使用する前に

ここでは、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

このガイドでは、Firepower Threat Defense デバイスに含まれている Firepower Device Manager の Web ベースのインターフェイスを使用して Firepower Threat Defense を設定する方法について説明します。

Firepower Device Manager を使うことで、小～中規模な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の設定が行えます。また、これは多くの Firepower Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

多数のデバイスを管理している場合、または Firepower Threat Defense で許可される、より複雑な機能や設定を使用したい場合、統合 Firepower Device Manager の代わりに Firepower Management Center デバイスを使用します。

Firepower Device Manager は次のデバイスで使用できます。

表 *1 : Firepower Device Manager* がサポートされるモデル

デバイス モデル	Firepower Threat Defense の最小ソフトウェア バージョン
Firepower 2110、2120、2130、2140	6.2.1
Firepower Threat Defense Virtual VMware 用	6.2.2

デバイス モデル	Firepower Threat Defense の最小ソフトウェア バージョン
Firepower Threat Defense Virtual カーネルベース仮想マシン（KVM）ハイパーバイザ用	6.2.3
ASA 5508-X、5516-X	6.1
ASA 5525-X、5545-X、5555-X	6.1
ASA 5506-X、5506H-X、5506W-X、5512-X	6.1
ASA 5515-X	6.1
ISA 3000（Cisco 3000 シリーズ産業用セキュリティ アプライアンス）	6.2.3

Firepower Device Manager/FTD 6.2 の新機能

リリース：2017 年 1 月 23 日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.2 で使用できる新機能を示します。

機能	説明
Cisco Defense Orchestrator のクラウド管理	Cisco Defense Orchestrator のクラウドベースのポータルを使用してデバイスを管理できます。**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[クラウド管理（Cloud Management）]** を選択します。Cisco Defense Orchestrator の詳細については、http://www.cisco.com/go/cdo を参照してください。
アクセス ルールのドラッグ アンド ドロップ	ルール テーブルで、アクセス ルールをドラッグ アンド ドロップして移動できます。
FTD ソフトウェア アップグレード	Firepower Device Manager 経由でソフトウェア アップグレードをインストールできます。**[デバイス（Device）]** > **[更新（Updates）]** を選択します。

機能	説明
FTD のデフォルト設定の変更	新しいデバイスまたは再イメージ化されたデバイスでは、デフォルト設定に次の重要な変更が含まれます。 • （ASA 5506-X、5506W-X、5506H-X）最初のデータ インターフェイスと ASA 5506W-X の Wi-Fi インターフェイスを除き、これらのデバイス モデルのその他すべてのデータインターフェイスは、「内部」ブリッジ グループに構造化され、有効化されます。DHCP サーバは内部のブリッジ グループにあります。ブリッジドインターフェイスにエンドポイントまたはスイッチを接続することができ、エンドポイントは 192.168.1.0/24 ネットワーク上のアドレスを取得します。 • 内部インターフェイス IP アドレスは 192.168.1.1 です。DHCP サーバは、アドレス プールの 192.168.1.5 ～ 192.168.1.254 のインターフェイスで定義されます。 • HTTPS アクセスは内部インターフェイスで有効なため、デフォルト アドレス（192.168.1.1）で内部インターフェイスを介して Firepower Device Manager を開くことができます。ASA 5506-X モデルでは、内部ブリッジ グループ メンバー インターフェイス経由でこれを実行できます。 • 管理ポートは、192.168.45.0/24 ネットワークの DHCP サーバをホストします。ワークステーションを管理ポートに直接接続して、IP アドレスを取得し、Firepower Device Manager を開いてデバイスを設定できます。 • OpenDNS のパブリック DNS サーバは、現在、管理インターフェイスのデフォルト DNS サーバです。以前は、デフォルト DNS サーバはありませんでした。デバイスの設定時に、別の DNS サーバを設定できます。 • 管理 IP アドレスのデフォルト ゲートウェイでは、データ インターフェイスを使用してインターネットにルーティングします。したがって、Management 物理インターフェイスをネットワークに配線する必要はありません。

機能	説明
管理インターフェイスおよびアクセスの変更	管理アドレス機能および Firepower Device Manager へのアクセス方法に対するいくつかの変更： • HTTPS（Firepower Device Manager 用）および SSH（CLI 用）接続に対するデータ インターフェイスを開くことができます。デバイスを管理するために、別の管理ネットワークを必要としたり、管理/診断物理ポートを内部ネットワークに接続したりする必要はありません。**[デバイス（Device）] > [システム設定（System Settings）] > [管理アクセス リスト（Management Access List）]** を選択します。 • システムは、外部インターフェイスのゲートウェイ経由でシステムデータベースのアップデートを取得できます。管理インターフェイスまたはネットワークからインターネットへの明示的なルートは必要ありません。デフォルトでは、データ インターフェイスを介して内部ルートを使用します。ただし、別の管理ネットワークを使用する場合、特定のゲートウェイを設定できます。**[デバイス（Device）] > [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。 • Firepower Device Manager を使用して、DHCP を介して IP アドレスを取得するように管理インターフェイスを設定できます。**[デバイス（Device）] > [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。 • スタティック アドレスを設定する場合、管理アドレスで DHCP サーバを設定できます。**[デバイス（Device）] > [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。

機能	説明
さまざまなユーザ インターフェイスの変更	次に、Firepower Device Manager ユーザ インターフェイスの注目すべき変更を示します。 • [デバイス（Device）] メイン メニュー項目。以前のリリースでは、このメニュー項目はデバイスのホスト名でした。また、開くページは、[デバイスダッシュボード（Device Dashboard）] ではなく [デバイスサマリー（Device Summary）] と呼ばれます。 • デバイスの初期設定時に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。最初のデータ インターフェイスがデフォルトの外部インターフェイスです。 • **[デバイス（Device）] > [システム設定（System Settings）] > [クラウド設定（Cloud Preferences）]** は、**[デバイス（Device）] > [システム設定（System Settings）] > [URLフィルタリング設定（URL Filtering Preferences）]** と呼ばれます。 • **[システム設定（System Settings）] > [DHCP サーバ（DHCP Server）]** ページは 2 つのタブで構成され、グローバル パラメータとは異なる DHCP サーバ テーブルが表示されます。
サイト間 VPN 接続	事前共有キーを使用して、サイト間のバーチャル プライベート ネットワーク（VPN）接続を設定できます。IKEv1 および IKEv2 接続を設定できます。

機能	説明
統合ルーティングおよびブリッジングのサポート	統合ルーティングおよびブリッジングによって、ブリッジ グループとルーテッド インターフェイスの間でルーティングする機能が提供されます。ブリッジ グループは、FTD デバイスがルーティングではなくブリッジするインターフェイスのグループです。FTDデバイスは、FTDデバイスがファイアウォールとして継続的に機能する本当のブリッジではありません。インターフェイス間のアクセス コントロールは管理され、すべての通常のファイアウォール チェックが実行されます。 この機能によって、ブリッジ グループを設定したり、ブリッジ グループ間およびブリッジ グループとルーテッドインターフェイスの間でルーティングするようにブリッジ グループを設定したりできます。ブリッジ グループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジグループのゲートウェイとして機能することによってルーティングに参加します。FTD デバイスにブリッジ グループを割り当てるための追加インターフェイスがある場合、統合ルーティングおよびブリッジングによって、外部のレイヤ 2 スイッチを使用するのではない別の方法が提供されます。BVI は、名前付きインターフェイスにすることができ、メンバー インターフェイスとは別にいくつかの機能（DHCP サーバなど）に参加できます。ここで、ブリッジ グループ メンバー インターフェイスで他の機能（NAT、アクセス コントロール ルールなど）を設定します。 **[デバイス（Device）] > [インターフェイス（Interfaces）]** を選択して、ブリッジ グループを設定します。

Firepower Device Manager/FTD 6.2.1 の新機能

リリース日：2017 年 5 月 15 日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.2.1 で使用できる新機能を示します。

（注） このリリースは、Firepower 2100 シリーズ のみに適用されます。

機能	説明
リモートアクセスVPNの設定	AnyConnect クライアントのリモート アクセス SSL VPN を設定できます。**[デバイス（Device）] > [リモート アクセス VPN（Remote Access VPN）]** グループから RA VPN を設定します。**[デバイス（Device）] > [スマート ライセンス（Smart License）]** グループから RA VPN ライセンスを設定します。
Firepower 2100 シリーズ デバイス設定	Firepower Device Manager を使用して、Firepower 2100 シリーズ デバイスで FTD を設定できます。

Firepower Device Manager/FTD 6.2.2 の新機能

リリース：2017年9月5日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.2.2 で使用できる新機能を示します。

機能	説明
ASA 5500-X シリーズ デバイスのリモートアクセスVPNの設定	ASA 5500-X シリーズ デバイスでは、AnyConnect クライアント用にリモート アクセス SSL VPN を設定できます。**[デバイス（Device）] > [リモート アクセス VPN（Remote Access VPN）]** グループから RA VPN を設定します。**[デバイス（Device）] > [スマート ライセンス（Smart License）]** グループから RA VPN ライセンスを設定します。
Firepower Threat Defense Virtual for VMware デバイス設定。	Firepower Device Manager を使用して Firepower Threat Defense Virtual for VMware デバイス上の FTD を設定できます。その他の仮想プラットフォームは、Firepower Device Manager ではサポートされません。 （注） Firepower Device Manager でサポートされるようにするには、新しい 6.2.2 イメージをインストールする必要があります。既存の仮想マシンを古いバージョンからアップグレードして Firepower Device Manager に切り替えることはできません。

Firepower Device Manager/FTD バージョン 6.2.3 の新機能

リリース：2018年3月29日

次の表に、Firepower Device Manager を使用して設定された場合に FTD 6.2.3 で使用できる新機能を示します。

機能	説明
SSL/TLS の復号	接続の内容を調べることができるように、SSL/TLS 接続を復号できます。復号しないと、暗号化された接続は、侵入およびマルウェアの脅威を識別したり、URLおよびアプリケーション使用状況ポリシーへの準拠を強制したりするための効果的な検査が行えません。**[Policies]** > **[SSL Decryption]** ページおよび **[Monitoring]** > **[SSL Decryption]** ダッシュボードが追加されました。 **注目** アクティブな認証を実装するアイデンティティポリシーは、SSL復号ルールを自動的に生成します。SSL復号をサポートしていないリリースからアップグレードする場合、SSL 復号ポリシーは、この種類のルールがある場合、自動的に有効になります。ただし、アップグレードの完了後、再署名の復号ルールで使用する証明書を指定する必要があります。アップグレード後すぐに SSL 復号設定を編集してください。
セキュリティ インテリジェンスのブラックリスト登録	新しい **[ポリシー（Policies）]** > **[セキュリティインテリジェンス（Security Intelligence）]** ページから設定できるセキュリティ インテリジェンス ポリシーにより、送信元/宛先の IP アドレスまたは宛先URLに基づいて、望ましくないトラフィックを早い段階でドロップできます。許可された接続もすべてアクセス コントロール ポリシーによって引き続き評価され、最終的にドロップされる可能性があります。セキュリティインテリジェンスを使用するには、脅威ライセンスを有効にする必要があります。 また、[ポリシー（Policies）] ダッシュボードの名前を [アクセスおよびSIルール（Access And SI Rules）] に変更し、セキュリティ インテリジェンス同等のルールがアクセス ルールとともにダッシュボードに含まれるようになりました。
侵入ルールの調整	アクセス制御ルールを適用する事前に定義された侵入ポリシー内の侵入ルールのアクションを変更できます。トラフィックに一致するイベント（警告）をドロップまたは生成する各ルールを設定したり、ルールを無効にしたりできます。有効になっているルールのアクション（ドロップまたは警告に設定）のみ変更できます。デフォルトで無効になっているルールを有効にはできません。侵入ルールを調整するには、**[ポリシー（Policies）]** > **[侵入（Intrusion）]** を選択します。

機能	説明
侵入ポリシーに基づく自動ネットワーク分析ポリシー（NAP）割り当て	以前のリリースでは、[Balanced Security and Connectivity] ネットワーク分析ポリシーが、特定の送信元/送信先のセキュリティゾーンとネットワーク オブジェクトの組み合わせに割り当てられた侵入ポリシーに関係なく、プリプロセッサ設定で常に使用されました。システムは自動的に NAP ルールを生成し、同じ名前の NAP と侵入ポリシーをそれらの基準に基づいてトラフィックに割り当てるようになりました。レイヤ 4 または 7 の基準を使用して異なる侵入ポリシーをトラフィック（それ以外は同じ送信元/送信先のセキュリティ ゾーンおよびネットワーク オブジェクトと一致する）に割り当てる場合、完全に一致する NAP および侵入ポリシーは取得されないことに注意してください。カスタム ネットワーク分析ポリシーは作成できません。
脅威、攻撃、およびターゲットのダッシュボード用のドリル ダウン レポート	脅威、攻撃、およびターゲットのダッシュボードに移動して、報告された項目についての詳細を表示できるようになりました。これらのダッシュボードは [Monitoring] ページで使用できます。 これらの新しいレポートのため、6.2.3 より前のリリースからアップグレードする場合は、これらのダッシュボードのレポートデータが失われます。
[Web Applications] ダッシュボード	新しい [Web Applications] ダッシュボードは、Google など、ネットワークで使用されている上位の Web アプリケーションを示します。このダッシュボードはアプリケーションのダッシュボードを強化し、HTTP の使用率などのプロトコル指向の情報を提供します。
新しいゾーンのダッシュボードが入力ゾーンと出力ゾーンのダッシュボードを置き換え	新しいゾーンのダッシュボードは、デバイスに入ってから出るトラフィックに対する上位セキュリティ ゾーンのペアを示します。このダッシュボードは、入力および出力ゾーンに対する個別のダッシュボードを置き換えます。
新しいマルウェア ダッシュボード	新しいマルウェア ダッシュボードは、上位のマルウェアのアクションと判定結果の組み合わせを示します。ドリルダウンして、関連付けられているファイル タイプの情報を参照できます。この情報を表示するには、アクセス ルールにファイル ポリシーを設定する必要があります。
自己署名入りの内部証明書、および内部 CA 証明書	自己署名入りの内部アイデンティティ証明書を生成できるようになりました。また、SSL 復号ポリシーで使用するための、自己署名付きの内部 CA 証明書を生成し、アップロードできるようになりました。これらの機能を、**[Objects]** > **[Certificates]** ページで設定します。

機能	説明
インターフェイスのプロパティ編集時に DHCP サーバの設定を編集する機能	インターフェイスのプロパティを編集すると同時に、インターフェイスに設定されている DHCP サーバの設定を編集できるようになりました。これにより、インターフェイスの IP アドレスを別のサブネットに変更する必要がある場合に、DHCP アドレス プールを簡単に再定義できます。
製品を改善し、効果的な技術サポートを提供するための、Cisco Success Network によるシスコへの利用状況や統計データの送信	Cisco Success Network に接続し、シスコにデータを送信できます。Cisco Success Network を有効にすることで、テクニカル サポートを提供するために不可欠な、使用状況の情報と統計情報をシスコに提供します。またこの情報により、シスコは製品を向上させ、未使用の使用可能な機能を認識させるため、ネットワーク内にある製品の価値を最大限に生かすことができます。Cisco Smart Software Manager でデバイスを登録するとき、または後から好きなときに、接続を有効にできます。接続はいつでも無効にできます。 Cisco Success Network はクラウド サービスです。**[Device]** > **[System Settings]** > **[Cloud Management]** ページの名前が [Cloud Services] に変更されました。同じページから、Cisco Defense Orchestrator を設定できます。
Firepower Threat Defense Virtual for Kernel-based Virtual Machine（KVM）ハイパーバイザデバイス設定	Firepower Device Manager を使用して Firepower Threat Defense Virtual for KVM デバイス上の FTD を設定できます。以前は、VMware のみがサポートされていました。 （注） Firepower Device Manager のサポートを得るには、新しい 6.2.3 イメージをインストールする必要があります。既存の仮想マシンを古いバージョンからアップグレードして Firepower Device Manager に切り替えることはできません。
ISA 3000（Cisco 3000 シリーズ産業用セキュリティアプライアンス）デバイスの設定	Firepower Device Manager を使用して ISA 3000 デバイス上の FTD を設定できます。ISA 3000 は脅威のライセンスのみをサポートしていることに注意してください。URL フィルタリングやマルウェアのライセンスはサポートしていません。したがって、ISA 3000 では URL フィルタリングやマルウェアのライセンスを必要とする機能は設定できません。

機能	説明
ルール データベースまたは VDB の更新でのオプションの展開	侵入ルール データベースまたは VDB を更新する、または更新スケジュールを設定する際に、更新が即時展開しないようにすることができます。更新プログラムは検査エンジンを再起動するため、展開時に瞬間的なトラフィックのドロップが発生します。自動的に展開しないことにより、トラフィックのドロップの影響が最小になる場合に展開を開始できます。 （注） VDB ダウンロードは、単独で Snort を再起動することもできますが、展開時に再起動が発生します。ダウンロード時の再起動を止めることはできません。
展開が Snort を再起動するかどうかを示す、改善されたメッセージ。さらに、展開時の Snort を再起動する必要性の低下	展開を開始する前に、Firepower Device Manager により、設定の更新で Snort の再起動が必要かどうかが示されます。Snort の再起動は、トラフィックの瞬間的なドロップを発生させます。したがって、展開がトラフィックに影響を与えず、すぐに実行できるかどうかがわかるようになったため、混乱が少ないときに展開できます。 さらに、以前のリリースでは展開の実行の度に Snort が再起動されていました。Snort は、次の理由でのみ再起動されるようになりました。 • ユーザが SSL 復号ポリシーを有効または無効にする • 更新されたルール データベースまたは VDB がダウンロードされた • ユーザが 1 つまたは複数の物理インターフェイス（ただしサブインターフェイスではない）で MTU を変更した
Firepower Device Manager の CLI コンソール	Firepower Device Manager から CLI コンソールを開くことができるようになりました。CLI コンソールは SSH またはコンソール セッションを模倣していますが、コマンドのサブセットのみ（**show**、**ping**、**traceroute**、および **packet-tracer**）を許可します。トラブルシューティングとデバイスのモニタリングに CLI コンソールを使用します。

機能	説明
管理アドレスへのアクセスのブロックのサポート	プロトコルが管理 IP アドレスにアクセスできないようにするため、すべての管理アクセスリストのエントリを削除できるようになりました。以前は、すべてのエントリを削除すると、すべてのクライアントIPアドレスからのアクセスを許可するようにシステムのデフォルトが設定されていました。6.2.3 へのアップグレードでは、以前からのプロトコル（HTTPS またはSSH）用の空の管理アクセス リストがあった場合、システムはすべての IP アドレス用のデフォルトの許可ルールを作成します。必要に応じて、これらのルールを削除できます。 また、SSH または HTTPS アクセスを無効にする場合を含み、Firepower Device Manager は CLI から管理アクセス リストに加えた変更を認識します。 少なくとも 1 つのインターフェイスに対する HTTPS アクセスを有効にしてください。そうしないとデバイスを設定および管理することができません。

機能	説明
デバイス CLI を使用した、機能の設定のための Smart CLI および FlexConfig	Smart CLI と FlexConfig により、まだ Firepower Device Manager ポリシーおよび設定では直接サポートされていない機能を設定できます。Firepower Threat Defense は、ASA 設定コマンドを使用していくつかの機能を実装します。ASA 設定コマンドの知識があり、専門家ユーザの場合、次の方法を使用して、デバイスでこれらの機能を設定できます。 • Smart CLI：（推奨される方法です。）Smart CLI テンプレートは、特定の機能の定義済みテンプレートです。機能に必要なすべてのコマンドが提供されているため、変数の値を選択するだけで済みます。システムにより選択が検証されるため、機能を正しく設定できる可能性が高まります。目的の機能の Smart CLI テンプレートが存在する場合は、この方法を使用する必要があります。このリリースでは、Smart CLI を使用して、OSPFv2 を設定できます。 • FlexConfig：FlexConfig ポリシーは、FlexConfig オブジェクトのコレクションです。FlexConfig オブジェクトは Smart CLI テンプレートより自由な形式であり、システムに CLI 変数はなく、データ検証も行われません。有効な一連のコマンドを作成するには、ASA 設定コマンドを知り、ASA 設定ガイドに従う必要があります。 **注意** Smart CLI と FlexConfig の利用は、ASA の強力なバックグラウンドを持つ上級者が自身のリスクで行う場合にかぎることをシスコは強く推奨します。ブラックリストに登録されていない任意のコマンドも設定できます。Smart CLI または FlexConfig を介して機能を有効にすると、その他の設定済みの機能に予期しない結果が発生する可能性があります。
Firepower Threat Defense REST API、および API Explorer	REST API を使用して、Firepower Device Manager を介してローカルで管理している Firepower Threat Defense デバイスをプログラムで操作できます。オブジェクトモデルを表示し、クライアントプログラムから作成できるさまざまな呼び出しのテストに使用できる API エクスプローラがあります。API エクスプローラを開くには、Firepower Device Manager にログインし、URL のパスを /#/api-explorer（https://ftd.example.com/#/api-explorer など）に変更します。

システムへのログイン

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

Firepower Device Manager Web インターフェイス

Firepower Device Manager はお使いの 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。Firepower Device Manager の代わりに、初期設定にも使用できます。

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

Firepower Device Manager へのログイン

Firepower Device Manager を使用して、システムを設定、管理、およびモニタします。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、または Internet Explorer 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つ必要があります。

始める前に

Firepower Device Manager には、**admin** ユーザ名のみを使用してログインできます。Firepower Device Manager アクセスするための追加ユーザは作成できません。

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。デフォルトでは、これは管理/診断インターフェイスの 192.168.45.45 です。
- 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。デフォルト（ほとんどのハードウェア プラットフォーム）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。 内部インターフェイスがブリッジ グループであるデバイス モデルでは、任意のブリッジ グループ メンバー インターフェイスを介してこのアドレスに接続できます。

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　**admin** のユーザ名とパスワードを入力して、[ログイン（Login）] をクリックします。

デフォルトの admin パスワードは Admin123 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（user）] アイコンのドロップダウン リストから [ログアウト（Log Out）] を選択するとログアウトできます。

CLI（コマンドライン インターフェイス）へのログイン

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

CLI にログインするには、次のいずれかを実行します。

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

（注）　Firepower 2100 デバイスでは、コンソールポートの CLI は FXOS です。**connect ftd** コマンドを使用して FTD CLI にアクセスできます。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 FTD 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。

- Firepower 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** ユーザ名（デフォルトのパスワードは **Admin123** です）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。

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。Firepower Device Manager の Web インターフェイスにはログインできません。

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、Firepower 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。

手順

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

ステップ 2 [パスワード（Password）] タブをクリックします。

ステップ 3 現在のパスワードを入力します。

ステップ 4 新しいパスワードを入力して確認します。

ステップ 5 [変更（Change）] をクリックします。

ユーザ プロファイルの設定

ユーザ 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（user）] アイコンのドロップダウンリストから、[プロファイル（Profile）] を選択します。

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

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

FTD CLI のローカル ユーザ アカウントの作成

FTD デバイスで CLI にアクセスするユーザを作成できます。これらのアカウントは管理アプリケーションへのアクセスは許可されず、CLI へのアクセスのみが有効になります。CLI はトラブルシューティングやモニタリング用に役立ちます。

複数のデバイス上にローカルユーザアカウントを一度に作成することはできません。デバイスごとに固有のローカルユーザ CLI アカウントのセットがあります。

手順

ステップ 1 config 権限を持つアカウントを使用してデバイスの CLI にログインします。

管理者ユーザアカウントには必要な権限がありますが、config 権限を持っていればどのアカウントでも問題ありません。SSH セッションまたはコンソール ポートを使用できます。

特定のデバイス モデルでは、コンソール ポートから FXOS CLI に移動します。**connect ftd** を使用して FTD の CLI にアクセスします。

ステップ 2 ユーザ アカウントを作成します。

configure user add *username* {**basic** | **config**}

次の権限レベルを持つユーザを定義できます。

- **config**：ユーザに設定アクセス権を付与します。すべてのコマンドの管理者権限がユーザに与えられます。

- **basic**：ユーザに基本的なアクセス権を付与します。ユーザはコンフィギュレーション コマンドを入力することはできません。

例：

次の例では、config アクセス権を使用して、joecool という名前のユーザ アカウントを追加します。パスワードは入力時に非表示となります。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

（注） 自分のパスワードを **configure password** コマンドを使用して変更できることをユーザに伝えます。

ステップ 3 （オプション）セキュリティ要件を満たすようにアカウントの性質を調整します。

アカウントのデフォルト動作を変更するには、次のコマンドを使用できます。

- **configure user aging** *username max_days warn_days*

  ユーザパスワードの有効期限を設定します。パスワードの最大有効日数と、有効期限が近づいたことをユーザに通知する警告を期限切れとなる何日前に発行するかを指定します。どちらの値も 1 ~ 9999 ですが、警告までの日数は最大日数以内にする必要があります。アカウントを作成した場合、パスワードの有効期限はありません。

- **configure user forcereset** *username*

  次回ログイン時にユーザにパスワードを強制的に変更するよう要求します。

- **configure user maxfailedlogins** *username number*

  アカウントがロックされる前の連続したログイン失敗の最大回数を 1 ~ 9999 までで設定します。**configure user unlock** コマンドを使用してアカウントのロックを解除します。新しいアカウントのデフォルトは、5 回連続でのログインの失敗です。

- **configure user minpasswdlen** *username number*

  パスワードの最小長を 1 ~ 127 までで設定します。

- **configure user strengthcheck** *username* {**enable** | **disable**}

  パスワードの変更時にユーザに対してパスワード要件を満たすように要求する、パスワードの強度確認を有効または無効にします。ユーザパスワードの有効期限が切れた場合、または **configure user forcereset** コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

ステップ 4 必要に応じてユーザ アカウントを管理します。

ユーザをアカウントからロックアウトしたり、アカウントを削除するか、またはその他の問題を修正したりしなければならない可能性があります。システムのユーザアカウントを管理するには、次のコマンドを使用します。

- **configure user access** *username* {**basic** | **config**}

  ユーザ アカウントの権限を変更します。

- **configure user delete** *username*

  指定したアカウントを削除します。

- **configure user disable** *username*

  指定したアカウントを削除せずに無効にします。ユーザは、アカウントを有効にするまでログインできません。

- **configure user enable** *username*

  指定したアカウントを有効にします。

- **configure user password** *username*

  指定したユーザのパスワードを変更します。ユーザは通常、**configure password** コマンドを使用して自分のパスワードを変更する必要があります。

- **configure user unlock** *username*

  ログイン試行の最大連続失敗回数の超過が原因でロックされたユーザアカウントをロック解除します。

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 （34 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 （20 ページ）

ステップ 2 初期設定の完了 （27 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（37ページ）を参照してください。

ステップ 3 ワイヤレス アクセス ポイント（ASA 5506W-X）の設定 （31 ページ）

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。

ハードウェア モデルのデフォルト設定は、内部インターフェイスにワークステーションを直接接続できるように設計されています。内部インターフェイスがブリッジ グループであるデバイス モデルでは、すべてのメンバー インターフェイスに接続できます。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。正しいネットワークでアドレスを取得するには、DHCPを使用します。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または管理インターフェイスを、アクティブなDHCPサーバがあるネットワークに接続しないでください。接続すると、内部ポートおよび管理ポートに対して実行されている既存の DHCP サーバとの競合が生じます。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、ワークステーションを直接管理ポートに接続し、初期設定を完了してから、不要なDHCPサーバを無効にします。その後、デバイスをネットワークに接続できます。

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。

ASA 5506-X、5506W-X および 5506H-X の配線

図 *1 : ASA 5506W-X*（*Wi-Fi* あり）、*5506-X*（*Wi-Fi* なし）

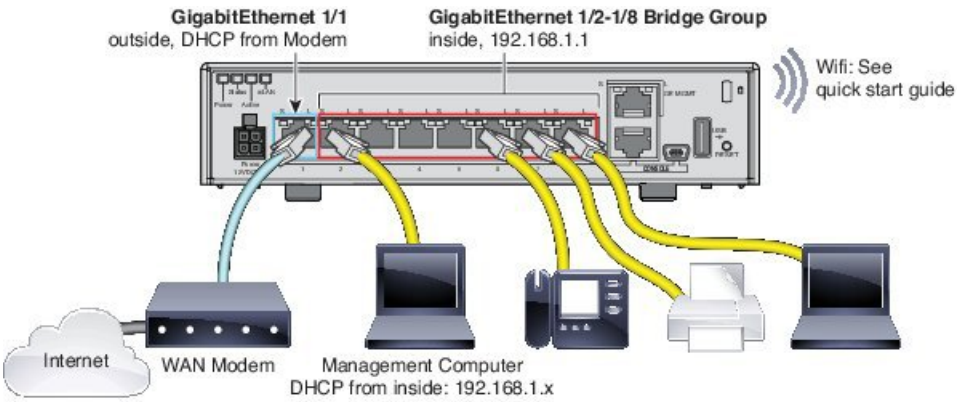
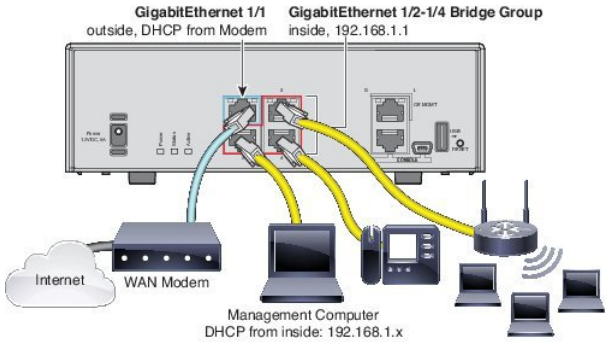


図 *2 : ASA 5506H-X*

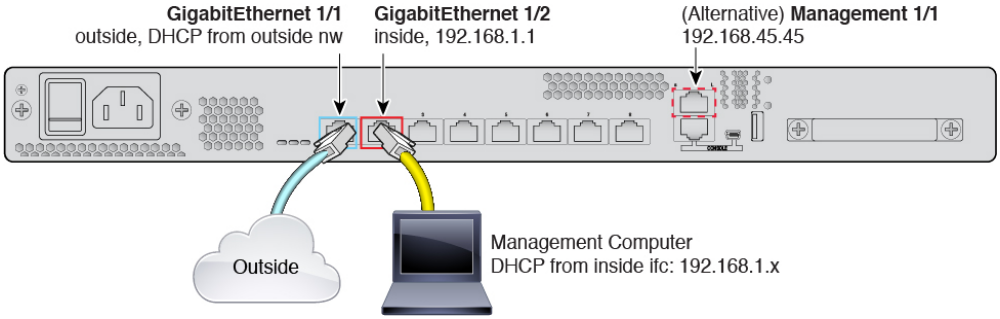


- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- デバイスを設定するために使用するワークステーションに、GigabitEthernet 1/2（または別の内部ブリッジ グループのメンバー ポート）を接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。

（注） 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、GigabitEthernet 1/2 などの内部ポートの 1 つにそのスイッチを接続することです。ただし、他のデバイスがスイッチのネットワーク上で DHCP サーバを実行していないことを確認する必要があります。これは、そのデバイスが内部ブリッジ グループ 192.168.1.1 で実行中のデバイスと競合するためです。

- 必要に応じて、内部ブリッジグループ内の別のポートに別のエンドポイントまたはスイッチを接続します。デバイスの初期設定が完了するのを待ってからエンドポイントを追加してもよいでしょう。スイッチを追加する場合、内部ブリッジ グループで実行中の DHCP サーバと競合するため、それらのネットワークで他の DHCP サーバが実行中でないことを確認します。

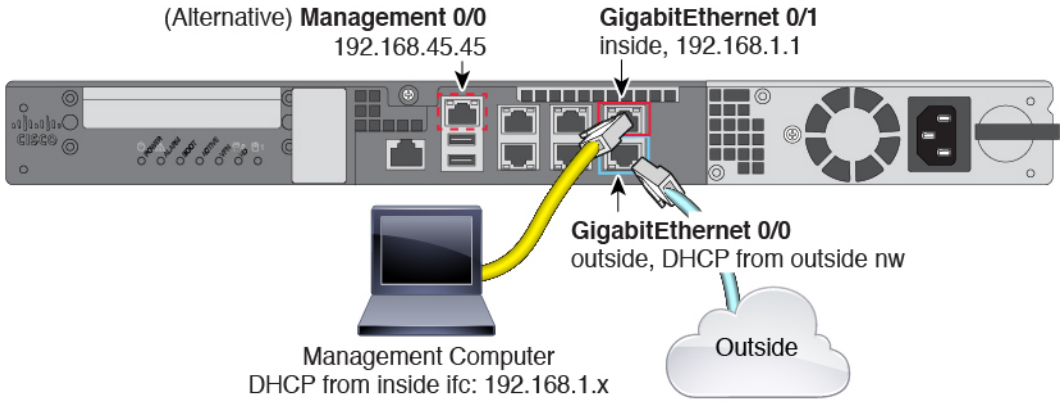
ASA 5508-X および 5516-X の配線



- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- GigabitEthernet 1/2 をデバイスを設定するために使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。

（注） 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、GigabitEthernet 1/2 にそのスイッチを接続することです。ただし、スイッチのネットワーク上の他のデバイスが DHCP サーバを実行しないように徹底する必要があります。内部インターフェイス 192.168.1.1 上で実行されているデバイスと競合するためです。

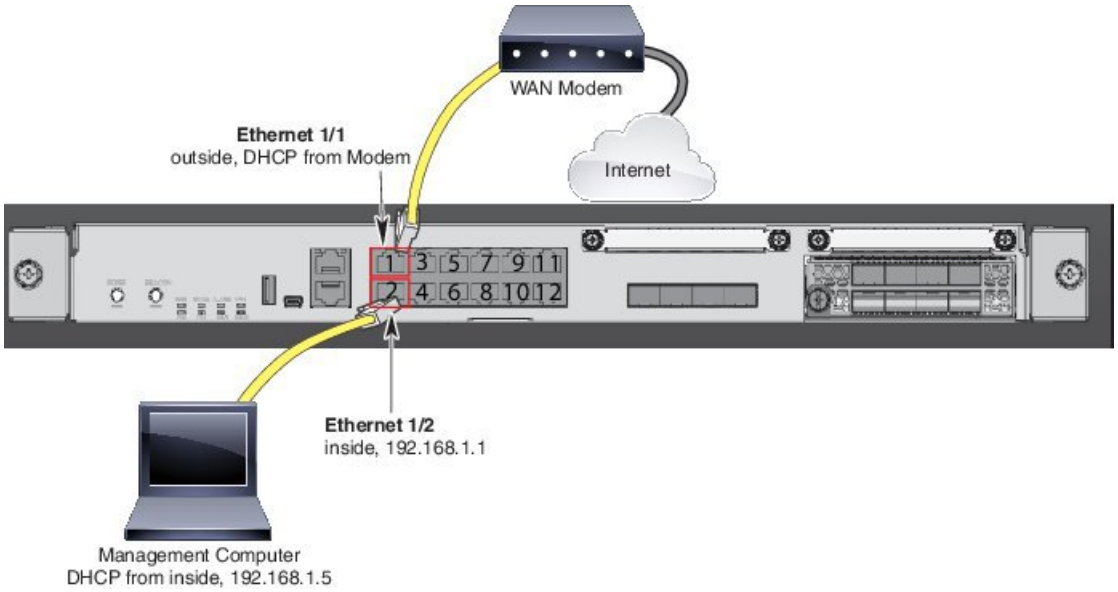
ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X の配線



- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 0/0 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- GigabitEthernet 0/1 をデバイスを設定するために使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。

（注） 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、GigabitEthernet 0/1 にそのスイッチを接続することです。ただし、他のデバイスがスイッチのネットワーク上で DHCP サーバを実行していないことを確認する必要があります。これは、そのデバイスが内部インターフェイス 192.168.1.1 で実行中のデバイスと競合するためです。

Firepower 2100の配線



- ISP/WAN モデムまたはその他の外部デバイスに Ethernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- Ethernet 1/2 をデバイスを設定するために使用するワークステーションに接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。

（注） 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、Ethernet 1/2 にそのスイッチを接続することです。ただし、他のデバイスがスイッチのネットワーク上で DHCP サーバを実行していないことを確認する必要があります。これは、そのデバイスが Ethernet 1/2、192.168.1.1 で実行中のデバイスと競合するためです。

仮想ケーブル接続： Firepower Threat Defense Virtual

Firepower 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 でお使いの仮想プラットフォームに対応した『Cisco Firepower Threat Defense Virtual Quick Start Guid』を参照してください。Firepower Device Manager は、VMware、KVM の各仮想プラットフォームでサポートされています。

Firepower 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。

管理インターフェイスの IP 設定は、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** で定義されている点に注意してください。**[デバイス（Device）]** > **[インターフェイス（Interfaces）]** > **[設定の表示（View Configuration）]** に一覧されている Management0/0（診断）インターフェイスの IP アドレスと同じではありません。

Firepower 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 Firepower 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、で説明しているように、プロセスがさらに複雑になりますFirepower Threat Defense Virtual へのインターフェイスの追加。

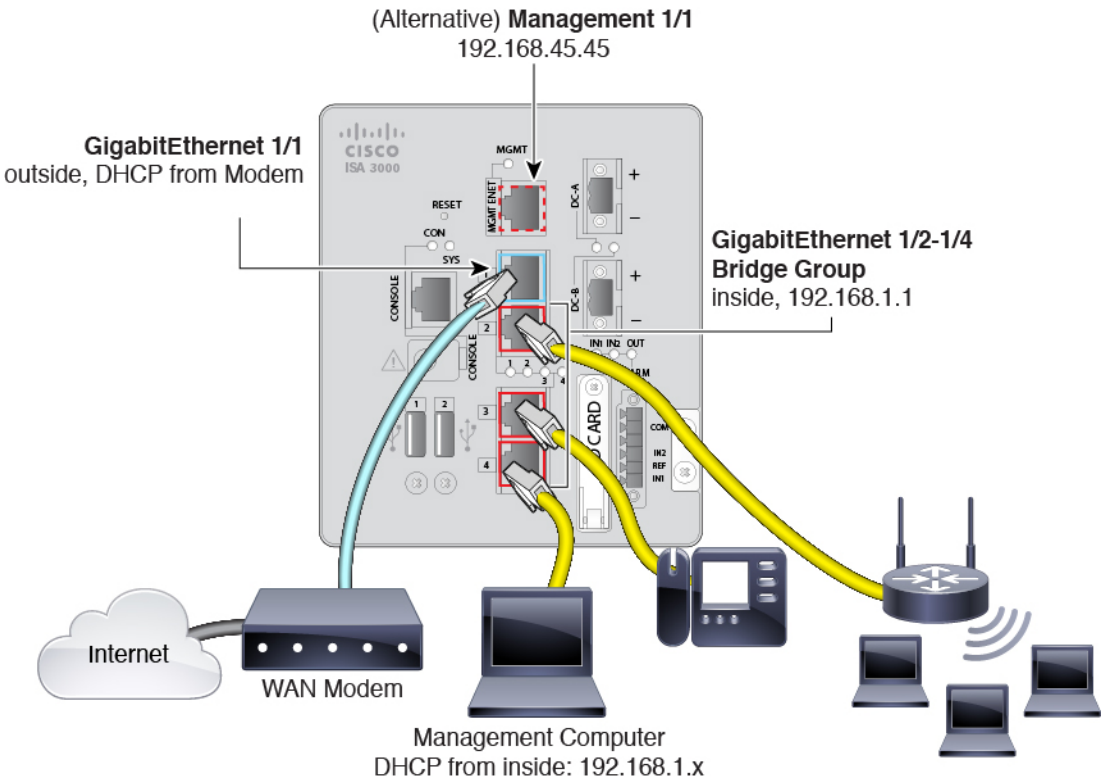
次の表は、VMware ネットワーク アダプタおよび送信元インターフェイスの、Firepower Threat Defense Virtual の物理インターフェイス名へのマッピングを示しています。追加のインターフェイスについては、命名は同じパターンに従い、関連する数字を 1 つずつ増やします。すべての追加インターフェイスはデータ インターフェイスです。仮想ネットワークの仮想マシンへの割り当ての詳細については、VMware のオンライン ヘルプを参照してください。

表 *2*: 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	Diagnostic0/0	管理と診断
Network adapter 2	GigabitEthernet0-0	GigabitEthernet 0/0	内部データ
Network adapter 3	GigabitEthernet0-1	GigabitEthernet 0/1	外部データ
Network adapter 4	GigabitEthernet0-2	GigabitEthernet0/2	データ トラフィック
Network adapter 5	GigabitEthernet0-3	GigabitEthernet 0/3	データ トラフィック
Network adapter 6	GigabitEthernet0-4	GigabitEthernet 0/4	データ トラフィック
Network adapter 7	GigabitEthernet0-5	GigabitEthernet 0/5	データ トラフィック
Network adapter 8	GigabitEthernet0-6	GigabitEthernet 0/6	データ トラフィック
Network adapter 9	GigabitEthernet0-7	GigabitEthernet 0/7	データ トラフィック
Network adapter 10	GigabitEthernet0-8	GigabitEthernet 0/8	データ トラフィック

ISA 3000 のケーブル配線

図 *3 : ISA 3000*



- ISP/WAN モデムまたはその他の外部デバイスに GigabitEthernet 1/1 を接続します。デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティック アドレスを設定することもできます。
- デバイスを設定するために使用するワークステーションに、GigabitEthernet 1/2（または別の内部ブリッジ グループのメンバー ポート）を接続します。DHCP を使用して IP アドレスを取得するようにワークステーションを設定します。ワークステーションは 192.168.1.0/24 ネットワーク上でアドレスを取得します。

（注） 管理ワークステーションへの接続には他にもいくつかの方法があります。また、管理ポートに直接接続することもできます。このワークステーションは、192.168.45.0/24 ネットワーク上で DHCP によりアドレスを取得します。別のオプションは、ワークステーションをスイッチに接続したまま、GigabitEthernet 1/2 などの内部ポートの 1 つにそのスイッチを接続することです。ただし、他のデバイスがスイッチのネットワーク上で DHCP サーバを実行していないことを確認する必要があります。これは、そのデバイスが内部ブリッジ グループ 192.168.1.1 で実行中のデバイスと競合するためです。

- 必要に応じて、内部ブリッジグループ内の別のポートに別のエンドポイントまたはスイッチを接続します。デバイスの初期設定が完了するのを待ってからエンドポイントを追加してもよいでしょう。スイッチを追加する場合、内部ブリッジ グループで実行中の DHCP サーバと競合するため、それらのネットワークで他の DHCP サーバが実行中でないことを確認します。

初期設定の完了

Firepower Device Manager に初めてログインする際には、デバイスのセットアップ 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。

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（20 ページ）および初期設定前のデフォルト設定 （34 ページ）を参照）。

次に、使用ハードウェア モデルの「内部」インターフェイスにワークステーションを接続します。内部インターフェイスがブリッジ グループであるモデルの場合、外部インターフェイス以外のデータ ポートである任意のブリッジ グループ メンバー インターフェイスに接続できます。また、管理/診断物理インターフェイスに接続できます。Firepower 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 Firepower Threat Defense Virtual を除く）。管理/診断用の物理インターフェイスは、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）を介してシステムのライセンシングとデータベースおよびその他の更新が取得されます。代わりに別の管理ネットワークを使用する場合は、初期設定の完了後、管理/診断インターフェイスをネットワークに接続して、別の管理ゲートウェイを設定できます。

手順

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

a) CLI で初期設定を完了していない場合、**https://***ip-address* にアクセスして Firepower Device Manager を開きます。アドレスは以下のいずれかになります。

- 内部インターフェイス、またはデフォルトの内部ブリッジ グループがあるモデルのいずれかの内部ブリッジ グループのデータ インターフェイスに接続している場合は、[https://192.168.1.1]。
- （Firepower Threat Defense Virtual に必要）Management 物理インターフェイスに接続されている場合は **https://192.168.45.45**。

b) ユーザ名 **admin**、およびパスワード **Admin123** を使用してログインします。

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

続行するには、これらの手順を完了する必要があります。

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

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

外部インターフェイス

- [IPv4の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動で静的 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（初期設定前のデフォルト設定 （34 ページ）を参照）。
- [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、または手動で静的 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

- [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、リンクをクリックして Smart Software Manager（SSM）のアカウントにログインし、新しいトークンを作成して、編集ボックスにそのトークンをコピーします。

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 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と無効化を参照してください。
- 新しいシステムの場合、デフォルトの内部ブリッジ グループがあるデバイス モデル上のその他のインターフェイスは、内部ブリッジグループのメンバーとして使用可能な状態になっています。エンドポイントをインターフェイスに直接接続できます。デフォルトの単一の物理インターフェイスがあるモデルの場合、その他のデータ インターフェイスを異なるネットワークに接続して、インターフェイスを設定できます。ブリッジ グループ メンバー インターフェイスの場合、ブリッジ グループからそれらのインターフェイスを削除して、追加の固有ネットワークを設定することもできます。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またはブリッジ グループ メンバー インターフェイスを介してデバイスを管理し、内部インターフェイスを介して CLI セッションを開きたい場合は、SSH 接続に対して内部インターフェイスまたはブリッジ グループを開きます。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。Firepower 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。

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 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。

ワイヤレス アクセス ポイント（ASA 5506W-X）の設定

ASA 5506W-X には、デバイスに統合されている Cisco Aironet 702i ワイヤレス アクセス ポイントが付属します。ワイヤレス アクセス ポイントは、デフォルトでは無効になっています。ワイヤレス無線を有効化し、SSID およびセキュリティの設定を行うには、アクセス ポイント Web インターフェイスに接続してください。

アクセス ポイントは、GigabitEthernet 1/9 インターフェイスを介して内部的に接続します。すべての Wi-Fi クライアントは GigabitEthernet 1/9 ネットワークに属します。セキュリティ ポリシーにより、Wi-Fi ネットワークが他のインターフェイス上の任意のネットワークにアクセスする方法が決まります。アクセス ポイントには、外部インターフェイスやスイッチ ポートは含まれません。

次の手順では、アクセスポイントを設定する方法について説明します。この手順では、デバイス セットアップ ウィザードが完了していると仮定します。代わりに手動でデバイスを設定した場合、設定に基づいて手順を調整する必要があります。

詳細については、次のマニュアルを参照してください。

- ワイヤレス LAN コントローラの使用の詳細については、『Cisco Wireless LAN Controller Software documentation』を参照してください。
- ワイヤレス アクセス ポイントのハードウェアおよびソフトウェアの詳細については、『Cisco Aironet 700 Series documentation』を参照してください。

始める前に

アクセス ポイントに到達できず、FTD デバイス推奨設定になっていて、他のネットワークの問題が見つからない場合、アクセス ポイントをデフォルト設定に復元できます。FTD CLI にアクセス（コンソール ポートに接続、または SSH アクセスを設定）する必要があります。FTD CLI から、次のコマンドを入力します。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password: <press enter, by default, the password is blank>
firepower# hw-module module wlan recover configuration
```

アクセス ポイントのトラブルシューティングをさらに行う必要がある場合、**session wlan console** コマンドを使用して、アクセス ポイント CLI に接続します。

手順

ステップ 1 ワイヤレス インターフェイス GigabitEthernet1/9 を設定して有効化します。

a) [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] グループでリンクをクリックしてインターフェイスのリストを表示します。

b) GigabitEthernet 1/9 インターフェイスの [編集（edit）] アイコン（）をクリックします。

c) 次のオプションを設定します。

- [インターフェイス名（Interface Name）]：インターフェイスの名前（たとえば **wifi** など）を入力します。
- [ステータス（Status）]：インターフェイスを有効にするには、スライダをクリックします。
- [IPv4アドレス（IPv4 Address）]：アドレス タイプに [スタティック（Static）] を選択し、アドレスおよびサブネット マスクを入力します。たとえば、192.168.10.1/24 などと入力します。

d) [保存（Save）] をクリックします。

ステップ 2 内部インターフェイスと同じセキュリティ ゾーンに Wi-Fi インターフェイスを追加します。

デバイスのセットアップ ウィザードでは、[inside_zone] というセキュリティ ゾーンの [内部（inside）] ブリッジグループのメンバーを設定します。Wi-Fi インターフェイスは、アクセス ポイントの Web インターフェイスに到達できるよう、同じゾーンに存在する必要があります（デフォルトの Inside_Inside_Rule アクセス ルールによって可能になりました）。

a) メニューの [オブジェクト（Objects）] をクリックし、コンテンツ テーブルから [セキュリティ ゾーン（Security Zones）] を選択します。

b) [inside_zone] の [編集（edit）] アイコン（）をクリックします。

c) [インターフェイス（Interfaces）] の下の [+] をクリックし、[wifi] インターフェイスを選択します。

ステップ 3 **Inside_zone** セキュリティゾーン内のインターフェイスの間でトラフィックを許可するアクセス制御ルールが存在することを確認します。

デバイスのセットアップ ウィザードでは、トラフィックが [inside_zone] から [outside_zone] に流れるようにするためのルールを作成します。これにより、内部ユーザがインターネットにアクセスできます。

またウィザードでは、内部ホストが互いに到達できるよう、[inside_zone] と [inside_zone] の間のトラフィックが流れるようにするためのルールも作成します。

[Inside_zone] に [wifi] インターフェイスを追加することで、Wi-Fi ユーザはこれらの両方のルールにも含まれるため、インターネットおよびその他の社内ユーザに到達できます。

ウィザードを完了していなかった場合、これらのルールが存在しない可能性があります。デフォルトのアクションではすべてのトラフィックをブロックするため、これらのルールを作成

する必要があります。次の手順では、[inside_zone] セキュリティ ゾーン内のインターフェイス間のトラフィックを有効にするルールを作成する方法について説明します。

a) メニューの [ポリシー（Policies）] をクリックします。
b) ルールを追加するには、[アクセスコントロール（Access Control）] テーブルの上の [+] をクリックします。
c) 少なくとも、ルール内の以下のオプションを設定します。
   - [タイトル（Title）]：ルールの名前を入力します。たとえば、「Inside_Inside」と入力します。
   - [アクション（Action）]：許可または信頼。
   - **[送信元/宛先（Source/Destination）]** > **[送信元ゾーン（Source Zones）]**：inside_zone を選択します。
   - **[送信元/宛先（Source/Destination）]** > **[宛先ゾーン（Destination Zones）]**：inside_zone を選択します。
d) [OK] をクリックします。

ステップ 4 ワイヤレス インターフェイスで、DHCP サーバを設定します。

DHCP サーバはアクセスポイントに接続するデバイスに IP アドレスを供給します。また、アクセス ポイント自体にもアドレスを提供します。

a) [the name of the device in the menu] をクリックします。[デバイス（Device）]
b) **[システム設定（System Settings）]** > **[DHCPサーバ（DHCP Server）]** をクリックします。
c) [DHCPサーバ（DHCP Servers）] タブをクリックします。
d) DHCP サーバ テーブルの上の [+] をクリックします。
e) 以下の DHCP サーバ プロパティを設定します。
   - [DHCPサーバの有効化（Enable DHCP Server）]：DHCP サーバを有効にするには、スライダをクリックします。
   - [インターフェイス（Interface）]：[wifi] インターフェイスを選択します。
   - [アドレスプール（Address Pool）]：DHCP クライアントのアドレス プールを入力します。たとえば、ワイヤレスインターフェイスのアドレス例を使用している場合、プールは 192.168.10.2-192.168.10.254 になります。プールは、インターフェイスの IP アドレスと同じサブネット上にある必要があり、インターフェイスのアドレスやブロードキャスト アドレスをプールに含めることはできません。
f) [追加（Add）] [OK] をクリックします。

ステップ 5 メニューの [展開（Deploy）] ボタンをクリックし、[今すぐ展開（Deploy Now）] ボタンをクリックし、変更をデバイスに展開します。

導入が完了するまで待機してから続行します。

ステップ 6 ワイヤレス アクセス ポイントを設定します。

ワイヤレス アクセス ポイントは、ワイヤレス インターフェイス用に定義された DHCP プールからアドレスを取得します。プール内の最初のアドレスを取得する必要があります。アドレスの例を使用した場合、これは「192.168.10.2」です。（最初のアドレスが機能しない場合は、プール内の次のアドレスを試します）。

a) 新しいブラウザ ウィンドウを使用し、ワイヤレス アクセス ポイントの IP アドレス、たとえば [http://192.168.10.2] に移動します。

アクセスポイントの Web インターフェイスが表示されます。

このアドレスを開くには、内部ネットワークまたはそのネットワークにルーティングできるネットワーク上にいる必要があります。

b) ユーザ名 **cisco**、パスワード **Cisco** を使用してログインします。

c) 左側の **[簡易設定（Easy Setup）]** > **[ネットワーク設定（Network Configuration）]** をクリックします。

d) [無線設定（Radio Configuration）] 領域で、[無線2.4GHz（Radio 2.4GHz）] および [無線5GHz（Radio 5GHz）] セクションのそれぞれに対して、少なくとも次のパラメータを設定し、セクションごとに [適用（Apply）] をクリックします。

- [SSID]：サービス セット識別子。ワイヤレス ネットワークの名前です。ユーザが Wi-Fi 接続用のワイヤレス ネットワークを選択する際に、この名前が表示されます。
- [ビーコンのブロードキャストSSID（Broadcast SSID in Beacon）]：このオプションを選択します。
- [ユニバーサル管理モード（Universal Admin Mode）]：無効。
- [セキュリティ（Security）]：どのセキュリティ オプションを使用するかを選択します。

ステップ 7 ワイヤレス アクセス ポイントの Web インターフェイスで、無線を有効化します。

a) 左側の [サマリー（Summary）] をクリックし、メイン ページの [ネットワーク インターフェイス（Network Interfaces）] で、2.4 GHz 無線に対応するリンクをクリックします。

b) **[設定（Settings）]** タブをクリックします。

c) [無線の有効化（Enable Radio）] の設定では、[有効化（Enable）] ラジオ ボタンをクリックし、ページ下部の [適用（Apply）] をクリックします。

d) 5 Ghz 無線についてこの手順を繰り返します。

初期設定前のデフォルト設定

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

多数のモデルにおいて、この設定では、Firepower Device Manager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、管理/診断用物理インターフェイスにコンピュータを接続し、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、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。

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	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	192.168.45.45	不可
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。 Firepower Threat Defense Virtual192.168.45.1	不可
管理インターフェイスのDHCPサーバ	アドレス プール 192.168.45.46 ～ 192.168.45.254 で有効です。 Firepower Threat Defense Virtual：DHCPサーバが有効になっていません。	不可
管理インターフェイスのDNSサーバ	OpenDNSのパブリックDNSサーバ、208.67.220.220および208.67.222.222。	可
内部インターフェイスのIPアドレス	192.168.1.1/24 Firepower Threat Defense Virtual192.168.45.1/24	不可
内部クライアントのDHCPサーバ	アドレス プール 192.168.1.5 ～ 192.168.1.254の内部インターフェイスで実行されます。 Firepower 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。	不可

設定	デフォルト	初期設定時に変更できるか
内部クライアントの DHCP 自動設定（自動設定では、WINS サーバおよび DNS サーバのアドレスを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	インターネットサービスプロバイダー（ISP）または上流に位置するルータから DHCP 経由で取得されます。	可

デバイス モデル別のデフォルト インターフェイス

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

Firepower 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
ASA 5506-X ASA 5506H-X ASA 5506W-X	GigabitEthernet 1/1	BVI1（外部インターフェイスを除く他のデータ インターフェイスをすべて含む）。5506W-X ではワイヤレス インターフェイス GigabitEthernet 1/9。
ASA 5508-X ASA 5516-X	GigabitEthernet 1/1	GigabitEthernet 1/2
ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	GigabitEthernet 0/0	GigabitEthernet 0/1
Firepower 2100 シリーズ	Ethernet1/1	Ethernet1/2
Firepower Threat Defense Virtual	GigabitEthernet 0/0	GigabitEthernet0/1
ISA 3000	GigabitEthernet 1/1	BVI1（すべてのデータ インターフェイスを含む、ただし、外部インターフェイスは除く）。

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。

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
管理者ユーザのパスワード	任意の入力値	明示的
管理 IP アドレス	192.168.45.45	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。 Firepower Threat Defense Virtual192.168.45.1	デフォルト
管理インターフェイス上の DHCP サーバ	アドレス プール 192.168.45.46 ～ 192.168.45.254 で有効です。 Firepower Threat Defense Virtual：DHCP サーバが有効になっていません。	デフォルト
管理インターフェイスの DNS サーバ	任意の入力値	明示的
管理ホスト名	**firepower** または任意の入力値	明示的
データ インターフェイスを通過する管理アクセス	データ インターフェイスの管理アクセス リスト ルールにより、内部インターフェイスを通過する HTTPS アクセスが許可されます。内部ブリッジ グループを持つモデルでは、内部ブリッジ グループの全メンバー インターフェイスがこの対象となります。SSH 接続は許可されません。IPv4 および IPv6 接続はいずれも許可されます。 Firepower 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
システム時間	選択したタイム ゾーンおよび NTP サーバ。	明示的
スマート ライセンス	基本ライセンスとともに登録したか、または評価期間を開始したか、いずれか選択した方法。 サブスクリプションライセンスは有効化されていません。スマート ライセンスのページに移動して、スマート ライセンスを有効化してください。	明示的

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
内部インターフェイスの IP アドレス	192.168.1.1/24 Firepower Threat Defense Virtual192.168.45.1/24	デフォルト
内部クライアントの DHCP サーバ	アドレス プール 192.168.1.5 ～ 192.168.1.254 の内部インターフェイスで実行されます。 Firepower 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。	デフォルト
内部クライアントに対する DHCP 自動設定（自動設定では、WINS サーバおよびDNS サーバ用のアドレスがクライアントに提供）	DHCP を使用して外部インターフェイスの IPv4 アドレスを取得している場合、DHCP 自動設定は外部インターフェイスに対して有効化されます。 静的アドレッシングを使用している場合は、DHCP 自動設定は無効になります。	明示的（ただし間接的）
データ インターフェイスの設定	• ASA 5506-X、 ISA 3000：外部インターフェイスを除くすべてのデータ インターフェイス（GigabitEthernet1/2 など）が有効になり、内部ブリッジ グループの一部となります。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。これらのインターフェイスには inside_1、inside_2 などと名前が付けられます。 • それ以外のすべてのモデル：外部および内部インターフェイスのみが設定され有効になります。他のすべてのデータ インターフェイスは無効になります。	デフォルト
外部の物理インターフェイスおよび IP アドレス	デバイス モデルに基づくデフォルトの外部ポート。初期設定前のデフォルト設定 （34 ページ）を参照してください。 IP アドレスは DHCP によって取得するか、入力したスタティック アドレスです（IPv4、IPv6、またはその両方）。	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
スタティック ルート	外部インターフェイスに対してスタティック IPv4 または IPv6 アドレスを設定すると、スタティックなデフォルトルートも IPv4 または IPv6 用に適宜設定され、このアドレスタイプ用に定義されたゲートウェイをポイントします。DHCP を選択した場合は、デフォルトルートはDHCP サーバから取得されます。 ネットワーク オブジェクトもこのゲートウェイ、および「any」アドレス（IPv4 の場合は 0.0.0.0/0、IPv6 の場合は ::/0）に合わせて作成されます。	暗黙的

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
セキュリティ ゾーン	内部インターフェイスを含む **inside_zone**。内部ブリッジ グループを持つモデルでは、内部ブリッジ グループ インターフェイスの全メンバーがゾーンに含まれます。 外部インターフェイスを含む **outside_zone**。 （これらのゾーンを編集して他のインターフェイスを追加することも、独自のゾーンを作成することも可能）。	暗黙的
アクセス コントロール ポリシー	inside_zone から outside_zone に送信されるすべてのトラフィックを信頼するルール。これにより、インスペクションなしで、ネットワーク内のユーザ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。 内部ブリッジ グループを持つモデルでは、inside_zone 内のインターフェイス間を伝送されるすべてのトラフィックを信頼する 2 番目のルールが作成されます。これにより、内部ネットワーク内のユーザ間で伝送されるすべてのトラフィックが、インスペクションを受けることなく許可されます。 他のすべてのトラフィックに対するデフォルト アクションは、ブロックです。つまり、外部から開始され、ネットワークに進入しようとするすべてのトラフィックが阻止されます。	暗黙的
NAT	（内部ブリッジ グループがないモデル）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。 （内部ブリッジ グループを持つモデル）内部ブリッジ グループの各メンバーに対し、インターフェイスのダイナミック PAT ルールにより、外部インターフェイスを宛先とするすべての IPv4 トラフィックの発信元アドレスは、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されます。これらは NAT ルール テーブルに表示されるため、必要に応じて後から編集できます。 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することができます。	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

Firepower 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 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（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 （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。

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

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

次に、グループの概要を示します。

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

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

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 （43 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、またはユーザまたはユーザ 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）]：ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティ インテリジェンス ポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセス コントロール ポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティ インテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスやURLの定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。セキュリティインテリジェンスの設定を参照してください。
- [NAT]（ネットワーク アドレス変換）：内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。NAT の設定を参照してください。
- [アクセス制御（Access Control）]：ネットワーク上で許可する接続の決定にアクセス コントロール ポリシーを使用します。セキュリティ ゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザまたはユーザ 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。侵入ポリシーの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 （43 ページ）を参照してください。

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、展開には自分の変更内容のみが含まれています。ただし、必要に応じて、システムが設定全体を再適用し、これがネットワークに悪影響を及ぼす可能性があります。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。

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 Firepower Device Manager を使用する Firepower 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 （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。

[展開サマリー（Deployment Summary）]ページが開きます。このウィンドウには、前回の展開リストに、展開の開始時点と完了時点での変更内容（「変更されたオブジェクト」）に関するサマリー情報と、各展開のステータスを記載したものが表示されます。

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、クリックすればこれまでの展開ジョブの結果を表示できます。

ステップ 2 [今すぐ展開（Deploy Now）] をクリックします。

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。
- ルール データベースが更新された。
- VDB が更新された。

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。

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、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、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：**[システム設定（System Settings）] > [DNSサーバ（DNS Server）]** を選択します。
- NTPサーバ：**[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。

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

FTD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コマンドラインインターフェイス（CLI）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ができますが、Firepower 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。

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 コンソールは基本 FTD 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。FDM 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。

Firepower 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。