Management Center での Threat Defense の展開

この章の対象読者

この章では、脅威に対する防御 の初期設定の方法と Management Center へのデバイスの登録方法について説明します。大規模ネットワークにおける一般的な展開では、複数の管理対象デバイスをネットワーク セグメントにインストールし、分析のためにトラフィックをモニターして、管理 Management Center にレポートします。これにより、管理、分析、およびレポート タスクの実行に使用できる Web インターフェイスがある集中管理コンソールを使用できます。

単一またはごく少数のデバイスのみが含まれるネットワークでは、Management Center のような高性能の多機能デバイスマネージャを使用する必要がなく、一体型の Device Manager を使用できます。Device Manager の 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、小規模ネットワークの導入に最もよく使用されるソフトウェアの基本機能を設定できます。

Cisco ISA 3000 では、脅威に対する防御 ソフトウェアか ASA ソフトウェアを実行できます。脅威に対する防御 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。「Cisco ASA および Firepower Threat Defense 再イメージ化ガイド」を参照してください。

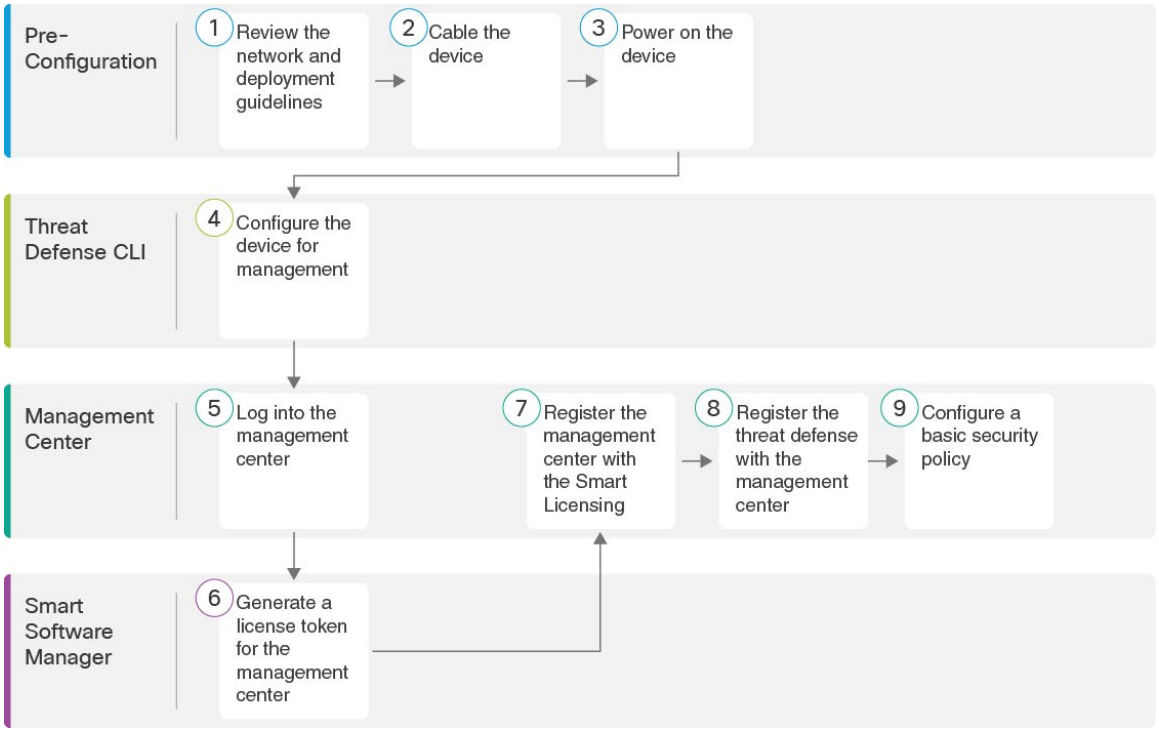
プライバシー収集ステートメント：ISA 3000 には個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザー名などの設定では、個人識別情報を使用できます。この場合、設定作業時や SNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

はじめる前に

Management Center の初期設定を展開して実行します。Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation GuideまたはCisco Secure Firewall Management Center Virtual 入門ガイドを参照してください。

エンドツーエンドの手順

シャーシで Management Center を使用して 脅威に対する防御 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	ネットワーク展開の確認 （3 ページ）。
2	事前設定	デバイスの配線 （8 ページ）。
3	事前設定	デバイスの電源投入 （12 ページ）。

4	Threat Defense CLI	CLI を使用した Threat Defense 初期設定の実行の完了 （13 ページ）。
5	Management Center	へのログインManagement Center （19 ページ）。
6	Smart Software Manager	Management Center のライセンスの取得 （20 ページ） ：Management Center のライセンストークンを生成します。
7	Management Center	Management Center のライセンスの取得 （20 ページ） ：スマートライセンシング サーバーに Management Center を登録します。
8	Management Center	Management Center への Threat Defense の登録 （21 ページ）。
9	Management Center	基本的なセキュリティポリシーの設定 （24 ページ）。

ネットワーク展開の確認

脅威に対する防御 は、管理1/1インターフェイスからか、または 6.7 以降ではデータインターフェイスから Management Center を使用して管理できます。デフォルトでは、Management 1/1 インターフェイスが有効になっており、IP アドレス（192.168.45.45）が設定されています。このインターフェイスは、最初に DHCP サーバーも実行します。初期設定時にマネージャとして Management Center を選択すると、DHCP サーバーは無効になります。コンソールポートでの初期セットアップ時に、管理インターフェイスと Management Center アクセス データ インターフェイスを設定できます。脅威に対する防御 を Management Center に接続した後は、他のインターフェイスを設定できます。

（注） データインターフェイスからの Management Center アクセスには、次の制限があります。

- マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。
- このインターフェイスは管理専用にできません。
- ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
- PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを 脅威に対する防御 と WAN モデムの間に配置する必要があります。
- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
- SSHはデータインターフェイスではデフォルトで有効になっていないため、後でManagement Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。

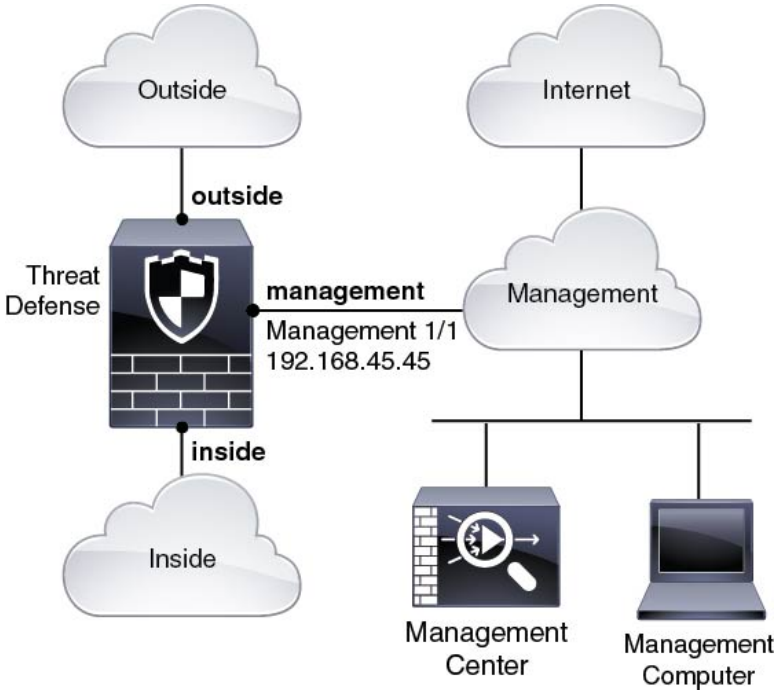
ネットワークに 脅威に対する防御 デバイスを配置する方法については、次のネットワーク配置例を参照してください。

個別の管理ネットワーク

Management Center と 脅威に対する防御 の両方で、ライセンシングと更新を行うには管理からのインターネットアクセスが必要です。

次の図に、Management Center と管理コンピュータが管理ネットワークに接続している ISA 3000 について考えられるネットワーク展開を示します。管理ネットワークには、ライセンシングと更新のためのインターネットへのパスがあります。

図 *1* : 個別の管理ネットワーク



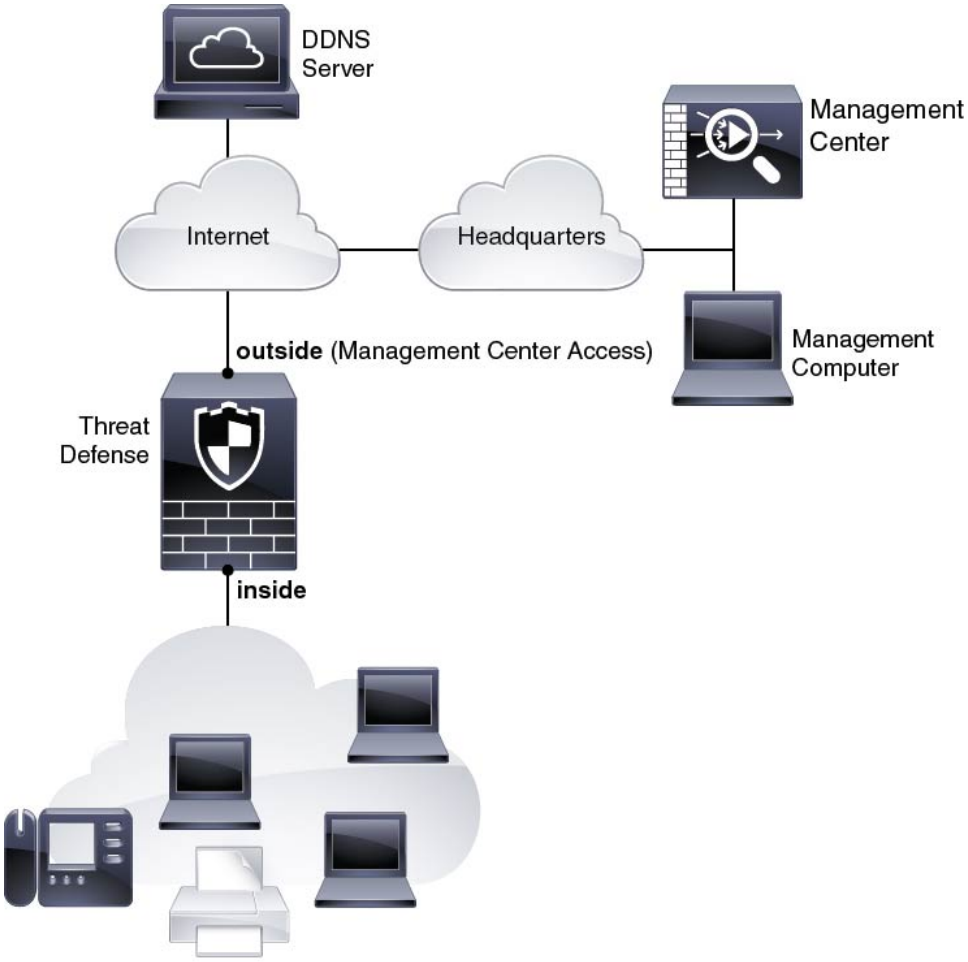
6.7 以降のリモート管理展開

（注） リモートブランチのセットアップでは、その展開に固有のスタンドアロンドキュメントを使用することを推奨します。

次の図に、外部インターフェイスを管理に使用した ISA 3000 向けに推奨されるネットワーク展開を示します。このシナリオは、本社から支社を管理する場合に最適です。脅威に対する防御 の初期セットアップを本社で実行し、事前に設定されたデバイスを支社の場所に送信できます。

脅威に対する防御 または Management Center のいずれかにパブリック IP アドレスまたはホスト名が必要です。DHCP を使用して 脅威に対する防御 でパブリック IP アドレスを受信する場合は、オプションで外部インターフェイスのダイナミック DNS（DDNS）を設定できます。DDNS は、脅威に対する防御 の IP アドレスが変更された場合に Management Center が完全修飾ドメイン名（FQDN）で 脅威に対する防御 に到達できるようにします。脅威に対する防御 でプライベート IP アドレスを受信する場合は、Management Center にはパブリック IP アドレスまたはホスト名が必要です。

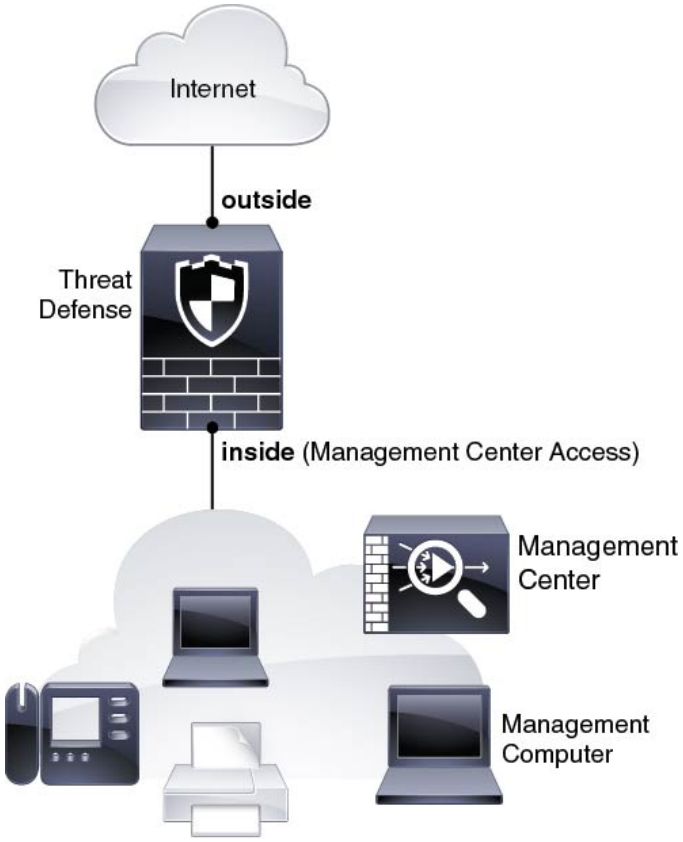
図 *2:* リモート管理の展開



6.7 以降の内部管理の展開

次の図に、内部インターフェイスを管理に使用した ISA 3000 向けに推奨されるネットワーク展開を示します。

図 *3 :* 内部管理の展開



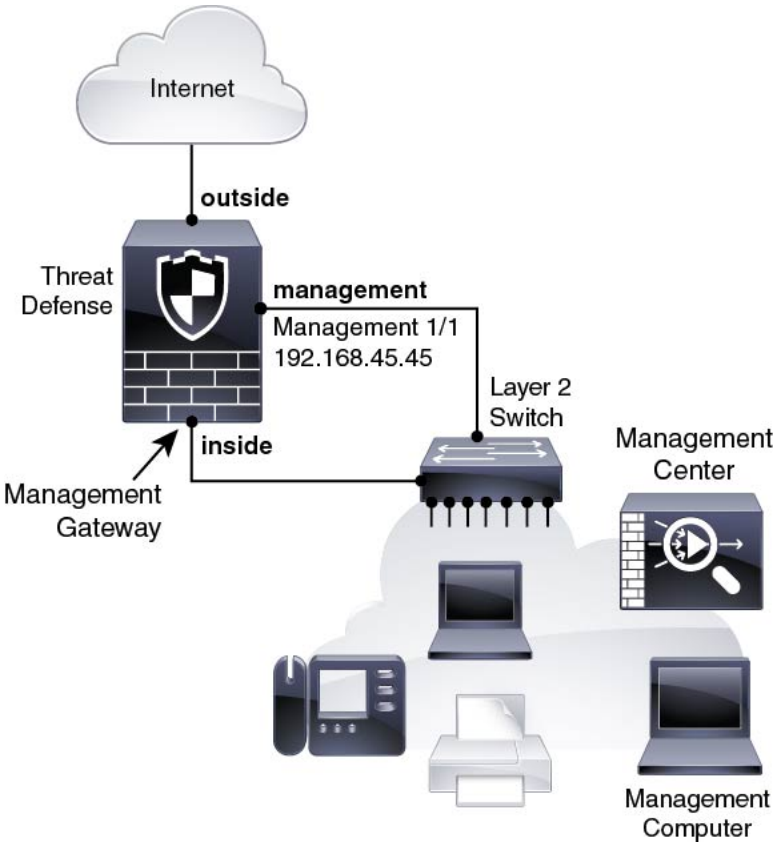
6.6 以前エッジネットワークの展開

6.6 以前では、Management Center は管理インターフェイス上の 脅威に対する防御 のみと通信できます。さらに、Management Center と 脅威に対する防御 の両方で、ライセンシングと更新を行うには管理からのインターネットアクセスが必要です。

次の図は、Management Center および 脅威に対する防御 管理用のインターネット ゲートウェイとして機能する場合の、ISA 3000 の可能なネットワーク展開を示しています。このシナリオは、たとえば 6.7 以降の高可用性展開にも使用できます。

次の図では、Management 1/1 をレイヤ 2 スイッチを介して内部のインターフェイスに接続するとともに、Management Center と管理コンピュータをスイッチに接続することにより、ISA 3000 が管理インターフェイスと Management Center のインターネットゲートウェイとして機能しています。（管理インターフェイスは 脅威に対する防御 上の他のインターフェイスとは別のものであるため、このような直接接続が許可されます）。

図 *4:* エッジ ネットワークの展開



デバイスの配線

ISA 3000 で推奨シナリオのいずれかに相当するケーブル接続を行うには、次の手順を参照してください。

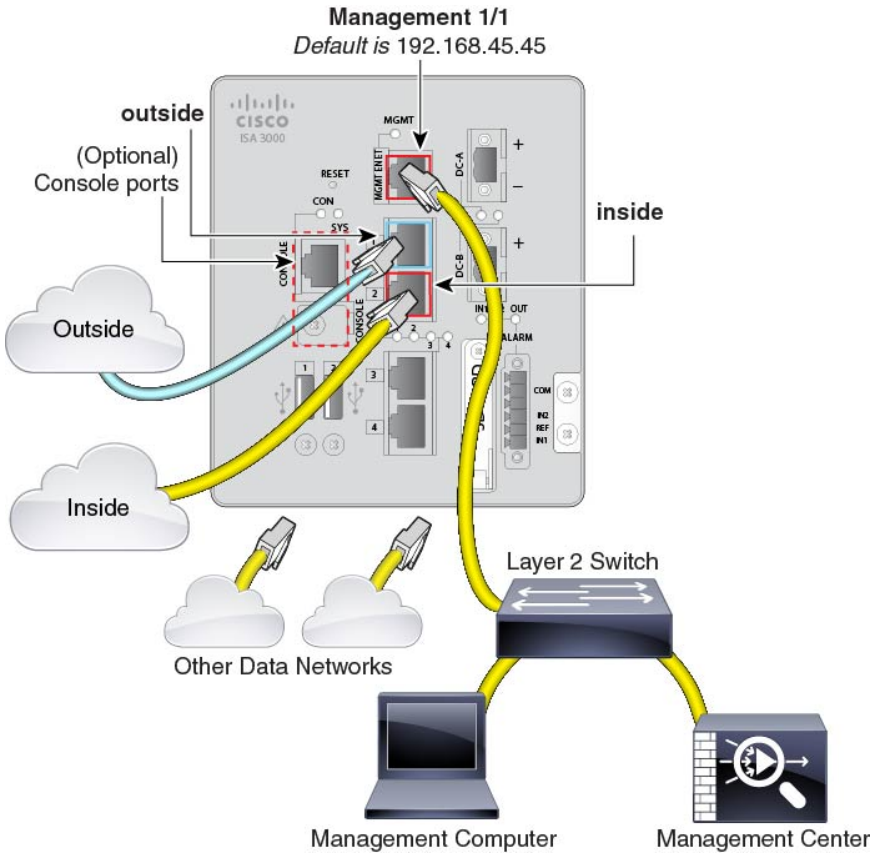
（注） ISA 3000 と Management Center の両方に同じデフォルトの管理 IP アドレス（192.168.45.45）が設定されています。このガイドでは、初期セットアップ時に異なる IP アドレスをデバイスに設定することを前提としています。6.5 以降の Management Center は、管理インターフェイス用の DHCP クライアントにデフォルト設定されていることに注意してください。ただし、DHCP サーバーが存在しない場合は、デフォルトで 192.168.45.45 になります。

（注） その他のトポロジも使用可能で、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。

手順

ステップ 1 別の管理ネットワーク用のケーブル配線

図 *5*: 個別の管理ネットワークのケーブル配線



a) 次のように管理ネットワークにケーブルを配線します。

- Management 1/1 インターフェイス
- Management Center
- 管理コンピュータ

b) 管理コンピュータをコンソールポートに接続します。管理インターフェイスへの SSH を使用しない場合は、コンソールポートを使用して初期設定のために CLI にアクセスする必要があります。

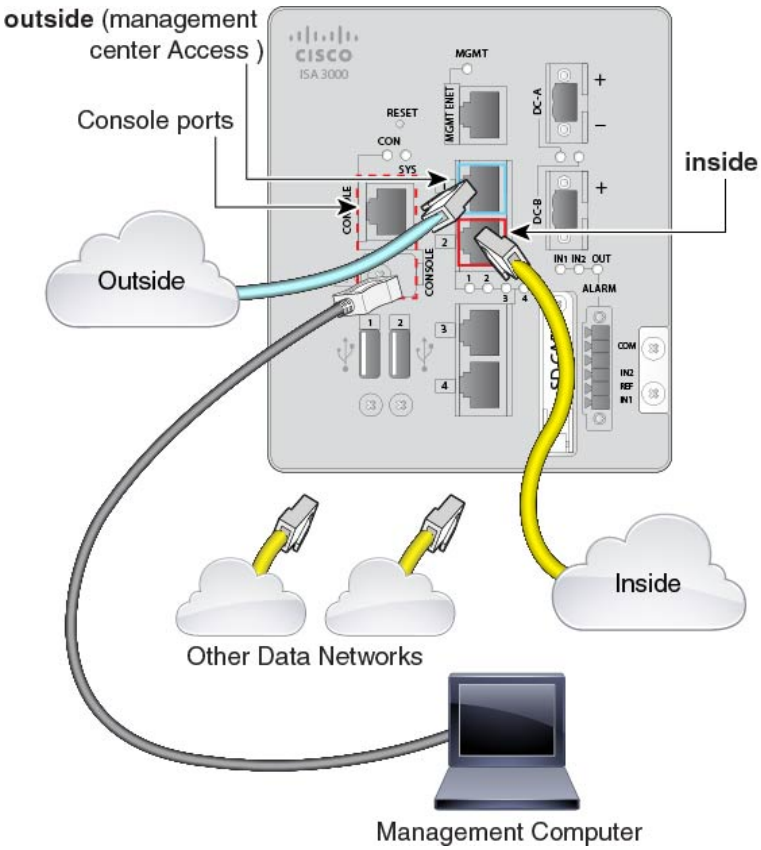
c) 内部インターフェイス（GigabitEthernet 1/2 など）を内部ルータに接続します。

d) 外部インターフェイス（GigabitEthernet 1/1 など）を外部ルータに接続します。

e) 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。

ステップ 2 （6.7 以降）リモート管理展開のケーブル接続：

図 *6:* リモート管理展開のケーブル接続



Management Center と管理コンピュータはリモートの本社にあり、脅威に対する防御 にはインターネット経由で到達できます。

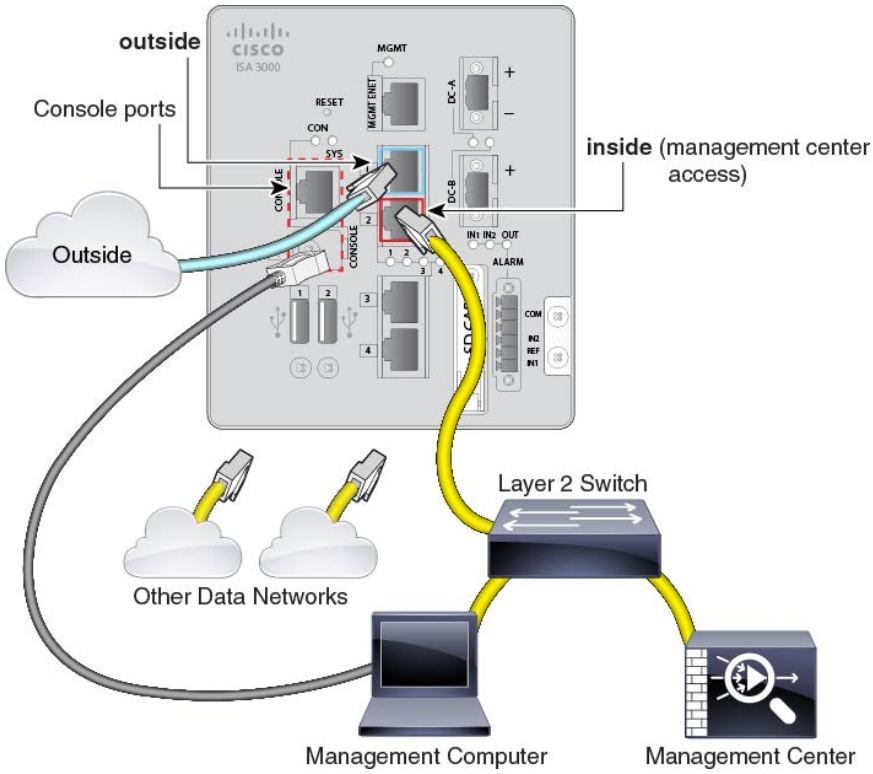
a) 管理コンピュータをコンソールポートに接続します。コンソールポートを使用して CLI にアクセスし、初期セットアップを行う必要があります。

   本社で CLI の初期セットアップを実行してから、脅威に対する防御 をリモートの支社に送信できます。支社では、日常的に使用するためのコンソール接続は必要ありません。ただし、トラブルシューティングに必要な場合があります。

b) 内部ネットワーク（GigabitEthernet 1/2 など）をケーブル接続します。
c) 外部インターフェイス（GigabitEthernet 1/1 など）を外部ルータに接続します。
d) 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。

ステップ 3 （6.7以降）内部管理展開のケーブル接続：

図 *7*: 内部管理展開のケーブル接続



Management Center と管理コンピュータは、他の内部エンドポイントとともに内部ネットワーク上に存在します。

a) 管理コンピュータをコンソールポートに接続します。コンソールポートを使用して CLI にアクセスし、初期セットアップを行う必要があります。

b) 内部ネットワーク（GigabitEthernet 1/2 など）に次のケーブルを接続します。

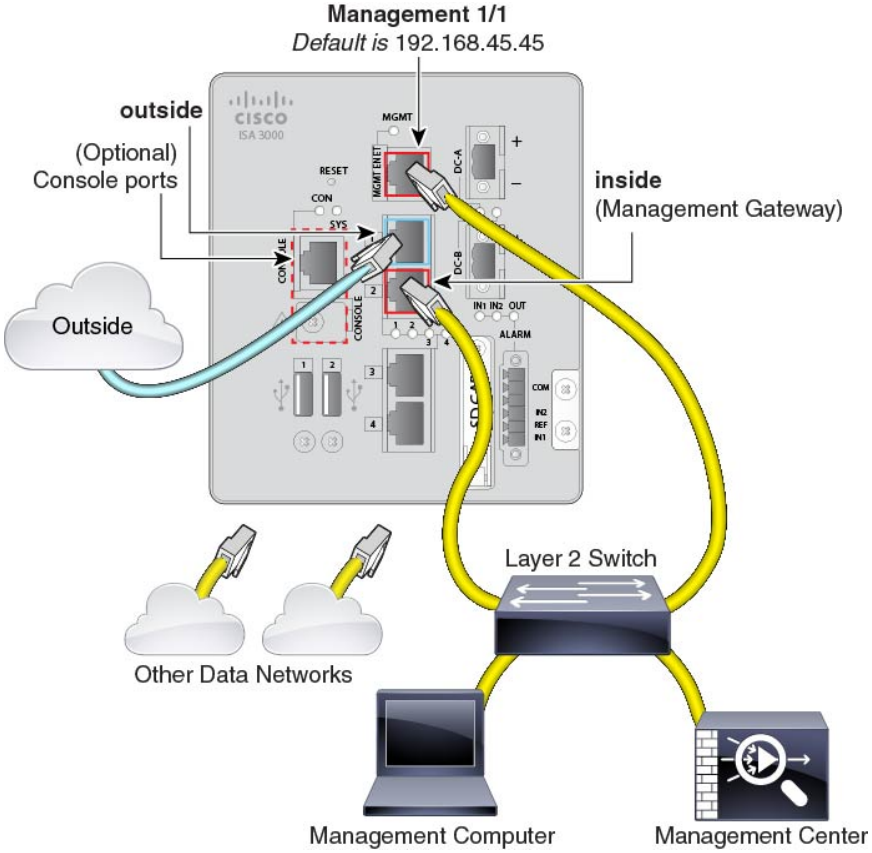
- Management Center
- 管理コンピュータ

c) 外部インターフェイス（GigabitEthernet 1/1 など）を外部ルータに接続します。

d) 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。

ステップ 4 （6.6 以降）エッジ展開用のケーブル接続。

図 *8 :* エッジ展開のケーブル配線



a) 以下の機器のケーブルをレイヤ 2 イーサネット スイッチに接続します。

- 内部インターフェイス（GigabitEthernet 1/2など）
- Management 1/1 インターフェイス
- Management Center
- 管理コンピュータ

b) 管理コンピュータをコンソールポートに接続します。管理インターフェイスへの SSH を使用しない場合は、コンソールポートを使用して初期設定のために CLI にアクセスする必要があります。

c) 外部インターフェイス（GigabitEthernet 1/1 など）を外部ルータに接続します。

d) 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 DC 電源で制御されます。電源ボタンはありません。

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 電源プラグは DC 電源に配線した後に ISA 3000 に接続します。

電源プラグの正しい配線手順については、『ハードウェア設定ガイド』の「DC 電源への接続」を参照してください。

ステップ 2 ISA 3000 デバイスの前面にあるシステム 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。緑色に点滅している場合、デバイスはブートアップ フェーズおよび POST（電源投入時自己診断テスト）の状態です。

すべてのデバイスが ISA 3000 に正しく接続されているか確認するには、『ハードウェア設置ガイド』の「接続の確認」を参照してください。

CLI を使用した Threat Defense 初期設定の実行の完了

脅威に対する防御 CLI に接続して初期設定を実行します。これには、セットアップウィザードを使用した管理 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が含まれます。専用の管理インターフェイスは、独自のネットワーク設定を持つ特別なインターフェイスです。6.7 以降：Management Center アクセスに管理インターフェイスを使用しない場合は、代わりに CLI を使用してデータインターフェイスを設定できます。また、Management Center 通信の設定を行います。

手順

ステップ 1 コンソールポートから、または管理インターフェイスへの SSH を使用して、脅威に対する防御 CLI に接続します。デフォルトで DHCP サーバーから IP アドレスが取得されます。ネットワーク設定を変更する場合は、切断されないようにコンソールポートを使用することを推奨します。

ステップ 2 ユーザー名 **admin** およびパスワード **Admin123** でログインします。

（注） パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。手順については、再イメージ化のガイドを参照してください。

ステップ 3 脅威に対する防御 に初めてログインすると、エンドユーザーライセンス契約（EULA）に同意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。

（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セットアップウィザード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 のコマンドリファレンスを参照してください。

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。

（注） 6.7以降：データインターフェイスで Management Center アクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。たとえば、データインターフェイスを介してバックプレーン経由でルーティングされる管理トラフィックは、データインターフェイス DNS サーバーではなく、管理インターフェイス DNS サーバーを使用して FQDN を解決します。

次のガイドラインを参照してください。

- [DHCP経由または手動でIPv4を設定しますか?（Configure IPv4 via DHCP or manually?）]：6.7 以降：管理インターフェイスではなくデータインターフェイスを Management Center アクセスに使用する場合は、[手動（manual）] を選択します。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。管理インターフェイスが DHCP に設定されている場合、管理用のデータインターフェイスを設定することはできません。これは、**data-interfaces** である必要があるデフォルトルートが DHCP サーバーから受信したルートで上書きされる可能性があるためです。
- [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（Enter the IPv4 default gateway for the management interface）]：6.7 以降：管理インターフェイスの代わりに Management Centerアクセスにデータインターフェイスを使用する場合は、ゲートウェイを [data-interfaces] に設定します。この設定は、Management Center アクセス データ インターフェイスを通じてルーティングできるように、バックプレーンを介して管理トラフィックを転送します。Management Center アクセスに管理インターフェイスを使用する場合は、Management 1/1 ネットワークでゲートウェイ IP アドレスを設定する必要があります。
- **ネットワーク情報が変更された場合は再接続が必要**：SSH で接続しているのに、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?）]：Management Center を使用するには「**no**」を入力します。**yes** と入力すると、代わりに Device Manager を使用することになります。
- [ファイアウォールモードを設定しますか（Configure firewall mode?）]：初期設定でファイアウォールモードを設定することをお勧めします。初期設定後にファイアウォールモードを変更すると、実行コンフィギュレーションが消去されます。データインターフェイス Management Center アクセスは、ルーテッド ファイアウォール モードでのみサポートされることに注意してください。

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]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

ステップ 4 この 脅威に対する防御 を管理する Management Center を特定します。

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the Management Center.Management Center を直接アドレス指定できない場合は、

DONTRESOLVE を使用します。また、*nat_id* も指定します。双方向の SSL 暗号化通信チャネルを2台のデバイス間に確立するには、少なくても1台以上のデバイス（Management Center または 脅威に対する防御 ）に到達可能な IP アドレスが必要です。このコマンドで **DONTRESOLVE** を指定するには、到達可能な IP アドレスまたはホスト名が 脅威に対する防御 に必要です。

- reg_key：脅威に対する防御 を登録するときに Management Center でも指定する任意のワンタイム登録キーを指定します。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。
- nat_id：一方の側で到達可能な IP アドレスまたはホスト名が指定されていない場合は、脅威に対する防御 を登録するときに Management Center にも指定する任意の一意のワンタイム文字列を指定します。この文字列は、 Management Center を **DONTRESOLVE** に設定した場合に必要です。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン（-）などがあります。この ID は、Management Center に登録する他のデバイスには使用できません。

（注） 管理にデータインターフェイスを使用する場合は、登録用に 脅威に対する防御 と Management Center の両方で NAT ID を指定する必要があります。

例：

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

Management Center が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに登録キーを入力し、ホスト名の代わりに DONTRESOLVE を指定します。

例：

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

脅威に対する防御 が NAT デバイスの背後にある場合は、次の例に示すように、一意の NAT ID とともに Management Center IP アドレスまたはホスト名を入力します。

例：

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

ステップ 5 （任意）（6.7 以降）Management Center アクセス用のデータインターフェイスを設定します。

configure network management-data-interface

その後、データインターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。

（注） このコマンドを使用する場合は、コンソールポートを使用する必要があります。管理インターフェイスに SSH を使用すると、接続が切断され、コンソールポートに再接続する必要が生じる場合があります。SSH の詳細な使用方法については、次を参照してください。

このコマンドの使用については、次の詳細を参照してください。

- データインターフェイスを管理に使用する場合、元の管理インターフェイスはDHCPを使用できません。初期セットアップ時にIPアドレスを手動で設定しなかった場合は、**configure network** {**ipv4** | **ipv6**} **manual** コマンドを使用して設定できるようになりました。管理インターフェイス ゲートウェイを **data-interfaces** に設定しなかった場合は、ここでこのコマンドで設定します。
- データインターフェイスからの Management Center アクセスには、次の制限があります。
  - マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。
  - このインターフェイスは管理専用にできません。
  - ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
  - PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを 脅威に対する防御 と WAN モデムの間に配置する必要があります。
  - インターフェイスを配置する必要があるのはグローバル VRF のみです。
  - 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
  - SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。
- 脅威に対する防御 を Management Center に追加すると、Management Center はインターフェイス設定（インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど）を検出して維持します。DNS サーバー設定の詳細については、次を参照してください。Management Center では、後で Management Center アクセスインターフェイス設定を変更できますが、脅威に対する防御 または Management Center が管理接続による再確立を妨げるような変更を加えないようにしてください。管理接続が中断された場合、脅威に対する防御 には以前の展開を復元する **configure policy rollback** コマンドが含まれます。
- DDNS サーバー更新の URL を設定すると、脅威に対する防御 は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、脅威に対する防御 は HTTPS 接続の DDNS サーバー証明書を検証できます。脅威に対する防御 は、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用するすべての DDNS サーバーをサポートします。
- このコマンドは、「データ」インターフェイス DNS サーバーを設定します。セットアップスクリプトで（または **configure network dns servers** コマンドを使用して）設定した管

理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。

Management Center では、この 脅威に対する防御 に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に 脅威に対する防御 を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む 脅威に対する防御 に後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center と 脅威に対する防御 を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。たとえば、管理インターフェイスを使用してデバイスを登録し、後で **configure network management-data-interface** コマンドを使用してデータインターフェイスを設定した場合、脅威に対する防御 設定と一致するように、DNS サーバーを含むこれらの設定のすべてを Management Center で手動で設定する必要があります。

- 管理インターフェイスは、脅威に対する防御 を Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。
- セットアップウィザードで設定した FQDN がこのインターフェイスに使用されます。
- コマンドの一部としてデバイス設定全体をクリアできます。このオプションはリカバリシナリオで使用できますが、初期セットアップや通常の操作には使用しないでください。
- データ管理を無効にするには、**configure network management-data-interface disable** コマンドを入力します。

例：

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to
change the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

例：

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
```

```
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to
change the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

ステップ 6 （任意）（6.7 以降）特定のネットワーク上の Management Center へのデータ インターフェイス アクセスを制限します。

configure network management-data-interface client *ip_address netmask*

デフォルトでは、すべてのネットワークが許可されます。

次のタスク

デバイスを Management Center に登録します。

へのログインManagement Center

Management Center を使用して、Threat Defense を設定および監視します。

始める前に

サポートされているブラウザの詳細については、使用するバージョンのリリースノート（https://www.cisco.com/go/firepower-notes）を参照してください。

手順

ステップ 1 サポートされているブラウザを使用して、次の URL を入力します。

https://*fmc_ip_address*

ステップ 2 ユーザー名とパスワードを入力します。

ステップ 3 [ログイン（Log In）] をクリックします。

Management Center のライセンスの取得

すべてのライセンスは、Management Center によって 脅威に対する防御 に提供されます。次のライセンスを購入できます。

- **脅威**：セキュリティインテリジェンスと次世代 IPS
- **マルウェア**：マルウェア防御
- **URL**：URL フィルタリング
- **RA VPN**：AnyConnect Plus、AnyConnect Apex、AnyConnect VPN のみ

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

始める前に

- 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。

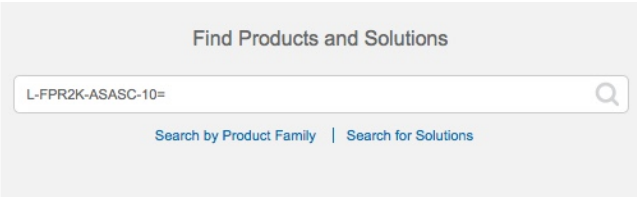
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用のスマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

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 [製品とソリューションの検索（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 *9:* 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-ISA3000T-TMC=

上記の PID のいずれかを注文に追加すると、次のいずれかの PID に対応する期間ベースのサブスクリプションを選択できます。

- L-ISA3000T-TMC-1Y
- L-ISA3000T-TMC-3Y
- L-ISA3000T-TMC-5Y

- RA VPN：『Cisco Secure Client 発注ガイド』を参照してください。

ステップ 2 まだ設定していない場合は、スマート ライセンシング サーバーに Management Center を登録します。

登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳細な手順については、Cisco Secure Firewall Management Center アドミニストレーション ガイドを参照してください。

Management Center への Threat Defense の登録

デバイスの IP アドレスかホスト名を使用して、手動で Threat Defense を Management Center に登録します。

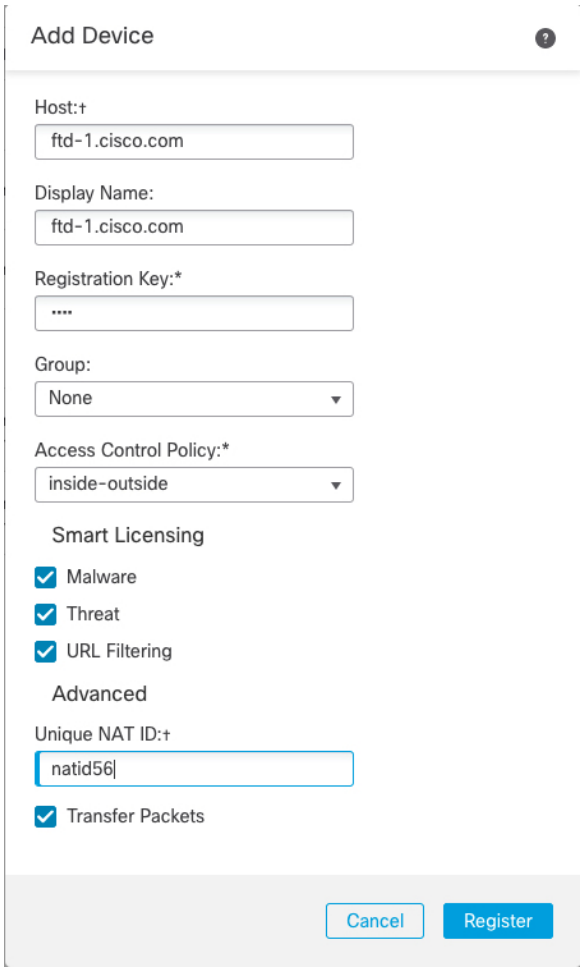
始める前に

- Threat Defense の最初の設定で設定した次の情報を収集します。
  - Threat Defense の管理 IP アドレスまたはホスト名、および NAT ID
  - Management Center の登録キー

手順

ステップ 1 Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[デバイスの追加（Add Device）] を選択します。



次のパラメータを設定します。

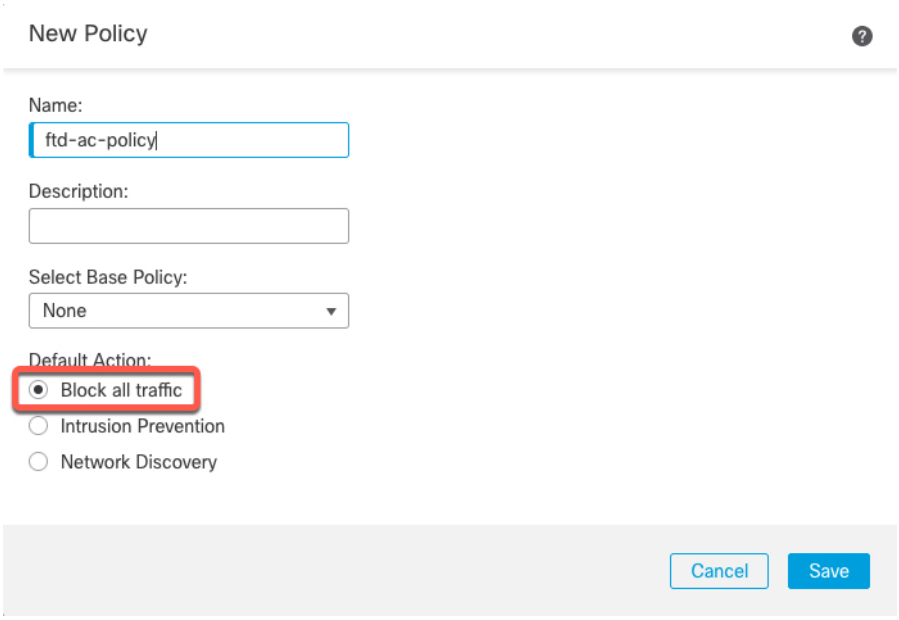
- [ホスト（Host）]：追加する Threat Defense の IP アドレスかホスト名を入力します。Threat Defense の最初の設定で Management Center の IP アドレスと NAT ID の両方を指定した場合は、このフィールドを空のままにしておくことができます。

  （注） HA 環境では、両方の Management Center が NAT の背後にある場合、プライマリ Management Center のホスト IP または名前なしで Threat Defense を登録できます。ただし、Threat Defense をセカンダリ Management Center に登録するには、Threat Defense の IP アドレスかホスト名を指定する必要があります。

- [表示名（Display Name）] フィールドに、Management Center に表示する Threat Defense の名前を入力します。
- [登録キー（Registration key）]：Threat Defense の最初の設定で指定したものと同じ登録キーを入力します。
- [ドメイン（Domain）]：マルチドメイン環境を使用している場合は、デバイスをリーフドメインに割り当てます。

- [グループ（Group）]：グループを使用している場合は、デバイスグループに割り当てます。
- [アクセスコントロールポリシー（Access Control Policy）]：初期ポリシーを選択します。使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を除いて、[新しいポリシーの作成（Create new policy）] を選択し、[すべてのトラフィックをブロック（Block all traffic）] を選択します。後でこれを変更してトラフィックを許可することができます。「内部から外部へのトラフィックの許可 （34 ページ）」を参照してください。

図 *10 : New Policy*



- [スマートライセンス（Smart Licensing）]：展開する機能に必要なスマートライセンスとして、[マルウェア（Malware）]（マルウェアインスペクションを使用する予定の場合）、[脅威（Threat）]（侵入防御を使用する予定の場合）、および [URL]（カテゴリベースの URL フィルタリングを実行する予定の場合）を割り当てます。**注**：デバイスを追加した後、**[システム（System）] > [ライセンス（Licenses）] > [スマートライセンス（Smart Licenses）]** ページから AnyConnect クライアント リモートアクセス VPN のライセンスを適用できます。
- [一意のNAT ID（Unique NAT ID）]：Threat Defense の最初の設定で指定した NAT ID を指定します。
- [パケットの転送（Transfer Packets）]：デバイスから Management Center へのパケット転送を許可します。このオプションを有効にして IPS や Snort などのイベントがトリガーされた場合は、デバイスが検査用としてイベントメタデータ情報とパケットデータを Management Center に送信します。このオプションを無効にした場合は、イベント情報だけが Management Center に送信され、パケットデータは送信されません。

ステップ 3 [登録（Register）]（別のデバイスを追加する場合は [別のデバイスを登録して追加（Register and Add Another）]）をクリックし、登録が成功したことを確認します。

登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが表示されます。Threat Defense が登録に失敗した場合は、次の項目を確認してください。

- ping：Threat Defense CLIにアクセスし、次のコマンドを使用して Management Center IP アドレスへの ping を実行します。

  ping system *ip_address*

  ping が成功しない場合は、**show network** コマンドを使用してネットワーク設定を確認します。Threat Defense 管理 IP アドレスを変更するには、**configure network {ipv4 | ipv6} manual** コマンドを使用します。 Management Center アクセス用にデータインターフェイスを設定した場合は、**configure network management-data-interface** コマンドを使用します。

- 登録キー、NAT ID、および Management Center IP アドレス：両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合は NAT ID を使用していることを確認します。**configure manager add** コマンドを使用して、Management Center で登録キーと NAT ID を設定することができます。

トラブルシューティングの詳細については、https://cisco.com/go/fmc-reg-error を参照してください。

基本的なセキュリティポリシーの設定

ここでは、次の設定を使用して基本的なセキュリティポリシーを設定する方法について説明します。

- 内部インターフェイスと外部インターフェイス：内部インターフェイスにスタティック IP アドレスを割り当て、外部インターフェイスに DHCP を使用します。
- DHCP サーバー：クライアントの内部インターフェイスで DHCP サーバーを使用します。
- デフォルトルート：外部インターフェイスを介してデフォルトルートを追加します。
- NAT：外部インターフェイスでインターフェイス PAT を使用します。
- アクセスコントロール：内部から外部へのトラフィックを許可します。

基本的なセキュリティ ポリシーを設定するには、次のタスクを実行します。

1	インターフェイスの設定 （25 ページ）。
2	DHCP サーバーの設定 （28 ページ）。

3	デフォルトルートの追加 （29 ページ）。
4	NAT の設定 （31 ページ）。
5	内部から外部へのトラフィックの許可 （34 ページ）。
6	設定の展開 （35 ページ）。

インターフェイスの設定

脅威に対する防御 インターフェイスを有効にし、それらをセキュリティゾーンに割り当てて IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。これらのインターフェイスの一部は、Web サーバーなどのパブリックアクセスが可能なアセットを配置する「緩衝地帯」（DMZ）となる場合があります。

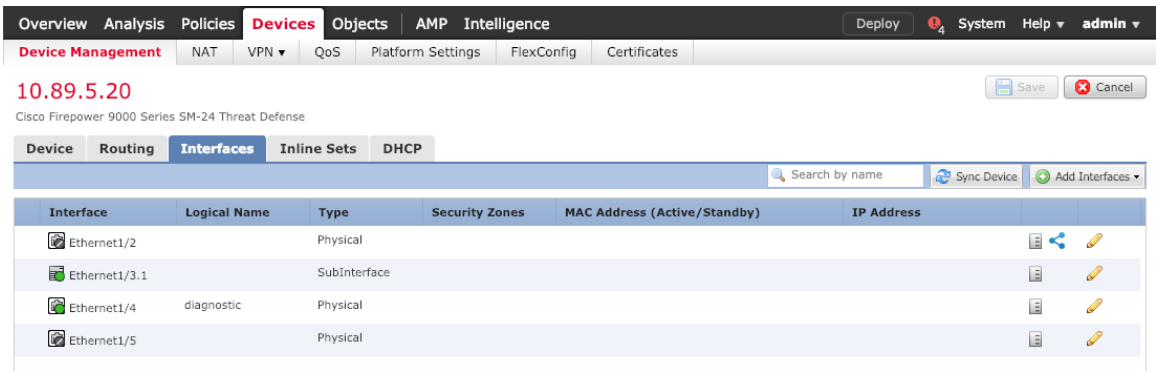
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCP によるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して、ルーテッドモードの内部インターフェイスを設定します。

手順

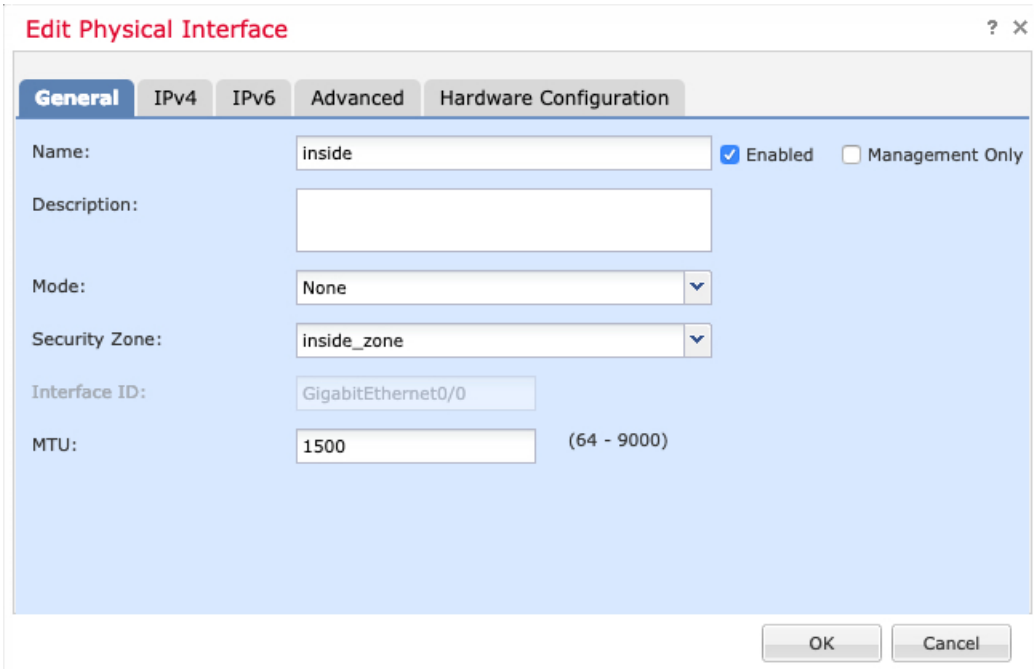
ステップ 1 [デバイス（Devices）]>[デバイス管理（Device Management）] の順に選択し、ファイアウォールの をクリックします。

ステップ 2 [インターフェイス（Interfaces）] をクリックします。



ステップ 3 内部に使用するインターフェイスの をクリックします。

[全般（General）] タブが表示されます。



a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに **inside** という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

c) [モード（Mode）] は [なし（None）] に設定したままにします。

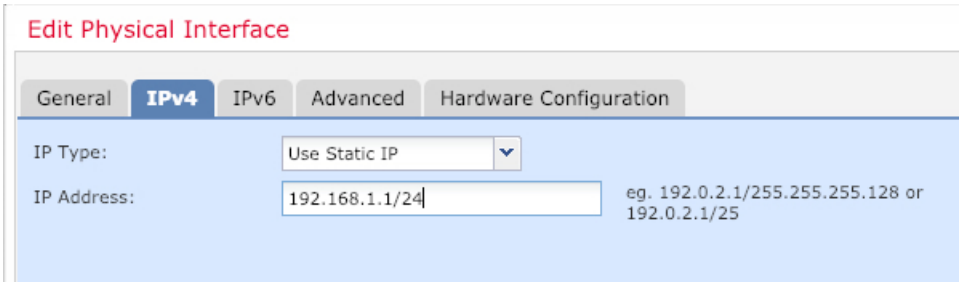
d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てる必要があります。インターフェイスは、1 つのセキュリティゾーンにのみ属することも、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみサポートしています。NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーで、ゾーンまたはインターフェイスグループを使用できます。

e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：ドロップダウンリストから [スタティックIPを使用する（Use Static IP）] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

  たとえば、**192.168.1.1/24** などと入力します。

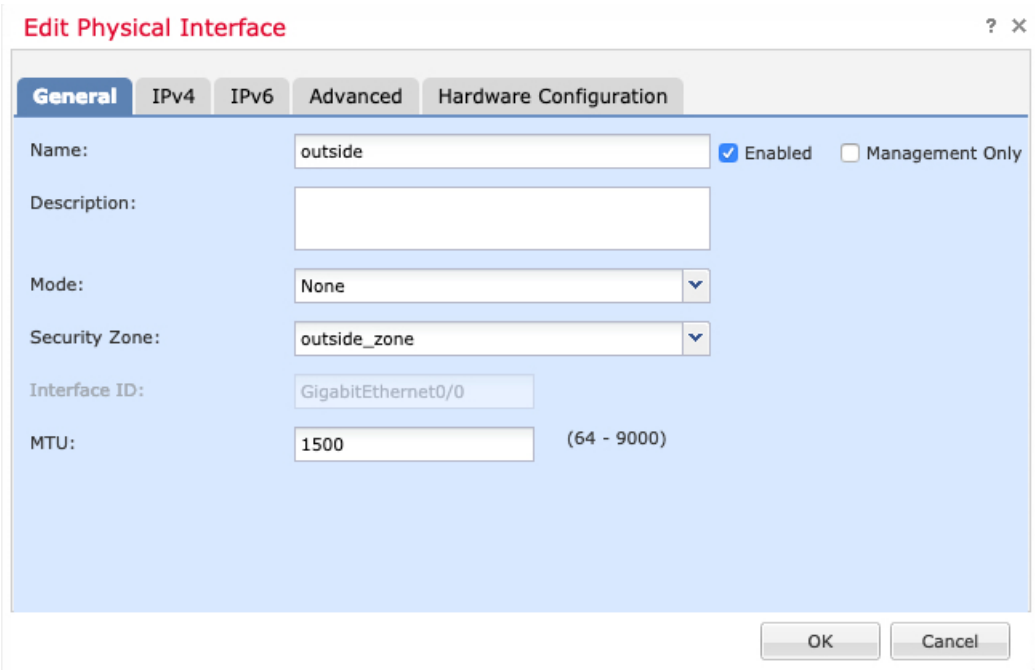


- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 4 「外部」に使用するインターフェイスをクリックします。

[全般（General）] タブが表示されます。



（注） 管理アクセス用にこのインターフェイスを事前に設定している場合、インターフェイスにはすでに名前が付けられており、有効化とアドレス指定が完了しています。これらの基本設定は変更しないでください。変更すると、Management Center の管理接続が中断されます。この画面でも、通過トラフィックポリシーのセキュリティゾーンを設定できます。

a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに「outside」という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

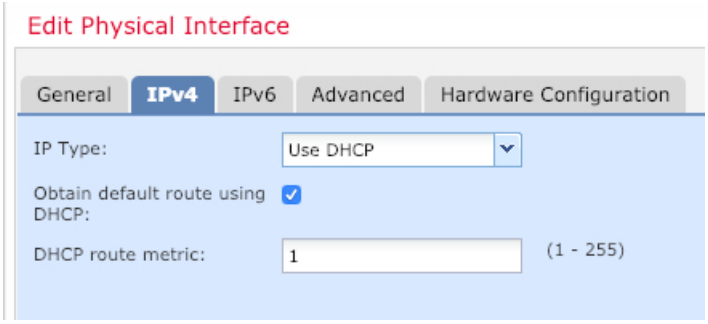
c) [モード（Mode）] は [なし（None）] に設定したままにします。

d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の外部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

たとえば、「outside_zone」という名前のゾーンを追加します。

e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：[DHCPの使用（Use DHCP）] を選択し、次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバーからデフォルト ルートを取得します。
  - [DHCPルートメトリック（DHCP route metric）]：アドミニストレーティブディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。



- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

DHCP サーバーの設定

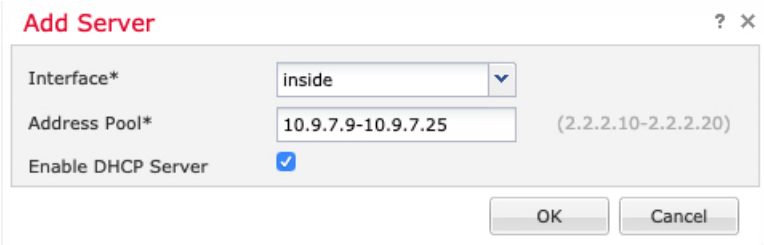
クライアントで DHCP を使用して 脅威に対する防御 から IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

ステップ 2 **[DHCP]** > **[DHCPサーバー（DHCP Server）]** を選択します。

ステップ 3 **[サーバー（Server）]** ページで、**[追加（Add）]** をクリックして、次のオプションを設定します。



- [インターフェイス（Interface）]：ドロップダウンリストからインターフェイスを選択します。
- [アドレスプール（Address Pool）]：DHCP サーバーが使用する IP アドレスの最下位から最上位の間の範囲を設定します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
- [DHCPサーバーを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバーを有効にします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

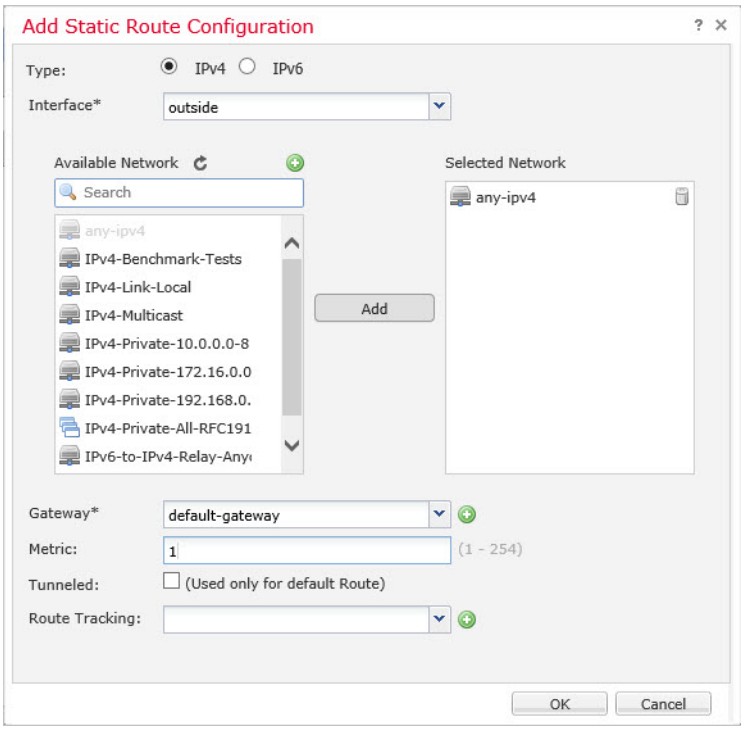
デフォルトルートの追加

デフォルトルートは通常、外部インターフェイスから到達可能なアップストリームルータを指し示します。外部インターフェイスに DHCP を使用する場合は、デバイスがすでにデフォルトルートを受信している可能性があります。手動でルートを追加する必要がある場合は、次の手順を実行します。DHCP サーバーからデフォルトルートを受信した場合は、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[スタティックルート（Static Route）]** ページの [IPv4ルート（IPv4 Routes）] または [IPv6ルート（IPv6 Routes）] テーブルに表示されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

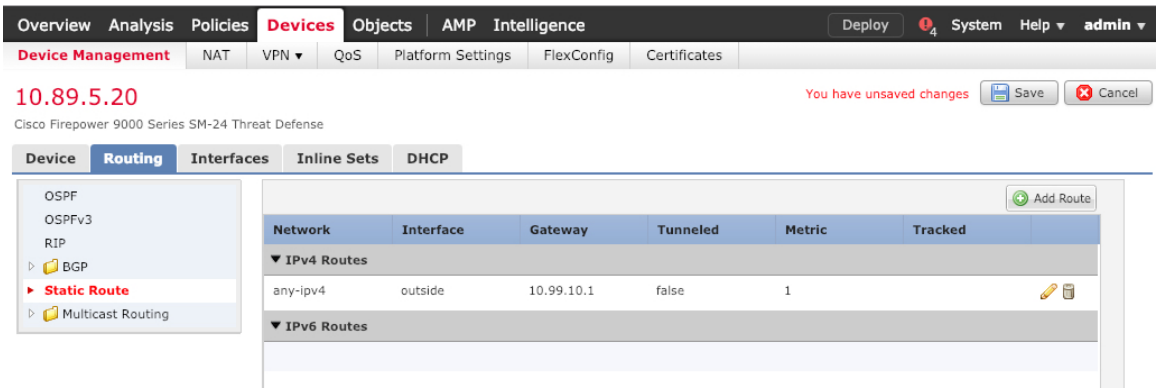
ステップ 2 **[ルーティング（Routing）]** > **[スタティックルート（Static route）]** を選択し、[ルートを追加（Add route）] をクリックして、次のように設定します。



- [タイプ（Type）]：追加するスタティックルートのタイプに応じて、[IPv4] または [IPv6] オプションボタンをクリックします。
- [インターフェイス（Interface）]：出力インターフェイスを選択します。通常は外部インターフェイスです。
- [使用可能なネットワーク（Available Network）]：IPv4 デフォルト ルートの場合は [ipv4] を選択し、IPv6 デフォルト ルートの場合は [any] を選択し、[追加（Add）] をクリックして [選択したネットワーク（Selected Network）] リストに移動させます。
- [ゲートウェイ（Gateway）] または [IPv6ゲートウェイ（IPv6 Gateway）]：このルートのネクストホップであるゲートウェイルータを入力または選択します。IP アドレスまたはネットワーク/ホストオブジェクトを指定できます。
- [メトリック（Metric）]：宛先ネットワークへのホップの数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。

ステップ 3 [OK] をクリックします。

ルートがスタティックルートテーブルに追加されます。



ステップ 4 [保存（Save）] をクリックします。

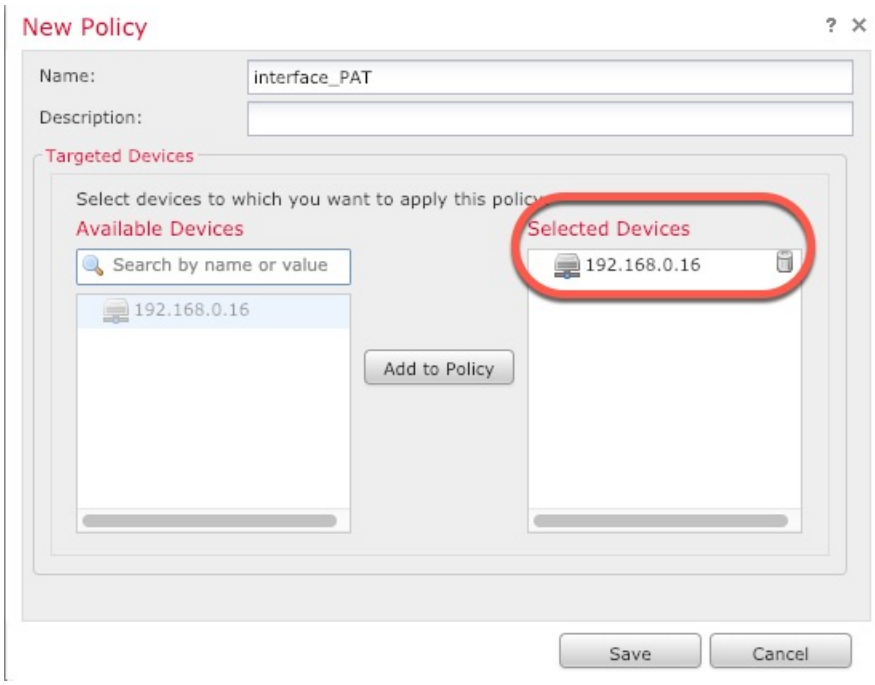
NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。

手順

ステップ 1 **[デバイス（Devices）] > [NAT]** をクリックし、**[新しいポリシー（New Policy）] > [Threat Defense NAT]** をクリックします。

ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。



ポリシーが Management Center に追加されます。引き続き、ポリシーにルールを追加する必要があります。

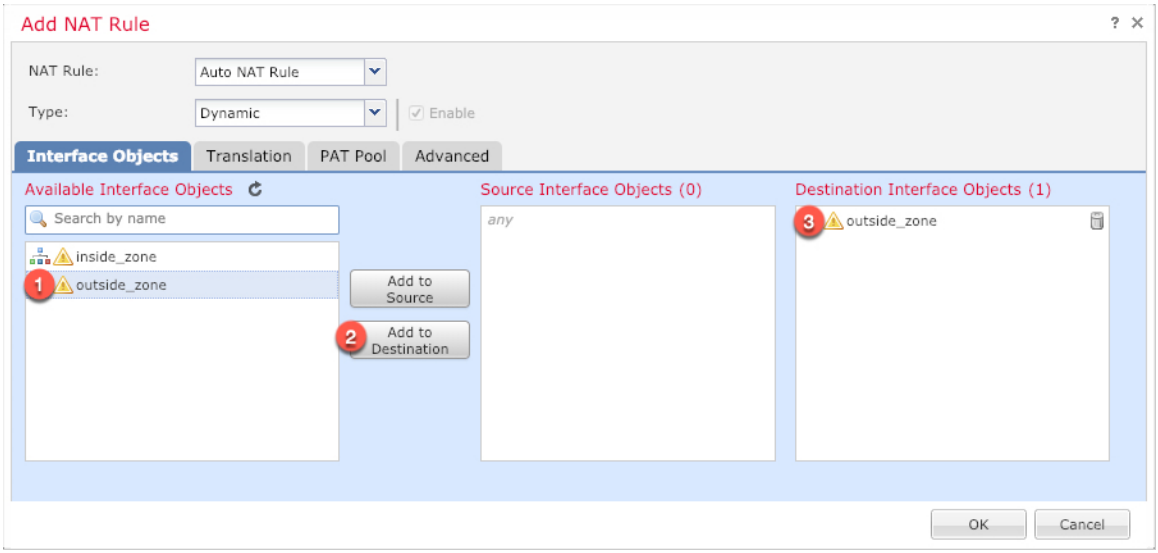
ステップ 3 [ルールの追加（Add Rule）] をクリックします。

[NATルールの追加（Add NAT Rule）] ダイアログボックスが表示されます。

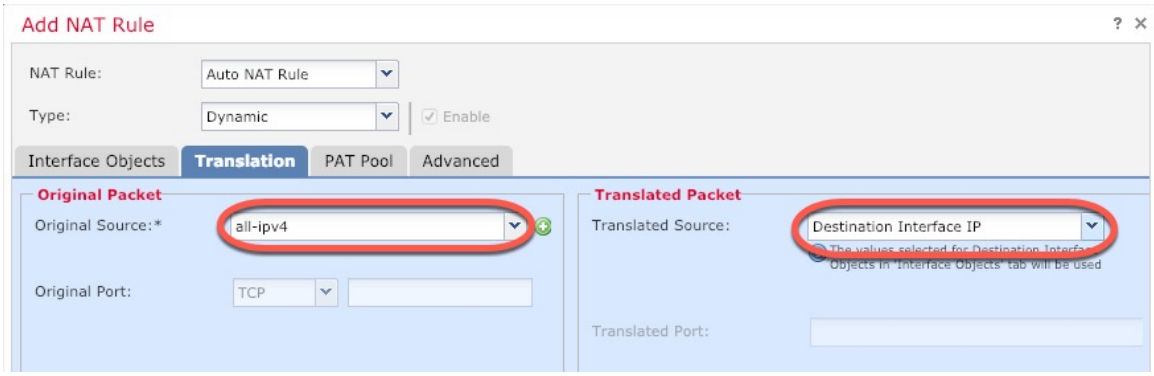
ステップ 4 基本ルールのオプションを設定します。

- [NATルール（NAT Rule）]：[自動NATルール（Auto NAT Rule）] を選択します。
- [タイプ（Type）]：[ダイナミック（Dynamic）] を選択します。

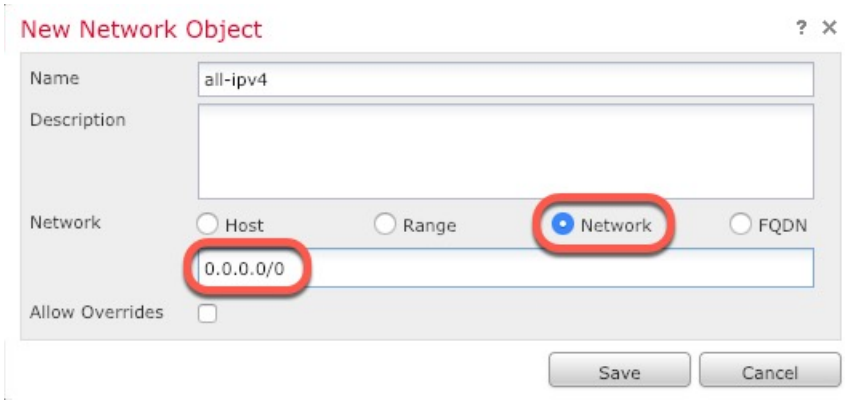
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。



ステップ 6 [変換（Translation）] ページで、次のオプションを設定します。



- [元の送信元（Original Source）]：をクリックして、すべての IPv4 トラフィック（0.0.0.0/0）のネットワークオブジェクトを追加します。

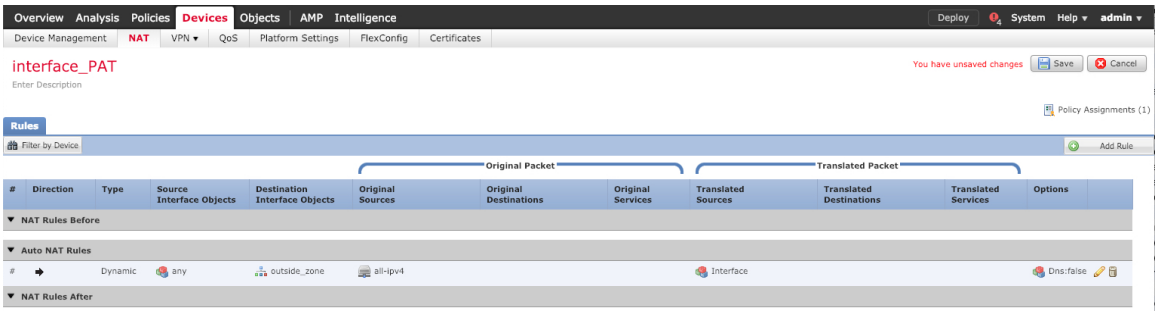


（注） 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元（Translated Source）]：[宛先インターフェイスIP（Destination Interface IP）] を選択します。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ルールが [ルール（Rules）] テーブルに保存されます。



ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

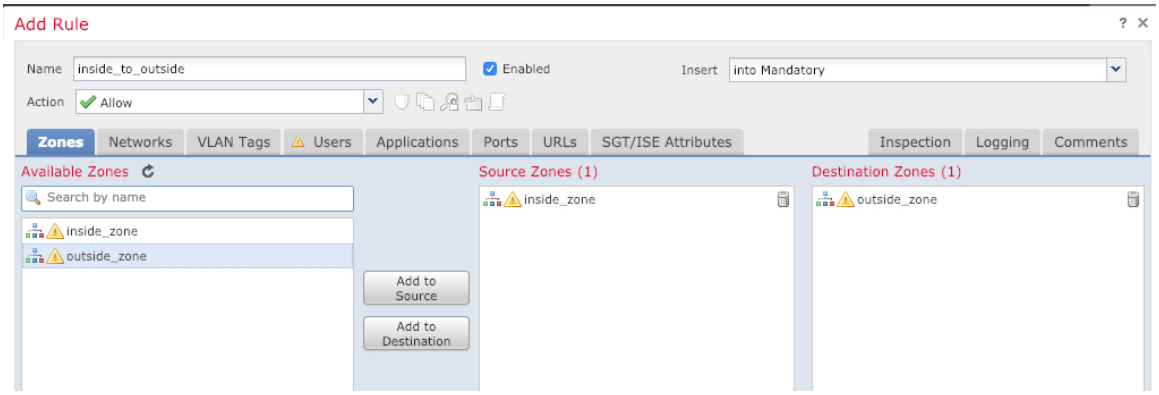
内部から外部へのトラフィックの許可

脅威に対する防御 を登録したときに、基本の [すべてのトラフィックをブロック（Block all traffic）] アクセス コントロール ポリシーを作成した場合は、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

手順

ステップ 1 **[ポリシー（Policy）] > [アクセスポリシー（Access Policy）] > [アクセスポリシー（Access Policy）]**を選択し、脅威に対する防御 に割り当てられているアクセス コントロール ポリシーの をクリックします。

ステップ 2 **[ルールを追加（Add Rule）]** をクリックし、次のパラメータを設定します。

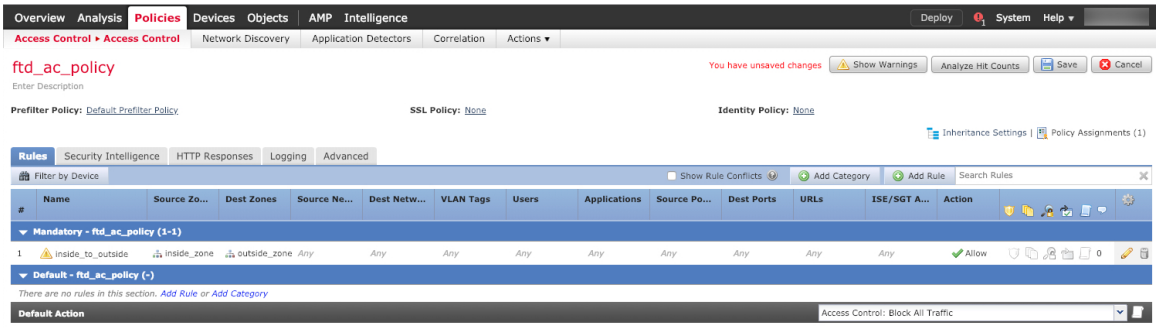


- [名前（Name）]：このルールに名前を付けます（たとえば、**inside_to_outside**）。
- [送信元ゾーン（Source Zones）]：[使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。
- [宛先ゾーン（Destination Zones）]：[使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

他の設定はそのままにしておきます。

ステップ 3 [追加（Add）] をクリックします。

ルールが [ルール（Rules）] テーブルに追加されます。



ステップ 4 [保存（Save）] をクリックします。

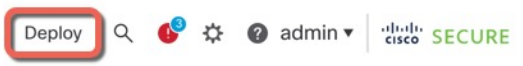
設定の展開

設定の変更を 脅威に対する防御 に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

手順

ステップ 1 右上の [展開（Deploy）] をクリックします。

図 *11 : [*展開（*Deploy***）*]***



ステップ 2 [すべて展開（Deploy All）] をクリックしてすべてのデバイスに展開するか、[高度な展開（Advanced Deploy）] をクリックして選択したデバイスに展開します。

図 *12* : すべて展開

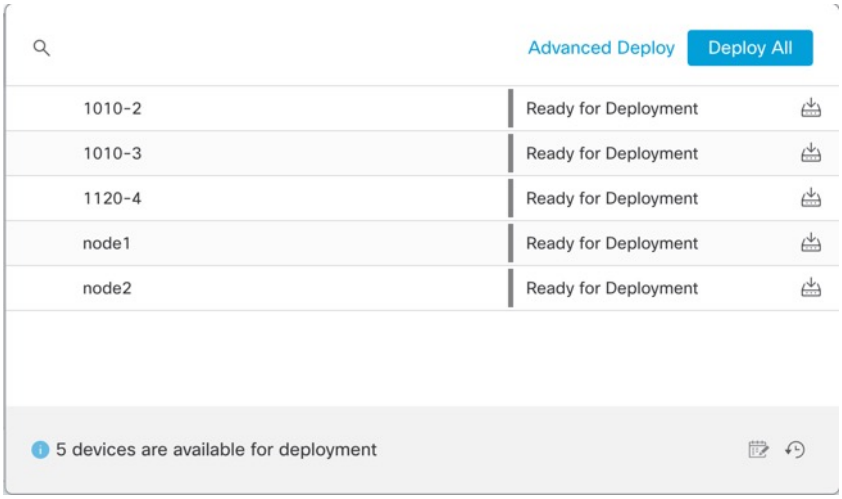
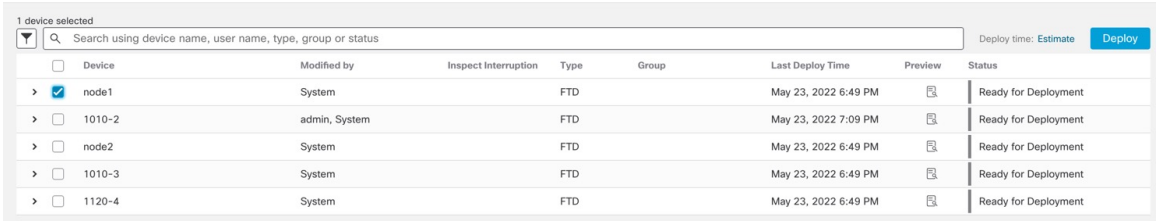
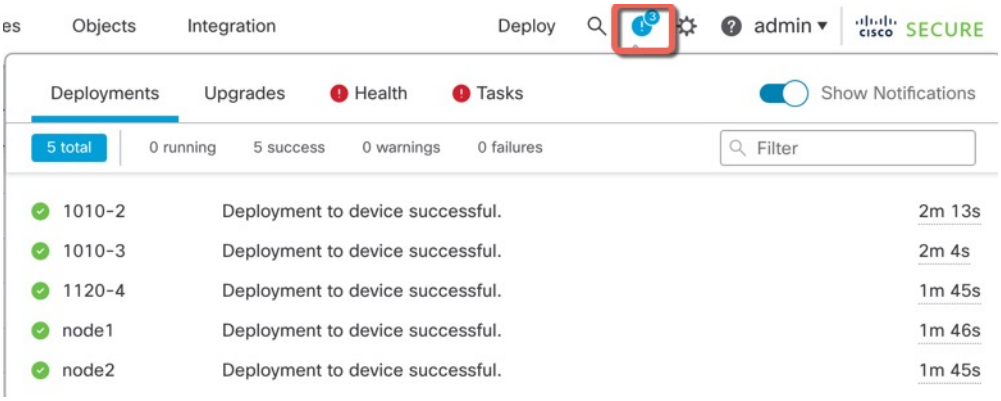


図 *13* : 高度な展開



ステップ 3 展開が成功したことを確認します。展開のステータスを表示するには、メニューバーの [展開（Deploy）] ボタンの右側にあるアイコンをクリックします。

図 *14* : 展開ステータス



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。

脅威に対する防御 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 にログインして、管理コンピュータをコンソールポート、RJ-45 ポート、ミニ USB ポートのいずれかに接続します。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください。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 ユーザー名 **admin**、および初期セットアップ時に設定したパスワードを使用して 脅威に対する防御 CLI にログインします（デフォルトは **Admin123**）。

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。

ファイアウォールの電源の切断

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おり、電源プラグを抜いたり、電源を切断したりすると、ファイアウォール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。

ISA 3000 シャーシには、外部電源スイッチはありません。Management Center のデバイス管理ページを使用してデバイスの電源を切断するか、 CLI を使用できます。

Management Center を使用したファイアウォールの電源の切断

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、ファイアウォール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。

（注） シャットダウンは 7.0.2+/7.2+ でサポートされています。

Management Center を使用してシステムを適切にシャットダウンできます。

手順

ステップ 1 **[Devices]** > **[Device Management]**を選択します。

ステップ 2 再起動するデバイスの横にある編集アイコン（）をクリックします。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [システム（System）]セクションでデバイスのシャットダウンアイコン（）をクリックします。

ステップ 5 プロンプトが表示されたら、デバイスのシャットダウンを確認します。

ステップ 6 シャットダウンプロセスをモニターします。デバイスを監視できない場合は、約3分間待ってシステムがシャットダウンしたことを確認します。

- コンソール：コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。次のプロンプトが表示されます。

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

To restart the device, you must Power cycle to the device.
```

ステップ 7 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

CLI におけるファイアウォールの電源の切断

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おり、電源プラグを抜いたり、電源を切断したりすると、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。ISA 3000 シャーシには、外部電源スイッチはありません。

（注） シャットダウンは 7.0.2+/7.2+ でサポートされています。

手順

ステップ 1 コンソールポートに接続して 脅威に対する防御 CLI にアクセスし、脅威に対する防御 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.

To restart the device, you must Power cycle to the device.
```

ステップ 2 脅威に対する防御 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、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。

次のステップ

Threat Defense の設定を続行するには、「Cisco Firepower ドキュメント一覧」にある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。

Management Center の使用に関する情報については、「Firepower Management Center Configuration Guide」を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。