Firepower Device Manager を使用した Cisco Firepower Threat Defense (ASA 5508-X、ASA 5516-X 用) クイック スタート ガイド

初版:2016 年 11 月 2 日

最終更新日:2018 年 12 月 12 日

バージョン:6.2 以降

1. 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 デバイス セットアップ ウィザードを使用して Firepower Threat Defense デバイスの初期設定を実行する方法について説明します。

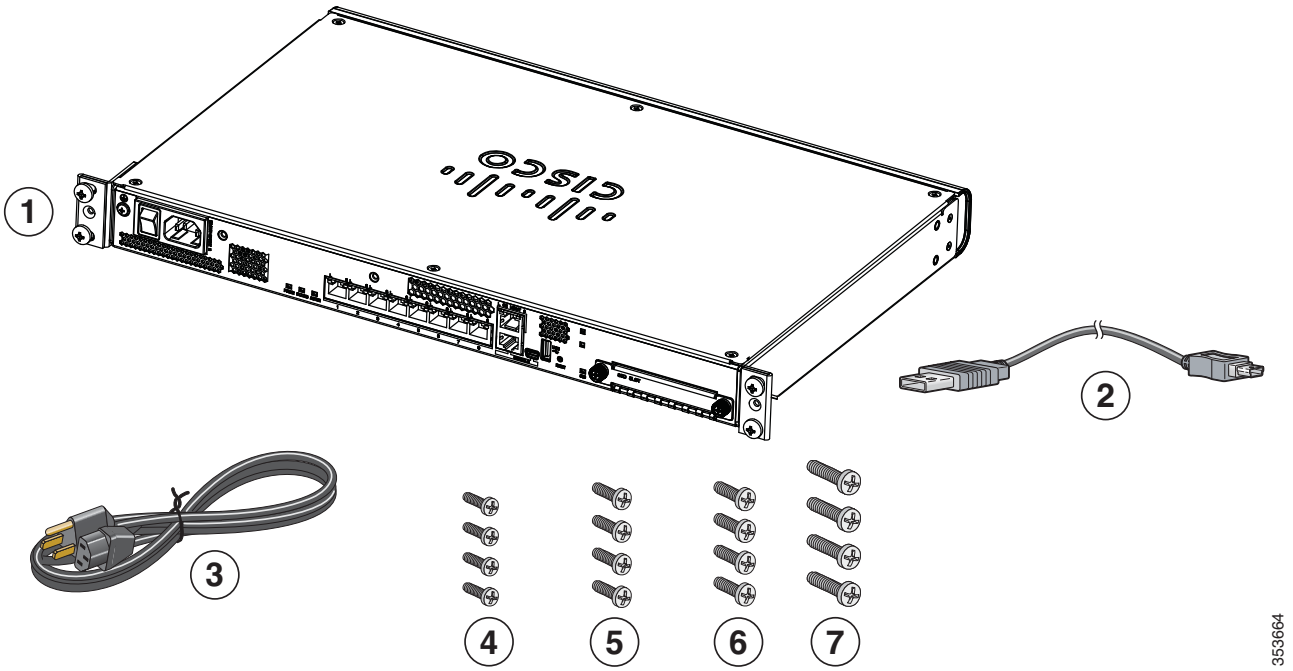
Firepower Device Manager では、小規模ネットワークに最も多く使用されるソフトウェアの基本機能を設定できます。特に、単一またはごく少数のデバイスが含まれるネットワーク向けに設計されていて、高性能の多機能デバイス マネージャを使用して多数の Firepower Threat Defense デバイスが含まれる大規模ネットワークを制御する必要のない用途に適しています。

膨大な数のデバイスを管理する場合、または Firepower Threat Defense で対応できる複雑な機能および構成を使用する場合は、一体型の Firepower Device Manager ではなく Firepower Management Center を使用してデバイスを構成してください。

CLI セットアップ ウィザードを使用して、Firepower Threat Defense デバイスのネットワーク接続を設定したり、デバイスを Firepower Management Center に登録にすることができます(http://www.cisco.com/go/ftd-asa-quick 参照)。

2. パッケージの内容

この項では、シャーシのパッケージの内容について説明します。この内容は変更される場合があるため、実際に含まれているアイテムは多かったり、少なかったりする場合があることにご注意ください。



1	ASA 5508-X または ASA 5516-X シャーシ	2	青いコンソール ケーブルおよびシリアル PC ターミナル アダプタ（DB-9 to RJ-45）
3	電源ケーブル	4	4 本の 10-32 プラス ネジ（ラック マウント用）
5	4 本の 12-24 プラス ネジ（ラック マウント用）	6	4 本の M6 プラス ネジ（ラック マウント用）
7	4 本の M4 プラス ネジ（ラック マウント用）		

3. ライセンス要件

Firepower Threat Defense デバイスには、Cisco Smart Licensing が必要です。Smart Licensing により、ライセンスの購入とライセンスのプールの一元管理を行うことができます。製品認証キー（PAK）ライセンスとは異なり、スマート ライセンスは特定のシリアル番号またはライセンス キーに関連付けられません。Smart Licensing を利用すれば、ライセンスの使用状況やニーズをひと目で評価することもできます。

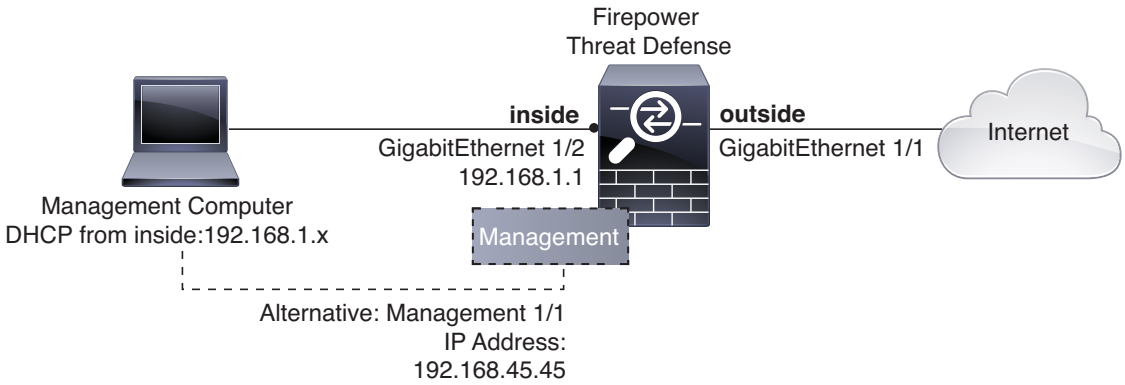
また、Smart Licensing では、まだ購入していない製品の機能を使用できます。Cisco Smart Software Manager に登録すると、すぐにライセンスの使用を開始できます。また、後でライセンスを購入することもできます。これによって、機能の展開および使用が可能になり、発注書の承認による遅延がなくなります。

Firepower 機能のスマート ライセンスを複数購入する場合は、それらのライセンスを Cisco Smart Software Manager（http://www.cisco.com/web/ordering/smart-software-manager/index.html）で管理できます。Smart Software Manager では、組織のマスター アカウントを作成できます。Cisco Smart Software Manager の詳細については、『*Cisco Smart Software Manager User Guide*』を参照してください。

Firepower Threat Defense デバイスや Firepower Threat Defense Virtual を購入すると、自動的に基本ライセンスが含まれます。すべての追加ライセンス（Threat、Malware、URL Filtering）はオプションです。Firepower Threat Defense のライセンスに関する詳細については、『*Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager*』の「Licensing the System」の章を参照してください。

4. ネットワークへの Firepower Threat Defense の導入

次の図に、ASA 5508-X または ASA 5516-X で推奨される Firepower Threat Defense のネットワーク導入を示します。



設定例では、次の動作によって上記のネットワーク導入を有効化します。

- **内部 --> 外部**へのトラフィック フロー
- **DHCP からの外部 IP** アドレス
- **内部**のクライアントに対する **DHCP**。内部インターフェイス上に DHCP サーバがあります。管理コンピュータを内部インターフェイスのいずれかに直接接続し、192.168.1.0/24 ネットワーク上のアドレスを取得できます。

  HTTPS アクセスは内部インターフェイス上で有効になるため、デフォルト アドレスの 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。
- また、**Management 1/1** に接続し、Firepower Device Manager を使用してデバイスのセットアップや管理を行うこともできます。管理インターフェイス上に DHCP サーバがあります。管理コンピュータをこのインターフェイスに直接接続し、192.168.45.0/24 ネットワーク上のアドレスを取得できます。

  HTTPS アクセスは管理インターフェイス上で有効になるため、デフォルト アドレスの 192.168.45.45 で管理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。

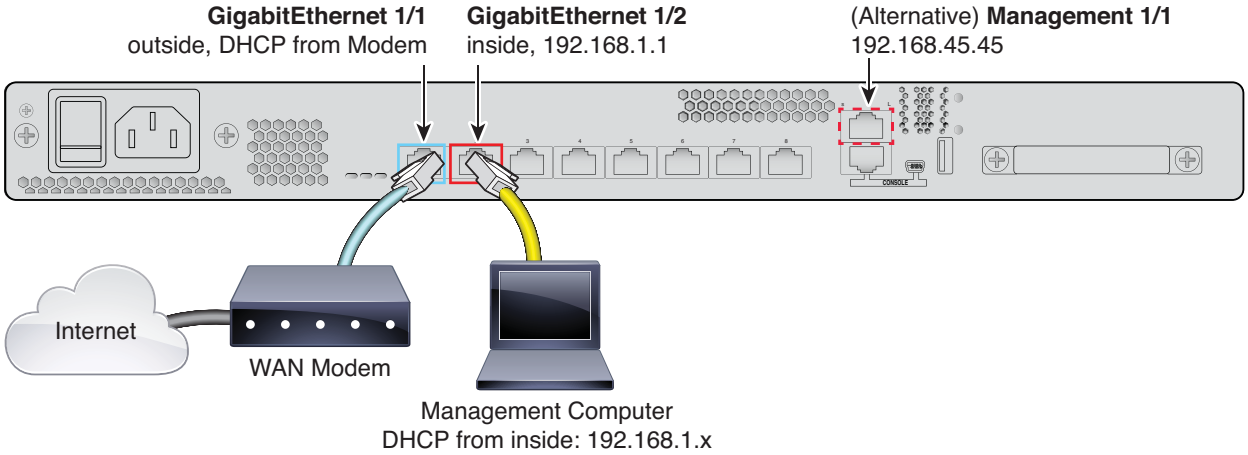
  (注) 物理的な管理インターフェイスは、Management 論理インターフェイスと Diagnostic 論理インターフェイスの間で共有されます。『*Firepower Threat Defense Configuration Guide for Firepower Device Manager*』の「Interfaces」の章を参照してください。
- Firepower Threat Defense システムには、ライセンスおよびアップデート用のインターネット アクセスが必要です。管理 IP アドレスのデフォルト ゲートウェイでは、データ インターフェイスを使用してインターネットにルーティングします。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。

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。ASA 5508-X または ASA 5516-X で上記のシナリオをケーブル接続するには、次の図を参照してください。

(注) 次の図は、内部ネットワークに接続された管理コンピュータを使用する簡単なトポロジを示しています。他のトポロジの使用も可能であり、基本的な論理ネットワーク接続、ポート、アドレッシング、構成の要件によって導入方法が異なります。

図 1　ASA 5508-X および 5516-X



手順

1. GigabitEthernet 1/1（外部）インターフェイスを ISP/WAN モデムまたはその他の外部デバイスに接続します。デフォルトでは、IP アドレスが DHCP を使用して取得されますが、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。
2. ローカルの管理ワークステーション（デバイスの設定に使用）を内部インターフェイス GigabitEthernet 1/2 に接続します。
3. 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。ワークステーションは 192.168.45.0/24 ネットワーク上で DHCP 経由で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。

5. Firepower Threat Defense デバイスの電源投入

手順

1. 電源コードを Firepower Threat Defense デバイスに接続し、電源コンセントに接続します。
2. Firepower Threat Defense デバイスの背面にある電源ボタンを押します。
3. Firepower Threat Defense デバイスの前面にある電源 LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。
4. Firepower Threat Defense デバイスの前面にあるステータス LED を確認します。緑色に点灯している場合は、電源投入診断に合格しています。

6. Firepower Device Manager の起動

初めて Firepower Device Manager にログインすると、デバイス セットアップ ウィザードが表示され、システムの初期設定を実行します。

はじめる前に

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。4. ネットワークへの Firepower Threat Defense の導入（3 ページ）に示したデフォルトの「外部」インターフェイスを使用します。

手順

1. ブラウザを開き、Firepower Device Manager 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。
   - 内部インターフェイスに接続されている場合は **https://192.168.1.1**。
   - 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**。
2. 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。
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。
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。

      [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。

   b. 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。

      [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。

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。
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。
7. [終了（Finish）] をクリックします。

次の作業

デバイス セットアップ ウィザードが完了したら、ポップアップにデバイスを設定するための次のオプションが表示されます。

- 他のインターフェイスをネットワークに接続している場合は、[インターフェイスの設定（Configure Interfaces）] を選択して、接続されているインターフェイスをそれぞれ設定します。
- デフォルトのアクセス ルールを変更する場合は、[ポリシーの設定（Configure Policy）] を選択して、トラフィック ポリシーの設定および管理を行います。

いずれかのオプションを選択するか、またはポップアップを閉じて [デバイスダッシュボード（Device Dashboard）] に戻ることができます。

7. 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。

- （ASA 5506-X を除く）外部および内部インターフェイス。その他のデータ インターフェイスは設定されません。
- （ASA 5506-X モデル）外部インターフェイスと、他のすべてのデータのインターフェイスが含まれる内部ブリッジ グループ。
- 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。
- 内部の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。

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

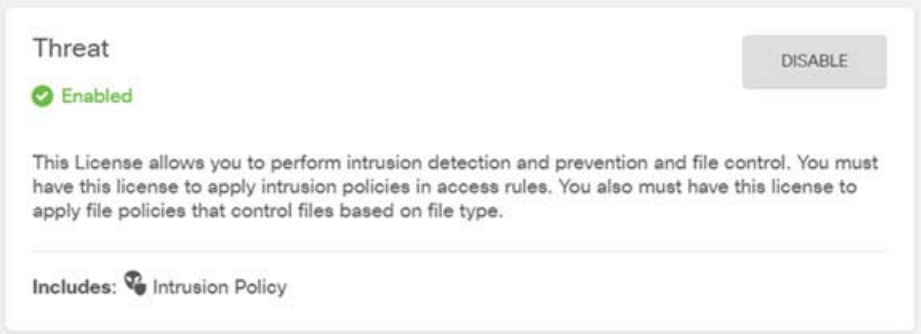
1. [デバイス（Device）] を選択してから、[スマート ライセンス（Smart License）] グループの [設定の表示（View Configuration）] をクリックします。

   オプションの脅威のライセンスを使用する場合は、[有効化（Enable）] をクリックします。

(注)ISA 3000 は脅威のライセンスのみサポートします。マルウェアまたは URL フィルタリング ライセンスはサポートしません。したがって、ISA 3000 ではマルウェアや URL フィルタリングのライセンスを必要とする機能は設定できません。

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。

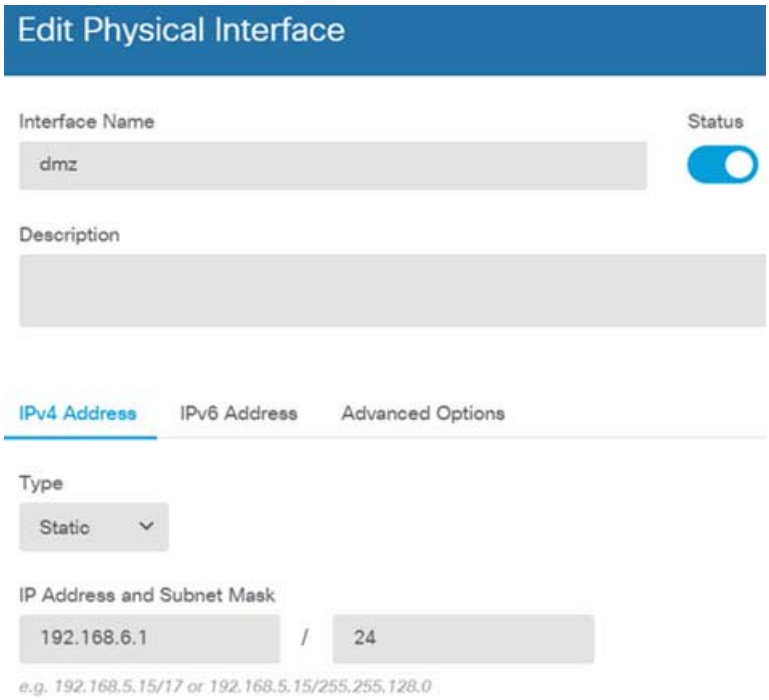


2. 他のインターフェイスを配線した場合は、[デバイス（Device）] を選択してから、[インターフェイス（Interfaces）] グループの [設定の表示（View Configuration）] をクリックして、配線した各インターフェイスを設定します。

   ASA 5506-X はすべての非外部データ インターフェイスを含むブリッジ グループで事前設定済みのため、これらのインターフェイスを設定する必要はありません。ただし、ブリッジ グループを分割したい場合は、編集して別々に扱いたいインターフェイスを削除できます。その後、別々のネットワークをホストするインターフェイスとしてそれらを設定できます。

   他のモデルでは、他のインターフェイスのブリッジ グループを作成、別々のネットワークを設定、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。



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）] を選択してから、目次から [セキュリティ ゾーン（Security Zones）] を選択します。

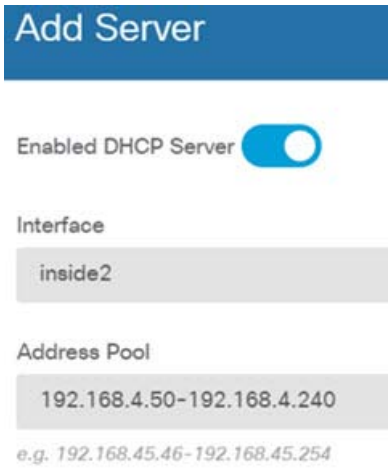
   編集または必要に応じて新しいゾーンを作成します。インターフェイスではなく、セキュリティ ゾーンに基づいてポリシーを構成するため、各インターフェイスはゾーンに属している必要があります。インターフェイスを構成する場合、ゾーンにインターフェイスを置くことはできません。このため、新しいインターフェイスを作成した後、または既存のインターフェイスの目的を変更した後には常にゾーン オブジェクトを編集する必要があります。

   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。

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（DHCP Server）] を選択してから、[DHCP サーバ（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 サーバを設定する方法を示しています。



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 [最初の静的ルートを作成（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。

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。

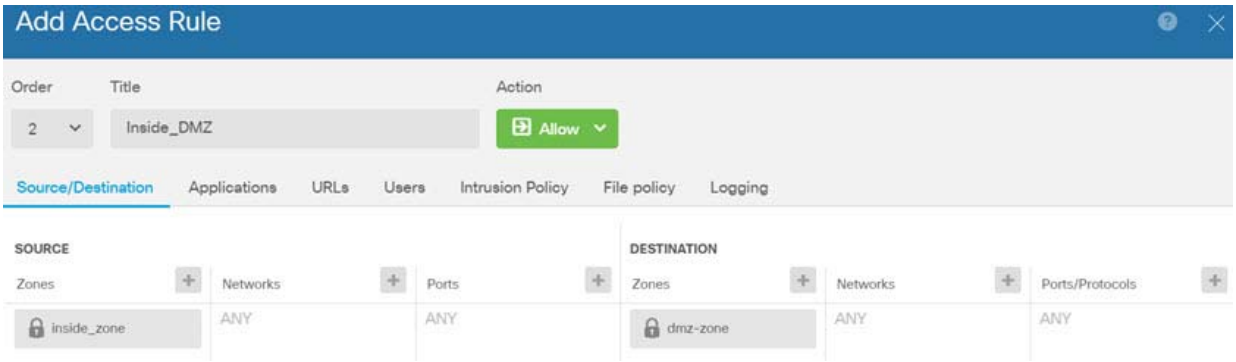
   ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィック フローを許可するアクセス制御ルールが必要です。他のセキュリティ ゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

   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**：暗号化された接続（HTTPS など）の侵入を検査する場合、または URL およびアプリケーション使用ポリシーへのコンプライアンスを適用する場合は、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。
- [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 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。



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。

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。

8. 次の作業

- Firepower Device Manager による Firepower Threat Defense の管理に関する詳細については、Firepower Threat Defense の構成ガイドまたは Firepower Device Manager のオンライン ヘルプを参照してください。