Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理

この章では、FDM を使用して管理されるスタンドアロンの FTDv デバイスを展開する方法について説明します。高可用性ペアを展開する場合は、FDM のコンフィギュレーション ガイドを参照してください。

Firepower Device Manager を使用した Firepower Threat Defense Virtual について

Firepower Threat Defense Virtual（FTDv）は、Cisco NGFW ソリューションの仮想化コンポーネントです。FTDv は、ステートフル ファイアウォール、ルーティング、VPN、Next-Generation Intrusion Prevention System（NGIPS）、Application Visibility and Control（AVC）、URL フィルタリング、高度なマルウェア防御（AMP）などの次世代ファイアウォールサービスを提供します。

FTDv の管理には Firepower Device Manager（FDM）を使用できます。これは、一部の Firepower Threat Defense モデルに組み込まれている Web ベースのデバイス セットアップ ウィザードです。FDM では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Firepower Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

多数のデバイスを管理している場合、または Firepower Threat Defense で許可される、より複雑な機能や設定を使用したい場合は、組み込みの Firepower Device Manager の代わりに Firepower Management Center を使用してデバイスを設定します。詳細については、Firepower Management Center を使用した Firepower Threat Defense Virtual の管理 を参照してください。

トラブルシューティングの目的で、管理インターフェイス上の SSH を使用して FTD CLI にアクセスすることも、Firepower CLI から FTD に接続することもできます。

デフォルト設定

FTDv 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 を接続することもできます。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。

FTDv は、初回起動時に少なくとも 4 つのインターフェイスで電源がオンになる必要があります。

- 仮想マシン上の 1 番目のインターフェイス（Management 0-0）は、管理インターフェイスです。
- 仮想マシンでの 2 番目のインターフェイスは診断インターフェイス（Diagnostic0-0）です。
- 仮想マシン上の 3 番目のインターフェイス（GigabitEthernet 0-0）は、外部インターフェイスです。
- 仮想マシン上の 4 番目のインターフェイス（GigabitEthernet 0-1）は、内部インターフェイスです。

データ トラフィック用に最大 6 つのインターフェイスを追加し、合計で 8 つのデータ インターフェイスを使用できます。追加のデータ インターフェイスについて、送信元ネットワークが正しい宛先ネットワークにマッピングされ、各データ インターフェイスが一意のサブネットまたは VLAN にマッピングされていることを確認します。「VMware インターフェイスの設定」を参照してください。

初期設定

FTDv の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。これには、セキュリティアプライアンスをネットワークに挿入して、インターネットまたは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の設定が含まれます。2 つの方法のいずれかでシステムの初期設定を行うことができます。

- FDM Web インターフェイスの使用（推奨）。FDM は Web ブラウザで実行します。このインターフェイスを使用して、システムを設定、管理、モニターできます。
- コマンド ライン インターフェイス（CLI）セットアップウィザードを使用します（オプション）。FDM の代わりに CLI のセットアップウィザードを初期設定に使用できます。またトラブルシューティングにCLIを使用できます。システムの設定、管理、監視には引き続きFDM使用します。「Firepower Threat Defense CLI ウィザードの起動（オプション）」を参照してください。

次のトピックでは、これらのインターフェイスを使用してシステムの初期設定を行う方法について説明します。

Firepower Device Manager の起動

Firepower Device Manager（FDM）を使用して、システムの構成、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） 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。

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。

手順

ステップ 1 ブラウザを使用して FDM にログインします。CLI での初期設定を完了していない場合は、Firepower Device Manager を **https:***ip-address* で開きます。このアドレスは次のいずれかになります。

- 管理アドレス。（ほとんどのプラットフォームの）デフォルトでは、管理インターフェイスはDHCPクライアントであるため、IPアドレスはDHCPサーバーによって異なります。
- FTDv が Microsoft Azure や Amazon Web Services などのパブリッククラウド環境に展開されている場合、パブリック IP アドレスはパブリックアドレスのプールから FTDv インスタンスに自動的に割り当てられます。クラウドダッシュボードからパブリック IP アドレスを見つけます。

ステップ 2 ユーザー名 **admin** とデフォルトのパスワードでログインします。

バージョン 7.0 以降では、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。

以前のリリースでは、デフォルトの管理者パスワードは **Admin123** でした。

ステップ 3 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 4 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） [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。

a) [外部インターフェイス（Outside Interface）]：これは、ゲートウェイモードまたはルータに接続するためのデータポートです。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。

[IPv4の設定（Configure IPv4）]：外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv4 アドレスを設定しないという選択肢もあります。

[IPv6の設定（Configure IPv6）]：外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ（Off）] を選択して、IPv6 アドレスを設定しないという選択肢もあります。

b) **[管理インターフェイス（Management Interface）]**

[DNSサーバ（DNS Servers）]：システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。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。

[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。

（注） デバイス セットアップ ウィザードを使用して Firepower Threat Defense デバイスを設定する場合は、アウトバウンドとインバウンドのトラフィックに対してシステムから 2 つのデフォルトアクセスルールが提供されます。初期セットアップ後に、これらのアクセスルールに戻って編集できます。

ステップ 5 システム時刻を設定し、[次へ（Next）] をクリックします。

a) [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。

b) [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 6 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。

評価ライセンスを使用するには、[登録せずに90日間の評価期間を開始する（Start 90 day evaluation period without registration）] を選択します。後でデバイスを登録し、スマートライセンスを取得するには、メニューからデバイスの名前をクリックして [デバイスダッシュボード（Device Dashboard）] に進み、[スマートライセンス（Smart Licenses）] グループのリンクをクリックします。

ステップ 7 [完了（Finish）] をクリックします。

次のタスク

- Firepower Device Manage を使用してデバイスを設定します。「Firepower Device Manager でデバイスを設定する方法 （5 ページ）」を参照してください。

Firepower Device Manager でデバイスを設定する方法

セットアップウィザードの完了後、いくつかの基本ポリシーが適切に設定された機能しているデバイスが必要です。

- 内部インターフェイスと外部インターフェイスのセキュリティゾーン。
- 内部から外部へのすべてのトラフィックを信頼するアクセスルール。
- 内部から外部へのすべてのトラフィックを外部インターフェイスの IP アドレスの固有のポートへ変換するインターフェイス NAT ルール。
- 内部インターフェイスまたはブリッジグループで実行されている DHCP サーバー。

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン（**?**）をクリックしてください。

手順

ステップ 1 [デバイス（Device）] を選択してから、[スマートライセンス（Smart License）] グループの [設定の表示（View Configuration）] をクリックします。

使用するオプションのライセンス（[脅威（Threat）]、[マルウェア（Malware）]、[URL]）でそれぞれ [有効化（Enable）] をクリックします。セットアップ中にデバイスを登録した場合は、必要な RA VPN ライセンスも有効にできます。必要かどうかわからない場合は、各ライセンスの説明を確認します。

登録していない場合は、このページから登録できます。[登録の要求（Request Register）] をクリックして、手順に従います。評価ライセンスの有効期限が切れる前に登録してください。

たとえば、有効な脅威ライセンスは次のようになります。

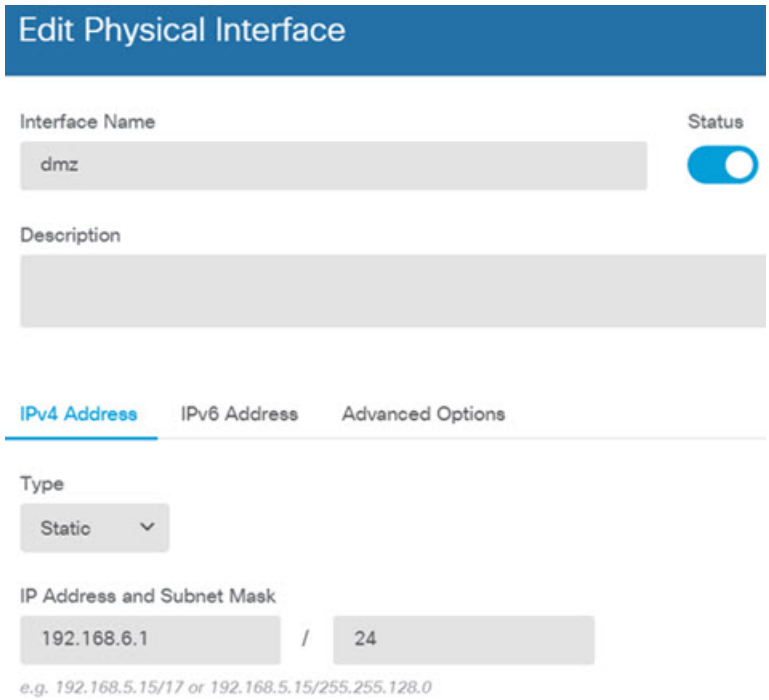
図 *1:* 有効な脅威ライセンス

ステップ 2 他のインターフェイスを設定した場合は、[デバイス（Device）] を選択してから、[インターフェイス（Interfaces）] グループの [設定の表示（View Configuration）] をクリックして、各インターフェイスを設定します。

他のインターフェイスのブリッジグループを作成するか、別々のネットワークを設定するか、または両方の組み合わせを設定できます。各インターフェイスの [編集（Edit）] アイコン（ ）をクリックして、IP アドレスなどの設定を定義します。

次の例では、Web サーバーなどのパブリックアクセス可能な資産を配置する「緩衝地帯」（DMZ）として使用するためのインターフェイスを構成します。完了したら [保存（Save）] をクリックします。

図 *2:* インターフェイスの編集



ステップ 3 新しいインターフェイスを構成する場合は、[オブジェクト（Objects）] を選択し、目次から[セキュリティゾーン（Security Zones）] を選択します。

編集または必要に応じて新しいゾーンを作成します。インターフェイスではなく、セキュリティゾーンに基づいてポリシーを構成するため、各インターフェイスはゾーンに属している必要があります。インターフェイスを構成する場合、ゾーンにインターフェイスを置くことはできません。このため、新しいインターフェイスを作成した後、または既存のインターフェイスの目的を変更した後には常にゾーン オブジェクトを編集する必要があります。

次の例では、DMZインターフェイスのために新しいDMZゾーンを作成する方法を示します。

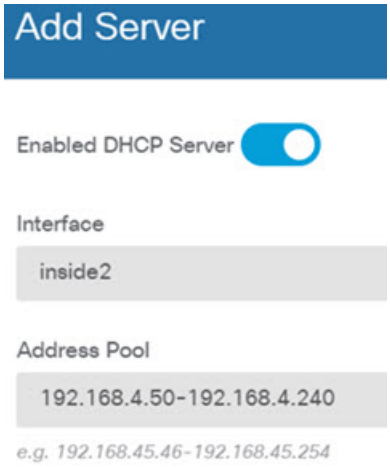
図 *3:* セキュリティ ゾーン オブジェクト

ステップ 4 内部クライアントで DHCP を使用してデバイスから IP アドレスを取得する場合は、**[デバイス（Device）]** > **[システム設定（System Settings）]** > **[DHCPサーバー（DHCP Server）]** を選択してから、**[DHCPサーバー（DHCP Servers）]** タブを選択します。

すでに内部インターフェイス用に構成されている DHCP サーバーがありますが、アドレス プールを編集したり、それを削除したりすることができます。他の内部インターフェイスを構成した場合は、それらのインターフェイス上に DHCP サーバーをセットアップするのがごく一般的です。[+] をクリックして各内部インターフェイスのサーバーとアドレスプールを構成します。

[構成（Configuration）] タブでクライアントに提供される WINS および DNS のリストを微調整することもできます。次の例では、アドレス プールの 192.168.4.50 ～ 192.168.4.240 で inside2 インターフェイス上の DHCP サーバーを設定する方法を示しています。

図 *4 : DHCP* サーバー



ステップ 5 [デバイス（Device）] を選択してから、[ルーティング（Routing）] グループで [設定の表示（View Configuration）]（または [最初のスタティックルートを作成（Create First Static Route）]）をクリックし、デフォルトルートを構成します。

デフォルト ルートは通常、外部インターフェイス以外に存在するアップストリームまたは ISP ルータを指しています。デフォルトの IPv4 ルートは任意の ipv4（0.0.0.0/0）、デフォルトの IPv6 ルートは任意の ipv6（::0/0）です。使用する IP バージョンごとにルートを作成します。外部インターフェイスのアドレスの取得に DHCP を使用する場合、必要なデフォルト ルートをすでに持っていることがあります。

（注） このページで定義したルートは、データ インターフェイス用のみです。管理インターフェイスには影響しません。**[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）]** で管理ゲートウェイを設定します。

次の例に、IPv4 のデフォルト ルートを示します。この例では、isp ゲートウェイは ISP ゲートウェイの IP アドレスを識別するネットワーク オブジェクトです（アドレスは ISP から取得する必要があります）。[ゲートウェイ（Gateway）] の下部の [新しいネットワークを作成する（Create New Network）] ドロップダウン リストをクリックしてこのオブジェクトを作成することができます。

図 *5:* デフォルトルート

ステップ 6 [ポリシー（Policies）] を選択してネットワークのセキュリティ ポリシーを構成します。

デバイス セットアップ ウィザードは、内部ゾーンと外部ゾーンの間のトラフィック フローを有効にします。また、外部インターフェイスを使用する場合に、全インターフェイスに対する

インターフェイス NAT も有効にします。新しいインターフェイスを構成した場合でも、内部ゾーン オブジェクトに追加する場合はそれらにアクセス制御ルールが自動的に適用されます。

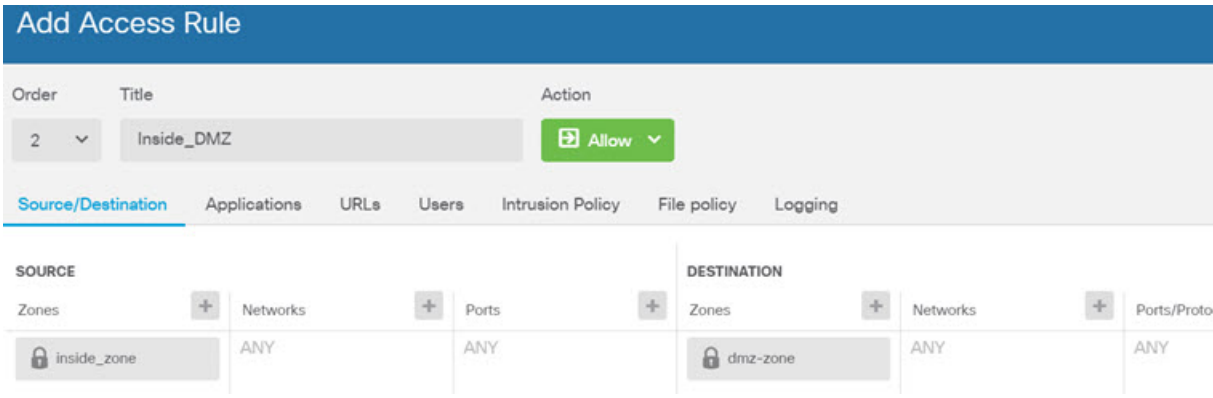
ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィックフローを許可するアクセス制御ルールが必要です。他のセキュリティ ゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、NAT およびアクセス ルールを微調整できます。次のポリシーを設定できます。

- [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。
- [アイデンティティ（Identity）]：個々のユーザーにネットワーク アクティビティを関連付ける、またはユーザーまたはユーザー グループのメンバーシップに基づいてネットワーク アクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザーを判定するためにアイデンティティ ポリシーを使用します。
- [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。
- [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。
- [アクセス制御（Access Control）]：ネットワーク上で許可する接続の決定にアクセス コントロール ポリシーを使用します。セキュリティ ゾーン、IP アドレス、プロトコル、ポート、アプリケーション、URL、ユーザーまたはユーザー グループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル（マルウェア）ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。
- [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。

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーンの間のトラフィックを許可する方法を示します。この例では、[接続の最後で（At End of Connection）] が選択されている場合、[ロギング（Logging）] を除いて他のいずれのタブでもオプションは設定されません。

図 *6*:アクセス コントロール ポリシー



ステップ 7 [デバイス（Device）] を選択してから、[更新（Updates）] グループで [設定の表示（View Configuration）] をクリックし、システムデータベースの更新スケジュールを設定します。

侵入ポリシーを使用している場合は、ルールと VDB のデータベースを定期的な更新を設定します。セキュリティ情報フィードを使用する場合は、それらの更新スケジュールを設定します。一致基準としてセキュリティポリシーで地理位置情報を使用する場合は、そのデータベースの更新スケジュールを設定します。

ステップ 8 メニューの [導入（Deploy）] ボタンをクリックし、[今すぐ導入する（Deploy Now）] ボタン（  ）をクリックして、変更内容をデバイスに展開します。

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。

次のタスク

Firepower Device Manager による Firepower Threat Defense Virtual の管理の詳細については、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』 または Firepower Device Manager のオンラインヘルプを参照してください。