FDM を使用した Firepower Threat Defense の展開

この章の対象読者

この章では、Firepower Device Manager（FDM）Web ベースのデバイス セットアップ ウィザードを使用して、Firepower Threat Defense（FTD）デバイスの初期セットアップと設定を完了する方法について説明します。

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 FDM 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 FTD で許可される、より複雑な機能や設定を使用する場合は、代わりに Firepower Management Center （FMC）を使用します。

（注） Cisco ASA 5508-X および 5516-X ハードウェアでは、FTD ソフトウェアまたは ASA ソフトウェアを実行できます。FTD と ASA の間で切り替えを行う際には、デバイスの再イメージ化が必要になります。「Reimage the Cisco ASA or Firepower Threat Defense Device」を参照してください。

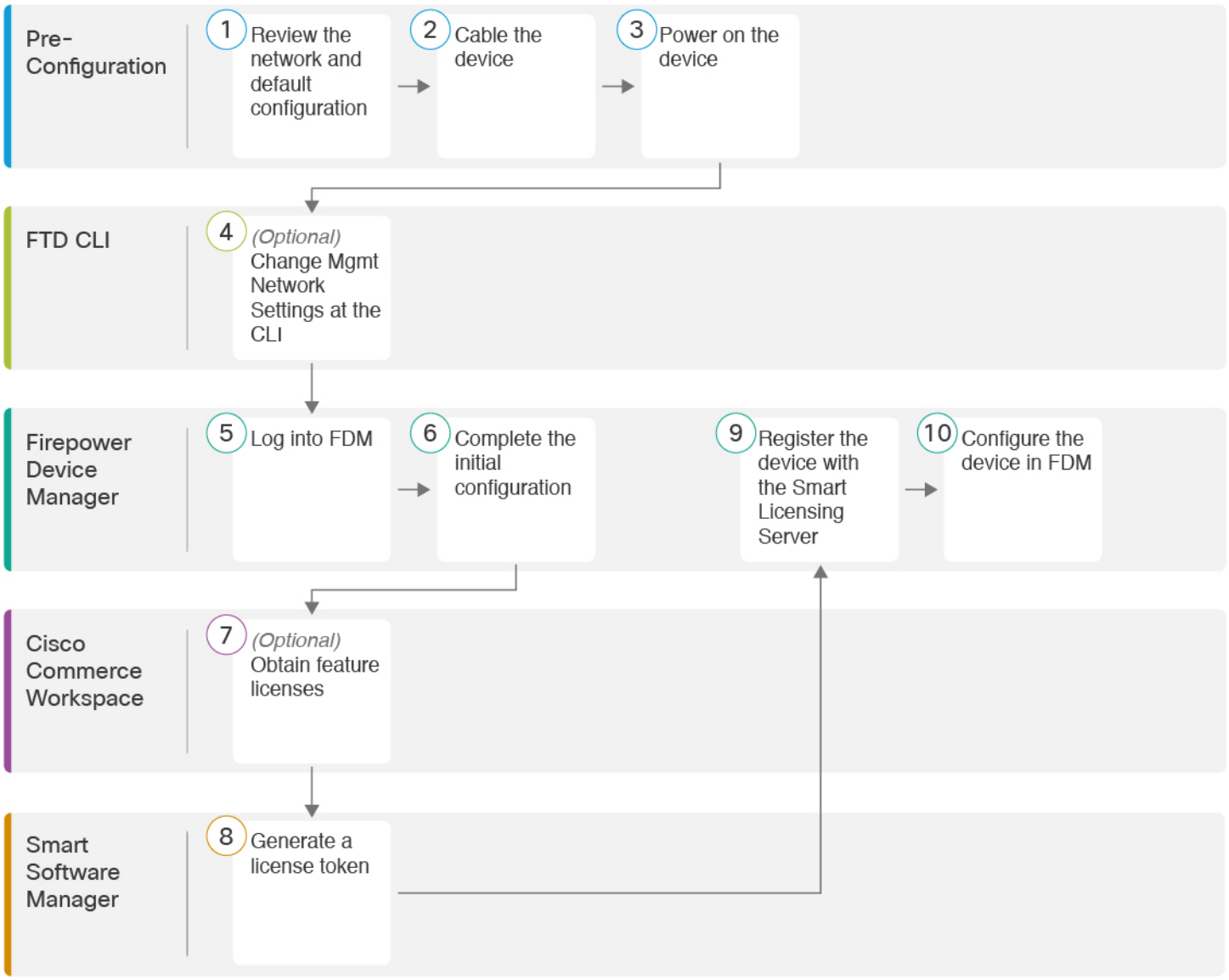
（注） **プライバシー収集ステートメント**：ASA 5508-X および 5516-X には個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザ名などの設定では、個人識別情報を使用できます。この場合、設定作業時や SNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

- エンドツーエンドの手順, on page 2
- ネットワーク配置とデフォルト設定の確認 （4 ページ）
- デバイスの配線, on page 7
- デバイスの電源投入 （8 ページ）

• （任意）CLI での管理ネットワーク設定の変更 （9 ページ）
• FDM へのログイン （10 ページ）
• 初期設定の完了 （11 ページ）
• ライセンスの設定 （13 ページ）
• Firepower Device Managerでのデバイスの設定 （19 ページ）
• Firepower Threat Defense CLI へのアクセス （24 ページ）
• デバイスの電源切断 （24 ページ）
• 次のステップ （26 ページ）

エンドツーエンドの手順

シャーシで FDM を使用して FTD を展開するには、次のタスクを参照してください。



1	事前設定	ネットワーク配置とデフォルト設定の確認, on page 4。
2	事前設定	デバイスの配線, on page 7
3	事前設定	デバイスの電源投入, on page 8。
4	FTD CLI	（任意）CLI での管理ネットワーク設定の変更, on page 9。
5	Firepower Device Manager	FDM へのログイン, on page 10。

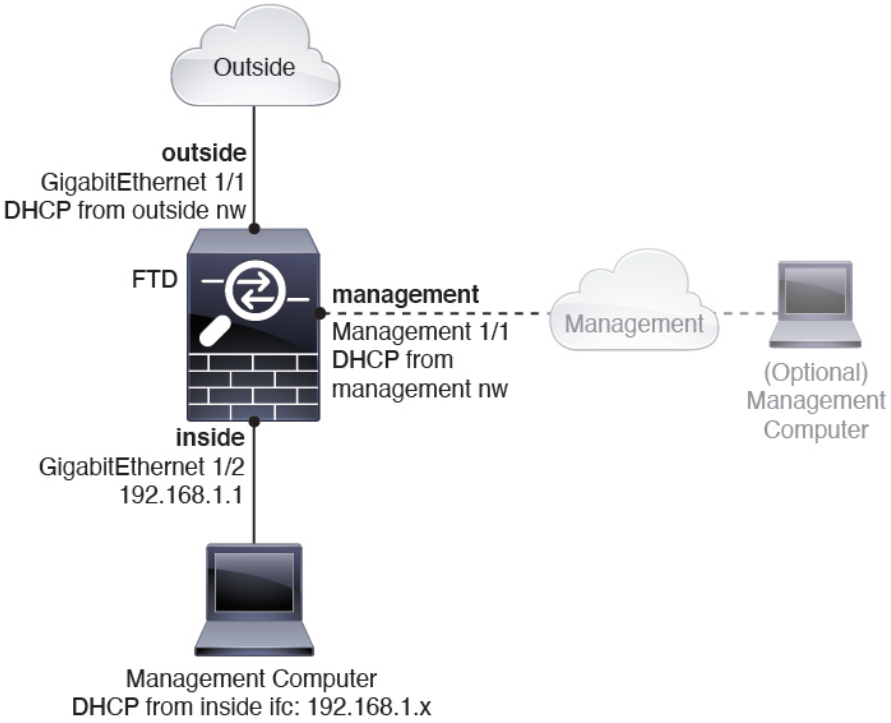
6	Firepower Device Manager	初期設定の完了, on page 11。
7	Cisco Commerce Workspace	ライセンスの設定, on page 13：ライセンス機能を取得します。
8	Smart Software Manager	ライセンスの設定, on page 13：ライセンス トークンを生成します。
9	Firepower Device Manager	ライセンスの設定, on page 13：スマート ライセンシング サーバにデバイスを登録します。
10	Firepower Device Manager	Firepower Device Managerでのデバイスの設定, on page 19。

ネットワーク配置とデフォルト設定の確認

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

（注） デフォルトの IP アドレスを使用できない場合（たとえば、デバイスを既存のネットワークに追加する場合）、コンソールポートに接続して、CLI で初期セットアップ（管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定など）を実行できます。「（任意）CLI での管理ネットワーク設定の変更 （9 ページ）」を参照してください。

図 *1* : 推奨されるネットワーク配置



（注） 6.5 以前の場合、Management 1/1 のデフォルト IP アドレスは 192.168.45.45 です。

デフォルト設定

初期設定後の Firepower デバイスの設定には次のものが含まれます。

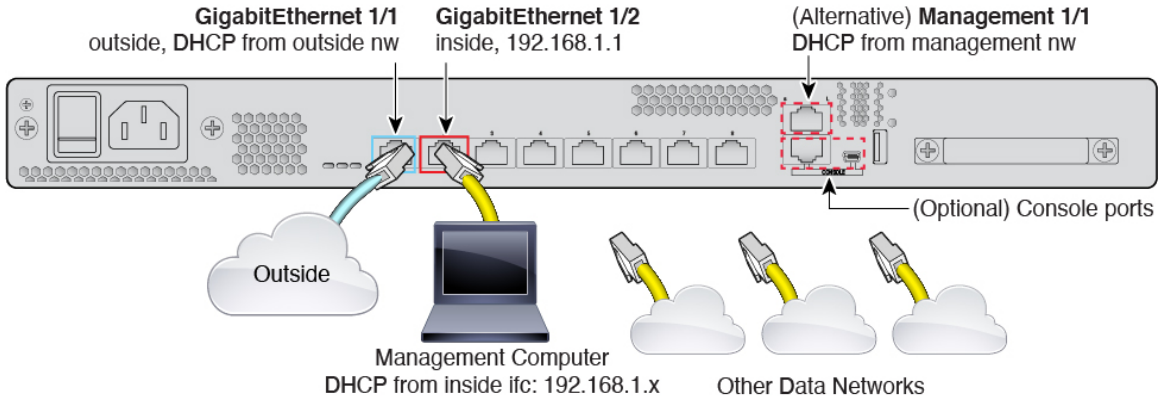
- **内部**：GigabitEthernet 1/2、IP アドレス 192.168.1.1
- **外部**：Ethernet 1/1、DHCP からの IP アドレス、またはセットアップ時に指定したアドレス
- **内部→外部**トラフィックフロー
- **管理**：Management 1/1（管理）
  - （6.6 以降）DHCP からの IP アドレス
  - （6.5 以前）IP アドレス 192.168.45.45

（注） Management 1/1 インターフェイスは、管理、スマートライセンス、およびデータベースの更新に使用されるデータインターフェイスとは別の特別なインターフェイスです。物理インターフェイスは、診断インターフェイスである 2 番目の論理インターフェイスと共有されます。診断はデータインターフェイスですが、syslog や SNMP など、他のタイプの管理トラフィック（デバイスとデバイス間）に限定されます。診断インターフェイスは通常使用されません。詳細については、『FDM configuration guide』を参照してください。

- **管理用の DNS サーバ**
  - （6.6 以降）管理 DHCP から取得されます。DNS サーバを受信しない場合、システムは OpenDNS：208.67.222.222、208.67.220.220、またはセットアップ時に指定したサーバを使用します
  - （6.5 以前）OpenDNS：208.67.222.222、208.67.220.220、またはセットアップ時に指定したサーバ
- **NTP**：Cisco NTP サーバ：0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org、またはセットアップ時に指定したサーバ
- **デフォルトルート**
  - **データインターフェイス**：外部 DHCP から取得したもの、またはセットアップ時に指定したゲートウェイ IP アドレス
  - **管理インターフェイス**：（6.6 以降）管理 DHCP から取得されます。ゲートウェイを受信しない場合、デフォルトルートはバックプレーンを介してデータインターフェイスを経由します。（6.5 以前）バックプレーンを介しデータインターフェイスを経由

    FTD 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。
- **DHCP サーバ**：内部インターフェイスおよび（6.5 以前のみ）管理インターフェイスで有効になります
- **FDM アクセス**：管理ホストと内部ホストに許可されます
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT

デバイスの配線



Note 6.5 以前の場合、Management 1/1 のデフォルト IP アドレスは 192.168.45.45 です。

管理 1/1 または GigabitEthernet 1/2 のいずれかで、ASA 5508-X または 5516-X を管理します。デフォルト設定でも、GigabitEthernet 1/1 は外部として設定されています。

Procedure

ステップ 1 Management Computer を次のいずれかのインターフェイスに接続します。

- GigabitEthernet 1/2：初期設定のために管理コンピュータを GigabitEthernet 1/2 に直接接続するか、GigabitEthernet 1/2 を内部ネットワークに接続します。GigabitEthernet 1/2 にはデフォルトの IP アドレス（192.168.1.1）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。
- 管理 1/1：管理コンピュータを管理ネットワークに接続します。管理 1/1 インターフェイスは、DHCP から IP アドレスを取得するため、ネットワークに DHCP サーバが含まれていることを確認してください。

  管理 1/1 の 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 PC 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, on page 9」を参照してください。

後で、他のインターフェイスから FDM 管理アクセスを設定できます。『FDM configuration guide』を参照してください。

ステップ 2 外部ネットワークを GigabitEthernet 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 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。

ステップ 3 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。

デバイスの電源投入

システムの電源は、デバイスの背面にあるロッカー電源スイッチによって制御されます。

始める前に

デバイスに対して信頼性の高い電力を供給することが重要です（たとえば、無停電電源装置（UPS）を使用）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

手順

ステップ 1 電源コードをデバイスに接続し、電源コンセントに接続します。

ステップ 2 シャーシの背面で、電源コードに隣接する標準的なロッカータイプの電源オン/オフ スイッチを使用して電源をオンにします。

ステップ 3 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。

図 *2:* 背面パネル

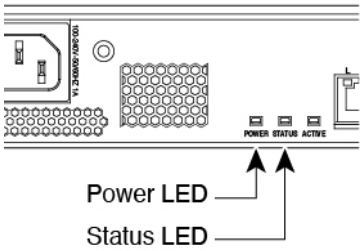
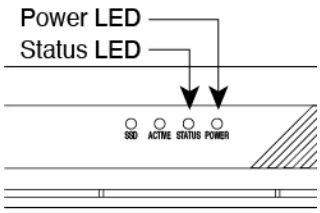


図 *3:* 前面パネル



ステップ 4 デバイスの前面または背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。

（任意）CLI での管理ネットワーク設定の変更

デフォルトの管理または内部 IP アドレスを使用できない場合（たとえば、デバイスを既存のネットワークに追加する場合や管理ネットワークに DHCP サーバが含まれていない場合）、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設定のみを指定できます。データインターフェイスの設定は FDM で指定する必要があります。

（注） 設定をクリア（たとえば、イメージを再作成することにより）しないかぎり、CLI セットアップスクリプトを繰り返すことはできません。ただし、これらの設定すべては、後から CLI で **configure network** コマンドを使用して変更できます。『FTD command reference』を参照してください。

手順

ステップ 1 FTD コンソールポートに接続します。詳細については、「Firepower Threat Defense CLI へのアクセス （24 ページ）」を参照してください。

ステップ 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。

ステップ 3 FTD に初めてログインすると、エンドユーザライセンス契約書（EULA）に同意して管理者パスワードを変更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）]：「**data-interfaces**」またはゲートウェイルータの IP アドレスを入力します。**data-interfaces** を設定すると、送信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依然として管理インターフェイスで FDM を使用できますが、管理でのリモート管理の場合は、管理ネットワークのゲートウェイルータの IP アドレスを入力する必要があります。データインターフェイスでの FDM 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。
- [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?）]：FDM を使用するには「**yes**」を入力します。「**no**」を入力することは、代わりに FMC を使用することを意味します。

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 change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
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 FDM にログインしてください。

FDM へのログイン

FDM にログインして FTD を設定します。

始める前に

- Firefox、Chrome、Safari、Edge、または Internet Explorer の最新バージョンを使用します。

手順

ステップ 1 ブラウザに次の URL を入力します。

- 内部（GigabitEthernet 1/2）：**https://192.168.1.1**。
- （6.6 以降）管理：**https://***management_ip*。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。CLI セットアップで管理 IP アドレスを変更した場合は、そのアドレスを入力します。
- （6.5 以前）管理：**https://192.168.45.45**。CLI セットアップで管理 IP アドレスを変更した場合は、そのアドレスを入力します。

ステップ 2 ユーザ名 admin、デフォルトパスワード Admin123 を使用してログインします。

次のタスク

- FDMセットアップウィザードを実行します。初期設定の完了 （11 ページ）を参照してください。

初期設定の完了

初期設定を完了するには、最初に FDM にログインしたときにセットアップ ウィザードを使用します。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。

- 外部（GigabitEthernet1/1）および内部インターフェイス（GigabitEthernet1/2）。
- 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で実行されている DHCP サーバ。

手順

ステップ 1 エンド ユーザ ライセンス契約書を読んで同意し、管理者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 2 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 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。

ステップ 3 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 4 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 のアカウントにログインします。ライセンスの設定 （13 ページ）を参照してください。

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。

ステップ 5 [終了（Finish）] をクリックします。

次のタスク

- 評価ライセンスを引き続き使用することもできますが、デバイスを登録してライセンスを取得することをお勧めします。ライセンスの設定 （13 ページ）を参照してください。

- また、デバイスの設定を選択することもできます。Firepower Device Managerでのデバイスの設定 （19 ページ）を参照してください。

ライセンスの設定

FTD は、ライセンスの購入およびライセンス プールの一元管理を可能にするシスコ スマート ソフトウェア ライセンシングを使用します。

シャーシを登録すると、License Authority によって シャーシと License Authority 間の通信に使用される ID 証明書が発行されます。また、適切な仮想アカウントにシャーシが割り当てられます。

基本ライセンスは自動的に含まれます。スマート ライセンシングでは、まだ購入していない製品機能を使用することはできませんが、次のオプション機能ライセンスを購入して準拠する必要があります。

- **脅威**：セキュリティ インテリジェンスと Cisco Firepower の次世代 IPS
- **マルウェア**：強化されたネットワーク向けの高度なマルウェア防御（AMP）
- **URL**：URL フィルタリング
- **RA VPN**：AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN 専用。

上記のライセンスに加えて、1、3、または5年のアップデートにアクセスするため、該当するサブスクリプションを購入する必要もあります。

システムのライセンシングの詳細については、『FDM Configuration Guide』を参照してください。

始める前に

- Cisco Smart Software Manager にマスター アカウントを持ちます。

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- （輸出コンプライアンス フラグを使用して有効化される）機能を使用するには、ご使用のシスコ スマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

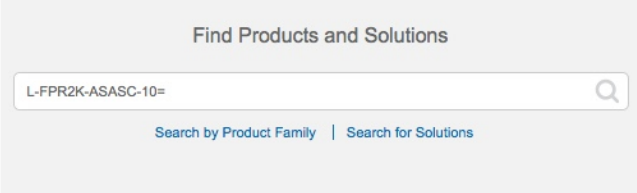
手順

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要

がある場合は、Cisco Commerce Workspace で [Find Products and Solutions] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *4*: ライセンス検索



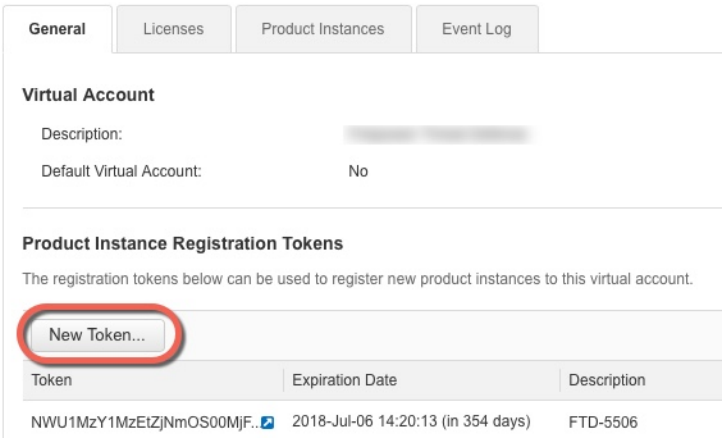
（注） PID が見つからない場合は、注文に手動で PID を追加できます。

- 脅威、マルウェア、および URL ライセンスの組み合わせ：
  - L-ASA5508T-TMC=
  - L-ASA5516T-TMC=
- 脅威、マルウェア、および URL サブスクリプションの組み合わせ：
  - L-ASA5508T-TMC-1Y
  - L-ASA5508T-TMC-3Y
  - L-ASA5508T-TMC-5Y
  - L-ASA5516T-TMC-1Y
  - L-ASA5516T-TMC-3Y
  - L-ASA5516T-TMC-5Y
- RA VPN：『Cisco AnyConnect Ordering Guide』を参照してください。

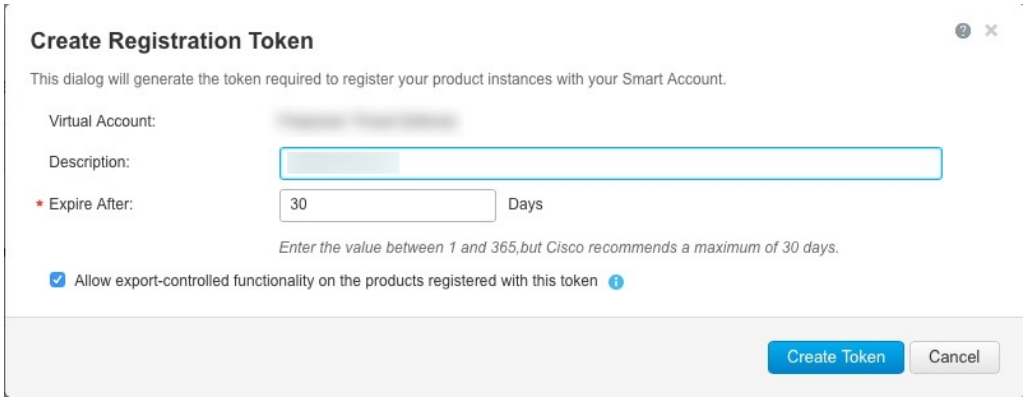
ステップ 2 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [インベントリ（Inventory）] をクリックします。

b) [全般（General）] タブで、[新規トークン（New Token）] をクリックします。



c) [Create Registration Token] ダイアログボックスで、以下の設定値を入力してから [Create Token] をクリックします。



- **[説明（Description）]**
- Expire After：推奨値は 30 日です。
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：高度暗号化が許可されている国の場合は輸出コンプライアンスフラグを有効にします。

トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [Token] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。FTD の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *5*: トークンの表示

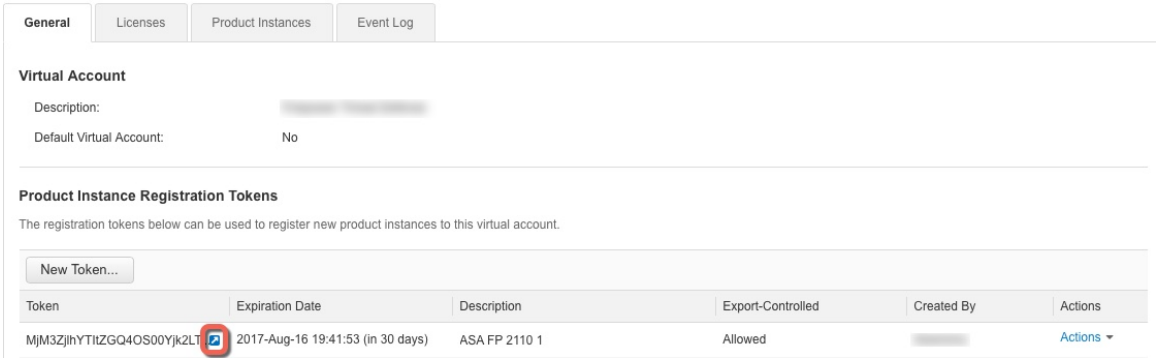
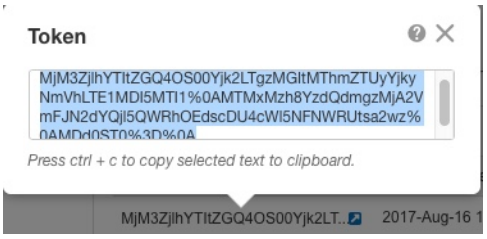


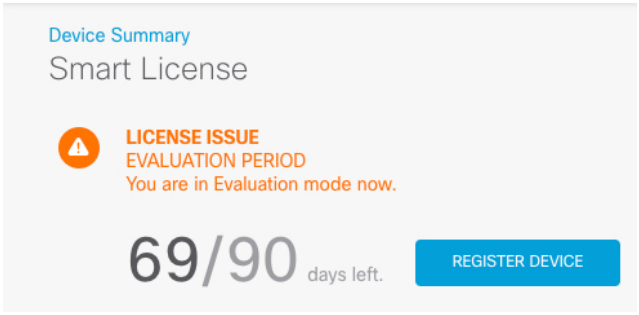
図 *6*: トークンのコピー



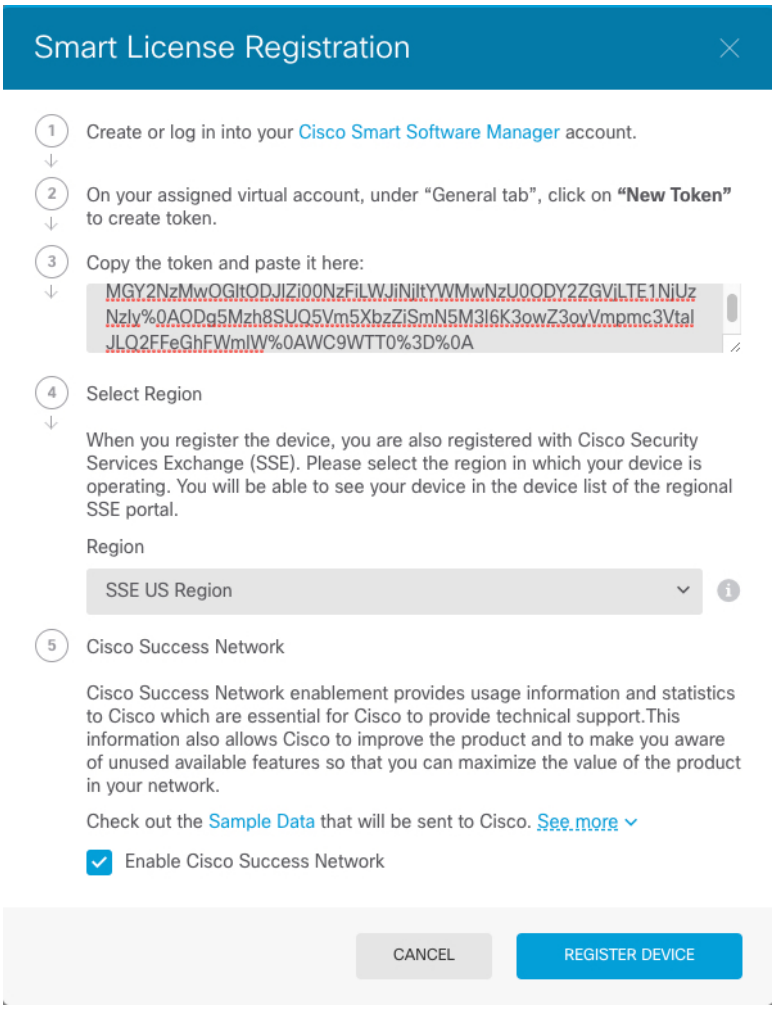
ステップ 3 FDM で、**[デバイス（Device）]** をクリックし、**[スマート ライセンス概要（Smart License summary）]** の **[設定の表示（View Configuration）]** をクリックします。

[スマート ライセンス（Smart License）] ページが表示されます。

ステップ 4 [デバイスの登録（Register Device）] をクリックします。

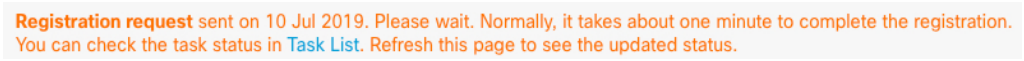


次に、[スマート ライセンス登録（Smart License Registration）] ダイアログボックスの指示に従って、トークンに貼り付けます。

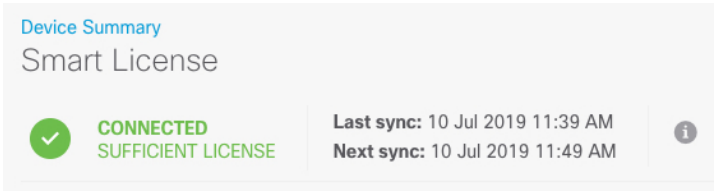


ステップ 5 [デバイスの登録（Register Device）] をクリックします。

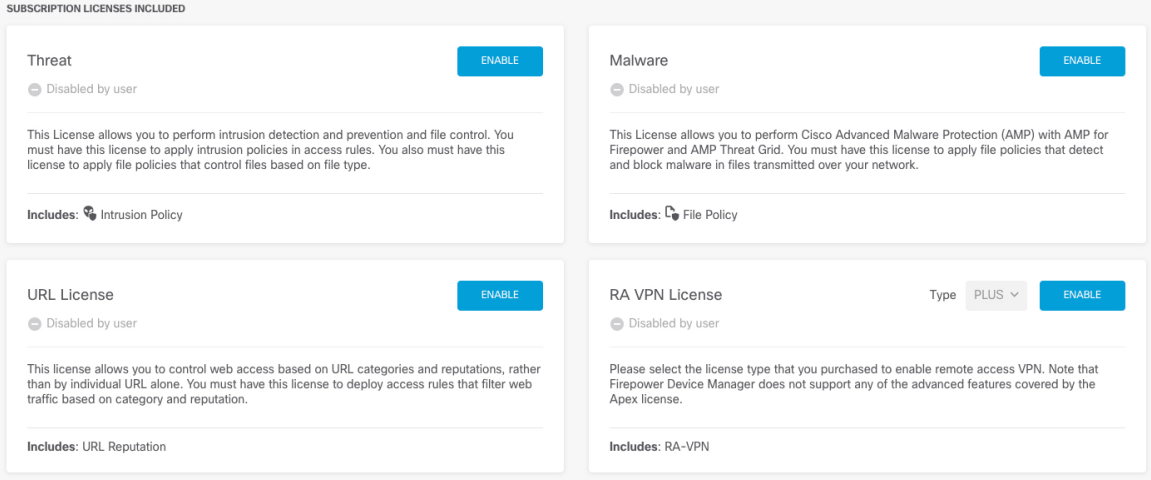
[スマート ライセンス（Smart License）] ページに戻ります。デバイス登録中は次のメッセージが表示されます。



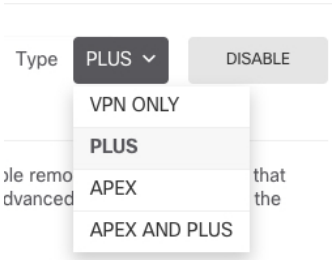
デバイスが正常に登録され、ページが更新されると、次のように表示されます。



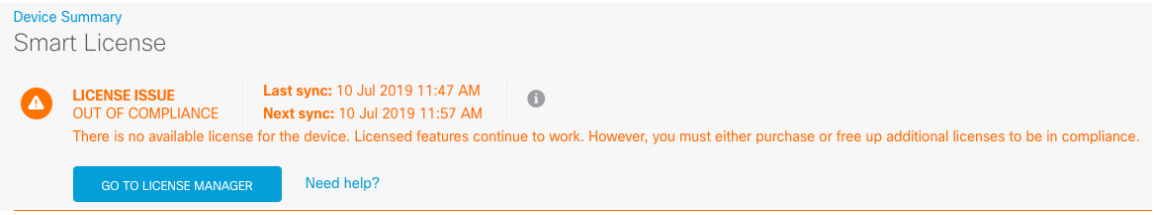
ステップ 6 必要に応じて、それぞれのオプション ライセンスの [有効化/無効化（Enable/Disable）] コントロールをクリックします。



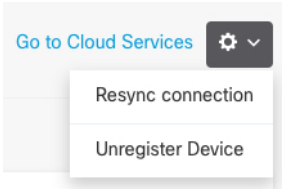
- [有効化（Enable）]：Cisco Smart Software Manager アカウントにライセンスを登録し、制御された機能が有効になります。ライセンスによって制御されるポリシーを設定し、展開できます。
- [無効化（Disable）]：Cisco Smart Software Manager アカウントのライセンスを登録解除し、制御された機能が無効になります。新しいポリシーの機能の設定も、その機能を使用するポリシーの展開もできません。
- **RA VPN** ライセンスを有効にした場合は、使用するライセンスのタイプ（[Plus]、[Apex]、[VPN 専用（VPN Only）]、または [Plus と Apex（Plus and Apex）] を選択します。



機能を有効にすると、アカウントにライセンスがない場合はページを更新した後に次の非準拠メッセージが表示されます。



ステップ 7 歯車ドロップダウン リストから [接続の再同期（Resync Connection）] を選択して、Cisco Smart Software Manager とライセンス情報を同期させます。



Firepower Device Managerでのデバイスの設定

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。

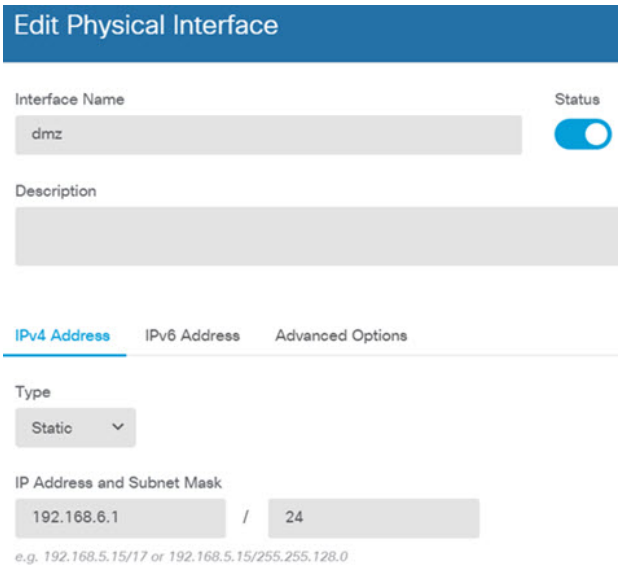
手順

ステップ 1 他のインターフェイスに有線接続する場合は、[デバイス（Device）] を選択して [インターフェイス（Interfaces）] の概要のリンクをクリックします。

各インターフェイスの編集アイコン（）をクリックしてモードを設定し、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。

図 7:インターフェイスの編集



ステップ 2 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。

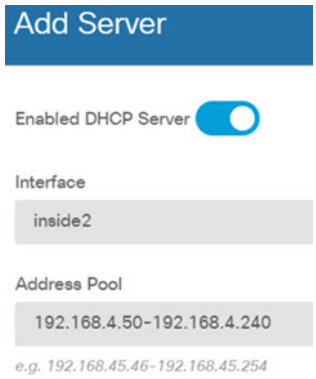
図 *8:* セキュリティ ゾーン オブジェクト

ステップ 3 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。

図 *9 : DHCP* サーバ



ステップ 4 [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 *10 :* デフォルトルート

ステップ 5 [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。

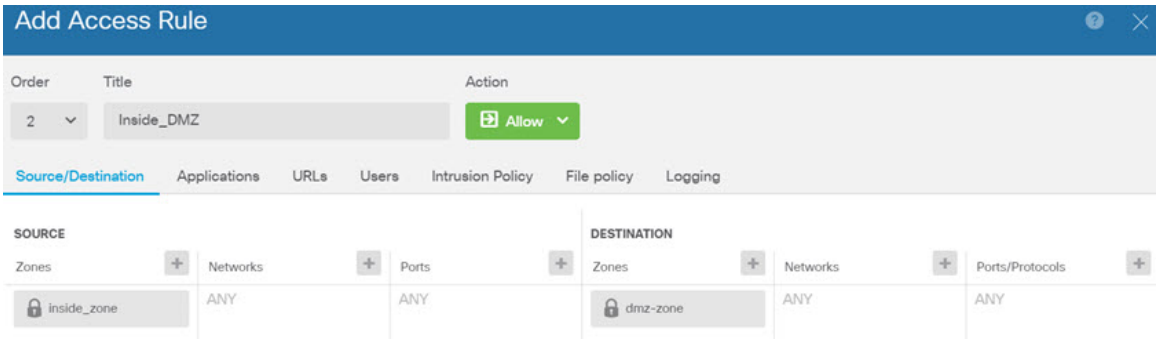
- [SSL復号（SSL Decryption）]：侵入、マルウェアなどについて暗号化された接続（HTTPS など）を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するにはSSL復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。
- [アイデンティティ（Identity）]：個々のユーザにネットワーク アクティビティを関連付ける、またはユーザまたはユーザ グループのメンバーシップに基づいてネットワーク アクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザを判定するためにアイデンティティ ポリシーを使用します。
- [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（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 *11*：アクセス コントロール ポリシー



ステップ 6 [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 7 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。

Firepower Threat Defense CLI へのアクセス

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 には、コンソール ポートに接続してアクセスできます。

FTD デバイスの管理インターフェイスに SSH で接続できます。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。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。

手順

ステップ 1 CLI にログインするには、管理コンピュータをコンソール ポートに接続します。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。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

ステップ 2 ユーザ名 **admin** と、初期セットアップ時に設定したパスワードを使用して FTD CLI にログインします。

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。使用法の詳細については、『*Cisco Firepower Threat Defense Command Reference*』 を参照してください。

デバイスの電源切断

FDM を使用してシステムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されていて、電源プラグを抜いたり、電源を切断したりすると、Firepower システムをグレースフルシャットダウンできないことを覚えておいてください。

手順

ステップ 1 コンソールポートに接続して FTD CLI にアクセスし、FTD をシャットダウンします。

shutdown

例：

```
> shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
Shutting down sfifd...                                             [  OK  ]
Clearing static routes
Unconfiguring default route                                        [  OK  ]
Unconfiguring address on br1                                       [  OK  ]
Unconfiguring IPv6                                                 [  OK  ]
Downing interface                                                  [  OK  ]
Stopping xinetd:
Stopping nscd...                                                   [  OK  ]
Stopping system log daemon...                                      [  OK  ]
Stopping Threat Defense ...
Stopping system message bus: dbus.                                 [  OK  ]
Un-mounting disk partitions ...
device-mapper: remove ioctl on root failed: Device or resource busy
[...]
mdadm: Cannot get exclusive access to /dev/md0:Perhaps a running process, mounted
filesystem or active volume group?
Stopping OpenBSD Secure Shell server: sshd
stopped /usr/sbin/sshd (pid 3520)
done.
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid
 3525)
acpid.
Stopping system message bus: dbus.
Stopping internet superserver: xinetd.
no /etc/sysconfig/kdump.conf
Deconfiguring network interfaces... ifdown: interface br1 not configured
done.
SSP-Security-Module is shutting down ...
Sending ALL processes the TERM signal ...
acpid: exiting
Sending ALL processes the KILL signal ...
Deactivating swap...
Unmounting local filesystems...

Firepower Threat Defense stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

ステップ 2 FTDがシャットダウンし、コンソールに「今すぐに電源をオフにする」と表示された場合は、電源スイッチをオフにし、必要に応じて電源を抜いてシャーシから電源を物理的に取り外します。

または、プロンプトで **y** を入力してシステムをリブートすることもできます。

次のステップ

FTDデバイスの設定を続行するには、Cisco Firepower ドキュメント一覧 でお使いのソフトウェアバージョンのマニュアルを参照してください。

FDM の使用に関する詳細については、『Firepower Device Manager 用 Cisco Firepower Threat Defense 構成ガイド』を参照してください。