はじめに

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。

本書の対象読者

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 のバージョン 7.7.0 における新機能

リリース：2025 年 3 月 5 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 7.7.0 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	
Cisco Secure Firewall 1230、1240、および 1250（ラックマウント）。	Secure Firewall CSF-1230 および CSF-1240 が導入されました。 • 8x1Gbps RJ-45 1000BASET/2.5BBASE-T 銅線 • 4x1Gbps SFP+ 光 Secure Firewall CSF-1250： • 8x2.5Gbps1000BASET/2.5BBASE-T 銅線 • 4x2.5Gbps SFP28 光 Cisco Secure Firewall CSF-1230,CSF-1240, and CSF-1250 Hardware Installation Guideを参照してください。
Cisco Secure Firewall 1210CP IEEE 802.3bt のサポート（PoE++ および Hi-PoE）。	IEEE 802.3bt のサポートに関連する次の改善が行われました。 • PoE++ と Hi-PoE：ポートあたり最大 90 W。 • シングルシグネチャおよびデュアルシグネチャの受電デバイス（PD）。 • パワーバジェットが先着順で行われます。 • **show power inline** にパワーバジェットフィールドが追加されました。 新しい/変更された画面：**[デバイス（Device）]>[インターフェイス（Interfaces）] > [PoE]** 新規/変更されたコマンド： **show power inline**
AWS、Azure、GCP のインスタンス。	次のファミリから Threat Defense Virtual のインスタンスを追加しました。 • AWS（Amazon Web Services）：C6i、C6a • Azure（Microsoft Azure）：Dv4、Dv5 • GCP（Google Cloud Platform）：E2、N1、N2D、C2D 参照： Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

機能	説明
ISO ベースの cloud-init シーディングを使用した VMware 向け Threat Defense Virtual の自動プロビジョニング。	ホスト名、パスワード、管理モード、ファイアウォール モード、ネットワーク設定、展開タイプなどの初期設定の詳細が含まれているテキスト ファイル（day0.iso）を使用して、VMware 向けの脅威防御仮想機能をすばやく展開できるようになりました。 Cisco Secure Firewall Threat Defense Virtual スタートアップガイドを参照してください。
ファイアウォールと IPS の機能	
インラインセットのハードウェアバイパスのサポート。	デバイスモデルがハードウェアバイパスをサポートしている場合、サポートされているインターフェイスを含むインラインセットに設定できるようになりました。 インラインセット設定に [バイパス（Bypass）] オプションが追加されました。
廃止：Snort 2	**アップグレードの影響。Snort 2 デバイスはアップグレードできません。** Snort 2 は廃止されました。Snort 2 デバイスをバージョン 7.7.0 以降にアップグレードすることはできません。**show snort counters** および **show snort preprocessor-memory-usage** コマンドと同様、Snort 2 に切り替える機能は削除されました。 アップグレードする前に、Snort 3 に切り替えてください。現在のバージョンに対応するガイドの「侵入ポリシー」の章を参照してください： Cisco Secure Firewall Device Manager 設定ガイド。
管理機能	
カスタムログインページ。	デバイスマネージャのログインページはカスタマイズできます。これには、ログイン ページに画像やテキストを追加することが含まれます。たとえば、免責事項と警告を含めて、ユーザーにログイン前の同意を求めることができます。このテキストは、SSH セッションでも表示されます。 **[システム設定（System Settings）] > [ログイン ページ（Login Page）]** ページが追加されました。

機能	説明
Google リモートプロシージャコール（gRPC）を使用したカスタムストリーミングテレメトリ。	Google リモートプロシージャコール（gRPC）を使用してデータを収集する外部テレメトリコレクタに、システムの正常性とテレメトリデータを送信するようにデバイスを設定できます。その後、テレメトリコレクタを使用してデバイスをモニターし、カスタム テレメトリ ソリューションと統合できます。 この機能を設定するには、 API を使用します（/devicesettings/default/telemetrystreamingconfig）。
Performance	
高可用性 Threat Defense の迅速なフェールオーバー。	Threat Defense の高可用性フェールオーバーにより、新しいアクティブデバイスがMACアドレスエントリごとにマルチキャストパケットを生成して、すべてのブリッジ グループ インターフェイスに送信し、アップストリームスイッチにルーティングテーブルを更新させます。このタスクは、データプレーンで非同期的に実行され、コントロールプレーンでの重要なフェールオーバータスクに特権が与えられるようになりました。これにより、フェールオーバーが迅速になり、ダウンタイムが減少します。
広帯域幅で暗号化されたアプリケーション トラフィックは、侵入インスペクションを不要なものとしてバイパスします。	特定の広帯域幅の暗号化されたアプリケーション トラフィックは、接続が許可ルールに一致する場合でも、侵入インスペクションを不要なものとしてバイパスするようになりました。侵入ルール（LSP）と脆弱性データベース（VDB）の更新により、バイパスされるアプリケーションが変更される可能性がありますが、現時点では、AnyConnect、IPsec、iCloud プライベート リレー、QUIC（HTTP/3 を含む）、Secure RTCP になっています。

機能	説明
FlexConfig を使用した、ブロックの枯渇からの Threat Defense の自動回復の設定。	サービスの中断によるダウンタイムを減らすために、新しい障害マネージャによりブロックの枯渇がモニターされて、必要に応じてデバイスが自動的にリロードされます。高可用性展開では、これによりフェールオーバーがトリガーされます。障害モニタリングは、新しいデバイスとアップグレードされたデバイスで自動的に有効になります。無効にするには、FlexConfig を使用します。 新規/変更された FlexConfig コマンド： • **fault-monitor block-depletion recovery-action** {**none** | **reload**} **none** を指定すると、自動リロードはオフになりますが、障害モニタリングはオフになりません。これを行うには、**no fault-monitoring** を使用します。 • **fault-monitor block-depletion monitor-interval** *seconds* 新規/変更された Threat Defense CLI コマンド：**show fault-monitor block-depletion** {**status** | **statistics**}
トラブルシューティング	
CPU プロファイラにアプリケーション識別の統計が含まれる。	CPU プロファイラに、アプリケーション識別の統計が含まれるようになりました。CPU プロファイリング（**cpu profile activate**）を有効にすると、特定のアプリケーショントラフィックの処理で使用されるリソースを確認できるようになりました。 新規/変更された CLI コマンド：**system support appid-cpu-profiling status**、**system support appid-cpu-profiling dump** 参照： Cisco Secure Firewall Threat Defense コマンドリファレンス
新しい IP フロー統計。	Cisco TAC の指示で脅威防御デバイスから IP フロー統計を収集する際に、新しい **all** パラメータは追加の統計（ポート、プロトコル、アプリケーション、累積遅延、および検査時間）を、指定されたファイルにログ記録します。 新規/変更されたコマンド：**system support flow-ip-profiling start flow-ip-file** *filename* **all** {**enable** | **disable**} Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。
セキュリティと強化	

機能	説明
Threat Defense CLI の Basic ユーザーのユーザー権限の制限。	Threat Defense CLI の Basic ユーザー権限の範囲が dig、ping、traceroute の各コマンドに制限されるようになりました。Basic 権限を持つユーザーを作成した場合は、そのユーザーを Config 権限に変更する必要があるかどうかを判断してください。ユーザーの権限レベルを変更するには、**configure user access** コマンドを使用します。 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。

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、システムの設定、管理、およびモニタが行えます。

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。

以下のトピックで、これらのインターフェイスへのログインやユーザアカウントを管理する方法について説明します。

ユーザ 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。

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（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。
- [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（例：https://ftd.example.com ）を開きます。

次のいずれかのアドレスを使用できます。設定済みであれば、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192.168.1.1に接続できます。95.1.使用モデルの内部IPアドレスの詳細については、初期セットアップ前のデフォルト設定 （30 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
ブラウザがサーバ証明書を認識するように設定されていない場合、信頼されてい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 ログイン画面に警告や免責事項などのテキストが含まれている場合は、その情報を読み、チェックボックスをオンにして契約に同意します。

ステップ 3 （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。

アクティビティが 30 分間ないと、セッションは期限切れになり、再度ログインするよう要求されます。ログアウトするには、ページの右上にあるユーザアイコン ドロップダウン メニューから [ログアウト（Log Out）] を選択します。

ステップ 4 （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。

コマンド ライン インターフェイス（CLI）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 で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 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 接続のインターフェイスを開く場合は、データインターフェイス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、 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

- 管理者がログインプロセスに警告や免責事項などのテキストを追加した場合は、ステートメントを読んで同意したことを確認する必要があります。
- 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]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 新規のパスワードを入力し、確認用にも入力します。

[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こと
- 数字が1桁以上含まれていること
- 特殊文字が1文字以上含まれていること
- 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 プロファイルの設定

ユーザ インターフェイスを設定したり、パスワードを変更することができます。

手順

ステップ 1 メニューの右上にあるユーザ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。

- [タスクのスケジューリングに使用するタイムゾーン（Time Zone for Scheduling Tasks）]：バックアップや更新などのタスクをスケジュールする際に使用するタイム ゾーンを選択します。別のゾーンを設定しても、ダッシュボードとイベントではブラウザのタイム ゾーンが使用されます。
- [カラー テーマ（Color Theme）]：ユーザ 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。

英語以外の言語でページを表示する

次の言語で GUI およびオンライン ヘルプを表示できます。

- フランス語（カナダ）
- 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

システム機能をネットワークで正しく動作させるには、初期設定を完了する必要があります。適切な導入には、ケーブルを正しく接続することや、デバイスをネットワークに挿入してインターネットや他の上流に位置するルータに接続するために必要なアドレスを設定することが含まれます。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から、デバイスにはいくつかのデフォルト設定が組み込まれています。詳細については、初期セットアップ前のデフォルト設定 （30 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 （13 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）

設定の詳細については、初期セットアップ後の設定 （33 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ネットワークと外部ネットワークに使用されることを前提としています。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場合、初期設定は簡単です。

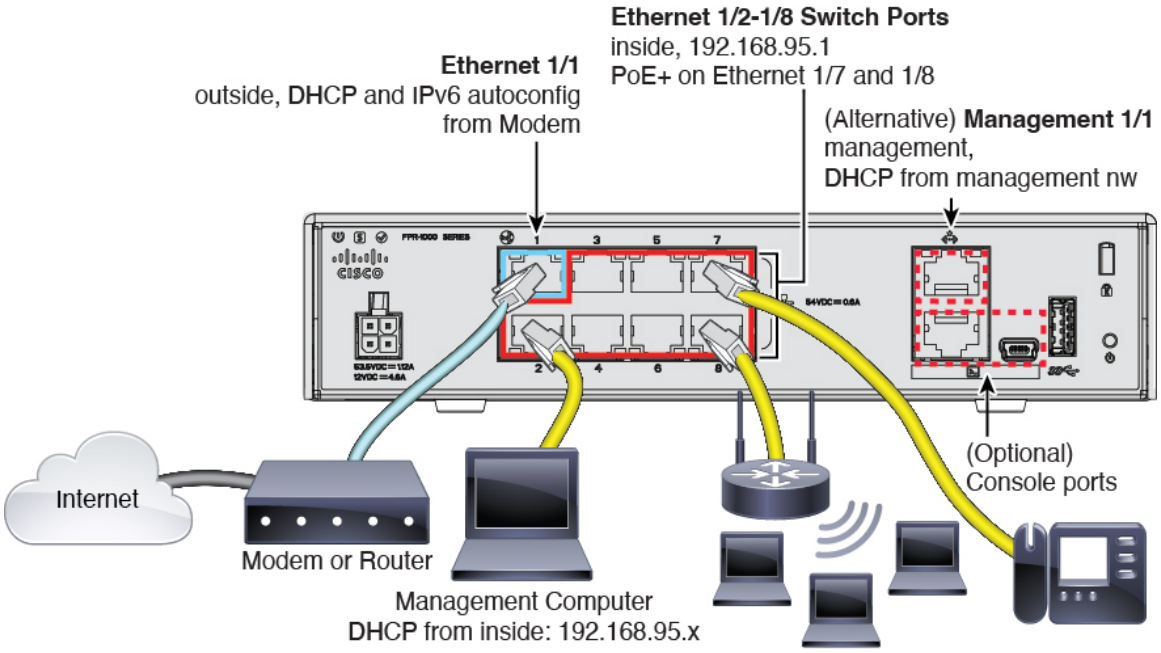
大半のモデルのデフォルト設定は、管理コンピュータを内部インターフェイスに接続するように設計されています。また、ワークステーションを管理ポートに直接接続することもできます。インターフェイスは別のネットワーク上にあるので、内部インターフェイスと管理ポートを同じネットワークに接続しないでください。

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。

ここでは、デバイスの設定に内部インターフェイスを使用する際、このトポロジでシステムをケーブル接続する方法を説明します。

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 ー 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 ー 1/8）。内部にはデフォルトの IP アドレス（192.168.951.1)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：管理コンピュータを管理ネットワークに接続します。Management 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 サーバが含まれていることを確認してください。

    管理 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 （24 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イーサネット 1/1 インターフェイスに接続します。

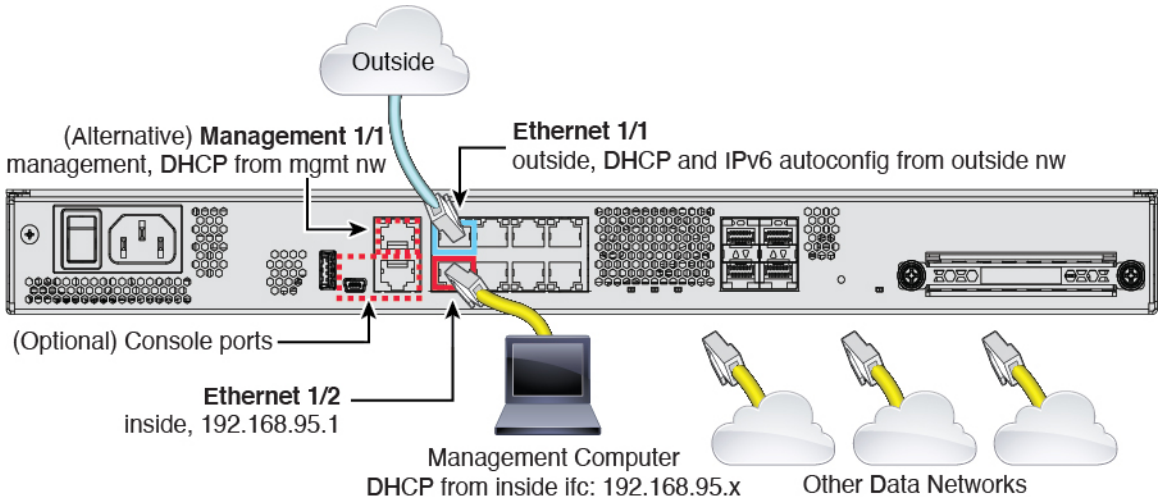
  デフォルトでは、IP アドレスは IPv4 DHCP および IPv6 自動設定を使用して取得しますが、初期設定時に静的アドレスを設定できます。
- 内部デバイスを残りのスイッチ ポート（Ethernet 1/2 ～ 1/8）に接続します。

  イーサネット 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



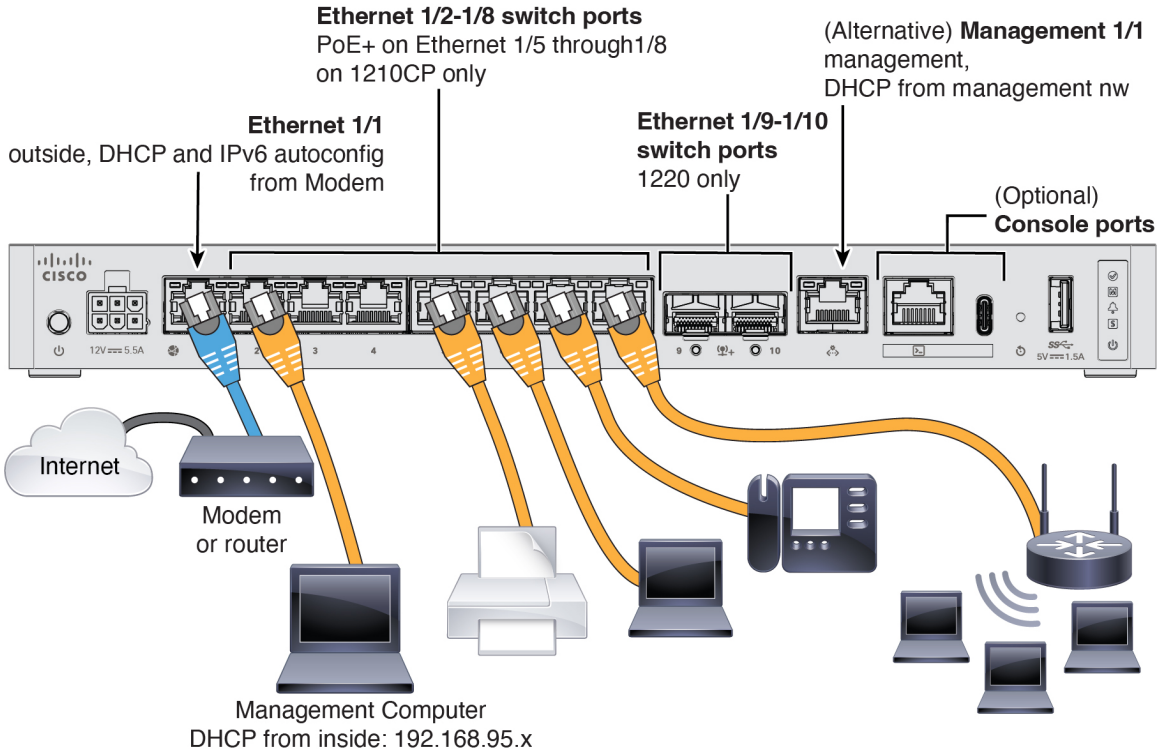
- 管理コンピュータを次のいずれかのインターフェイスに接続します。
  - Ethernet 1/2：初期設定のために管理コンピュータを Ethernet 1/2 に直接接続するか、Ethernet 1/2 を内部ネットワークに接続します。イーサネット 1/2 にはデフォルトの IP アドレス（192.168.951.1)があり、クライアント(管理コンピュータを含む)にIPアドレスを提供するためにDHCPサーバも実行されるため、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください。
  - Management 1/1（ラベル「MGMT」）：管理コンピュータを管理ネットワークに接続します。Management 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 サーバが含まれていることを確認してください。

    管理 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 （24 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。

Secure Firewall 1210/1220 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（1210）または 1/10（1220）：管理コンピュータをいずれかの内部スイッチ ポート（イーサネット 1/2 ～ 1/8（1210）または 1/10（1220））に直接接続します。内部にはデフォルトの IP アドレス（192.168.95.1）があり、クライアントに IP アドレスを提供するために DHCP サーバーも実行されます（管理コンピュータを含む）。したがって、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：管理コンピュータを管理ネットワークに接続します。Management 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 サーバが含まれていることを確認してください。

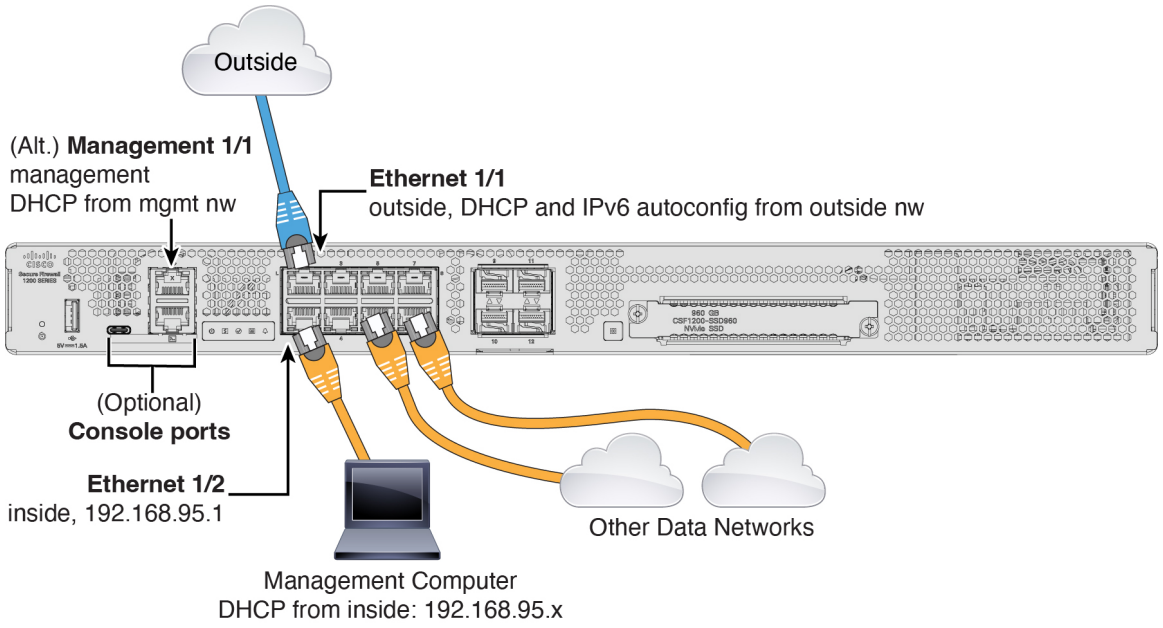
    管理 1/1 IP アドレスをデフォルトから変更し、静的 IP アドレスを設定する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。（任意）CLI での管理ネットワーク設定の変更 （24 ページ）を参照してください。

  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イーサネット 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（イーサネット 1/2 ～ 1/8（1210）または 1/10（1220））に接続します。
- Secure Firewall 1220 のイーサネット ポート 1/9 および 1/10 は SFP+ ポートです。
- Secure Firewall 1210CP のイーサネット ポート 1/5 ～ 1/8 は Power over Ethernet+（PoE+）です。

Secure Firewall 1230/1240/1250 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。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：管理コンピュータを管理ネットワークに接続します。Management 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 サーバが含まれていることを確認してください。

    管理 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 （24 ページ）を参照してください。

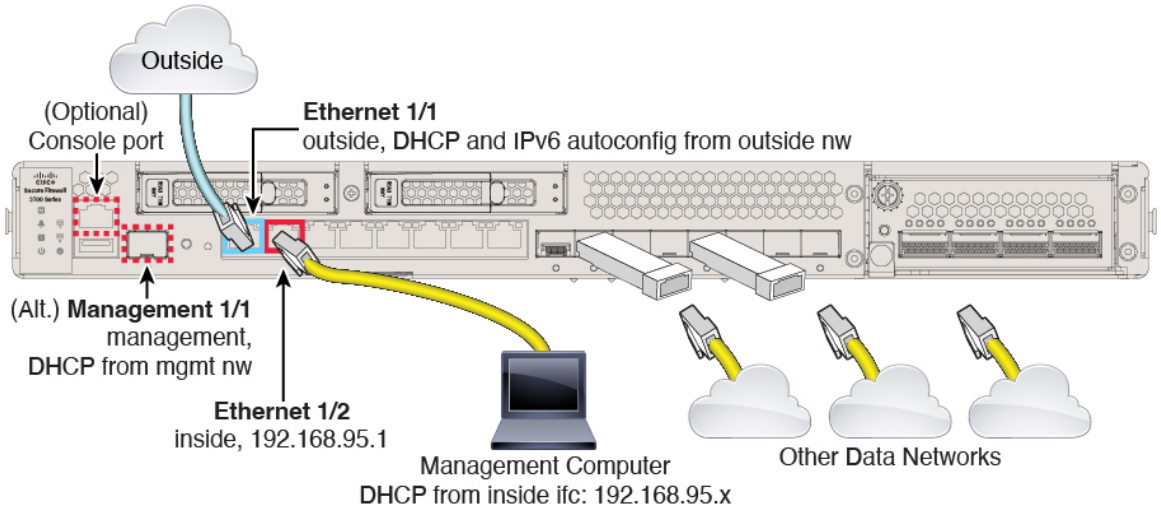
  後で、他のインターフェイスから管理アクセスを設定できます。
- 外部ネットワークを Ethernet1/1 インターフェイスに接続します。

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。イーサネット 1/9 ～ 1/12 は、SFP/SFP+ インターフェイスです。

Cisco Secure Firewall 3100 のケーブル配線

図 *3 : Cisco Secure Firewall 3100* のケーブル配線



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ている IP アドレスを決定する必要があります。

    管理 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 （24 ページ）を参照してください。

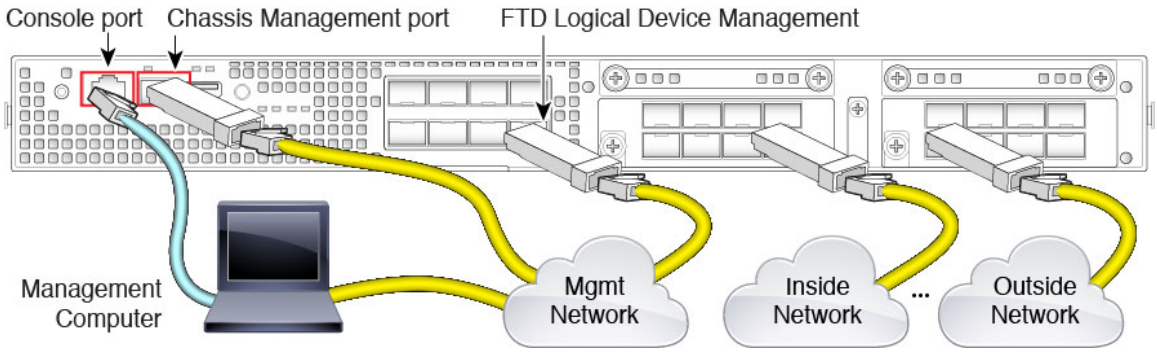
（注） Management 1/1 は、SFP モジュールを必要とする 10 Gb 光ファイバインターフェイスです。

- 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。

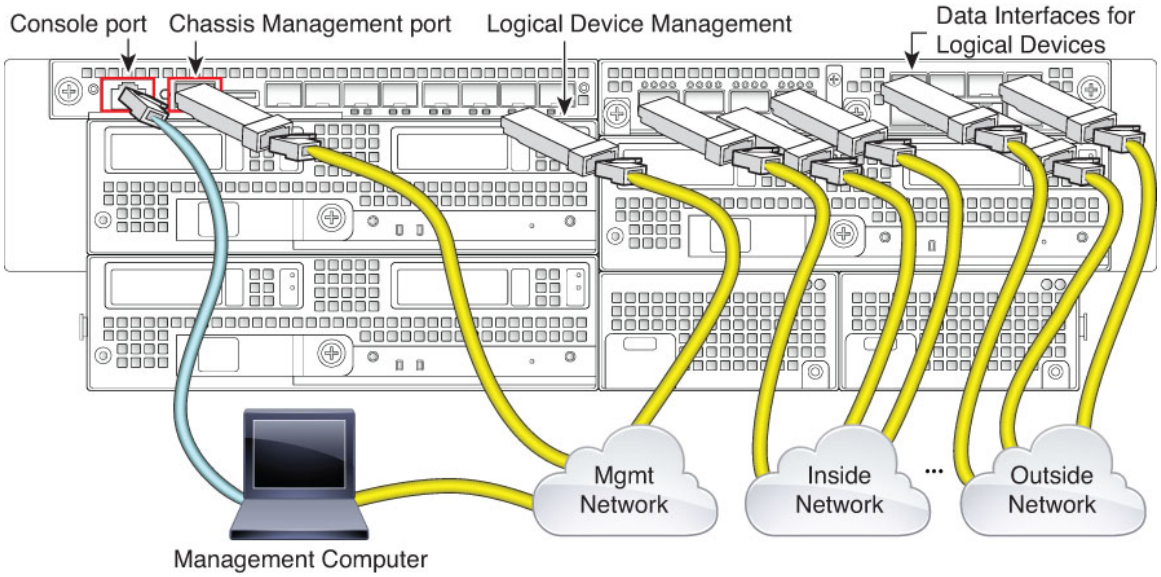
シャーシの初期設定、継続的なモニタリング、および論理デバイスの使用のために、次のインターフェイスを配線します。

- 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: 設定および継続的なシャーシ管理のために、シャーシ管理ポートを管理ネットワークに接続します。
- 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、および論理デバイスの使用のために、次のインターフェイスを配線します。

- 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: 設定および継続的なシャーシ管理のために、シャーシ管理ポートを管理ネットワークに接続します。

- 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。FXOS 管理用に予約されているシャーシ管理ポートを除く、シャーシ上の任意のインターフェイスを選択できます。管理インターフェイスは論理デバイス間で共有することも、論理デバイスごとに個別のインターフェイスを使用することもできます。通常、管理インターフェイスはすべての論理デバイスで共有します。個別のインターフェイスを使用する場合は、インターフェイスを単一の管理ネットワークに配置します。ただし、実際のネットワーク要件は異なる場合があります。
- 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。トラフィックはすべて、1つのインターフェイス上のシャーシを終端とし、別の論理デバイスに到達するには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 ライセンスを使用し、システム データベースの更新を入手するには、管理インターフェイスでインターネット接続が必要です。

したがって、Management0/0 と GigabitEthernet0/1（内部）の両方を仮想スイッチで同じネットワークに接続できるように、デフォルト設定が設計されています。デフォルト管理アドレスはゲートウェイとして内部 IP アドレスを使用します。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、外部インターフェイスの順に経由し、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である限り、内部インターフェイスに使用しているサブネットとは異なるサブネットに Management0/0 を接続することもできます。管理インターフェイスの IP アドレスとゲートウェイをネットワークに対して適切に設定してください。

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 にアクセスするとと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。

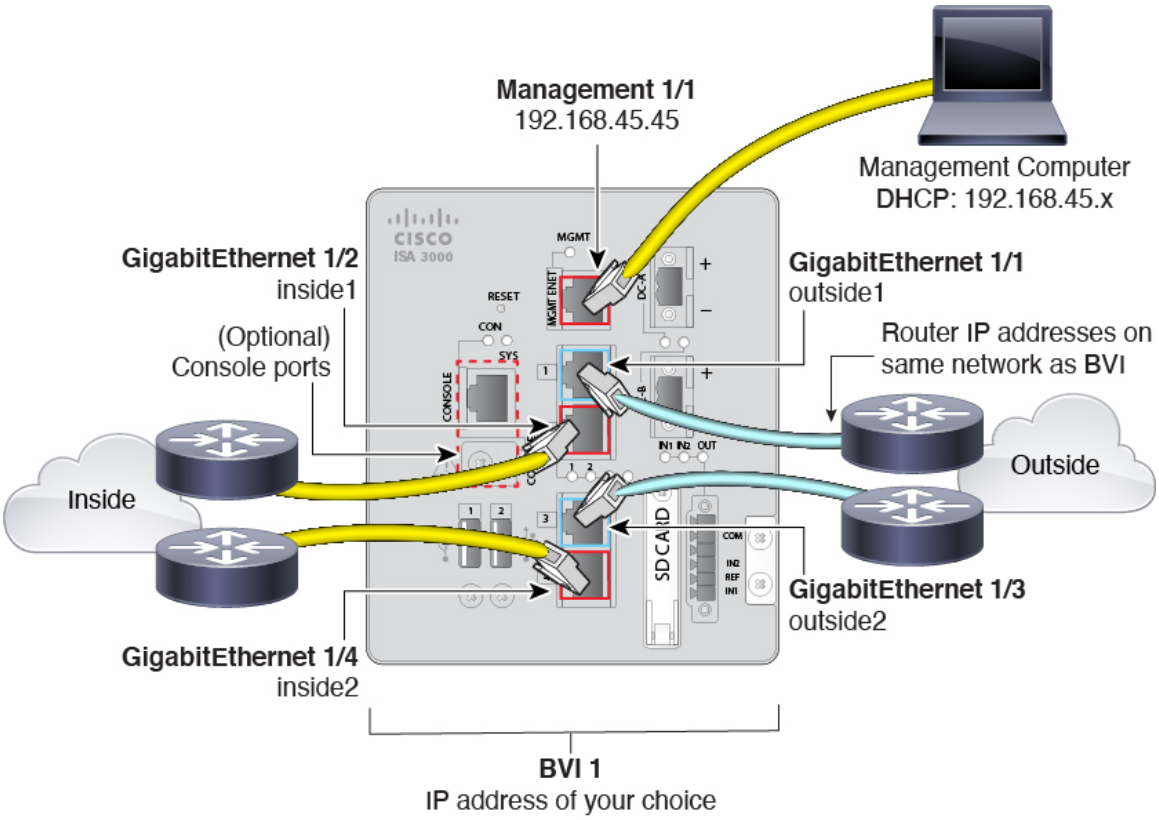
次の表は、VMware ネットワーク アダプタおよび送信元インターフェイスの、Threat Defense Virtual の物理インターフェイス名へのマッピングを示しています。追加のインターフェイスについては、命名は同じパターンに従い、関連する数字を 1 つずつ増やします。すべての追加インターフェイスはデータ インターフェイスです。仮想ネットワークの仮想マシンへの割り当ての詳細については、VMware のオンライン ヘルプを参照してください。

表 *1:* 送信元ネットワーク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
ネットワークアダプタ 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
Network adapter 4	GigabitEthernet0-1	GigabitEthernet 0/1	内部データ
ネットワークアダプタ 5	GigabitEthernet0-2	GigabitEthernet0/2	データ トラフィック
Network adapter 6	GigabitEthernet 0-3	GigabitEthernet0/3	データ トラフィック
Network adapter 7	GigabitEthernet 0-4	GigabitEthernet0/4	データ トラフィック
Network adapter 8	GigabitEthernet 0-5	GigabitEthernet0/5	データ トラフィック
Network adapter 9	GigabitEthernet 0-6	GigabitEthernet0/6	データ トラフィック
Network adapter 10	GigabitEthernet 0-7	GigabitEthernet0/7	データ トラフィック

ISA 3000 のケーブル配線

図 *4 : 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もあります。（任意）CLI での管理ネットワーク設定の変更 （24 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

デフォルトの管理 IP アドレスを使用できない場合、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。とはいえ、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、「コマンドラインインターフェイス（CLI）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（ケーブルモデム、ルータなど）に接続されていることを確認します。エッジ導入の場合、インターネット対応ゲートウェイに接続されていなければなりません。データ センター導入の場合、バックボーン ルータに接続されている必要があります。使用しているモデルのデフォルトの「外部」インターフェイスを使用してください（インターフェイスの接続 （13 ページ）および初期セットアップ前のデフォルト設定 （30 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、システムはインターネットに接続されたデータ インターフェイス（通常は外部インターフェイス）からシステム ライセンスおよびデータベースやその他の更新を取得します。別個の管理ネットワークを使用する必要がある場合は、初期設定が完了した後に、管理インターフェイスをネットワークに接続し、別個の管理ゲートウェイを設定できます。

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 （24 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。

これらのステップを完了しなければ、次のステップに進めません。

ステップ 3 外部インターフェイスと管理インターフェイスについて以下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、インターフェイスの設定がデバイスに導入されます。インターフェイスは「outside」という名前で「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の IPv4 アドレス。DHCP を使用するか、手動で静的 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（初期セットアップ前のデフォルト設定 （30 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、手動で静的 IP アドレス、プレフィックス 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、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の DNS サーバ。名前解決に使用する DNS サーバのアドレスを 1 つ以上入力します。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た後、デフォルトに戻す場合は、[OpenDNS を使用（Use OpenDNS）] をクリックすると該当する IP アドレスがフィールドにリロードされます。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。

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、手動で NTP サーバのアドレスを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。

システムに必要なライセンスを取得して適用するには、スマート ライセンス アカウントが必要です。最初は 90 日間の評価ライセンスを使用して、後でスマート ライセンスを設定するので構いません。

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。前述の設定については、画面上のテキストで詳しく説明されています。

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、[スマートライセンス（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 ライセンスの範囲の機能（カテゴリ ベースの URL フィルタリング、侵入検査、マルウェア対策など）を使用する場合は、それぞれの機能に必要なライセンスを有効にします。オプション ライセンスのイネーブル化とディセーブル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については、サブネットの追加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。
- 使用例を調べて、製品の使用方法を学んでください。「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）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある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の [アクション（Actions）] 列にマウスを合わせ、編集アイコン（  ）をクリックします。

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

内部ネットワークでDHCPサーバがすでに実行されている場合、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 メニューの [展開（Deploy）] ボタンをクリックして、変更を展開します。

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。

初期セットアップ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。詳細は以下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 （24 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	初期設定中に変更できるか
管理者ユーザ用のパスワード	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。	はい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。

設定	デフォルト	初期設定中に変更できるか
管理ゲートウェイ	デバイス上のデータ インターフェイス。通常は、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。	はい
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。 Threat Defense Virtual192.168.45.1/24	いいえ

設定	デフォルト	初期設定中に変更できるか
内部クライアント用の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：DHCP サーバが有効になっていません。 ISA 3000：DHCP サーバが有効になっていません。 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。	いいえ
内部クライアント用の DHCP 自動設定。（自動設定により、クライアントに WINS および DNS サーバのアドレスが提供されます。）	外部インターフェイス上で有効になります。	はい（ただし、間接的）。外部インターフェイスに静的IPv4アドレスを設定した場合は、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。	はい

デバイス モデル別のデフォルト インターフェイス

初期設定中に、別の内部インターフェイスと別の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割り当てを変更するには、インターフェイスとDHCPの設定を編集します。インターフェイスを非スイッチドインターフェイスとして設定するには、そのインターフェイスをブリッジ グループから削除する必要があります。

Threat Defense デバイス	外部インタフェース	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。

Threat Defense デバイス	外部インタフェース	内部インターフェイス
Firepower 1120、1140、1150	Ethernet1/1	Ethernet1/2
Cisco Secure Firewall 1210/1220	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。
Cisco Secure Firewall 1230/1240/1250	Ethernet1/1	Ethernet1/2
Cisco 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	GigabitEthernet0/0	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、デバイス設定には以下の設定が含まれます。次の表は、特定の設定が明示的に選択したものか、他の選択に基づいて自動的に定義されたものかを示しています。すべての「暗黙的」の設定を確認し、必要であれば編集します。

（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	構成	明示的、暗黙的またはデフォルト設定
管理者ユーザ用のパスワード。	入力したもの	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。	これがデフォルトです。
管理ゲートウェイ	デバイス上のデータ インターフェイス。通常は、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	これがデフォルトです。
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, 208.67.222.222、IPv6: 2620:119:35::35、またはユーザの入力値。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設定した DNS サーバ。	明示的
管理ホスト名。	**firepower** か、入力したもの。 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
データ インターフェイスを介した管理アクセス。	データ インターフェイスの管理アクセス リスト ルールは、内部インターフェイス経由の HTTPS アクセスを許可します。SSH 接続は許可されません。IPv4 と IPv6 接続の両方が許可されます。 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。 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。	暗黙的

設定	構成	明示的、暗黙的またはデフォルト設定
システム時刻	選択したタイム ゾーンと NTP サーバです。 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：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	ベース ライセンスで登録したもの、または有効化した評価期間のうち、いずれか選択したものです。 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。有効化するにはスマート ライセンス ページに移動します。	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は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。 Threat Defense Virtual192.168.45.1/24	これがデフォルトです。
内部クライアント用の 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：DHCP サーバが有効になっていません。 ISA 3000：DHCP サーバが有効になっていません。 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。	これがデフォルトです。
内部クライアント用の DHCP 自動設定。（自動設定により、クライアントに WINS および DNS サーバのアドレスが提供されます。）	DHCP を使用して外部インターフェイスの IPv4 アドレスを取得する場合、外部インターフェイス上で有効化されます。 スタティック アドレッシングを使用する場合、DHCP 自動構成は無効化されます。	明示的、ただし間接的

設定	構成	明示的、暗黙的またはデフォルト設定
データ インターフェイス構成	• Firepower 1010 および Secure Firewall 1210/1220: 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。エンドポイントまたはスイッチをこれらのポートに接続し、DHCP サーバから内部インターフェイスのためにアドレスを取得できます。 • 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。	これがデフォルトです。
外部の物理インターフェイスと 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です。初期セットアップ前のデフォルト設定 （30 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は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	構成	明示的、暗黙的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スタティック IPv4 または IPv6 アドレスを設定する場合、必要に応じてスタティック デフォルト ルートが IPv4/IPv6 に設定され、そのアドレス タイプに対して定義したゲートウェイを指し示します。DHCP を選択すると、デフォルト ルートは DHCP サーバから取得されます。 ネットワーク オブジェクトも、ゲートウェイと「すべての」アドレス、つまり IPv4 の場合は 0.0.0.0/0、IPv6 の場合は ::/0 に対して作成されます。	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か、独自のゾーンを作成することができます）	暗黙的
アクセス コントロール ポリシー	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です。これは、ネットワーク内のユーザから外部に出るすべてのトラフィックと、それらの接続に対するリターン トラフィックを検証せずに許可します。 他のすべてのトラフィックに適用されるデフォルトのアクションは、ブロックです。これにより、外部からのトラフィックはすべてネットワークに入ることができなくなります。 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、内部にいるユーザ間、および外部にいるユーザ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	構成	明示的、暗黙的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

設定の基本

ここでは、デバイスの設定に関する基本的な方法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。

項目が見にくい場合は、ユーザプロファイルで別の配色を選択してください。ページの右上のユーザ アイコン 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、インターフェイスおよび管理ステータスの表示 （45 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。高可用性（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。

画像の下には、設定可能なさまざまな機能のグループが表示され、各グループの設定の概要や、システム設定の管理に使用できるアクションも一緒に表示されます。

ステップ 2 各グループのリンクをクリックすると、設定を行ったりアクションを実行したりできます。

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の他に、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）]：ルーティング設定。デフォルト ルートを定義する必要があります。設定によっては、他のルートが必要になる場合があります。ルーティングを参照してください。
- [更新（Updates）]：位置情報、侵入ルール、脆弱性データベースの更新、およびシステム ソフトウェア アップグレード。これらの機能を使用する場合は、データベース更新を最新の状態に保つために定期的な更新スケジュールを設定してください。また、定期的な更新スケジュールが実行され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します。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。この中には、デバイスの初期セットアップ時に設定され、その後はほとんど変更されることがない基本設定も含まれます。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状態を表示します。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。機能によって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）]：システム設定のバックアップ、または以前のバックアップの復元を実行します。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 の要請を受けたときに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 デバイスの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、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 （42 ページ）」を参照してください。

次のタスク

メインメニューにある [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、[オブジェクト（Objects）] をクリックして、これらのポリシーに必要なオブジェクトを設定することもできます。

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、接続を復号する必要があります。SSL 復号ポリシーを使用して、どの接続を復号する必要があるか判断します。検査後にシステムが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 のユーザにネットワーク アクティビティを関連付ける場合、またはユーザやユーザ 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を判断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）：NAT ポリシーを使用して内部 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します。NAT の設定を参照してください。
- [アクセス制御（Access Control）]：アクセス制御ポリシーを使用してネットワーク上で許可する接続を決定します。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、ユーザまたはユーザ グループでフィルター処理できます。また、アクセス制御ルールを使用して侵入およびファイル（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 ポリシーの設定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ても、侵入ポリシーを編集して特定の侵入ルールを有効または無効にすることができます。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 （42 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。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

ポリシーや設定を更新した場合、その変更内容はすぐにはデバイスに適用されません。設定を変更するには、次の 2 つの手順を実行します。

1. 設定情報を修正します。
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、潜在的な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。

必要な変更をすべて完了した後、次の手順に従って変更をデバイスに展開します。

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変更 （44 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つことができます。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変更

設定変更の展開時に、次の設定またはアクションによりインスペクションエンジンが再起動されます。

注意 展開時には、リソースに対する需要に伴い、少数のパケットが検査なしでドロップされることがあります。また、一部の設定の展開時に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が、これによりトラフィック検査が中断され、トラフィックがドロップされます。

導入

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 つまたは複数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が更新されました。
- ハイ アベイラビリティ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、検査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、その際に検査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

バイナリ変更が含まれており、システムの再起動を必要としないシステム更新またはパッチをインストールする際には、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ていることがあります。バイナリ変更が含まれていないパッチでは、Snort の再起動が必要となることが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。

インターフェイスおよび管理ステータスの表示

[デバイス概要（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の選択設定が表示されます。[デバイス概要（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、各要素のステータスに基づいて色が変わります。要素にマウス ポインタを合わせると、追加情報が表示されるものがあります。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） グラフィックのインターフェイス部分（インターフェイス ステータス情報を含む）は、[インターフェイス（Interfaces）] ページと **[監視（Monitoring）]** > **[システム（System）]** ダッシュボードにも表示されます。

インターフェイス ステータス

ポートにマウス ポインタを合わせると、その IP アドレス、有効ステータス、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か、または DHCP を使用して取得することができます。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 ポートでは次のカラー コーディングが使用されます。

- 緑色：インターフェイスが設定され、有効であり、リンクが稼動しています。
- 灰色：インターフェイスは無効です。
- オレンジ色/赤色：インターフェイスが設定され、有効ですが、リンクは停止しています。インターフェイスが有線接続している場合、これは修正する必要があるエラー状況です。インターフェイスが有線接続していない場合、これは想定されるステータスです。

内部/外部ネットワーク接続

グラフィックでは、次の条件で、外部（またはアップストリーム）ネットワークまたは内部ネットワークに接続するポートが示されています。

- 内部ネットワーク：内部ネットワークのポートは、「inside」という名前のインターフェイスについてのみ表示されます。その他の内部ネットワークがある場合、これらは表示されません。インターフェイスに 1 つも「inside」という名前が指定されていない場合、内部ポートとしてマークされるポートはありません。
- 外部ネットワーク：外部ネットワークのポートは、「outside」という名前のインターフェイスについてのみ表示されます。内部ネットワークと同様に、この名前は必須です。この名前が指定されていない場合、外部ポートとしてマークされるポートはありません。

管理設定ステータス

このグラフィックには、ゲートウェイ、DNS サーバ、NTP サーバ、スマート ライセンスが設定されているかどうかと、それらの設定が正しく機能しているかどうかが示されています。

緑色は機能が設定されており正しく機能していることを示し、灰色は機能が設定されていないか正しく機能していないことを示します。たとえば、サーバに到達できない場合、DNS ボックスは灰色です。詳細情報を表示するには、アイコンにマウス ポインタを合わせます。

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：**[システム設定（System Settings）]** > **[DNS サーバ（DNS Server）]** の順に選択します。
- NTP サーバ：**[システム設定（System Settings）]** > **[NTP（NTP）]** の順に選択します。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）] グループの [設定の表示（View Configuration）] リンクをクリックします。

システムのタスク ステータスの表示

システムのタスクには、データベース更新の取得および適用など、直接の介入なしに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]**>**[デバイス管理]**>**[監査ログ]**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 ステータスを評価します。

解決しない問題が見つかった場合、デバイス設定を修正しなければならないことがあります。たとえば、データベース更新を入手できない問題が続く場合、デバイスの管理 IP アドレスでインターネットへのパスが存在しないことを示しています。タスクに示される問題の中には、Cisco Technical Assistance Center（TAC）に問い合わせる必要があるものもあります。

タスク リストでは次の操作を行えます。

- [成功（Success）] または [障害（Failures）] ボタンをクリックして、ステータスに基づいたリストのみを表示する。
- 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。
- [完了したすべてのタスクを削除（Remove All Completed Tasks）] をクリックして、実行していないタスクをリストから削除する。

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。