



使用する前に

次のトピックでは、Secure Firewall Threat Defense（旧称 Firepower Threat Defense）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](#)（1 ページ）
- [Device Manager /Threat Defense バージョン 7.4.1 の新機能](#)（1 ページ）
- [システムへのログイン](#)（6 ページ）
- [システムの設定](#)（11 ページ）
- [設定の基本](#)（36 ページ）

このガイドの対象読者

このマニュアルでは、脅威に対する防御デバイスに組み込まれた Secure Firewall Device Manager（旧称 Firepower Device Manager）の Web ベース設定インターフェイスを使用して脅威に対する防御を設定する方法について説明します。

Device Manager 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、これは多くの脅威に対する防御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、または脅威に対する防御で許可される、より複雑な機能や設定を使用したい場合は、組み込みの Device Manager の代わりに Secure Firewall Management Center（旧称 Firepower Management Center）を使用してデバイスを設定します。

Device Manager /Threat Defense バージョン 7.4.1 の新機能

リリース日：2023 年 12 月 13 日

次の表に、Device Manager を使用して構成した場合に脅威に対する防御 7.4.1 で使用可能な新規機能を示します。

機能	説明
プラットフォーム機能	
Firepower 1010E のサポートが再開されています。。	バージョン 7.2.3 で導入され、バージョン 7.3 で一時的に廃止された Firepower 1010E のサポートが再開されています。
Cisco Secure Firewall 3130 および 3140 向けのネットワークモジュール。	<p>Cisco Secure Firewall 3130 および 3140 向けに次のネットワークモジュールが導入されました。</p> <ul style="list-style-type: none"> • 2 ポート 100G QSFP+ ネットワークモジュール (FPR3K-XNM-2X100G) <p>参照 : Cisco Secure Firewall 3110、3120、3130、3140 ハードウェア設置ガイド</p>
VPN 機能	
Cisco Secure Firewall 3100 向け VTI ループバック インターフェイスの IPSec フローのオフロード。	<p>アップグレードの影響。条件を満たす接続のオフロードが開始されます。</p> <p>Cisco Secure Firewall 3100 では、VTI ループバック インターフェイスを介した適格な IPSec 接続がデフォルトでオフロードされるようになりました。以前は、この機能は物理インターフェイスでのみサポートされていました。この機能はアップグレードにより自動的に有効になります。</p> <p>FlexConfig と flow-offload-ipsec コマンドを使用して構成を変更できます。</p>
インターフェイス機能	

機能	説明
<p>マージされた管理インターフェイスと診断インターフェイス。</p>	<p>アップグレードの影響。アップグレード後にインターフェイスをマージします。</p> <p>7.4以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。7.4以降にアップグレードし、診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。</p> <p>7.4以降にアップグレードし、診断インターフェイスの設定がある場合は、インターフェイスを手動でマージすることも、診断インターフェイスを引き続き個別に使用することもできます。ただし、診断インターフェイスのサポートは今後のリリースで廃止されるため、できるだけ早くインターフェイスをマージしてください。</p> <p>マージモードでは、デフォルトでデータルーティングテーブルを使用するように AAA トラフィックの動作も変更されます。管理専用ルーティングテーブルは、設定で管理専用インターフェイス（管理を含む）を指定した場合にのみ使用できるようになりました。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [Devices] > [Interfaces] > [Management] インターフェイス • (インターフェイスに移動) [System Settings] > [Management Interface] • [Devices] > [Interfaces] > [Merge Interface action needed] > [Management Interface Merge] <p>新規/変更されたコマンド：show management-interface convergence</p>
<p>Azure と GCP 上の 3 つのインターフェイスを使用して Threat Defense Virtual を展開します。</p>	<p>Azure と GCP で (4 つではなく) 3 つのインターフェイスを使用して Threat Defense Virtual を展開できるようになりました。そのためには、診断インターフェイスを削除します。</p> <p>制約事項：この機能は、新規展開でのみサポートされます。アップグレードされたデバイスではサポートされていません。</p> <p>参照：Cisco Secure Firewall Threat Defense Virtual スタートアップガイド</p>
<p>Firepower 1000 シリーズ、Firepower 2100、および Cisco Secure Firewall 3100 に対するインラインセット。</p>	<p>Firepower 1000 シリーズ、Firepower 2100、および Cisco Secure Firewall 3100 デバイスでインラインセットを設定できます。[インターフェイス (Interface)] ページに [インラインセット (inline sets)] タブを追加しました。</p>

機能	説明
ライセンス機能	
<p>ライセンス名の変更およびキャリアライセンスのサポート。</p>	<p>ライセンス名が次のように変更されました。</p> <ul style="list-style-type: none"> • Threat は IPS に変更 • Malware は Malware Defense に変更 • Base は Essentials に変更 • AnyConnect Apex は Secure Client Premier に変更 • AnyConnect Plus は Secure Client Advantage に変更 • AnyConnect VPN Only は Secure Client VPN Only に変更 <p>さらに、キャリアライセンスを適用できるようになりました。これにより、GTP/GPRS、Diameter、SCTP、および M3UA インスペクションを設定できます。これらの機能を設定するには、FlexConfig を使用します。</p>
管理およびトラブルシューティングの機能	
<p>デフォルトの NTP サーバーが更新されました。</p>	<p>アップグレードの影響。 システムは新しいリソースに接続します。</p> <p>デフォルトの NTP サーバーは、sourcefire.pool.ntp.org から time.cisco.com に変更されました。別の NTP サーバーを使用するには、[デバイス (Device)] を選択し、[システム設定 (System Settings)] パネルで [タイムサービス (Time Services)] をクリックします。</p>
<p>HTTPS 管理ユーザーアクセス用の SAML サーバー。</p>	<p>HTTPS 管理アクセスに外部認証を提供するように SAML サーバーを設定できます。外部ユーザーには、管理者、監査管理者、暗号管理者、読み取り/書き込みユーザー、読み取り専用ユーザーの認証アクセスタイプを設定できます。SAML サーバーを使用する場合は、ログインに共通アクセスカード (CAC) を使用できます。</p> <p>SAML アイデンティティ ソース オブジェクトの設定を更新し、該当オブジェクトを受け入れるように [システム設定 (System Settings)] > [管理アクセス (Management Access)] ページを更新しました。</p>

機能	説明
<p>Threat Defense 高可用性ペアの設定の不一致を検出します。</p>	<p>CLI を使用して、Threat Defense 高可用性ペアの設定の不一致を検出できるようになりました。</p> <p>新規/変更された CLI コマンド：show failover config-sync error、show failover config-sync stats</p> <p>参照：Cisco Secure Firewall Threat Defense コマンドリファレンス</p>
<p>Cisco Secure Firewall 3100 でドロップされたパケットをキャプチャします。</p>	<p>MAC アドレステーブルの不整合に起因するパケット損失は、デバッグ機能に影響を与える可能性があります。Cisco Secure Firewall 3100 は、これらのドロップされたパケットをキャプチャできるようになりました。</p> <p>新規/変更された CLI コマンド：capture コマンドの [drop {disable mac-filter}]。</p> <p>参照：Cisco Secure Firewall Threat Defense コマンドリファレンス</p>
<p>FXOS アップグレードに含まれるファームウェアのアップグレード。</p>	<p>シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。</p> <p>Firepower 4100/9300 の場合、バージョン 2.14.1 以降への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。</p> <p>ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアのアップグレード中は手動で再起動またはシャットダウンしないでください。</p> <p>参照：Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド</p>

機能	説明
Firepower 1000/2100 および Firepower 4100/9300 のデータプレーン障害後の迅速な回復。	<p>Firepower 1000/2100 または Firepower 4100/9300 のデータプレーンプロセスがクラッシュすると、デバイスを再起動する代わりにプロセスがリロードされます。データプレーンをリロードすると、Snort を含む他のプロセスも再起動します。ブートアップ中にデータプレーンがクラッシュした場合、デバイスは通常のリロード/リブートシーケンスに従うため、リロードループが回避されます。</p> <p>この機能は、新しいデバイスとアップグレードされたデバイスの両方でデフォルトで有効になっています。無効にするには、FlexConfig を使用します。</p> <p>新規/変更された ASA CLI コマンド：data-plane quick-reload、show data-plane quick-reload status</p> <p>新規/変更された Threat Defense CLI コマンド：show data-plane quick-reload status</p> <p>サポートされているプラットフォーム：Firepower 1000/2100、Firepower 4100/9300</p> <p>参照：Cisco Secure Firewall Threat Defense コマンドリファレンス および Cisco Secure Firewall ASA シリーズ コマンドリファレンス</p>

システムへのログイン

脅威に対する防御 デバイスには、次の 2 つのインターフェイスがあります。

Device Manager Web インターフェイス

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。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、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。

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。

admin
Administrator 

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 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ー (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、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。
- [暗号管理者 (Cryptographic Admin)] : 証明書、復号ポリシー、秘密キーなどの暗号化関連機能を設定できます。他の機能への読み取り専用アクセス。
- [監査管理者 (Audit Admin)] : ユーザーのログイン履歴と監査ログを表示し、監査関連のアクションを実行できます。設定機能への読み取り専用アクセス。

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。

Device Manager へのログイン

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 Device Manager にログインできます。ただし、[Device Manager および 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（28 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 （ローカルユーザーおよびRADIUSのみ）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。



ステップ3 （SAML サーバーのみ）[ログイン (Login)] ボタンの横にある [シングルサインオン (SSO) (Single-Sign On (SSO))] リンクをクリックします。

これにより、ログイン用の SAML サーバーに移動します。ログイン情報を入力しないでください。リンクをクリックするだけです。ローカルのログイン情報を入力して[ログイン (Login)] をクリックすると、ローカルデータベースを使用してログインします。

SAML サーバーのログインページで、通常どおりにログインします。ログインに共通アクセスカード (CAC) を使用する場合は、リンクをクリックして証明書を使用してサインインします。デバイスマネージャは、CAC 認証を直接処理しません。

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 および Secure Firewall デバイスモデルでは、コンソールポートの CLI は Secure Firewall eXtensible オペレーティングシステム (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脅威に対する防御 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 はシャード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脅威に対する防御 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。

- Threat Defense Virtual 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** ユーザー名または別の CLI ユーザー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、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。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、[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、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、[プロフィール (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。

[生成 (Generate)] をクリックすると、ランダムな 16 文字のパスワードが生成されます。[パスワードの表示 (Show Password)] () ボタンをクリックして、マスクされていないパス

ワードを表示します。次に、[クリップボードにコピー (Copy To Clipboard)] リンクをクリックして、[確認 (Confirm)] フィールドにパスワードを貼り付けます。

このページには、パスワードの最小要件が含まれています。これらの最小要件は変更できません。パスワードは次のとおりです。

- 8 ~ 128 文字である
- 小文字と大文字がそれぞれ 1 文字以上含まれている
- 数字が 1 桁以上含まれている
- 特殊文字が 1 文字以上含まれている
- 同じ文字の繰り返しが含まれていない

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、[プロフィール (Profile)] を選択します。



ステップ 2 [プロフィール (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。

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（28 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（12 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（24 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（31 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。

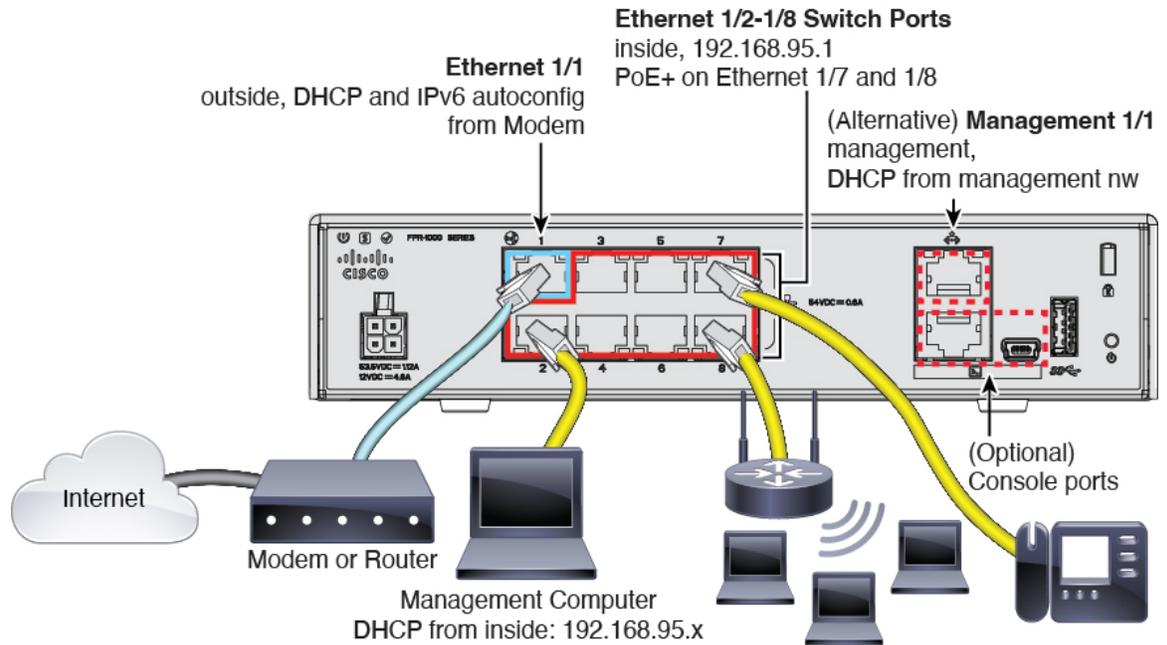
大半のモデルのデフォルト設定は、管理コンピュータを内部インターフェイスに接続するように設計されています。あるいは、管理ポートに直接ワークステーションを接続することもできます。インターフェイスはさまざまなネットワーク上にあるため、内部インターフェイスと管理ポートを同じネットワークに接続しようとしないでください。

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。

次に、デバイスを設定するために内部インターフェイスを使用するときの、このトポロジでのシステムの配線方法を示します。

Firepower 1010 のケーブル配線

図 1: Firepower 1010 のケーブル配線



- 管理コンピュータを次のいずれかのインターフェイスに接続します。
 - イーサネット 1/2 ~ 1/8 : 管理コンピュータを内部スイッチポートのいずれかに直接接続します (イーサネット 1/2 ~ 1/8)。内部にはデフォルトの IP アドレス (192.168.95.1) があり、クライアント (管理コンピュータを含む) に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください。
 - 管理 1/1 : 管理コンピュータを管理ネットワークに接続します。管理 1/1 インターフェイスは、DHCP から IP アドレスを取得するため、ネットワークに DHCP サーバーが含まれていることを確認してください。

Management 1/1 IP アドレスをデフォルトから変更し、静的 IP アドレスを設定する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要があります。「[\(任意\) CLI での管理ネットワーク設定の変更 \(22 ページ\)](#)」を参照してください。

後で、他のインターフェイスから管理アクセスを設定できます。

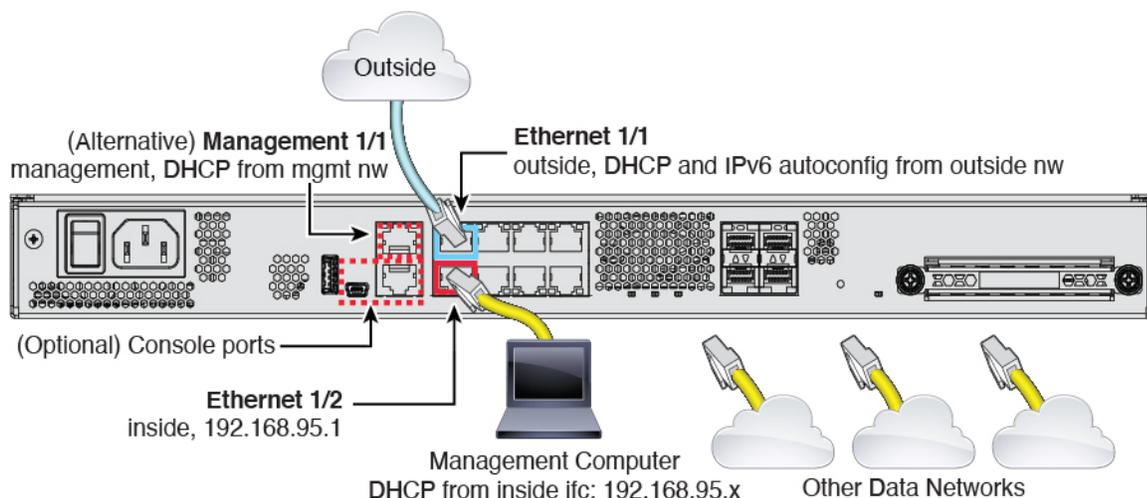
- 外部ネットワークを Ethernet 1/1 インターフェイスに接続します。
デフォルトでは、IP アドレスは IPv4 DHCP および IPv6 自動設定を使用して取得しますが、初期設定時に静的アドレスを設定できます。
- 内部デバイスを残りのスイッチポート (Ethernet 1/2 ~ 1/8) に接続します。
Ethernet 1/7 および 1/8 は Power over Ethernet+ (PoE+) ポートです。



(注) PoE は Firepower 1010E ではサポートされていません。

Firepower 1100 のケーブル配線

図 2: Firepower 1100 のケーブル配線



- 管理コンピュータを次のいずれかのインターフェイスに接続します。
 - Ethernet 1/2 : 初期設定のために管理コンピュータを Ethernet 1/2 に直接接続するか、Ethernet 1/2 を内部ネットワークに接続します。イーサネット 1/2 にはデフォルトの IP アドレス (192.168.95.1) があり、クライアント (管理コンピュータを含む) に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください。
 - Management 1/1 (ラベル「MGMT」) : 管理コンピュータを管理ネットワークに接続します。管理 1/1 インターフェイスは、DHCP から IP アドレスを取得するため、ネットワークに DHCP サーバーが含まれていることを確認してください。

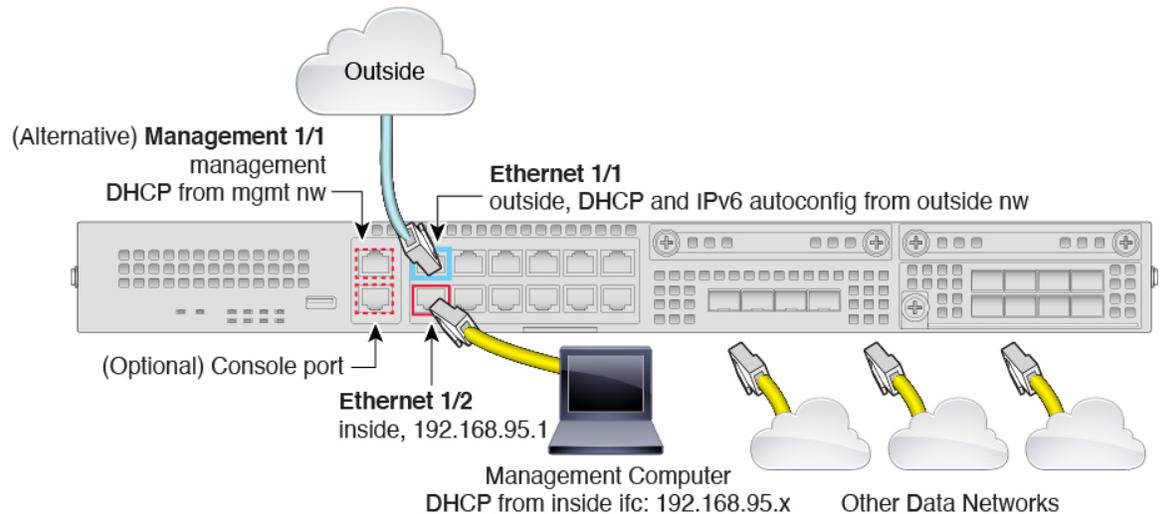
Management 1/1 IP アドレスをデフォルトから変更し、静的 IP アドレスを設定する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要があります。「[\(任意\) CLI での管理ネットワーク設定の変更 \(22 ページ\)](#)」を参照してください。

後で、他のインターフェイスから管理アクセスを設定できます。

- 外部ネットワークを Ethernet 1/1 インターフェイス (ラベル「WAN」) に接続します。
デフォルトでは、IP アドレスは IPv4 DHCP および IPv6 自動設定を使用して取得しますが、初期設定時に静的アドレスを設定できます。
- 残りのインターフェイスに他のネットワークを接続します。

Firepower 2100 のケーブル配線

図 3: Firepower 2100 のケーブル配線



- 管理コンピュータを次のいずれかのインターフェイスに接続します。
 - Ethernet 1/2 : 初期設定のために管理コンピュータを Ethernet 1/2 に直接接続するか、Ethernet 1/2 を内部ネットワークに接続します。イーサネット 1/2 にはデフォルトの IP アドレス (192.168.95.1) があり、クライアント (管理コンピュータを含む) に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください。
 - Management 1/1 (ラベル「MGMT」) : 管理コンピュータを管理ネットワークに接続します。管理 1/1 インターフェイスは、DHCP から IP アドレスを取得するため、ネットワークに DHCP サーバーが含まれていることを確認してください。

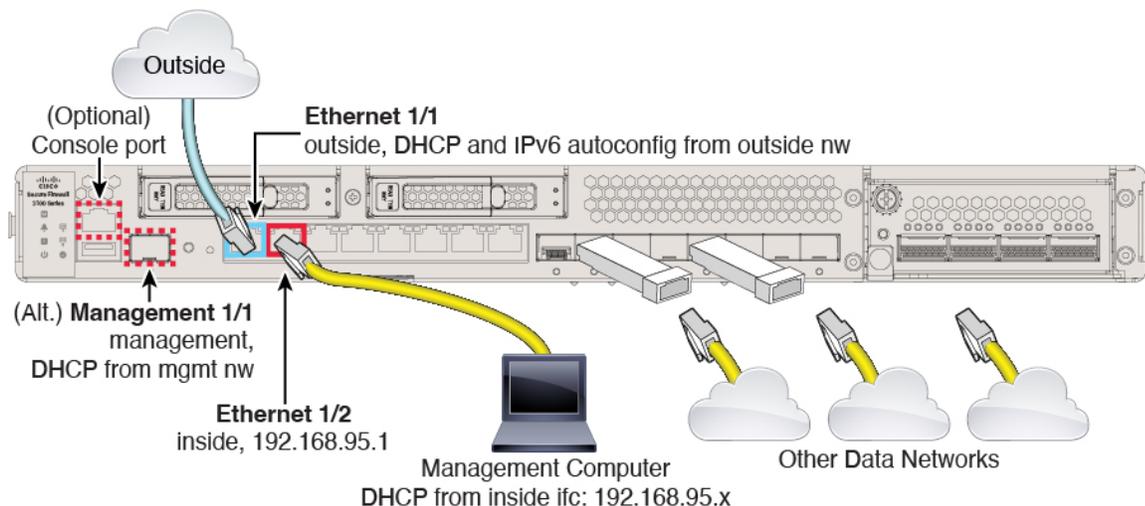
Management 1/1 IP アドレスをデフォルトから変更し、静的 IP アドレスを設定する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「[\(任意\) CLI での管理ネットワーク設定の変更 \(22 ページ\)](#)」を参照してください。

後で、他のインターフェイスから管理アクセスを設定できます。

- 外部ネットワークを Ethernet 1/1 インターフェイス (ラベル「WAN」) に接続します。デフォルトでは、IP アドレスは IPv4 DHCP および IPv6 自動設定を使用して取得しますが、初期設定時に静的アドレスを設定できます。
- 残りのインターフェイスに他のネットワークを接続します。

Cisco Secure Firewall 3100 のケーブル配線

図 4: Cisco Secure Firewall 3100 のケーブル接続



Management 1/1 または Ethernet 1/2 のいずれかで Threat Defense デバイスを管理します。デフォルト設定でも、Ethernet1/1 を外部として設定します。

- 管理コンピュータを次のいずれかのインターフェイスに接続します。
 - Ethernet 1/2 : 初期設定のために管理コンピュータを Ethernet 1/2 に直接接続するか、Ethernet 1/2 を内部ネットワークに接続します。Ethernet 1/2 にはデフォルトの IP アドレス (192.168.95.1) があり、(管理コンピュータを含む) クライアントに IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の内部ネットワークの設定と競合しないようにしてください。
 - Management 1/1 : Management 1/1 を管理ネットワークに接続し、管理コンピュータが管理ネットワーク上にあるか、またはアクセスできることを確認します。Management 1/1 は、管理ネットワーク上の DHCP サーバーから IP アドレスを取得します。このインターフェイスを使用する場合は、管理コンピュータから IP アドレスに接続できるように、ファイアウォールに割り当てられる IP アドレスを決定する必要があります。

Management 1/1 IP アドレスをデフォルトから変更し、静的 IP アドレスを設定する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「[\(任意\) CLI での管理ネットワーク設定の変更 \(22 ページ\)](#)」を参照してください。



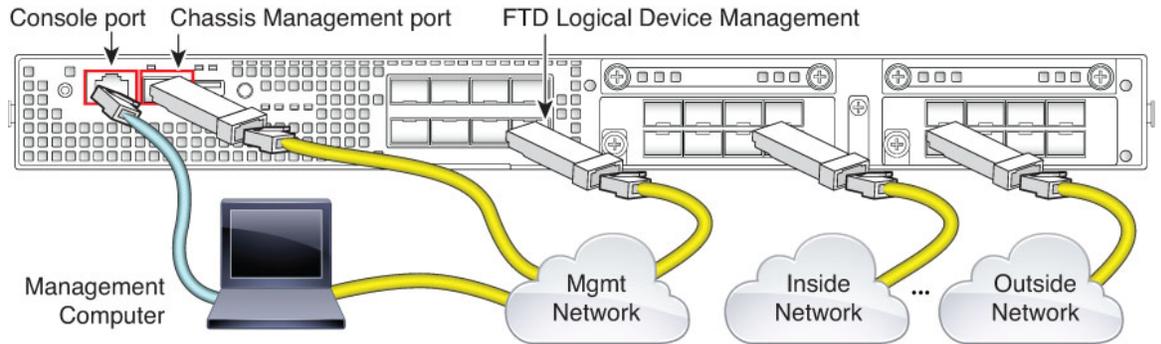
(注) Management 1/1 は、SFP モジュールを必要とする 10 Gb 光ファイバインターフェイスです。

- 外部ネットワークを Ethernet1/1 インターフェイスに接続します。

デフォルトでは、IP アドレスは IPv4 DHCP および IPv6 自動設定を使用して取得しますが、初期設定時に静的アドレスを設定できます。

- 残りのインターフェイスに他のネットワークを接続します。

Firepower 4100 のケーブル配線



論理デバイスの管理インターフェイスで脅威に対する防御の初期設定を実行します。後で、任意のデータ インターフェイスから管理を有効にすることができます。脅威に対する防御 デバイスでは、ライセンスと更新にインターネットアクセスが必要です。デフォルトの動作では、デバイスの展開時に指定したゲートウェイ IP アドレスに管理トラフィックをルーティングします。そうではなく、バックプレーンを介してデータインターフェイスに管理トラフィックをルーティングする必要がある場合は、後で **Device Manager** でその設定が行えます。

シャーシの初期設定、継続的なモニタリング、論理デバイスの使用には、次のインターフェイスにケーブルを配線します。

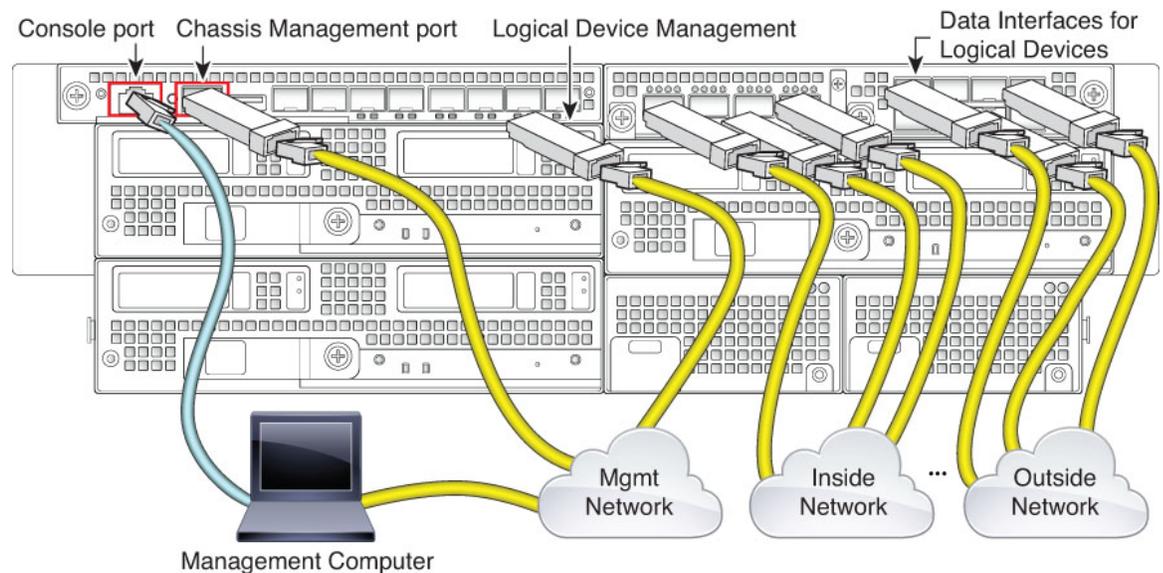
- **コンソールポート**：管理コンピュータをコンソールポートに接続して、シャーシの初期設定を実行します。Firepower 4100 には RS-232-to-RJ-45 シリアルコンソールケーブルが含まれています。接続には、サードパーティ製のシリアル-USB ケーブルが必要になる場合があります。
- **シャーシ管理ポート**：シャーシ管理ポートを管理ネットワークに接続し、シャーシの設定と継続的な管理を行います。
- **Threat Defense 論理デバイス管理インターフェイス**：FXOS 管理用に予約されているシャーシ管理ポートを除き、シャーシ上の任意のインターフェイスを選択できます。
- **データインターフェイス**：データインターフェイスを論理デバイスデータネットワークに接続します。物理インターフェイス、EtherChannel、およびブレイクアウトポートを設定して、大容量のインターフェイスを分割できます。

高可用性の場合は、フェールオーバー/ステートリンクにデータインターフェイスを使用します。



- (注) コンソールポート以外のすべてのインターフェイスには、SFP/SFP+/QSFP のトランシーバーが必要です。サポートされているトランシーバーについては、『[Hardware Installation Guide](#)』を参照してください。

Firepower 9300 のケーブル配線



論理デバイスの管理インターフェイスで脅威に対する防御の初期設定を実行します。後で、任意のデータインターフェイスから管理を有効にすることができます。脅威に対する防御デバイスでは、ライセンスと更新にインターネットアクセスが必要です。デフォルトの動作では、デバイスの展開時に指定したゲートウェイ IP アドレスに管理トラフィックをルーティングします。そうではなく、バックプレーンを介してデータインターフェイスに管理トラフィックをルーティングする必要がある場合は、後で **Device Manager** でその設定が行えます。

シャーシの初期設定、継続的なモニタリング、論理デバイスの使用には、次のインターフェイスにケーブルを配線します。

- **コンソールポート**：管理コンピュータをコンソールポートに接続して、シャーシの初期設定を実行します。Firepower 9300 には RS-232-to-RJ-45 シリアルコンソールケーブルが含まれています。接続には、サードパーティ製のシリアル-USB ケーブルが必要になる場合があります。
- **シャーシ管理ポート**：シャーシ管理ポートを管理ネットワークに接続し、シャーシの設定と継続的な管理を行います。
- **論理デバイス管理インターフェイス**：1 つ以上のインターフェイスを使用して論理デバイスを管理します。シャーシ管理ポート以外は、シャーシ上の任意のインターフェイスを選択できます。シャーシ管理ポートは、FXOS 管理用に予約されています。管理インターフェイスは論理デバイス間で共有できます。また、論理デバイスごとに別のインターフェ

イスを使用することもできます。通常は、管理インターフェイスをすべての論理デバイスと共有します。または、別個のインターフェイスを使用する場合は、それらを単一の管理ネットワークに配置します。ただし、正確なネットワーク要件は場合によって異なります。

- データインターフェイス：データインターフェイスを論理デバイスデータネットワークに接続します。物理インターフェイス、EtherChannel、およびブレイクアウトポートを設定して、大容量のインターフェイスを分割できます。ネットワークのニーズに応じて、複数の論理デバイスを同じネットワークまたは異なるネットワークに配線できます。別の論理デバイスに到達するために、すべてのトラフィックが1つのインターフェイス上のシャーシから出て、別のインターフェイスに戻る必要があります。

高可用性の場合は、フェールオーバー/ステートリンクにデータインターフェイスを使用します。



- (注) コンソールポート以外のすべてのインターフェイスには、SFP/SFP+/QSFP のトランシーバーが必要です。サポートされているトランシーバーについては、『[Hardware Installation Guide](#)』を参照してください。

Threat Defense Virtual の仮想ケーブル接続

Threat Defense Virtual をインストールするには、<http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/products-installation-guides-list.html> で、ご使用の仮想プラットフォームに対応したクイックスタートガイドを参照してください。Device Manager は、次の仮想プラットフォーム（VMware、KVM、Microsoft Azure、Amazon Web Services（AWS））でサポートされています。

Threat Defense Virtual のデフォルト設定では、管理インターフェイスと内部インターフェイスは同じサブネットに配置されます。スマートライセンスを使用する場合やシステムデータベースへの更新プログラムを取得する場合は、管理インターフェイスにインターネット接続が必要です。

そのため、デフォルト設定は、Management 0/0 と GigabitEthernet 0/1（内部）の両方を仮想スイッチ上の同じネットワークに接続できるように設計されています。デフォルトの管理アドレスは、内部 IP アドレスをゲートウェイとして使用します。したがって、管理インターフェイスは内部インターフェイスを介してルーティングし、その後、外部インターフェイスを介してルーティングして、インターネットに到達します。

また、インターネットにアクセスできるネットワークを使用している限り、内部インターフェイス用に使用されているサブネットとは異なるサブネットに Management 0/0 を接続するオプションもあります。ネットワークに適切な管理インターフェイスの IP アドレスとゲートウェイが設定されていることを確認してください。

Threat Defense の物理インターフェイスへの VMware ネットワークアダプタとインターフェイスのマッピング方法

VMware Threat Defense Virtual デバイス用に最大 10 のインターフェイスを設定できます。少なくとも 4 つのインターフェイスを設定する必要があります。

Management0-0 送信元ネットワークが、インターネットにアクセスできる VM ネットワークに関連付けられていることを確認します。これは、システムが Cisco Smart Software Manager にアクセスしてシステムデータベース更新をダウンロードすることを可能にするために必要です。

OVFをインストールするときにネットワークを割り当てます。インターフェイスを設定しておけば、後でVMwareクライアントを介して仮想ネットワークを変更できます。ただし、新しいインターフェイスを追加する必要がある場合は、必ずリストの最後にインターフェイスを追加してください。他の場所でインターフェイスを追加または削除した場合、ハイパーバイザによってインターフェイスの番号が再設定され、その結果、設定内のインターフェイスIDが誤った順番になります。

次の表は、VMware ネットワーク アダプタおよび送信元インターフェイスの、Threat Defense Virtual の物理インターフェイス名へのマッピングを示しています。追加のインターフェイスについては、命名は同じパターンに従い、関連する数字を1つずつ増やします。すべての追加インターフェイスはデータインターフェイスです。仮想ネットワークの仮想マシンへの割り当ての詳細については、VMware のオンラインヘルプを参照してください。

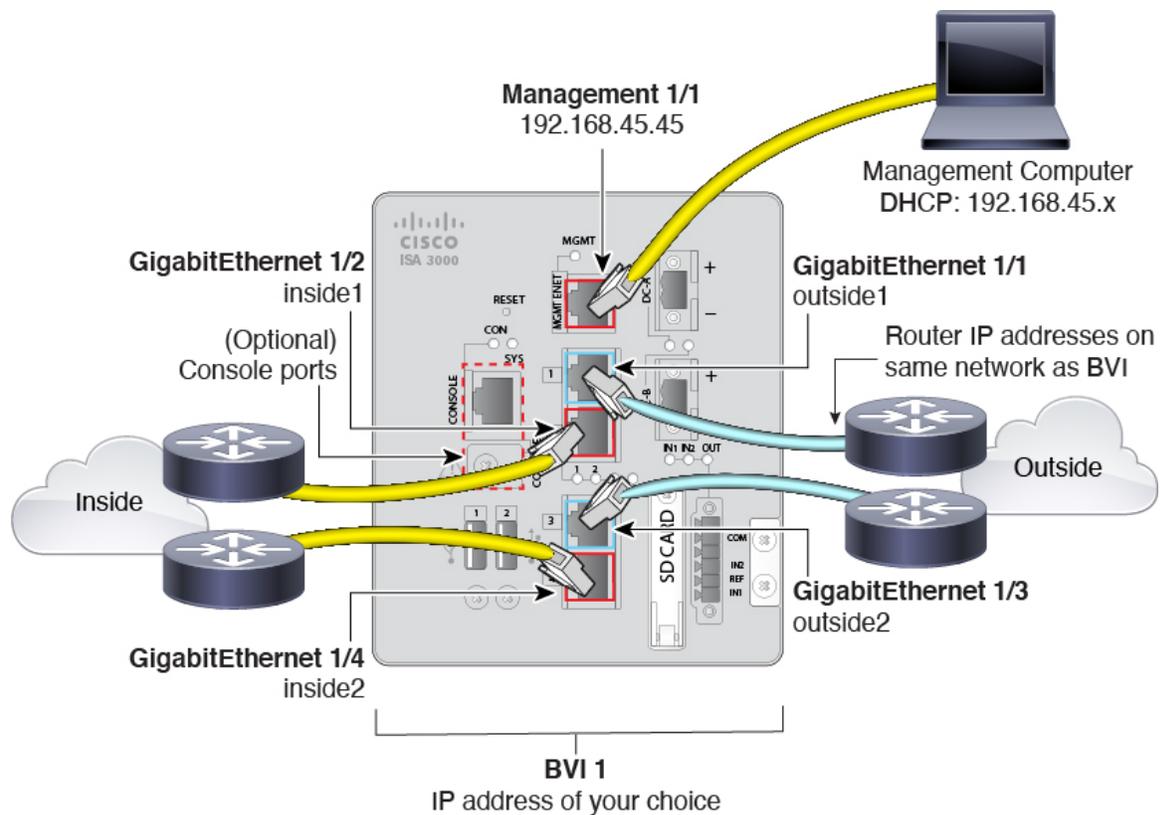
表 1: 送信元から宛先ネットワークへのマッピング

ネットワークアダプタ	送信元ネットワーク	宛先ネットワーク（物理インターフェイス名）	機能
Network adapter 1	Management0-0	Management0/0	管理
Network adapter 2	内部使用のため予約済み。	内部使用のため予約済み。	内部使用のため予約済み。
ネットワークアダプタ 3	GigabitEthernet0-0	GigabitEthernet 0/0	外部データ
ネットワークアダプタ 4	GigabitEthernet0-1	GigabitEthernet 0/1	内部データ
ネットワークアダプタ 5	GigabitEthernet0-2	GigabitEthernet 0/2	データ トラフィック
ネットワークアダプタ 6	GigabitEthernet 0-3	GigabitEthernet 0/3	データ トラフィック
ネットワークアダプタ 7	GigabitEthernet 0-4	GigabitEthernet 0/4	データ トラフィック
ネットワークアダプタ 8	GigabitEthernet 0-5	GigabitEthernet 0/5	データ トラフィック

ネットワークアダプタ	送信元ネットワーク	宛先ネットワーク（物理インターフェイス名）	機能
ネットワークアダプタ 9	GigabitEthernet 0-6	GigabitEthernet 0/6	データ トラフィック
ネットワークアダプタ 10	GigabitEthernet 0-7	GigabitEthernet 0/7	データ トラフィック

ISA 3000 のケーブル配線

図 5: ISA 3000



- GigabitEthernet 1/1 を外部ルータに接続し、GigabitEthernet 1/2 を内部ルータに接続します。これらのインターフェイスによってハードウェアバイパスペアが形成されます。
- GigabitEthernet 1/3 を冗長外部ルータに接続し、GigabitEthernet 1/4 を冗長内部ルータに接続します。

銅線ポートを備えたモデルの場合は、これらのインターフェイスによってハードウェアバイパスペアが形成されます。ファイバはハードウェアバイパスをサポートしていません。これらのインターフェイスは、他方のペアで障害が発生した場合に冗長ネットワークパス

を提供します。これら4つのデータインターフェイスはすべて、選択した同じネットワーク上に存在します。BVI 1 の IP アドレスを、内部ルータおよび外部ルータと同じネットワーク上に配置するように設定する必要があります。

- Management 1/1 を管理コンピュータ（またはネットワーク）に接続します。

Management 1/1 の IP アドレスをデフォルトから変更する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要があります。「(任意) CLI での管理ネットワーク設定の変更 (22 ページ)」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 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 \(9 ページ\)](#) を参照してください。

ステップ 2 ユーザー名 **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、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 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 **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 **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 **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、**Management Center** デバイスの管理には **オンプレミス** または **クラウド** 配信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 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 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

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（12 ページ）](#) および [初期設定前のデフォルト設定（28 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。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 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ス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（22 ページ）](#)」を参照してください。

手順

ステップ1 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 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**
 - (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、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、エンドユーザー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ず。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 \(28 ページ\)](#) 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があります。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：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。

初期設定前のデフォルト設定

ローカルマネージャ (Device Manager) を使用して 脅威に対する防御 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 \(22 ページ\)](#)) 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。 Threat Defense Virtual192.168.45.45 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。 Threat Defense Virtual192.168.45.1	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	<p>192.168.95.1/24</p> <p>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。</p> <p>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。</p> <p>Threat Defense Virtual 192.168.45.1/24</p>	不可。
内部クライアントの DHCP サーバ	<p>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。</p> <p>Firepower 4100/9300: No DHCP server enabled.</p> <p>ISA 3000: DHCP サーバが有効になっていません。</p> <p>Threat Defense Virtual : 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。</p>	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	<p>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。</p> <p>IPv6 : 自動設定。</p> <p>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。</p> <p>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。</p>	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。

Threat Defense デバイス	外部インターフェイス	内部インターフェイス
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 シリーズ	Ethernet1/1	Ethernet1/2
Secure Firewall 3100 シリーズ	Ethernet1/1	Ethernet1/2
Firepower 4100 シリーズ	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 appliance	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。
Threat Defense Virtual	GigabitEthernet 0/0	GigabitEthernet0/1
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) Firepower4100/9300 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。 Threat Defense Virtual : 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 Threat Defense Virtual : 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	<p>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。</p> <p>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。</p> <p>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。</p> <p>Threat Defense Virtual: 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。</p>	暗黙的
システム時間	<p>選択したタイム ゾーンおよび NTP サーバー。</p> <p>Firepower 4100/9300 : システム時刻はシャードから継承されます。</p> <p>ISA 3000 : Cisco NTP サーバー : 0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org。</p>	明示的
スマート ライセンス	<p>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。</p> <p>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。</p>	明示的
内部インターフェイスの IP アドレス	<p>192.168.95.1/24</p> <p>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。</p> <p>ISA 3000 : なし。BVII の IP アドレスは手動で設定する必要があります。</p> <p>Threat Defense Virtual192.168.45.1/24</p>	デフォルト
内部クライアントの DHCP サーバ	<p>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。</p> <p>Firepower 4100/9300: No DHCP server enabled.</p> <p>ISA 3000: DHCP サーバが有効になっていません。</p> <p>Threat Defense Virtual : 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。</p>	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）	<p>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。</p> <p>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。</p>	明示的（ただし間接的）
データ インターフェイスの設定	<ul style="list-style-type: none"> • Firepower 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（BV11）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	<p>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（28 ページ）を参照してください。</p> <p>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）。</p> <p>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。</p> <p>ISA 3000 : なし。BV11 の IP アドレスは手動で設定する必要があります。</p>	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	<p>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。</p> <p>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。</p>	暗黙的
セキュリティゾーン	<p>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。</p> <p>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。</p> <p>（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）。</p>	暗黙的
アクセス コントロール ポリシー	<p>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。</p> <p>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。</p> <p>Firepower 4100/9300 : 事前設定されたアクセスルールはありません。</p> <p>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。</p>	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	<p>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。</p> <p>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。</p> <p>Firepower 4100/9300 : NAT は事前に設定されていません。</p> <p>ISA 3000 : NAT は事前設定されていません。</p>	暗黙的

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

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 \(43 ページ\)](#) 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。ここでは、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、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 \(40 ページ\)](#) 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。フィールドを使用すると、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 \(40 ページ\)](#) 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、編集する項目を探ることができます。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。次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。?!|{}<>:%。次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インスペクション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** 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 \(42 ページ\)](#) 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。

- [完全な展開を強制 (Force a full deployment)] : 問題があり、システムに変更だけではなく完全な設定を展開するように強制する場合は、[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 [完全な展開を適用 (Apply Full Deployment)] を選択することができます。完全な展開の場合はトラフィックが中断されるため、[展開 (Deploy)] をクリックする前に、このアクションを実行することを確認する必要があります。
- [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。確認を求められません。
- [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 방법이 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。

インターフェイス ステータス

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

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、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脅威に対する防御 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)、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。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。

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。

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、Device Manager と脅威に対する防御 REST API を使用してデバイスを設定できます。実際には、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 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、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 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、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、Device Manager で使用できない設定への API の変更は 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 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。

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。