192.168.95.254 です。 Firepower 4100/9300: No DHCP server enabled. ISA 3000: DHCP サーバが有効になっていません。 FTDv：内部インターフェイスのアドレスプールは 192.168.45.46 ～ 192.168.45.254 です。	デフォルト

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
内部クライアントに対するDHCP自動設定（自動設定では、WINSサーバおよびDNSサーバ用のアドレスがクライアントに提供）	DHCPを使用して外部インターフェイスのIPv4アドレスを取得している場合、DHCP自動設定は外部インターフェイスに対して有効化されます。 静的アドレッシングを使用している場合は、DHCP自動設定は無効になります。	明示的（ただし間接的）
データ インターフェイスの設定	• 1010：外部インターフェイスEthernet1/1は物理ファイアウォール インターフェイスです。その他すべてのインターフェイスは、有効になっているVLAN1（内部インターフェイス）の一部であるスイッチポートです。これらのポートにエンド ポイントまたはスイッチを接続すると、内部インターフェイスのアドレスをDHCP サーバーから取得できます。 • Firepower 4100/9300：データインターフェイスはすべて無効になります。 • ISA 3000：データインターフェイスはすべて有効になり、同じブリッジグループ（BVI1）の一部になります。GigabitEthernet1/1および1/3は外部インターフェイスで、GigabitEthernet1/2および1/4は内部インターフェイスです。GigabitEthernet1/1（外部1）と1/2（内部1）、およびGigabitEthernet1/3（外部2）と1/4（内部2）（非光ファイバモデルのみ）は、ハードウェアバイパスペアとして設定されます。 • その他すべてのモデル：外部および内部インターフェイスのみが設定され、有効化されます。他のすべてのデータ インターフェイスは無効になります。	デフォルト
外部の物理インターフェイスおよびIPアドレス	デバイス モデルに基づくデフォルトの外部ポート。初期設定前のデフォルト設定 （9ページ）を参照してください。 IPアドレスはDHCPおよびIPv6自動設定により取得されるか、入力したスタティックアドレスです（IPv4、IPv6、または両方）。 Firepower 4100/9300：データインターフェイスが事前設定されていません。 ISA 3000：なし。BVI1のIPアドレスは手動で設定する必要があります。	インターフェイスはデフォルト アドレッシングは明示的

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
スタティック ルート	外部インターフェイスに対してスタティック IPv4 または IPv6 アドレスを設定すると、スタティックなデフォルトルートも IPv4 または IPv6 用に適宜設定され、このアドレスタイプ用に定義されたゲートウェイをポイントします。DHCP を選択した場合は、デフォルトルートは DHCP サーバーから取得されます。 ネットワーク オブジェクトもこのゲートウェイ、および「any」アドレス（IPv4 の場合は 0.0.0.0/0、IPv6 の場合は ::/0）に合わせて作成されます。	暗黙的
セキュリティ ゾーン	内部インターフェイスを含む **inside_zone**。Firepower 4100/9300 では、このセキュリティゾーンにインターフェイスを手動で追加する必要があります。 外部インターフェイスを含む **outside_zone**。Firepower 4100/9300 では、このゾーンにインターフェイスを手動で追加する必要があります。 （これらのゾーンを編集して他のインターフェイスを追加することも、独自のゾーンを作成することも可能）。	暗黙的
アクセス コントロール ポリシー	inside_zone から outside_zone に送信されるすべてのトラフィックを信頼するルール。これにより、インスペクションなしで、ネットワーク内のユーザーからのすべてのトラフィックを外部に出すことができ、これらの接続のすべてのリターン トラフィックが許可されます。 他のすべてのトラフィックに対するデフォルト アクションは、ブロックです。つまり、外部から開始され、ネットワークに進入しようとするすべてのトラフィックが阻止されます。 Firepower 4100/9300：事前設定されたアクセスルールはありません。 ISA 3000：inside_zone から outside_zone へのすべてのトラフィックを信頼するルール、および outside_zone から inside_zone へのすべてのトラフィックを信頼するルール。トラフィックがブロックされます。デバイスには、inside_zone 内のインターフェイスと outside_zone 内のインターフェイス間のすべてのトラフィックを信頼するルールもあります。これにより、内部にいるユーザー間、および外部にいるユーザー間のすべてのトラフィックが検査なしで許可されます。	暗黙的

設定項目	設定	明示的/暗黙的な設定、またはデフォルト設定
NAT	インターフェイスの動的PATルールは、外部インターフェイスへの任意の IPv4 トラフィックの発信元アドレスを、外部インターフェイスの IP アドレス上の一意のポートに変換します。 補足的な非表示の PAT ルールにより、内部インターフェイスを通過する HTTPS アクセス、およびデータ インターフェイスを経由する管理アドレスのルーティングが有効化されます。これらは NAT テーブルには含まれませんが、CLI で **show nat** コマンドを使用すれば確認できます。 Firepower 4100/9300：NAT は事前に設定されていません。 ISA 3000：NAT は事前設定されていません。	暗黙的

システムへのログイン

Firepower Threat Defense デバイスには、次の 2 つのインターフェイスがあります。

FDM Web インターフェイス

Firewall Device Managerは Web ブラウザで実行されます。このインターフェイスを使用して、システムを設定、管理、モニターできます。

コマンドライン インターフェイス（CLI、コンソール）

CLIはトラブルシューティングに使用します。Firewall Device Managerの代わりに初期設定に使用することもできます。

次に、これらのインターフェイスにログインし、ユーザーアカウントを管理する方法を説明します。

ユーザー ロールで表示および実行可能な対象の制御

ユーザー名はロールに割り当てられ、Firewall Device Manager で何を実行できるか、また何を表示できるかがユーザーロールによって決まります。ローカルに定義される [管理者（admin）] ユーザにはすべての権限がありますが、別のアカウントを使用してログインすると権限が少なくなります。

Firewall Device Manager ウィンドウの右上隅にユーザー名と権限レベルが表示されます。

権限は次のとおりです。

- [管理者（Administrator）]：すべての機能を表示および使用できます。
- [読み取り/書き込みユーザー（Read-Write User）]：読み取り専用ユーザーが実行できることをすべて実行できます。また、設定を編集および展開することもできます。アップグレードのインストール、バックアップの作成と復元、監査ログの表示、他の Firewall Device Manager ユーザーセッションの終了など、システムクリティカルなアクションに対してのみ制限があります。
- [読み取り専用ユーザ（Read-Only User）]：ダッシュボードおよび設定を表示できますが、変更することはできません。変更しようとすると、権限がないことを示すエラーメッセージが表示されます。

これらの権限は、CLI ユーザーが利用できる権限とは関連していません。

Firewall Device Manager へのログイン

Firewall Device Manager を使用して、システムの設定、管理、モニターを行います。ブラウザで設定可能な機能を、コマンドライン インターフェイス（CLI）で設定することはできません。セキュリティ ポリシーを実装するには、Web インターフェイスを使用する必要があります。

Firefox、Chrome、Safari、Edge ブラウザの最新バージョンを使用します。

（注） 誤ったパスワードを入力し、3 回連続してログインに失敗した場合、アカウントは 5 分間ロックされます。再度ログインを試みる前に待機する必要があります。

始める前に

最初は、**admin** ユーザー名を使用してのみ Firewall Device Manager にログインできます。ただし、Firewall Device Manager および Firewall Threat Defense ユーザーアクセスの管理に説明されているように、外部 AAA サーバに定義されている追加ユーザの認証は設定できます。

アクティブなログインは一度に 5 つまで可能です。これには、デバイスマネージャにログインしているユーザーと、有効期限の切れていない API トークンなどのアクティブな API セッションが含まれます。この制限を超えると、最も古いセッション（デバイスマネージャログインまたは API トークン）が期限切れになり、新しいセッションが許可されます。これらの制限は、SSH セッションには適用されません。

手順

ステップ 1 ブラウザを使用して、システムのホームページ（https://ftd.example.com など）を開きます。

次のいずれかのアドレス使用できます。設定済みのものであれば、IPv4 アドレス、IPv6 アドレス、または DNS 名を使用できます。

- 管理アドレス。（ほとんどのプラットフォームの）デフォルトでは、管理インターフェイスはDHCPクライアントであるため、IPアドレスはDHCPサーバーによって異なります。
- HTTPS アクセス用に開いたデータ インターフェイスのアドレス。（ほとんどのプラットフォームの）デフォルトでは、「内部」インターフェイスで HTTPS アクセスが許可されているため、デフォルトの内部アドレス 192.168.95.1 に接続できます。使用モデルの内部 IP アドレスの詳細については、初期設定前のデフォルト設定 （9 ページ）を参照してください。

  HTTPSデータポートを変更した場合は、URLにカスタムポートを含める必要があります。たとえば、ポートを 4443 に変更した場合は、https://ftd.example.com:4443 のようなURLにします。

ヒント
ブラウザがサーバー証明書を認識するように設定されていない場合、信頼できない証明書に関する警告が表示されます。証明書を例外として受け入れるか、または信頼できるルート証明書ストアの証明書を受け入れます。

ステップ 2 デバイスに定義されているユーザー名とパスワードを入力し、[ログイン（Login）] をクリックします。

事前定義されたユーザであるユーザ名 **admin** を使用できます。デフォルトの admin パスワードはAdmin123です。AWSでは、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）]**>**[ユーザーデータ（User Data）]**）していなければ、デフォルトの管理者パスワードは AWS のインスタンス ID です。

セッションは非アクティブの状態が 30 分間続くと期限切れになり、再度ログインするように求められます。ページの右上にある [ユーザー（user）] アイコンのドロップダウン リストから [ログアウト（Log Out）] を選択するとログアウトできます。

CLI（コマンドライン インターフェイス）へのログイン

コマンドラインインターフェイス（CLI）を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLIセッションからポリシーを設定することはできません。

CLI にログインするには、次のいずれかを実行します。

- デバイスに付属のコンソール ケーブルを使用し、9600 ボー、8 データ ビット、パリティなし、1 ストップ ビット、フロー制御なしに設定されたターミナルエミュレータを用いて PC をコンソールに接続します。コンソール ケーブルの詳細については、デバイスのハードウェア ガイドを参照してください。

（注） Firepowerデバイスモデルでは、コンソールポートのCLIはSecure Firewall eXtensible Operating System（FXOS）です。一部のデバイスモデルでは、**connect ftd** コマンドを使用して Firepower Threat Defense CLI にアクセスできます。Firepower 4100/9300 の場合は、アプリケーションのコンソールへの接続を参照してください。FXOS CLI はシャーシ レベルのトラブルシューティングにのみ使用します。基本設定、モニタリング、および通常のシステムのトラブルシューティングには Firepower Threat Defense CLI を使用します。FXOS コマンドの詳細については、FXOS のマニュアルを参照してください。

- FTDv の場合は、仮想コンソールを開きます。
- SSH クライアントを使用して、管理 IP アドレスに接続します。 SSH 接続用のインターフェイスを開いている場合、データ インターフェイス上のアドレスにも接続できます（管理アクセス リストの設定を参照）。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。**admin** ユーザ名または別の CLI ユーザアカウントを使用してログインします。デフォルトの admin パスワードは Admin123 です。AWS では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）]** > **[ユーザーデータ（User Data）]**）していなければ、 Firewall Threat Defense Virtual のデフォルトの管理者パスワードは AWS のインスタンス ID です。

ヒント

- ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用方法の情報については、『Cisco Firepower Threat Defense コマンド リファレンス』（http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html）を参照してください。
- **configure user add** コマンドを使用して、CLI にログインできるローカルユーザアカウントを作成できます。ただし、これらのユーザは CLI のみにログインできます。Firewall Device Manager Web インターフェイスにはログインできません。
- 外部サーバで SSH アクセス用のユーザアカウントを作成できます。SSH アクセス用の外部認証の設定については、Firewall Threat Defense CLI（SSH）ユーザー用の外部認証（AAA）設定を参照してください。

パスワードの変更

パスワードは定期的に変更する必要があります。次の手順では、Firewall Device Manager にログインしているときにパスワードを変更する方法について説明します。

（注） CLI にログインしている場合は、**configure password** コマンドを使用してパスワードを変更できます。別の CLI ユーザーのパスワードを変更するには、**configure user password** *username* コマンドを使用します。

始める前に

この手順は、ローカルユーザにのみ適用されます。ユーザアカウントが外部 AAA サーバで定義されている場合、そのサーバでパスワードを変更する必要があります。

手順

ステップ 1 メニューの右上にある [ユーザー（user）] アイコンのドロップダウンリストから、[プロファイル（Profile）] を選択します。

ステップ 2 [パスワード（Password）] タブをクリックします。

ステップ 3 現在のパスワードを入力します。

ステップ 4 新しいパスワードを入力して確認します。

ステップ 5 [変更（Change）] をクリックします。

ユーザー プロファイルの設定

ユーザー インターフェイスの設定を行い、パスワードを変更できます。

手順

ステップ 1 メニューの右上にある [ユーザー（user）] アイコンのドロップダウンリストから、[プロファイル（Profile）] を選択します。

ステップ 2 [プロファイル（Profile）] タブで次の設定を行い、[保存（Save）] をクリックします。

- [スケジュールするタスクのタイム ゾーン（Time Zone for Scheduling Tasks）]：バックアップや更新などのタスクのスケジュールに使用するタイム ゾーンを選択します。別のゾーンを設定すると、ブラウザのタイム ゾーンはダッシュボードやイベントに使用されます。

- [カラー テーマ（Color Theme）]：ユーザー インターフェイスで使用するカラー テーマを選択します。

ステップ 3 [パスワード（Password）] タブで新しいパスワードを入力し、[変更（Change）] をクリックします。

英語以外の言語でのページの表示

次の言語で GUI およびオンラインヘルプを表示できます。

- 中国語
- 英語（デフォルト）
- 日本語
- 韓国語

これらの言語を使用するには、ブラウザの設定でその言語を選択する必要があります。製品自体には言語設定がありません。

お使いのブラウザで特定の言語がサポートされていない場合、製品はその言語で表示されません。たとえば、フランス語バージョンは、カナダのフランス語を使用するようにブラウザを設定した場合にのみ表示されます。別のタイプのフランス語を選択すると、製品は英語になります。

システムの設定

ネットワークでシステムが正しく機能するためには、初期設定を完了する必要があります。展開を成功させるには、ケーブルを正しく接続し、デバイスをネットワークに挿入し、インターネットや他のアップストリーム ルータに接続するために必要なアドレスを設定する必要があります。次の手順で、このプロセスについて説明します。

始める前に

初期設定を開始する前に、デバイスにはいくつかのデフォルト設定が含まれています。詳細は、初期設定前のデフォルト設定 （9 ページ）を参照してください。

手順

ステップ 1 インターフェイスの接続 （23 ページ）

ステップ 2 セットアップウィザードを使用した初期設定の完了 （25 ページ）

設定の結果の詳細については、初期セットアップ後の設定（12ページ）を参照してください。

インターフェイスの接続

デフォルト設定では、特定のインターフェイスが内部および外部ネットワークに使用されると仮定しています。これらの前提に基づいてネットワーク ケーブルをインターフェイスに接続すると、初期設定の実行が容易になります。

大半のモデルのデフォルト設定は、管理コンピュータを内部インターフェイスに接続するように設計されています。あるいは、管理ポートに直接ワークステーションを接続することもできます。インターフェイスはさまざまなネットワーク上にあるため、内部インターフェイスと管理ポートを同じネットワークに接続しようとしないでください。

内部インターフェイスを、アクティブなDHCPサーバを持つネットワークに接続しないでください。内部インターフェイスですでに稼働中の DHCP サーバと競合してしまいます。ネットワークに別の DHCP サーバを使用する必要がある場合は、初期設定の後に不要な DHCP サーバを無効にします。

ケーブル接続図については、使用モデルのスタートアップガイドを参照してください。

（任意）CLI での管理ネットワーク設定の変更

デフォルトの IP アドレスを使用できない場合（たとえば、デバイスを既存のネットワークに追加する場合）、コンソールポートに接続して、CLI で初期セットアップ（管理IPアドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定など）を実行できます。管理インターフェイスのみを設定できます。内部インターフェイスや外部インターフェイスは設定できません。これらは後で GUI を使用して設定できます。

（注） 展開時に IP アドレスを手動で設定するため、Firepower 4100/9300 にこの手順を使用する必要はありません。

（注） 設定をクリア（たとえば、イメージを再作成することにより）しないかぎり、CLIセットアップスクリプトを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。*Cisco Secure Firewall Threat Defense コマンドリファレンス*を参照してください。

手順

ステップ 1 Firewall Threat Defense コンソール ポートに接続します。詳細については、CLI（コマンドライン インターフェイス）へのログイン （19 ページ）を参照してください。

ステップ 2 ユーザ名 **admin** を使用してログインします。

デフォルトの admin パスワードは Admin123 です。AWS では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）]** > **[ユーザーデータ（User Data）]**）していなければ、 Firewall Threat Defense Virtual のデフォルトの管理者パスワードは AWS のインスタンス ID です。

ステップ 3 Firewall Threat Defense に初めてログインすると、エンドユーザーライセンス契約（EULA）に同意して管理者パスワードを変更するように求められます。その後、CLI セットアップスクリプトが表示されます。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次のガイドラインを参照してください。

- [管理インターフェイスの IPv4 デフォルトゲートウェイを入力します（Enter the IPv4 default gateway for the management interface）]：手動 IP アドレスを設定した場合は、「**data-interfaces**」またはゲートウェイルータの IP アドレスのいずれかを入力します。**data-interfaces** を設定すると、アウトバウンド管理トラフィックがバックプレーン経由で送信され、データインターフェイスが終了します。この設定は、インターネットにアクセスできる個別の管理ネットワークがない場合に役立ちます。管理インターフェイスから発信されるトラフィックには、インターネットアクセスを必要とするライセンス登録とデータベースの更新が含まれます。**data-interfaces** を使用する場合、管理ネットワークに直接接続していれば管理インターフェイスで Firewall Device Manager（または SSH）を引き続き使用できますが、特定のネットワークまたはホストのリモート管理の場合は、**configure network static-routes** コマンドを使用して静的ルートを追加する必要があります。データインターフェイスでの Firewall Device Manager の管理は、この設定の影響を受けないことに注意してください。DHCP を使用する場合、システムは DHCP によって提供されるゲートウェイを使用します。DHCP がゲートウェイを提供しない場合は、フォールバックメソッドとして **data-interfaces** を使用します。
- [ネットワーク情報が変更された場合は再接続が必要になります（If your networking information has changed, you will need to reconnect）]：SSH でデフォルトの IP アドレスに接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか（Manage the device locally?）]： または Firewall Device Manager を使用するには [はい（yes）] を入力します。[いいえ（no）] と応えると、 デバイスの管理にはを使用することになります。

例：

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

ステップ 4 新しい管理 IP アドレスで Firewall Device Manager にログインしてください。

セットアップウィザードを使用した初期設定の完了

Firewall Device Manager に初めてログインする際に、デバイス セットアップ ウィザードを使用してシステムの初期設定を完了します。

ハイ アベイラビリティ設定でデバイスを使用する予定の場合は、2台の装置でのハイ アベイラビリティの準備を参照してください。

（注） Firepower 4100/9300 と ISA 3000 は、セットアップウィザードをサポートしていないため、この手順はこれらのモデルには適用されません。Firepower 4100/9300 の場合、シャーシから論理デバイスを展開するときにすべての初期設定が行われます。ISA 3000 の場合、出荷前に特殊なデフォルト設定が適用されます。

始める前に

データ インターフェイスがゲートウェイ デバイス（たとえば、ケーブル モデムやルータなど）に接続されていることを確認します。エッジの導入では、これはインターネット向けのゲートウェイになります。データセンター導入の場合は、これがバックボーン ルータになります。使

用モデルのデフォルトの「外部」インターフェイスを使用します（インターフェイスの接続（23 ページ）および初期設定前のデフォルト設定 （9 ページ）を参照）。

以上の確認が済んだら、管理コンピュータをハードウェアモデルの「inside」インターフェイスに接続します。または、管理インターフェイスに接続することもできます。Firewall Threat Defense Virtual については、管理 IP アドレスに接続できることを確認するだけで十分です。

（管理 IP アドレスからインターネットへの接続が必要な Firewall Threat Defense Virtual を除く。）管理インターフェイスをネットワークに接続する必要はありません。デフォルトでは、インターネットに接続するデータインターフェイス（通常、外部インターフェイス）を通じてシステムのライセンシングとデータベースおよびその他の更新が取得されます。独立した管理ネットワークを使用する場合は、Management インターフェイスをネットワークに接続し、初期セットアップ完了後に独立した管理ゲートウェイを設定することもできます。

デフォルトの IP アドレスにアクセスできない場合に管理インターフェイスのネットワーク設定を変更するには、「（任意）CLI での管理ネットワーク設定の変更 （23 ページ）」を参照してください。

手順

ステップ 1 Firewall Device Manager にログインします。

a) CLI での初期設定を完了していない場合は、**https://***ip-address* で Firewall Device Manager を開きます。このアドレスは次のいずれかになります。

- 内部インターフェイスに接続されている場合：**https://192.168.95.1**
- （Firewall Threat Defense Virtual の場合は必須） 管理インターフェイスに接続している場合：**https://192.168.45.45**。
- （他のすべてのモデル）管理インターフェイスに接続している場合：**https://***dhcp_client_ip*

b) ユーザ名 **admin** を使用してログインします。デフォルトの admin パスワードは Admin123 です。AWS では、初期展開時にユーザーデータを使用してデフォルトのパスワードを定義（**[高度な詳細（Advanced Details）]** > **[ユーザーデータ（User Data）]**）していなければ、 Firewall Threat Defense Virtual のデフォルトの管理者パスワードは AWS のインスタンス ID です。。

ステップ 2 これがシステムへの初めてのログインであり、CLI セットアップウィザードを使用していない場合、エンドユーザライセンス契約を読んで承認し、管理パスワードを変更するように求められます。

続行するには、これらの手順を完了する必要があります。

ステップ 3 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ（Next）] をクリックします。

注意

[次へ（Next）]をクリックすると、設定がデバイスに展開されます。インターフェイスの名前は「外部」となり、「outside_zone」セキュリティゾーンに追加されます。設定値が正しいことを確認します。

外部インターフェイス

- [IPv4の設定（Configure IPv4）]：外部インターフェイス用のIPv4アドレスです。DHCPを使用するか、または手動でスタティックIPアドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ（Off）]を選択して、IPv4アドレスを設定しないという選択肢もあります。デフォルトの内部アドレスと同じサブネットに（静的に、またはDHCPを介して）IPアドレスを設定しないでください（初期設定前のデフォルト設定 （9 ページ）を参照）。セットアップウィザードを使用してPPPoEを設定することはできません。インターフェイスがDSLモデム、ケーブルモデム、またはISPへの他の接続に接続されており、ISPがPPPoEを使用してIPアドレスを提供している場合は、PPPoEが必要になる場合があります。ウィザードの完了後にPPPoEを設定できます。物理インターフェイスの設定を参照してください。
- [IPv6の設定（Configure IPv6）]：外部インターフェイス用のIPv6アドレスです。DHCPを使用するか、または手動でスタティックIPアドレス、プレフィックス、およびゲートウェイを入力できます。[オフ（Off）]を選択して、IPv6アドレスを設定しないという選択肢もあります。

[管理インターフェイス（Management Interface）]

- [DNSサーバ（DNS Servers）]：システムの管理アドレス用のDNSサーバ。名前解決用に1つ以上のDNSサーバのアドレスを入力します。デフォルトは、OpenDNSパブリックDNSサーバ、またはDHCPサーバから取得したDNSサーバです。フィールドを編集し、デフォルトに戻したい場合は、[OpenDNSを使用（Use OpenDNS）]をクリックすると、フィールドに適切なIPアドレスがリロードされます。ISPは、特定のDNSサーバを使用するよう要求する場合があります。ウィザードを完了した後にDNS解決が機能しない場合は、管理インターフェイスのDNSのトラブルシューティングを参照してください。
- [ファイアウォールホスト名（Firewall Hostname）]：システムの管理アドレスのホスト名です。

ステップ4 システム時刻を設定し、[次へ（Next）]をクリックします。

- [タイムゾーン（Time Zone）]：システムのタイムゾーンを選択します。
- [NTPタイムサーバ（NTP Time Server）]：デフォルトのNTPサーバを使用するか、使用しているNTPサーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。

ステップ5 システムのスマートライセンスを設定します。

スマートライセンスのアカウントを取得し、システムが必要とするライセンスを適用する必要があります。最初は90日間の評価ライセンスを使用し、後でスマートライセンスを設定できます。

デバイスを今すぐ登録するには、デバイスを登録するオプションを選択し、リンクをクリックして Smart Software Manager アカウントにログインしてから、新しいトークンを生成して、そのトークンを編集ボックスにコピーします。また、サービスリージョンを選択し、Cisco Success Network に使用状況データを送信するかどうかを決定する必要もあります。画面上のテキストは、これらの設定について詳しく説明しています。

デバイスをまだ登録しない場合は、評価モードオプションを選択します。評価期間は最大 90 日です。後でデバイスを登録してスマートライセンスを取得する場合は、[デバイス（Device）] をクリックしてから、[Smart Licenses] グループでリンクをクリックします。

ステップ 6 [終了（Finish）] をクリックします。

次のタスク

- オプションライセンスでカバーされている機能（カテゴリベースの URL フィルタリング、侵入インスペクション、マルウェア対策など）を使用する場合は、必要なライセンスを有効にします。オプション ライセンスの有効化または無効化を参照してください。
- 他のデータインターフェイスを個々のネットワークに接続して、それらのインターフェイスを設定します。インターフェイスの設定の詳細については、サブネットを追加する方法およびインターフェイスを参照してください。
- 内部インターフェイスを使用してデバイスを管理する場合、内部インターフェイスで CLI セッションを開くには、内部インターフェイスで SSH 接続を開始します。管理アクセスリストの設定 を参照してください。
- 製品の使用方法については、使用例で学習してください。ベストプラクティス：Firewall Threat Defense の使用例 を参照してください。

外部インターフェイスの IP アドレスを取得できない場合の対処方法

デフォルトのデバイス設定には内部インターフェイスのスタティック IPv4 アドレスが含まれています。初期デバイス セットアップ ウィザードを使用してこのアドレスを変更することはできません。ただし、後で変更することはできます。

デフォルトの内部 IP アドレスが、デバイスに接続されている他のネットワークと競合する可能性があります。これは特に、外部インターフェイスで DHCP を使用してインターネット サービス プロバイダー（ISP）からアドレスを取得する場合に該当します。一部の ISP は、内部ネットワークと同じサブネットをアドレス プールとして使用しています。同じサブネットのアドレスを持つ 2 つのデータ インターフェイスを持つことはできないため、ISP からの競合するアドレスを外部インターフェイスに設定することはできません。

内部スタティック IP アドレスと外部インターフェイスの DHCP が提供するアドレスの間に競合がある場合は、接続図には、外部インターフェイスは管理上動作しているが IPv4 アドレスが割り当てられていないことが示されます。

この場合セットアップ ウィザードは正常に完了し、デフォルト NAT、アクセス、およびその他のポリシーや設定がすべて設定されます。競合を解消するには、次の手順に従います。

始める前に

ISP に正常に接続できることを確認します。サブネット競合がある場合外部インターフェイスのアドレスを取得できませんが、単に ISP への接続がない場合にも外部インターフェイスのアドレスを取得できません。

手順

ステップ 1 [デバイス（Device）] をクリックして、[インターフェイス（Interfaces）] サマリーのリンクをクリックします。

ステップ 2 内部インターフェイス行の [操作（Actions）] カラムにカーソルを置き、[編集（edit）] アイコン（  ）をクリックします。

ステップ 3 [IPv4アドレス（IPv4 Address）] タブで、一意のサブネットのスタティック アドレス（192.168.2.1/24、192.168.46.1/24 など）を入力します。デフォルトの管理アドレスは 192.168.45.45/24 であるため、このサブネットは使用しないでください。

また、内部ネットワークですでに DHCP サーバが実行されている場合は、DHCP を使用してアドレスを取得することもできます。ただし最初に、[このインターフェイスにDHCPサーバーを定義済み（DHCP SERVER IS DEFINED FOR THIS INTERFACE）] グループで [削除（Delete）] をクリックして、インターフェイスから DHCP サーバーを削除する必要があります。

ステップ 4 [このインターフェイスにDHCPサーバーを定義済み（DHCP SERVER IS DEFINED FOR THIS INTERFACE）] 領域で [編集（Edit）] をクリックして、DHCP プールを新しいサブネットの範囲に変更します（たとえば、192.168.2.5-192.168.2.254）。

ステップ 5 [OK] をクリックしてインターフェイスの変更を保存します。

ステップ 6 変更を展開するには、メニューの [展開（Deploy）] ボタンをクリックします。

ステップ 7 [今すぐ展開（Deploy Now）] をクリックします。

展開が完了すると、外部インターフェイスに IP アドレスが割り当てられていることが接続グラフィックで示されるはずです。内部ネットワークのクライアントを使用して、インターネットまたはその他のアップストリーム ネットワークに接続できることを確認します。

設定の基本

ここでは、デバイスの設定に関する基本的な手順について説明します。

デバイスの設定

Firewall Device Manager に最初にログインするとき、基本設定の構成のセットアップウィザードを利用できます。ウィザードを完了したら、次の方法を使用してその他の機能を設定し、デバイス設定を管理します。

各項目が視覚的に区別しにくい場合、ユーザー プロファイルから異なるカラー スキームを選択します。ページ右上の [ユーザー（user）] アイコンのドロップダウン メニューから、[プロファイル（Profile）] を選択します。

手順

ステップ 1 [デバイス（Device）] をクリックして **[デバイス概要（Device Summary）]** に移動します。

ダッシュボードには、有効なインターフェイスやキー設定が設定されているか（緑色）またはまだ設定が必要であるかなど、デバイスの視覚的なステータスが表示されます。詳細については、「インターフェイスと管理ステータスの表示 （37 ページ）」を参照してください。

ステータス イメージの上にはデバイス モデルの概要、ソフトウェア バージョン、VDB（システムと脆弱性のデータベース）バージョンがあり、前回の侵入ルールは更新されています。この領域には、機能を設定するためのリンクを含め、ハイ アベイラビリティ ステータスも表示されます。ハイアベイラビリティ（フェールオーバー）を参照してください。また、クラウド登録ステータスも表示されます。ここには、クラウド管理を使用している場合、デバイスが登録されているアカウントが表示されます。クラウド サービスの設定を参照してください。

イメージの下には設定可能なさまざまな機能のグループがあり、各グループの設定の概要、およびシステム設定を管理するために行うことができるアクションが表示されます。

ステップ 2 設定を行うか、またはアクションを実行するには、各グループのリンクをクリックします。

次に、グループの概要を示します。

- [インターフェイス（Interface）]：管理インターフェイスに加えて、少なくとも 2 つのデータインターフェイスを設定する必要があります。インターフェイスを参照してください。
- [ルーティング（Routing）]：ルーティングの設定。デフォルト ルートを定義する必要があります。他のルートは設定に応じて必要になります。ルーティングを参照してください。
- [更新（Updates）]：地理位置情報、侵入ルールと脆弱性のデータベースの更新、およびシステム ソフトウェアのアップグレード。これらの機能を使用する場合、最新のデータベースの更新情報を確実にするため、定期的な更新スケジュールを設定します。定期的なスケジュールの更新が発生する前に更新をダウンロードする必要がある場合にも、このページにアクセスできます。システム データベースおよびフィードの更新を参照してください。

- [システム設定（System Settings）]：このグループにはさまざまな設定が含まれます。デバイスの初期設定時に構成し、その後ほとんど変更しない基本設定などがあります。システム設定を参照してください。
- [スマートライセンス（Smart License）]：システム ライセンスの現在のステータスを示します。システムを使用するには、適切なライセンスをインストールする必要があります。一部の機能では追加のライセンスが必要です。システムのライセンスを参照してください。
- [バックアップと復元（Backup and Restore）]：システム設定をバックアップするか、以前のバックアップを復元します。システムのバックアップと復元を参照してください。
- [トラブルシューティング（Troubleshoot）]：Cisco Technical Assistance Center の依頼により、トラブルシューティング ファイルを生成します。トラブルシューティング ファイルの作成を参照してください。
- [サイト間VPN（Site-to-Site VPN）]：このデバイスとリモート デバイス間のサイト間バーチャル プライベート ネットワーク（VPN）接続。サイト間 VPN の管理を参照してください。
- [リモートアクセスVPN（Remote Access VPN）]：内部ネットワークへの外部クライアントの接続を可能にするリモートアクセス仮想プライベートネットワーク（VPN）構成です。リモート アクセス VPN の設定を参照してください。
- [詳細設定（Advanced Configuration）]：FlexConfig および Smart CLI を使用して、Firewall Device Manager を使用して設定できない機能を設定します。詳細設定を参照してください。
- [デバイス管理（Device Administration）]：監査ログを表示するか、設定のコピーをエクスポートします。監査と変更管理を参照してください。

ステップ 3 変更を展開するには、メニューの [展開（Deploy）] ボタンをクリックします。

変更は、それらを展開するまでデバイスで有効になりません。変更の展開 （33 ページ） を参照してください。

次のタスク

メイン メニューの [ポリシー（Policies）] をクリックし、システムのセキュリティ ポリシーを設定します。また、これらのポリシーで必要なオブジェクトを設定するには、[オブジェクト（Objects）] をクリックします。

セキュリティ ポリシーの設定

組織のアクセプタブル ユース ポリシーを実装して不正侵入やその他の脅威からネットワークを保護するにはセキュリティ ポリシーを使用します。

手順

ステップ 1 [ポリシー（Policies）] をクリックします。

[セキュリティポリシー（Security Policies）] ページには、システムを経由する接続の一般的な流れ、およびセキュリティ ポリシーが適用される順序が表示されます。

ステップ 2 ポリシーの名前をクリックして構成します。

アクセス制御ポリシーは常に必要ですが、各ポリシータイプを構成する必要はない場合があります。次に、ポリシーの概要を示します。

- [SSL復号（SSL Decryption）]：侵入、マルウェアなどについて暗号化された接続（HTTPSなど）を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するにはSSL復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。SSL 復号ポリシーの設定を参照してください。
- [アイデンティティ（Identity）]：個々のユーザーにネットワーク アクティビティを関連付ける、またはユーザーまたはユーザー グループのメンバーシップに基づいてネットワーク アクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザーを判定するためにアイデンティティ ポリシーを使用します。アイデンティティ ポリシーの設定を参照してください。
- [セキュリティ インテリジェンス（Security Intelligence）]：セキュリティ インテリジェンス ポリシーを使用して、選択されているIPアドレスまたはURLとの接続をすぐにドロップします。既知の不正なサイトをブロックすれば、アクセス制御ポリシーでそれらを考慮する必要がなくなります。シスコでは、セキュリティインテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスやURLの定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。セキュリティインテリジェンスの設定を参照してください。
- [NAT]（ネットワーク アドレス変換）：内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。NAT の設定を参照してください。
- [アクセス制御（Access Control）]：ネットワーク上で許可する接続の決定にアクセス コントロール ポリシーを使用します。セキュリティ ゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザーまたはユーザー グループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル（マルウェア）ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。アクセス コントロール ポリシーを設定するを参照してください。

- [侵入（Intrusion）]：侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。侵入ポリシーを参照してください。

ステップ 3 変更を展開するには、メニューの [展開（Deploy）] ボタンをクリックします。

変更は、それらを展開するまでデバイスで有効になりません。変更の展開 （33 ページ） を参照してください。

ルールまたはオブジェクトを検索

ポリシールールまたはオブジェクトのリストで全文検索を使用すると、編集する項目を探すことができます。これは、数百のルールのあるポリシーや長いオブジェクトリストを処理するときに特に便利です。

ルールとオブジェクトで検索を使用する方法は、任意のタイプのポリシー（侵入ポリシーを除く）またはオブジェクトの場合と同様です。[検索（Search）] フィールドに検索する文字列を入力し、Enter を押します。

この文字列は、ルールまたはオブジェクトの任意の部分に存在でき、部分文字列にすることができます。アスタリスク * は、0 個以上の文字に一致するワイルドカードとして使用できます。?、~、!、{、}、<、>、:、% の文字を含めないでください。検索文字列の一部としてサポートされていません。;、#、& の文字は無視されます。

文字列は、グループのオブジェクト内に出現することがあります。たとえば、IP アドレスを入力し、そのアドレスを指定するネットワークオブジェクトまたはグループを検索することができます。

完了したら、検索ボックスの右側にある [x] をクリックしてフィルタをクリアします。

変更の展開

ポリシーまたは設定を更新した場合、変更がすぐにはデバイスに適用されません。設定の変更には、次の 2 つの手順を実行します。

1. 変更を行います。
2. 変更を展開します。

この手順により、デバイスを「部分的に設定された」状態で実行することなく、関連する変更のグループ化を行えるようになります。ほとんどの場合、展開には変更だけが含まれます。ただし、必要に応じてシステムは設定全体を再適用し、それがネットワークを中断させる場合があります。さらに、いくつかの変更では検査エンジンの再起動が必要であり、この再起動中に

トラフィックがドロップされます。したがって、発生し得る混乱の影響が最小限になるタイミングで変更を展開するように検討してください。

（注） 展開ジョブが失敗した場合、システムは、一部の変更を以前の設定にロールバックする必要があります。ロールバックには、データプレーン設定のクリアと以前のバージョンの再展開が含まれます。これにより、ロールバックが完了するまでトラフィックが中断されます。

目的の変更を完了した後、次の手順を使用して変更を展開します。

注意 Firewall Threat Defense デバイスは、インスペクションエンジンがソフトウェアのリソースの問題が原因でビジー状態である、または設定の展開中にエンジンの再起動が必要なためダウンしているときに、トラフィックをドロップします。再起動が必要な変更の詳細については、インスペクション エンジンを再起動する設定の変更 （35 ページ）を参照してください。

手順

ステップ 1 Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

このアイコンは、展開されていない変更がある場合にドット マークで強調表示されます。

[保留中の変更（Pending Changes）] ウィンドウには、設定の展開バージョンと保留中の変更との比較が表示されます。それらの変更は、削除された要素、追加された要素、または編集された要素を示すために色分けされています。色の説明については、ウィンドウの凡例を参照してください。

展開でインスペクションエンジンの再起動が必要な場合は、再起動を必要とする変更の詳細を示すメッセージがページに表示されます。この時点で一時的なトラフィック損失を許容できない場合は、ダイアログを閉じ、変更を展開する良いタイミングを待ちます。

アイコンが強調表示されていない場合でも、アイコンをクリックすると最後に成功した展開ジョブの日時を確認できます。展開履歴を表示するリンクもあり、クリックすると展開ジョブだけを表示するようにフィルタ処理された監査ページに移動します。

ステップ 2 変更内容に問題がない場合は、[今すぐ展開（Deploy Now）] をクリックして、ジョブをすぐに開始できます。

ウィンドウに展開が進行中であることが示されます。ウィンドウを閉じるか、または展開が完了するまで待機できます。展開が進行中の間にウィンドウを閉じても、ジョブは停止しませ

ん。結果は、タスクリストや監査ログで確認できます。ウィンドウを開いたままにした場合、[展開履歴（Deployment History）] リンクをクリックすると結果が表示されます。

状況に応じて、次の手順を実行できます。

- [ジョブの命名（Name the Job）]：展開ジョブに名前を付けるには、[今すぐ展開（Deploy Now）] ボタンのドロップダウン矢印をクリックして、[展開ジョブの命名（Name the Deployment Job）] を選択します。名前を入力して [展開（Deploy）] をクリックします。名前は、ジョブの一部として監査および展開履歴に表示されるため、ジョブの検索が容易になります。

  たとえば、ジョブの名前を「DMZ Interface Configuration」にした場合、成功した展開の名前は「Deployment Completed: DMZ Interface Configuration」になります。さらに、その名前は、展開ジョブに関連する [タスク開始（Task Started）] イベントと [タスク完了（Task Completed）] イベントの [イベント名（Event Name）] として使用されます。

- [変更の破棄（Discard Changes）]：保留中の変更をすべて破棄するには、**[詳細オプション（More Options）] > [すべて破棄（Discard All）]** をクリックします。確認を求められます。

- [変更のコピー（Copy Changes）]：変更の一覧をクリップボードにコピーするには、**[詳細オプション（More Options）] > [クリップボードにコピー（Copy to Clipboard）]** をクリックします。このオプションは、変更の数が 500 未満の場合にのみ機能します。

- [変更のダウンロード（Download Changes）]：変更の一覧をファイルとしてダウンロードするには、**[詳細オプション（More Options）] > [テキストとしてダウンロード（Download as Text）]** をクリックします。自分のワークステーションにファイルを保存するように求められます。このファイルは YAML 形式です。YAML 形式に対応しているエディタがない場合は、テキスト エディタで表示できます。

インスペクション エンジンを再起動する設定の変更

設定の変更を展開した場合、次の設定またはアクションはいずれもインスペクションエンジンを再起動します。

注意 展開時に、リソース需要が高まった結果、いくつかのパケットがインスペクションなしでドロップされることがあります。さらに、一部の設定の展開では、インスペクションエンジンを再起動する必要があり、トラフィックインスペクションが中断され、トラフィックがドロップされます。

展開

一部の変更ではインスペクションエンジンの再起動が必要で、これにより一時的なトラフィック損失が発生します。インスペクションエンジンの再起動が必要な変更は、次のとおりです。

- SSL 復号ポリシーが有効化または無効化された。

- 1 つ以上の物理インターフェイス上（サブインターフェイスではありません）で MTU が変更された。
- アクセス制御ルールのファイル ポリシーを追加または削除します。
- VDB が更新された。
- 高可用性設定が作成または破棄された。

さらに、Snort プロセスがビジー状態で CPU の合計使用率が 60% を超えている場合、展開中に一部のパケットがドロップされることがあります。**show asp inspect-dp snort** コマンドを使用して、Snort の現在の CPU 使用率を確認できます。

システム データベースの更新

ルール データベースまたは VDB に更新プログラムをダウンロードした場合は、それらをアクティブにするために更新プログラムを展開する必要があります。この展開により、インスペクション エンジンが再起動される場合があります。手動で更新プログラムをダウンロードする、または更新プログラムのスケジュールを設定する場合は、ダウンロードが完了した後に、システムが変更を自動で展開する必要があるかどうかを指定できます。更新プログラムを自動的に展開するシステムがない場合は、次に変更を展開したときに更新プログラムが適用され、その際にインスペクション エンジンが再起動される場合があります。

システム アップデート

システムを再起動せずに、バイナリの変更が含まれるシステム更新プログラムまたはパッチをインストールする場合は、インスペクション エンジンを再起動する必要があります。バイナリの変更には、インスペクション エンジン、プリプロセッサ、脆弱性データベース（VDB）または共有オブジェクト ルールの変更が含まれることがあります。場合によって、バイナリの変更を含まないパッチで、Snort の再起動が必要になることもある点に注意してください。

完全な展開を強制するいくつかの変更の設定

ほとんどの場合、展開には変更だけが含まれます。ただし、必要に応じてシステムは設定全体を再適用し、それがネットワークを中断させる場合があります。次に、完全な展開を強制するいくつかの変更を示します。

- セキュリティ インテリジェンス ポリシーまたはアイデンティティ ポリシーは、最初は有効になっています。
- セキュリティ インテリジェンス ポリシーとアイデンティティ ポリシーの両方が無効になっています。
- データを再利用する場合の EtherChannel の作成。
- EtherChannel の削除。
- EtherChannel のメンバー インターフェイス アソシエーションの変更。
- 設定で使用されているインターフェイスの削除。たとえば、アクセス コントロール ルールで使用されるセキュリティ ゾーンの一部であるサブインターフェイスを削除します。

- FlexConfig ポリシーの一部である FlexConfig オブジェクトの変更、またはオブジェクトに negate 行が含まれていない場合のポリシーからのオブジェクトの削除。negate 行を省略すると、FlexConfig オブジェクトによって生成された設定を削除する特定の方法がないため、システムは強制的に完全に展開されます。各 FlexConfig オブジェクトに適切な negate 行を常に含めることで、この問題を回避できます。

インターフェイスと管理ステータスの表示

[デバイスの概要（Device Summary）]には、デバイスのグラフィカル ビューと管理アドレス用の設定が含まれています。[デバイスの概要（Device Summary）] を開くには、[デバイス（Device）] をクリックします。

このグラフィックの要素は、要素のステータスに基づいて色が変わります。要素をマウス オーバーすると、追加情報が提供される場合があります。このグラフィックを使用して、次の項目をモニターできます。

（注） インターフェイス ステータス情報を含む、グラフィックのインターフェイス部分は、[インターフェイス（Interfaces）] ページおよび **[モニタリング（Monitoring）]** > **[システム（System）]** ダッシュボードでも使用可能です。

Interface Status

ポートをマウス オーバーすると、その IP アドレスと有効なリンク ステータスが表示されます。IP アドレスはスタティックに割り当てることもできれば、DHCP を使用して取得することもできます。ブリッジ仮想インターフェイス（BVI）をマウス オーバーすると、メンバー インターフェイスのリストが表示されます。

インターフェイス ポートは、次のカラー コーディングを使用します。

- 緑：インターフェイスは設定され、有効で、リンクは稼働中です。
- グレー：インターフェイスは無効です。
- オレンジ/赤：インターフェイスが設定され、有効ですが、リンクがダウンしています。インターフェイスが有線の場合、これは修正が必要なエラー状態です。インターフェイスが有線でない場合、これは予期されるステータスです。

内部、外部ネットワーク接続

グラフィックは、次の条件に従い、外部（またはアップストリーム）ネットワークおよび内部ネットワークに接続されているポートを示します。

- 内部ネットワーク：「inside」という名前のインターフェイスの場合のみ、内部ネットワークのポートが表示されます。その他に内部ネットワークが存在する場合、それらは表示されません。いずれのインターフェイスにも「inside」と命名していない場合は、ポートは内部ポートとしてマークされません。

- 外部ネットワーク：「outside」という名前のインターフェイスの場合のみ、外部ネットワークのポートが表示されます。内部ネットワークと同様に、この名前は必須であり、存在しない場合は、ポートは外部ポートとしてマークされません。

管理設定のステータス

グラフィックは、管理アドレス用にゲートウェイ、DNS サーバー、NTP サーバー、スマートライセンスが設定されているかどうか、さらに、それらの設定が正常に機能しているかどうかを示します。

緑は機能が設定され正常に動作していることを示し、グレーは機能が設定されていないか、正常に動作していないことを示しています。たとえば、サーバーに到達不能な場合は、DNS ボックスがグレーになります。要素をマウス オーバーすると、詳細が表示されます。

問題が見つかった場合は、次のように修正します。

- 管理ポートおよびゲートウェイ：**[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** を選択します。
- DNSサーバー：**[システム設定（System Settings）]** > **[DNSサーバー（DNS Server）]** を選択します。
- NTPサーバー：**[システム設定（System Settings）]** > **[NTP]** を選択します。NTP のトラブルシューティングも参照してください。
- スマート ライセンス：[スマートライセンス（Smart License）] グループ内の [設定の表示（View Configuration）] リンクをクリックします。

システム タスク ステータスの表示

システム タスクには、さまざまなデータベースの更新の取得や適用など、直接関与することなく実行されるアクションが含まれます。これらのタスクのリストとそのステータスを表示し、これらのシステム タスクが正常に完了したことを確認できます。

タスクリストには、システムタスクと展開ジョブの統合ステータスが表示されます。監査ログにはより詳細な情報が含まれており、**[デバイス（Device）]** > **[デバイス管理（Device Administration）]** > **[監査ログ（Audit Log）]** の下にあります。たとえば、監査ログにはタスクの開始とタスクの終了ごとに個別のイベントが表示されます。一方、タスクリストではそれらのイベントが単一のエントリにマージされます。さらに、展開の監査ログエントリには、展開された変更に関する詳細情報が含まれています。

手順

ステップ 1 メインメニューの [タスクリスト（Task List）] ボタンをクリックします。

タスクリストが開き、システムタスクのステータスと詳細が表示されます。

ステップ 2 タスクのステータスを評価します。

永続的な問題がある場合は、デバイス設定を修正する必要があります。たとえば、データベースの更新を永続的に取得できない場合、デバイスの管理 IP アドレスにインターネットへのパスがないと示される場合があります。タスクの説明に挙げられている問題については、Cisco Technical Assistance Center（TAC）に問い合わせる必要があります。

タスク リストでは、次の操作を実行できます。

- これらのステータスに基づいてリストをフィルタするには、[成功（Success）] または [失敗（Failures）] ボタンをクリックします。
- タスクをリストから削除するには、[削除（delete）] アイコン（  ）をクリックします。
- 進行中でないすべてのタスクのリストを空にするには、[完了したタスクをすべて削除（Remove All Completed Tasks）] をクリックします。

CLI コンソールを使用した設定の監視およびテスト

Firewall Threat Defense デバイスには、監視およびトラブルシューティングに使用できる CLI（コマンド ライン インターフェイス）が組み込まれています。SSH セッションを開いてすべてのシステムコマンドにアクセスすることはできますが、Firewall Device Manager で CLI コンソールを開いて、さまざまな **show** コマンド、**ping**、**traceroute**、および **packet-tracer** などの読み取り専用コマンドを使用することもできます。管理者権限を持っている場合は、**failover**、**reboot**、および **shutdown** コマンドを入力することもできます。

ページ間の移動、設定、および機能の展開を行っている間、CLI コンソールを開いたままにしておくことができます。たとえば、新しいスタティックルートを展開した後で、CLI コンソールで **ping** を使用して、ターゲットネットワークに到達できることを確認できます。

CLI コンソールでは基本 Firepower Threat Defense CLI を使用します。CLI コンソールを使用して、診断 CLI、エキスパート モード、および FXOS CLI（FXOS を使用するモデル）に入ることはできません。このような他の CLI モードに入る必要がある場合は、SSH を使用します。

コマンドの詳細については、Cisco Firepower Threat Defense コマンド リファレンス、https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.htmlを参照してください。

注：

- **ping** は CLI コンソールでサポートされていますが、**ping system** コマンドはサポートされていません。
- システムは最大で2つのコマンドを同時に処理できます。そのため、別のユーザが（たとえば、REST API を使用して）コマンドを発行している場合は、その他のコマンドの完了を待ってからコマンドを入力する必要があります。問題が解決しない場合は、CLI コンソールの代わりに SSH セッションを使用します。

- コマンドは、展開された設定に基づいて情報を返します。Firewall Device Manager で設定を変更しても、展開していない場合は、コマンド出力に変更の結果が表示されません。たとえば、新しいスタティックルートを作成しても展開していない場合、そのルートは**show route** 出力に表示されません。

手順

ステップ 1 Web ページの右上にある [CLIコンソール（CLI Console）] ボタンをクリックします。

ステップ 2 プロンプトにコマンドを入力し、[Enter] を押します。

コマンドの中には他より出力まで時間がかかるものもありますが、しばらくお待ちください。コマンドの実行がタイムアウトになったというメッセージが表示されたら、もう一度試してください。**show perfstats** など、対話型の応答が必要なコマンドを入力した場合にも、タイムアウトエラーが発生します。問題が解決しない場合は、CLI コンソールの代わりに SSH クライアントを使用する必要があります。

このウィンドウを使用する方法について、いくつかのヒントを次に示します。

- コマンドの一部を入力した後で [Tab] キーを押すと、オート コンプリートが作動します。また、Tab はコマンド内のその位置で使用可能なパラメータをリストします。また、Tab は 3 つのレベルまでキーワードを示します。3 つのレベルを過ぎると、コマンド リファレンスを使用して詳細を確認する必要があります。
- コマンドの実行を停止するには、Ctrl+C を押します。
- ウィンドウを移動するには、ヘッダー内の任意の箇所をクリックしたままウィンドウを目的の位置にドラッグします。
- ウィンドウサイズを変更するには、[展開（Expand）] （）または [折りたたみ（Collapse）] （  ）ボタンをクリックします。
- [別のウィンドウに切り離す（Undock Into Separate Window）] （）ボタンをクリックすると、ウィンドウが Web ページから独自のブラウザ ウィンドウに切り離されます。再度ドッキングするには、[メインウィンドウにドッキング（Dock to Main Window）] （  ）ボタンをクリックします。
- クリックしてドラッグすると、テキストが強調表示されます。次に Ctrl+C を押すと、出力がクリップボードにコピーされます。
- すべての出力を消去するには、[CLIのクリア（Clear CLI）] （  ）ボタンをクリックします。
- [最後の出力のコピー（Copy Last Output）] （）ボタンをクリックすると、最後に入力したコマンドからの出力がクリップボードにコピーされます。

ステップ 3 完了したら、コンソール ウィンドウを閉じます。**exit** コマンドは使用しないでください。

Firewall Device Manager へのログインに使用するクレデンシャルにより CLI へのアクセスが検証されますが、コンソール使用時は実際には CLI にログインしていません。

Firewall Device Manager と REST API の併用

ローカル管理モードでデバイスをセットアップする場合、FDM と Firepower Threat Defense REST API を使用してデバイスを設定できます。実際には、Firewall Device Manager は REST API を使用してデバイスを設定します。

ただし、REST API は Firewall Device Manager で利用できる機能に加えて、その他の機能を提供できることを理解してください。したがって、所定の機能について、Firewall Device Manager で設定を確認するときには表示できない、REST API を使用した設定を行うことができます。

REST API で利用できて Firewall Device Manager で利用できない機能を設定する場合は、設定が完了していない可能性がある、Firewall Device Manager を使用したすべての機能（リモートアクセス VPN など）に変更を加えます。API のみの設定が維持されるかどうかは場合によって異なります。多くの場合、Firewall Device Manager で使用できない設定への API の変更は Firewall Device Manager の編集により維持されます。所定の機能については、変更が維持されているかどうかを確認する必要があります。

一般的には、所定の機能について Firewall Device Manager と REST API の両方を同時に使用しないようにする必要があります。代わりに、デバイスを設定するために、機能ごとにいずれかの方法を選択します。

APIエクスプローラを使用してAPIメソッドを表示および試すことができます。[詳細オプション（More options）] ボタン（⋮）をクリックし、[APIエクスプローラ（API Explorer）] を選択します。

通信ポートとインターネットアクセス要件

以下のトピックでは、デバイスで利用可能なすべての機能を動作させるために、デバイスで開いている必要があるポートと、アクセスが必要なインターネットサイトについて説明します。制限方式またはエアギャップ方式で運用している場合は、要件を満たすために、これらのポートとインターネットサイトの一部またはすべてをブロックできます。それ以外の場合は、これらのポートが開いていて、これらのサイトにアクセス可能であることを確認します。

デバイスで使用される通信ポート

次の表に、さまざまなサービス用に開いている必要があるポートを示します。アクセス制御ルールを使用して、サービスに面するインターフェイス、または関連付けられたプロトコルを使用してデバイスにアクセスできる必要があるユーザーに面するインターフェイスで、これら

のポートへのアクセスが開かれていることを確認します。機能を使用しない場合は、これらのポートを閉じたままにできます。

表 2: インバウンドポート

インバウンドポート	プロトコル/機能	詳細
TCP/22	SSH	アプライアンス コマンド ライン インターフェイスへのリモート接続を保護します。 （注） **copy** コマンド、または外部通信を実行する別のコマンドを使用する場合は、そのアウトバウンドポートを開く必要があります。たとえば、FTP を使用する場合は TCP/20、21 です。
UDP/161	SNMP	SNMP ポーリング経由で MIB にアクセスできるようにします。
TCP/443	HTTPS	次のサービスに使用されます。 • FDM への管理接続。 • Firepower Threat Defense REST API • リモートアクセス VPN SSL 接続。RA VPN のカスタムポートを設定する場合は、そのポートを開きます。
TCP/885	キャプティブ ポータル	キャプティブ ポータルのアイデンティティ ソースと通信します。これがデフォルトポートです。別のポートを設定する場合は、カスタムポートを開きます。詳細については、アイデンティティ ポリシー設定の構成 を参照してください。
TCP/8989	Cisco Support Diagnostics	許可された要求を受け入れます。また、このポートで接続を開始します。

表 3: アウトバウンドポート

アウトバウンドポート	プロトコル/機能	詳細
UDP/53 （使用している場合。）TCP/53	DNS	DNS 用です。通常、UDP/53 が DNS に使用されます。ただし、DNS over TCP を使用する場合は、TCP/53 も開きます。
UDP/67 UDP/68	DHCP	DHCP 用です。
UDP/123	NTP	時刻を同期します。
UDP/162	SNMP	リモート トラップ サーバーに SNMP アラートを送信します。

アウトバウンドポート	プロトコル/機能	詳細
TCP/389 TCP/636	LDAP、LDAPS	外部認証用に LDAP サーバーと通信します。 カスタムポートを設定する場合は、そのポートを開きます。AD アイデンティティ レルムの設定を参照してください。
TCP/443	HTTPS	インターネットとの間でデータを送受信します（データベースの更新のダウンロードなど）。
UDP/514	Syslog	リモート syslog サーバーにシステムログメッセージを送信します。
UDP/1812 UDP/1813	RADIUS	外部認証とアカウンティングのために RADIUS サーバーと通信します。 カスタムポートを設定する場合は、そのポートを開きます。RADIUS サーバーの設定を参照してください。
UDP/8514	Secure Network Analytics Manager	クラウドに syslog メッセージを送信します。
TCP/8989	Cisco Support Diagnostics	使用状況情報および統計情報を送信します。このポートの接続も受け入れます。

デバイスがアクセスするインターネットリソース

次の機能が正しく動作するには、関連するインターネットリソースにアクセスできる必要があります。デバイスは、必要に応じてポート TCP/80 および TCP/443 を使用します。

表 *4*: デバイスがアクセスするインターネットリソース

機能	理由	高可用性	リソース
CA 証明書バンドル	システム定義により毎日決まった時刻に、新しいCA証明書についてクエリを実行します。ローカルCAバンドルには、いくつかのシスコのサービスにアクセスするための証明書が含まれています。 この機能は、CLI で **configure cert-update auto-update** コマンドを使用して構成されます。 7.0(5)、7.1(0.3)、7.2(4)、7.3 以降のバージョンで利用できます。	各ピアがそれぞれの証明書をダウンロードします。	cisco.com/security/pki/

機能	理由	高可用性	リソース
Malware Defense 1	AMP Cloud ルックアップ。	両方のピアが検索を実行します。	適切な Cisco Secure Endpoint およびマルウェア分析操作に必要なサーバーアドレス
	ファイル事前分類とローカルのマルウェア分析のシグニチャ更新をダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	動的分析のためにファイルを送信します。 動的分析結果のクエリ。	両方のピアが動的分析レポートの送信または、クエリを実行します。	fmc.api.threatgrid.com fmc.api.threatgrid.eu fmc.api.threatgrid.ca fmc.api.threatgrid.com.au fmc.api.threatgrid.in
セキュリティ インテリジェンス	セキュリティ インテリジェンス フィードをダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	intelligence.sourcefire.com
URL フィルタリング	URL カテゴリおよびレピュテーション データをダウンロードします。 URL カテゴリおよびレピュテーション データを手動でクエリ（ルックアップ）します。 未分類 URL のクエリ。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	URL： • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates-dyn-talos.sco.cisco.com • updates.ironport.com IPv4 ブロック： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPv6 ブロック： • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48
Cisco Smart Software Manager	Smart Software Manager と通信します。	アクティブなピアが通信します。	www.cisco.com

機能	理由	高可用性	リソース
Cisco Success Network	使用状況情報および統計情報を送信します。	アクティブなピアが通信します。	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com
Cisco Support Diagnostics	許可された要求を受け入れ、使用状況の情報と統計情報を送信します。	アクティブなピアが通信します。	api-sse.cisco.com:8989
一般的なクラウドサービス	—	—	api sse.cisco.com
Cisco XDR 統合	イベントを Cisco Security Cloud に送信するようにデバイスを構成します。	アクティブなピアが通信します。	Cisco Secure Firewall Threat Defense と Cisco XDR 統合ガイド
時刻の同期	展開内で時間を同期します。 プロキシ サーバではサポートされません。	両方のピアが NTP サーバーと通信します。	ユーザーにより設定済み。 デフォルトのサーバー： • 0.sourcefire.pool.ntp.org • 1.sourcefire.pool.ntp.org • 2.sourcefire.pool.ntp.org
侵入ルール	侵入ルール（SRU/LSP）をダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	talosintelligence.com
脆弱性データベース	VDB アップデートをダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	support.sourcefire.com
地理位置情報データベース	GeoDB アップデートをダウンロードします。	アクティブ ピアでダウンロードが実行され、スタンバイへ同期します。	support.sourcefire.com

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。