リモート Threat Defense による Management Center の展開

この章の対象読者

使用可能なすべてのアプリケーションとマネージャを表示するには、最適なアプリケーションとマネージャを見つける方法 を参照してください。この章の内容は、 Management Center での脅威に対する防御 の展開に適用されます。

この章では、中央本社にある Management Center を使用して 脅威に対する防御 を管理する方法について説明します。Management Center がローカル管理ネットワークに存在するローカル展開については、Management Center での Threat Defense の展開を参照してください。

ファイアウォールについて

ハードウェアでは、Threat Defense ソフトウェアまたは ASA ソフトウェアを実行できます。Threat Defense 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。現在インストールされているものとは異なるソフトウェアバージョンが必要な場合も再イメージ化が必要です。Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド を参照してください。

ファイアウォールは、Secure Firewall eXtensible オペレーティングシステム（FXOS）と呼ばれる基盤となるオペレーティングシステムを実行します。ファイアウォールは FXOS Secure Firewall Chassis Manager をサポートしていません。トラブルシューティング用として限られた CLI のみがサポートされています。詳細については、Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）を参照してください。

プライバシー収集ステートメント：ファイアウォール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。

リモート管理の仕組み

Management Center でインターネットを介して Threat Defense を管理できるようにするには、Management Center マネージャアクセスについて管理インターフェイスの代わりに外部インターフェイスを使用します。ほとんどのリモート支社には 1 つのインターネット接続しかないため、外部からマネージャにアクセスして中央管理を行えるようにします。

（注） 管理接続は、それ自身とデバイスの間の安全な TLS-1.3 暗号化通信チャネルです。セキュリティ上の理由から、サイト間 VPN などの追加の暗号化トンネル経由でこのトラフィックを実行する必要はありません。たとえば、VPN がダウンすると、管理接続が失われるため、シンプルな管理パスをお勧めします。

1. CLI を使用して Threat Defense を事前設定してから、リモート分散拠点に Threat Defense を送信します。
2. 分散拠点で、脅威に対する防御 をケーブル接続し、電源をオンにします。
3. Management Center を使用して 脅威に対する防御 の登録を完了します。

Threat Defense マネージャ アクセス インターフェイス

このガイドでは**外部**インターフェイスアクセスについて説明します。これは、リモート分散拠点で発生する可能性が最も高いシナリオであるためです。マネージャアクセスは外部インターフェイスで発生しますが、専用の管理インターフェイスも引き続き関連します。管理インターフェイスは、Threat Defense データインターフェイスとは別に設定される特別なインターフェイスであり、独自のネットワーク設定があります。

- データインターフェイスでマネージャ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ネットワーク設定が使用されます。
- すべての管理トラフィックは、引き続き管理インターフェイスを発信元または宛先とします。
- データインターフェイスでマネージャアクセスを有効にすると、Threat Defense はバックプレーンを介して管理インターフェイスに着信管理トラフィックを転送します。
- 発信管理トラフィックの場合、管理インターフェイスはバックプレーンを介してデータインターフェイスにトラフィックを転送します。

マネージャのアクセス要件

データインターフェイスからのマネージャアクセスには、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。冗長性を目的として、Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
- 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 Threat Defense 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。
- 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。
- 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。
- クラスタリングはサポートされません。この場合、管理インターフェイスを使用する必要があります。

ハイ アベイラビリティ要件

デバイスのハイアベイラビリティを備えたデータインターフェイスを使用する場合は、次の要件を参照してください。

- マネージャアクセスには、両方のデバイスで同じデータインターフェイスを使用します。
- 冗長マネージャ アクセス データ インターフェイスはサポートされていません。
- DHCP は使用できません。静的 IP アドレスのみがサポートされています。DDNS や ゼロタッチプロビジョニング など、DHCP に依存する機能は使用できません。
- 同じサブネット内に異なる静的 IP アドレスがあります。
- IPv4 または IPv6 のいずれかを使用します。両方を設定することはできません。
- 同じマネージャ設定（**configure manager add** コマンド）を使用して、接続が同じであることを確認します。
- データインターフェイスをフェールオーバーリンクまたはステートリンクとして使用することはできません。

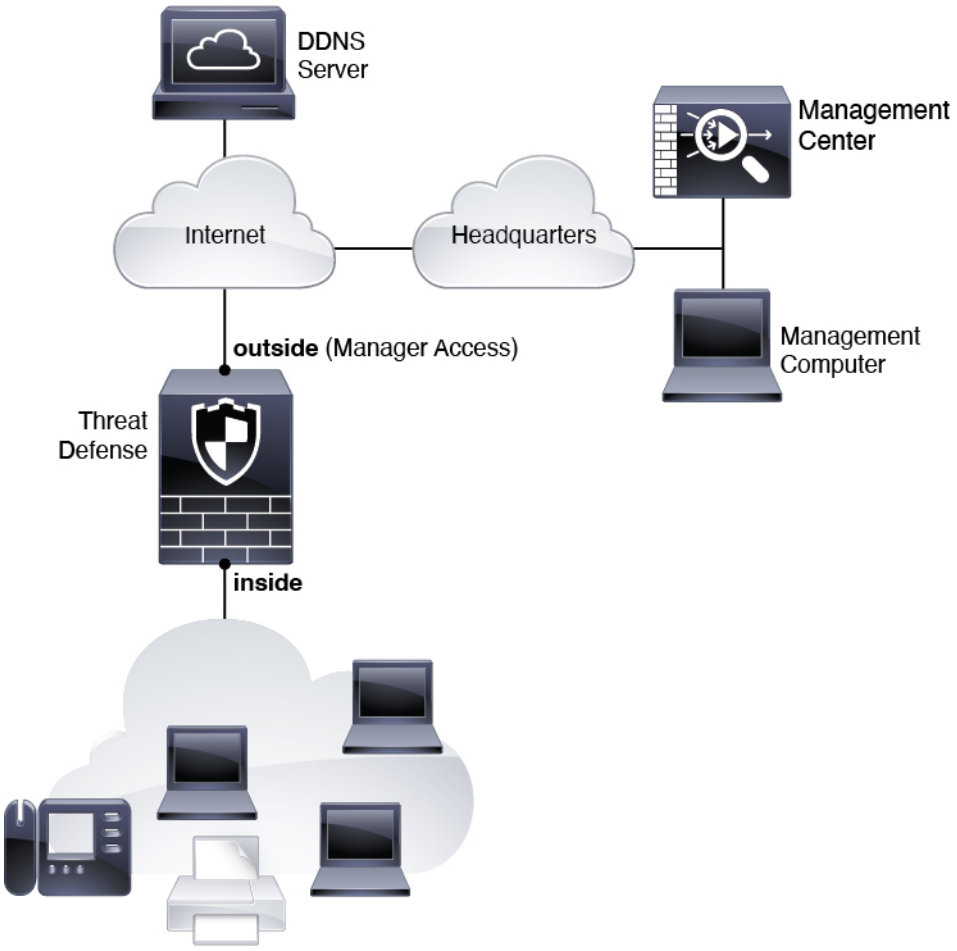
リモート ブランチ ネットワーク

次の図に、ファイアウォールの一般的なネットワーク展開を示します。

- Management Center は中央本社にあります。

- Threat Defense はマネージャアクセスに外部インターフェイスを使用します。
- Threat Defense と Management Center ではどちらも、インバウンド管理接続を許可するためのパブリック IP アドレスまたはホスト名が必要であり、初期設定のためにこのような IP アドレスを把握しておかなければなりません。DHCP IP の割り当ての変更に対応するために、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）を設定することもできます。

図 *1*:



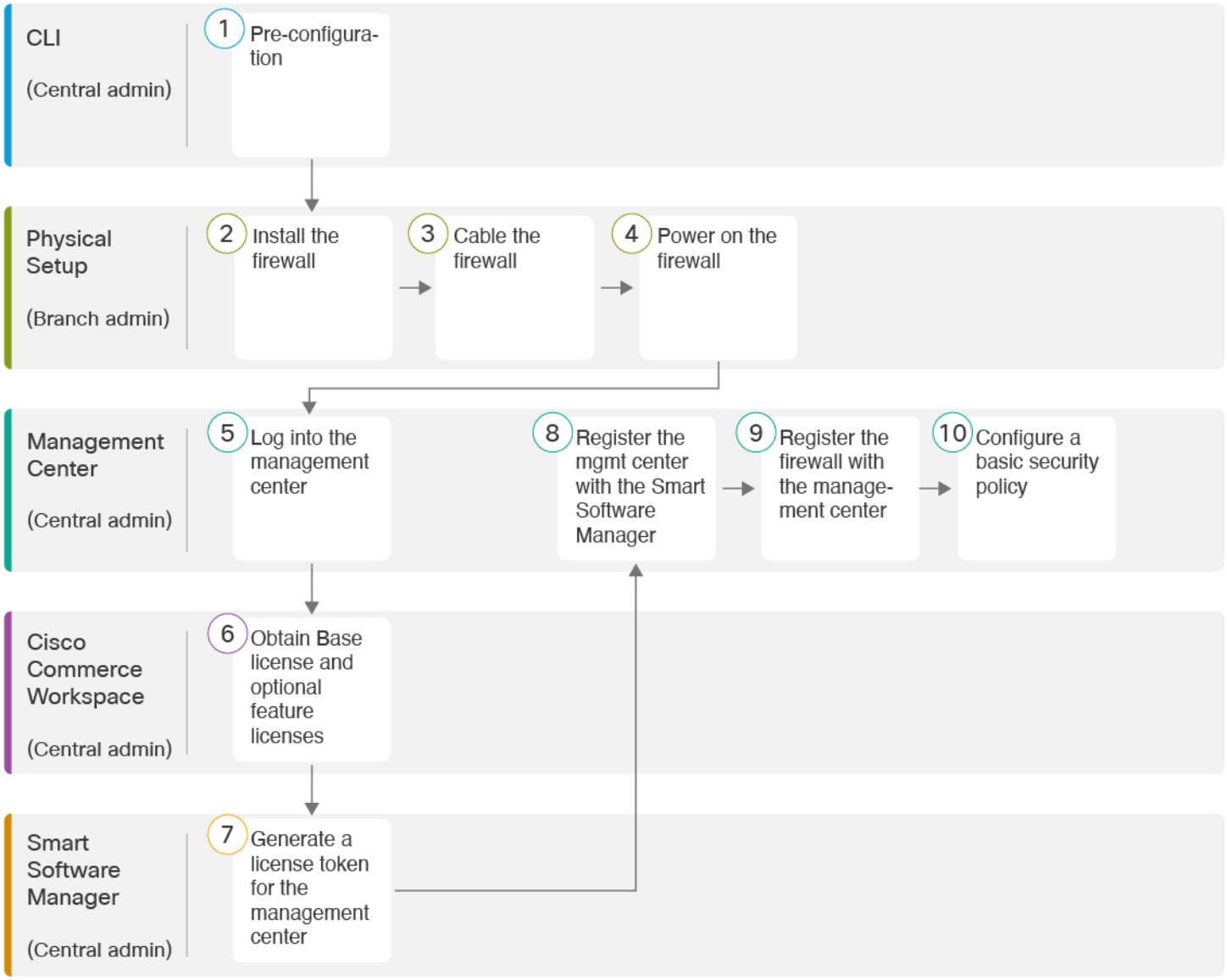
はじめる前に

Management Center の初期設定を展開して実行します。使用モデルのスタートアップガイドを参照してください。

エンドツーエンドのタスク

Management Center を使用して Threat Defense を展開するには、次のタスクを参照してください。

図 2: エンドツーエンドのタスク



1	CLI （中央の管理者）	• （任意）ソフトウェアの確認と新しいバージョンのインストール （6 ページ） • CLI を使用した事前設定 （8 ページ）。

2	物理的なセットアップ （支社の管理者）	ファイアウォールをインストールします。ハードウェア設置ガイドを参照してください。
3	物理的なセットアップ （支社の管理者）	ファイアウォールのケーブル接続 （14 ページ）。
4	物理的なセットアップ （支社の管理者）	ファイアウォールの電源投入 （15 ページ）
5	Management Center （中央の管理者）	Management Centerへのログイン。
6	Cisco Commerce Workspace （中央の管理者）	基本ライセンスとオプションの機能ライセンスを購入します（「Management Centerのライセンスの取得 （16 ページ）」）。
7	Smart Software Manager （中央の管理者）	Management Center のライセンストークンを生成します（「Management Center のライセンスの取得 （16 ページ）」）。
8	Management Center （中央の管理者）	スマート ライセンシング サーバーに Management Center を登録します（「Management Center のライセンスの取得 （16 ページ）」）。
9	Management Center （中央の管理者）	Management Center へのデバイスの追加 （18 ページ）。
10	Management Center （中央の管理者）	基本的なセキュリティポリシーの設定 （21 ページ）。

中央の管理者による事前設定

Threat Defense は、分散拠点に送信する前に手動で事前に設定する必要があります。

（任意）ソフトウェアの確認と新しいバージョンのインストール

ソフトウェアのバージョンを確認し、必要に応じて別のバージョンをインストールするには、次の手順を実行します。ファイアウォールを設定する前に対象バージョンをインストールすることをお勧めします。別の方法として、稼働後にアップグレードを実行することもできますが、設定を保持するアップグレードでは、この手順を使用するよりも時間がかかる場合があります。

実行するバージョン

ソフトウェア ダウンロード ページのリリース番号の横にある、金色の星が付いている Gold Star リリースを実行することをお勧めします。https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html に記載されているリリース戦略も参照してください。たとえば、この速報では、（最新機能を含む）短期的なリリース番号、長期的なリリース番号（より長期間のメンテナンスリリースとパッチ）、または非常に長期的なリリース番号（政府認定を受けるための最長期間のメンテナンスリリースとパッチ）について説明しています。

手順

ステップ 1 コンソール ポートに接続します。詳細については、Threat Defense および FXOS CLI へのアクセス （35 ページ）を参照してください。

admin ユーザとデフォルトパスワードの **Admin123** を使用してログインします。

FXOS CLI に接続します。初めてログインしたとき、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

（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、初期設定へのリセットを実行して、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。初期設定へのリセット手順については、『FXOS troubleshooting guide 』を参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 2 FXOS CLI で、実行中のバージョンを表示します。

scope ssa

show app-instance

例：

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name      Slot ID     Admin State      Operational State     Running Version
Startup Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                   1           Enabled          Online                7.6.0.65
```

```
7.6.0.65          Not Applicable
```

ステップ 3 新しいバージョンをインストールする場合は、次の手順を実行します。

a) 管理インターフェイスに静的 IP アドレスを設定する必要がある場合は、「CLI を使用した事前設定 （8 ページ）」を参照してください。デフォルトでは、管理インターフェイスは DHCP を使用します。

管理インターフェイスからアクセスできるサーバーから新しいイメージをダウンロードする必要があります。

b) FXOS のトラブルシューティング ガイドに記載されている再イメージ化の手順を実行します。

ファイアウォールが再起動したら、FXOS CLI に再度接続します。

c) FXOS CLI で、管理者パスワードを再度設定するように求められます。

ゼロタッチプロビジョニングの場合は、デバイスをオンボーディングする際、すでにパスワードが設定されているため、[パスワードのリセット（Password Reset）] エリアで必ず [いいえ（No...）] を選択してください。

d) デバイスをシャットダウンします。CLI におけるファイアウォールの電源の切断 （38 ページ） を参照してください。

CLI を使用した事前設定

セットアップウィザードを使用して、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を行います。

手順

ステップ 1 ファイアウォールの電源を入れます。

（注） Threat Defense を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

ステップ 2 コンソールポートで Threat Defense CLI に接続します。

コンソールポートは FXOS CLI に接続します。

ステップ 3 ユーザー名 **admin** およびパスワード **Admin123** でログインします。

初めて FXOS にログインしたときは、パスワードを変更するよう求められます。このパスワードは、SSH の Threat Defense ログインにも使用されます。

（注） パスワードがすでに変更されていてわからない場合は、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。再イメージ化の手順については、FXOS のトラブルシューティング ガイドを参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

ステップ 4 Threat Defense CLI に接続します。

connect ftd

例：

```
firepower# connect ftd
>
```

ステップ 5 Threat Defense 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、SSH接続を使用している場合は、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、管理インターフェイスの設定用の CLI セットアップスクリプトが表示されます。

データインターフェイスでマネージャ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。

（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。Cisco Secure Firewall Threat Defense 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。

次のガイドラインを参照してください。

- [IPv4を設定しますか?（Do you want to configure IPv4?）]、[IPv6を設定しますか?（Do you want to configure IPv6?）]：これらのタイプのアドレスの少なくとも 1 つに **y** を入力します。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。
- **IPv4 は DHCP 経由または手動のどちらで設定しますか？IPv6 は DHCP、ルータ、または手動のどれで設定しますか？**：**[手動（manual）]** を選択します。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**または**管理インターフェイスの IPv6 ゲートウェイを入力**：ゲートウェイが **data-interfaces** になるように設定します。この設定は、マネージャ アクセス データ インターフェイスを通じて回送できるように、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。
- [ファイアウォールモードを設定しますか？（Configure firewall mode?）]：**routed** と入力します。外部マネージャアクセスは、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ています。

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 configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
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]:
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'


DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
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 6 マネージャアクセス用の外部インターフェイスを設定します。

configure network management-data-interface

その後、外部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。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、管理インターフェイスでは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事前に設定できます。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。

- Threat Defense 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、後でマネージャ アクセス インターフェイス構成を変更できますが、Threat Defense または Management Center が管理接続の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、Threat Defense 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、Threat Defense 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、Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Threat Defense 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 Threat Defense 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 Threat Defense 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Threat Defense 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 Threat Defense 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、Threat Defense 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、Threat Defense 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://dwinchester: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 manager access from any network, if you wish to
 change the manager 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 manager access from any network, if you wish to
 change the manager 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 7 （任意） 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。

ステップ 8 この Threat Defense 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。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 Threat Defense ）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 Threat Defense に必要です。
- reg_key：Threat Defense 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：Management Center でも指定する、任意で一意の 1 回限りの文字列を指定します。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 Threat Defense と Management Center の両方で NAT ID を指定する必要があります。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。

例：

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

ステップ 9 デバイスをリモート支社に送信できるように Threat Defense をシャットダウンします。

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。

a) **shutdown** コマンドを入力します。
b) 電源 LED とステータス LED を観察して、シャーシの電源が切断されていることを確認します（LED が消灯）。
c) シャーシの電源が正常に切断されたら、必要に応じて電源プラグを抜き、シャーシから物理的に電源を取り外すことができます。

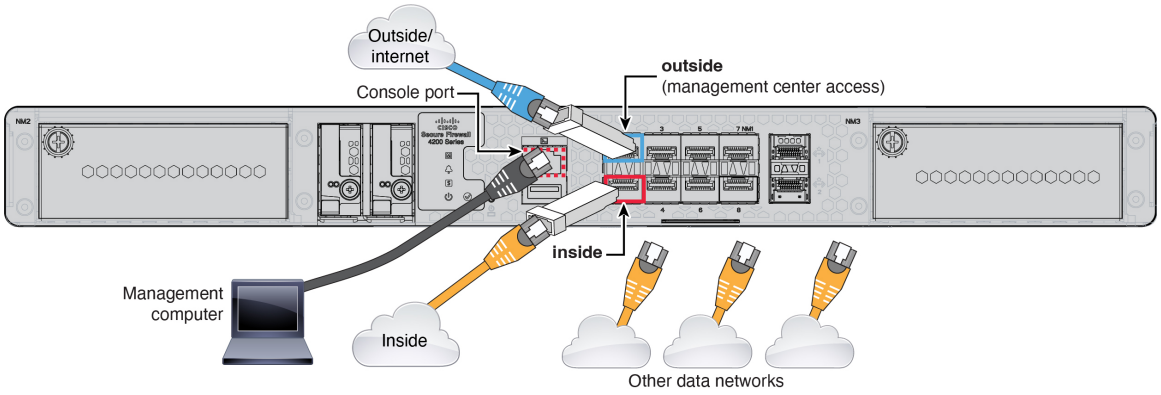
支社へのインストール

中央の本社から Threat Defense を受け取ったら、外部インターフェイスからインターネットにアクセスできるように、ファイアウォールにケーブルを接続して電源をオンにするだけです。そうすると、中央の管理者は設定を完了できます。

ファイアウォールのケーブル接続

Management Center と管理コンピュータはリモートの本社にあり、Threat Defense にはインターネット経由で到達できます。Cisco Secure Firewall 4200 をケーブル接続するには、次の手順を参照してください。

図 *3*: リモート管理展開のケーブル接続



始める前に

- データインターフェイスポートに SFP を取り付けます。組み込みポートは、SFP モジュールを必要とする 1/10/25 Gb SFP ポートです。
- （オプション）コンソールケーブルを入手します。デフォルトではファイアウォールにコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。

手順

ステップ 1 シャーシを取り付けます。ハードウェア設置ガイドを参照してください。
ステップ 2 外部インターフェイス（Ethernet 1/1 など）を外部ルータに接続します。
ステップ 3 内部インターフェイス（Ethernet 1/2 など）を内部スイッチまたはルータに接続します。
ステップ 4 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 5 （任意） 管理コンピュータをコンソールポートに接続します。

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。

ファイアウォールの電源投入

システムの電源は、ファイアウォール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。電源スイッチは、ソフト通知スイッチとして実装されています。これにより、システムのグレースフル シャットダウンがサポートされ、システム ソフトウェアおよびデータの破損のリスクが軽減されます。

（注） Threat Defense を初めて起動するときは、初期化に約 15 ～ 30 分かかります。

始める前に

ファイアウォールに対して信頼性の高い電力を供給することが重要です（無停電電源装置（UPS）を使用するなど）。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。

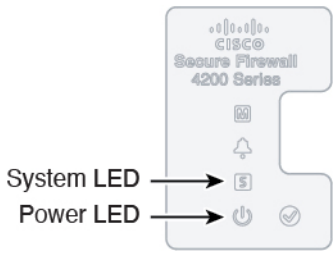
手順

ステップ 1 電源コードをファイアウォールに接続し、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 ファイアウォールの背面にある電源 LED を確認します。緑色に点灯している場合は、ファイアウォールの電源が入っています。

図 *4 :* システムおよび電源 *LED*



ステップ 4 ファイアウォールの背面にあるシステム LED を確認します。緑色に点灯している場合は、電源投入診断に合格しています。

（注） スイッチを ON から OFF に切り替えると、システムの電源が最終的に切れるまで数秒かかることがあります。この間は、シャーシの前面パネルの電源 LED が緑に点滅します。電源 LED が完全にオフになるまで電源を切らないでください。

中央の管理者による事後設定

外部インターフェイスからインターネットにアクセスできるようにリモート支社の管理者が Threat Defense をケーブル接続すると、Threat Defense を Management Center に登録してデバイスの設定を完了できます。

Management Centerへのログイン

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

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。オプションで、次の機能ライセンスを購入できます。

- **Essentials**（必須）Essentials ライセンス。
- **IPS**：セキュリティインテリジェンスと次世代 IPS
- **マルウェア防御**：マルウェア防御
- **URL フィルタリング**：URL フィルタリング
- **Cisco Secure Client**：Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）

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 のアカウントが必要です。

  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。

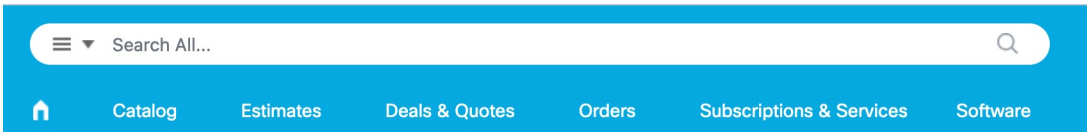
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用のスマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

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。

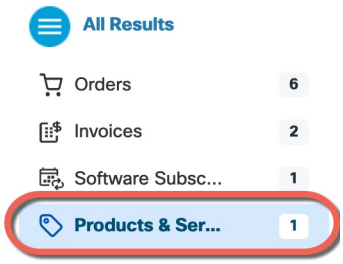
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、自身でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [すべて検索（Search All）] フィールドを使用します。

図 5 : ライセンス検索



結果から、[製品とサービス（Products and Services）] を選択します。

図 6 : 結果



次のライセンス PID を検索します。

（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。

- Essentials ライセンス：
  - L-FPR4215-BSE=
  - L-FPR4225-BSE=

- L-FPR4245-BSE=

- IPS、マルウェア防御、および URL ライセンスの組み合わせ：
  - L-FPR4215T-TMC=
  - L-FPR4225T-TMC=
  - L-FPR4245T-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-FPR4215T-TMC-1Y
  - L-FPR4215T-TMC-3Y
  - L-FPR4215T-TMC-5Y
  - L-FPR4225T-TMC-1Y
  - L-FPR4225T-TMC-3Y
  - L-FPR4225T-TMC-5Y
  - L-FPR4245T-TMC-1Y
  - L-FPR4245T-TMC-3Y
  - L-FPR4245T-TMC-5Y

- キャリアライセンス：
  - L-FPR4200-FTD-CAR=

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

ステップ 2 まだの場合は、Smart Software Manager 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。詳細については、『Management Center コンフィグレーション ガイド』を参照してください。

Management Center へのデバイスの追加

デバイスの IP アドレスまたはホスト名と登録キーを使用して、手動で Threat Defense を Management Center

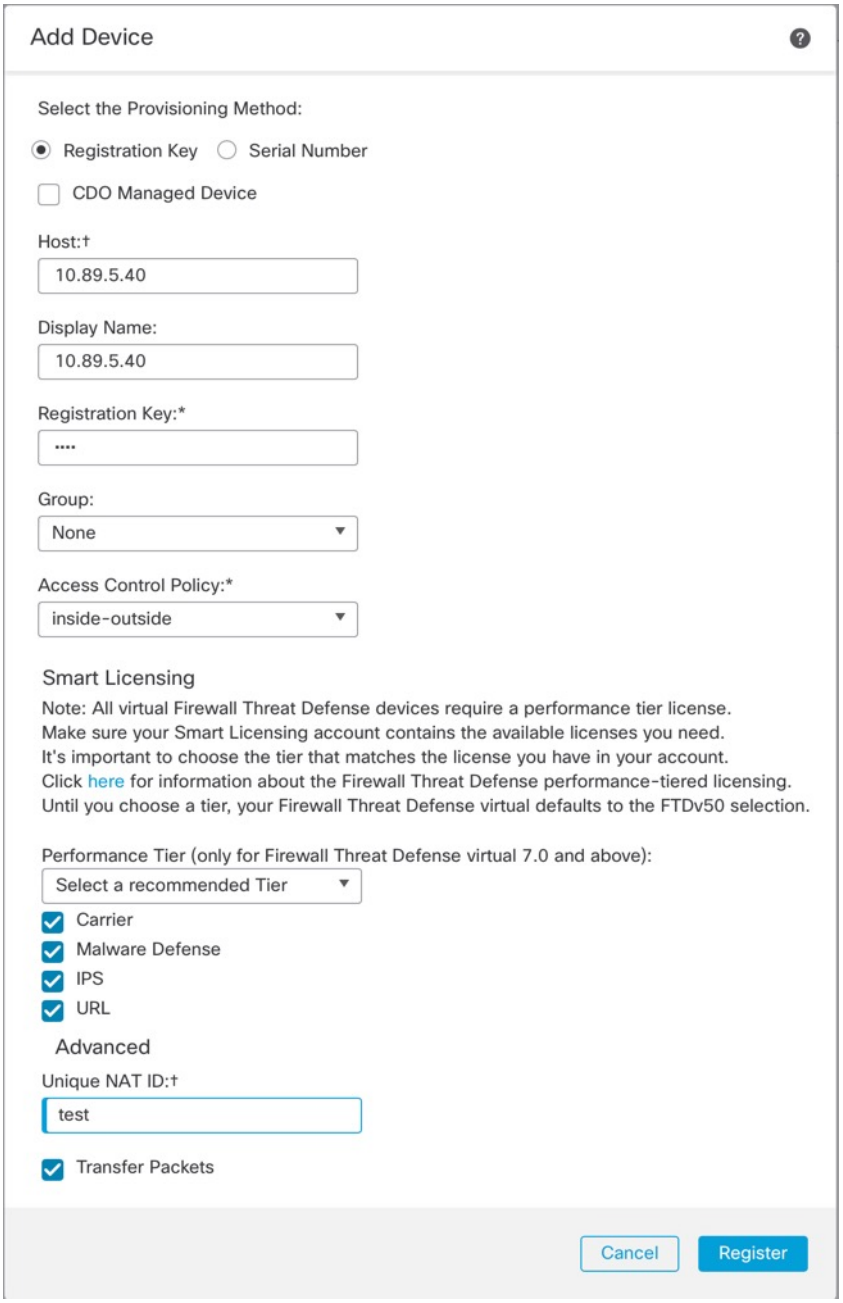
手順

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。

登録キー方式がデフォルトで選択されています。

図 7: 登録キーを使用したデバイスの追加



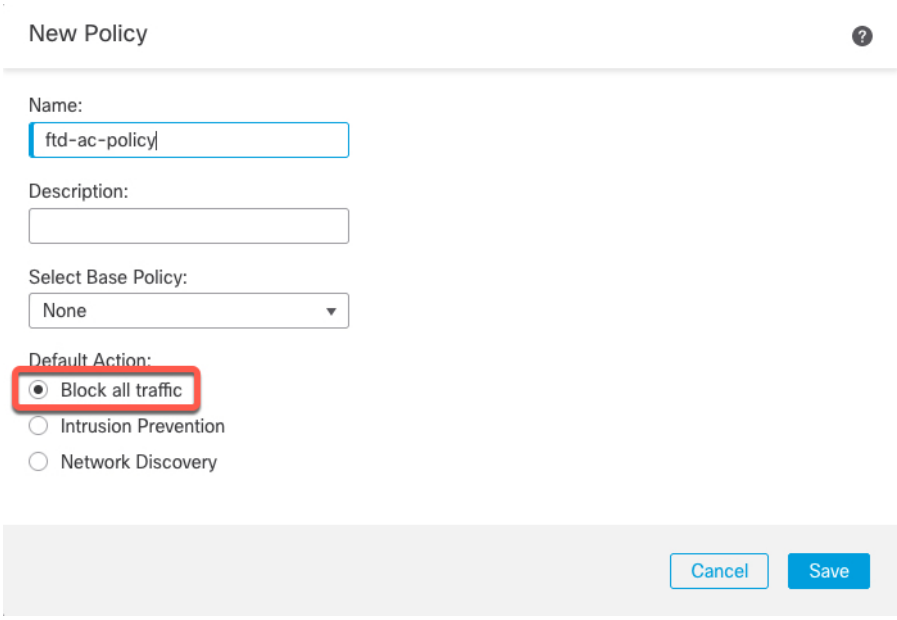
次のパラメータを設定します。

- [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」を参照してください。

図 *8*：新しいポリシー



- **スマートライセンス**：展開する機能に必要なスマートライセンスを割り当てます。**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 セキュアクライアント 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）] をクリックし、正常に登録され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 の 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必要がある場合は、**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、Threat Defense 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ます。マネージャアクセス設定の一部として外部インターフェイスの基本設定を構成しましたが、まだそのインターフェイスをセキュリティゾーンに割り当てる必要があります。
- 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。
- 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。
- SSH：マネージャ アクセス インターフェイスで SSH を有効にします。

インターフェイスの設定

Threat Defense 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。ブレークアウト インターフェイスも設定します。.

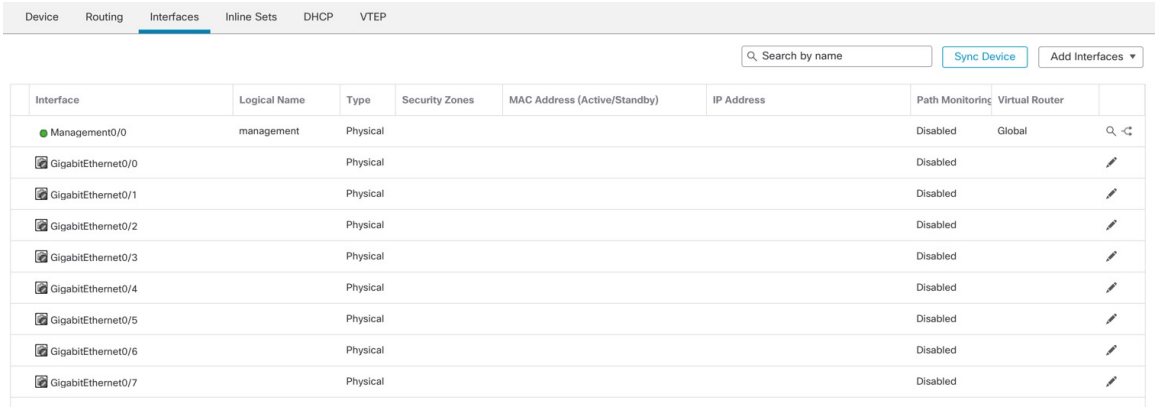
次の例では、DHCPによるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して、ルーテッドモードの内部インターフェイスを設定します。

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 **[編集（Edit）]**（✎）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。

図 *9:* インターフェイス



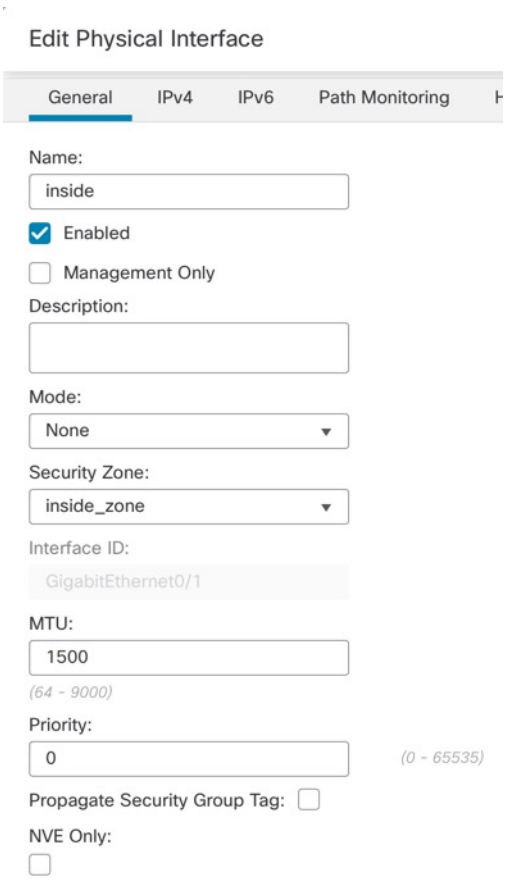
ステップ 3 （一部のモデルで使用可能な）40 Gb インターフェイスから 4 つの 10 Gb ブレークアウト インターフェイスを作成するには、インターフェイスのブレークアウトアイコンをクリックします。

設定で 40 Gb インターフェイスをすでに使用している場合は、ブレークアウトを続行する前に設定を削除する必要があります。

ステップ 4 内部に使用するインターフェイスの **[編集（Edit）]**（✎）をクリックします。

[全般（General）] タブが表示されます。

図 *10 : [General]* タブ



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。

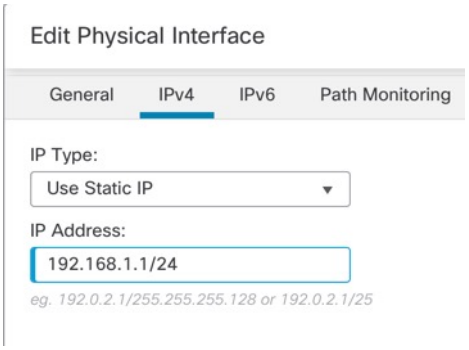
たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てる必要があります。インターフェイスは、1 つのセキュリティゾーンにのみ属することも、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向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。

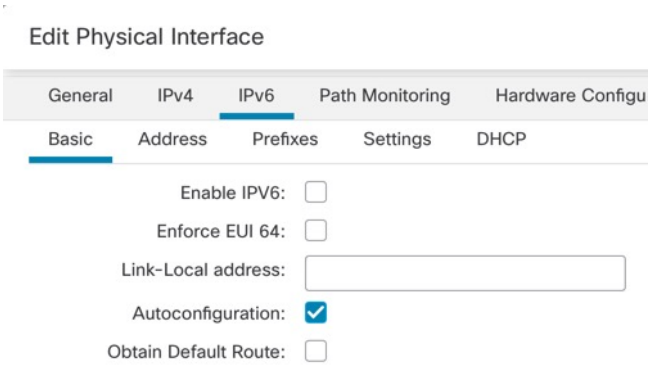
  たとえば、**192.168.1.1/24** などと入力します。

  図 *11 : [IPv4]* タブ



- [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。

  図 *12 : [IPv6]* タブ

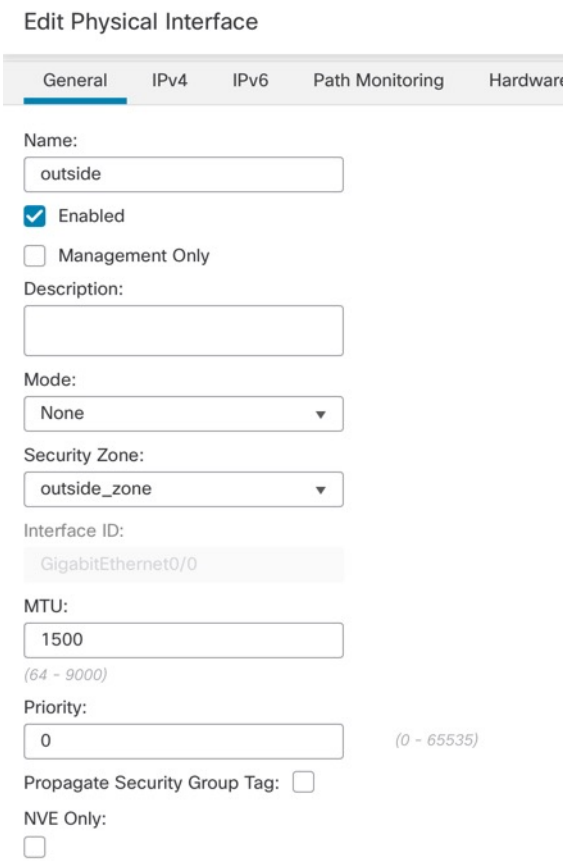


f) [OK] をクリックします。

ステップ 5 「外部」に使用するインターフェイスの **[編集（Edit）]**（✎）をクリックします。

[全般（General）] タブが表示されます。

図 *13 : [General]* タブ



マネージャ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ため、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する必要があります。

a) [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。

b) [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

DHCP サーバーの設定

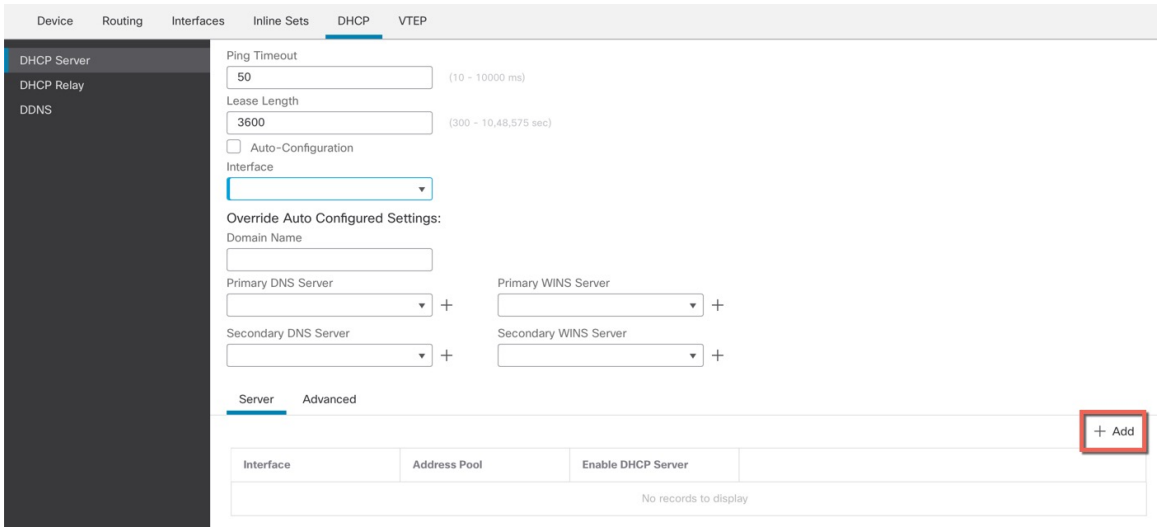
クライアントで DHCP を使用して 脅威に対する防御 から IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

手順

ステップ 1 [デバイス（Devices）]、[デバイス管理（Device Management）] の順に選択し、デバイスの **[編集（Edit）]**（✎）をクリックします。>

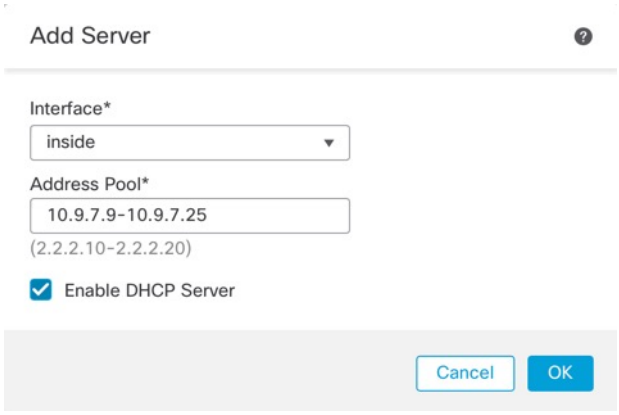
ステップ 2 **[DHCP]** > **[DHCPサーバー（DHCP Server）]** を選択します。

図 ***14 : DHCP*** サーバー



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。

図 ***15 :*** サーバーの追加



- [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。

NAT の設定

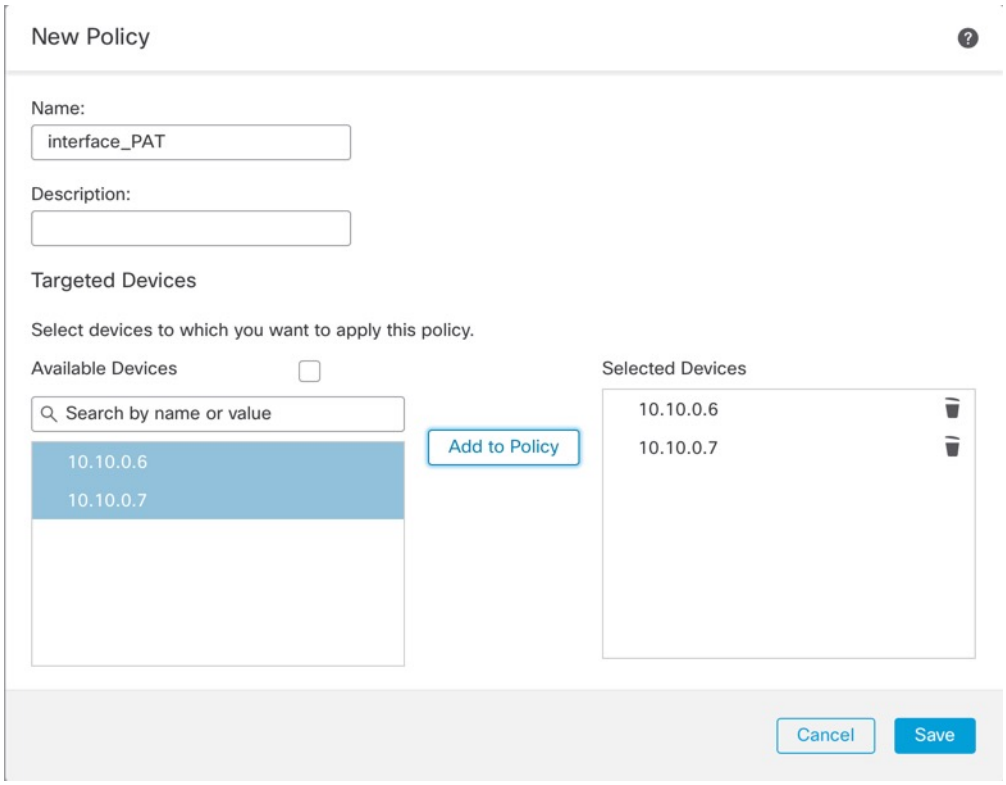
一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。

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。

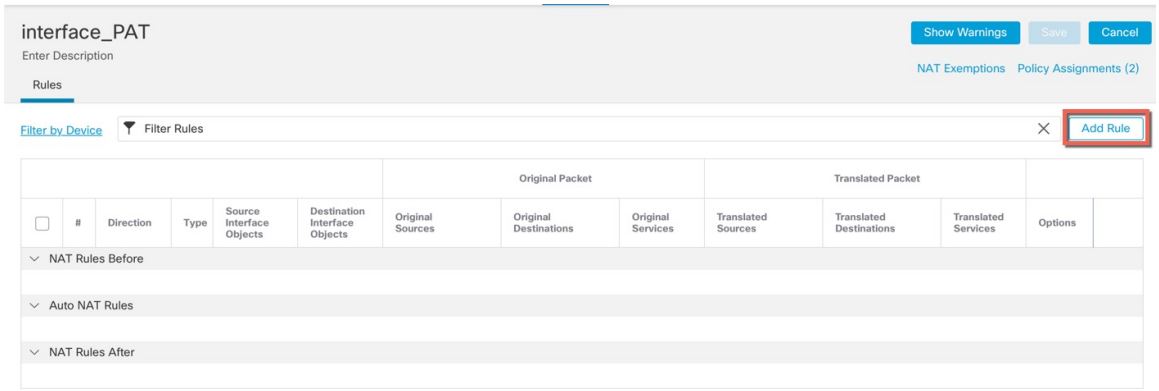
ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。

図 *16* : 新しいポリシー



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。

図 *17* : *NAT* ポリシー

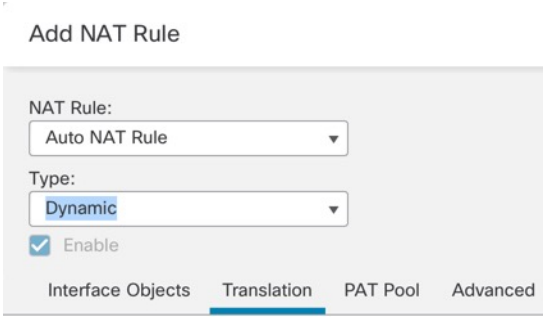


ステップ 3 [ルールの追加（Add Rule）] をクリックします。

[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。

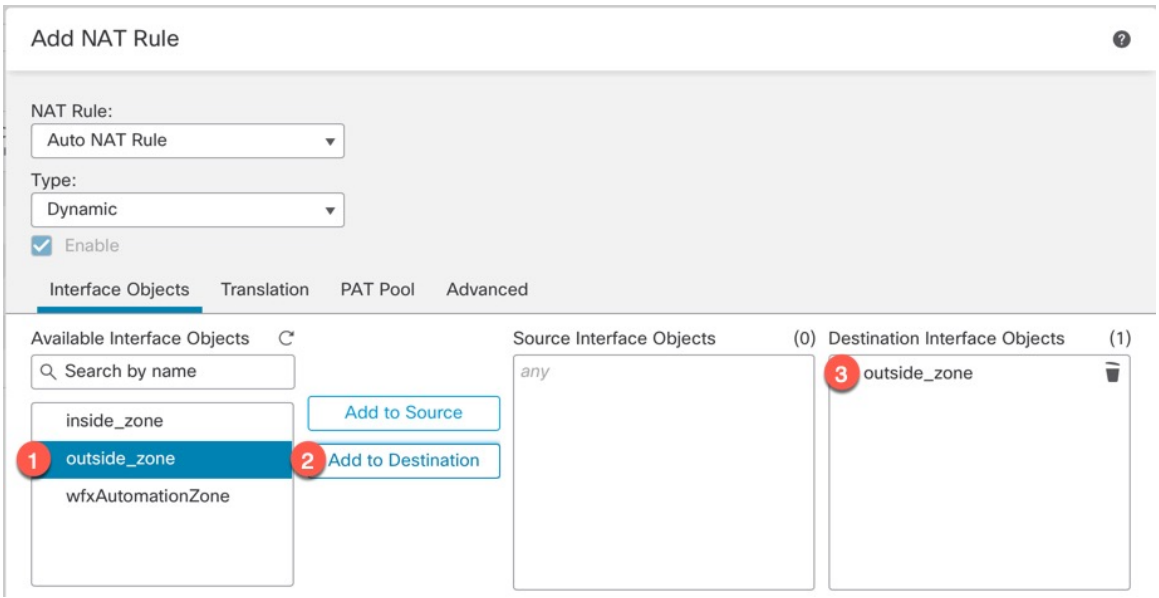
図 *18* : 基本ルールのオプション



- [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。

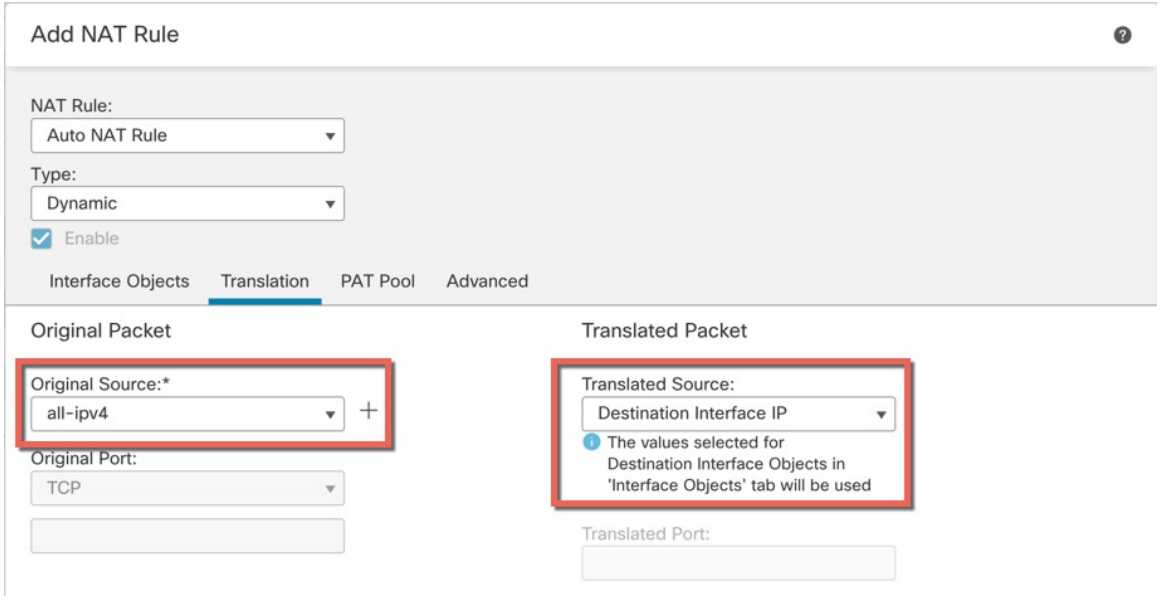
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。

図 *19* : インターフェイス オブジェクト



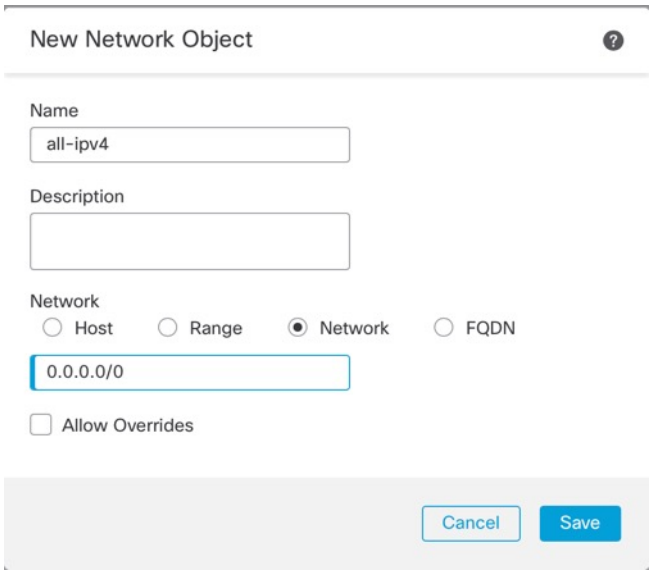
ステップ 6 [変換（Translation）] ページで、次のオプションを設定します。

図 *20 :* トランスレーション



- **[元の送信元（Original Source）]**：**Add (＋)** 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。

  図 *21 :* 新しいネットワークオブジェクト



  （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

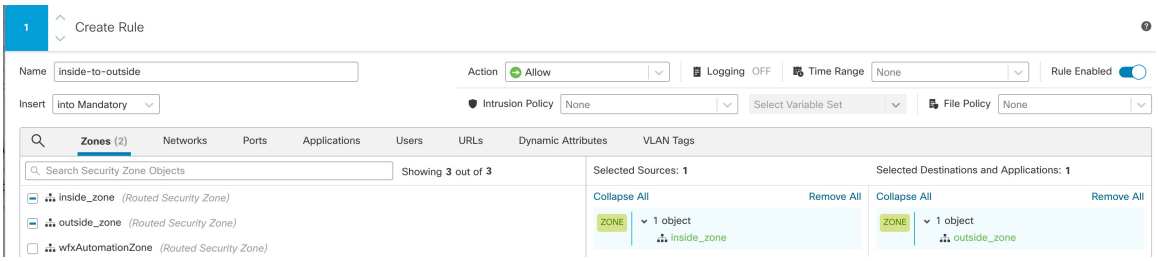
脅威に対する防御 を登録したときに、基本の [すべてのトラフィックをブロック（Block all traffic）] アクセス コントロール ポリシーを作成した場合は、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

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）] の順に選択し、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 **[編集（Edit）]**（✎）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。

図 *22*：ルールの追加



- **[名前（Name）]**：このルールに名前を付けます（たとえば、**inside-to-outside**）。
- **[選択した送信元（Selected Sources）]**：**[ゾーン（Zones）]** から内部ゾーンを選択し、**[送信元ゾーンを追加（Add Source Zone）]** をクリックします。
- **[選択した宛先とアプリケーション（Selected Destinations and Applications）]**：**[ゾーン（Zones）]** から外部ゾーンを選択し、**[宛先ゾーンを追加（Add Destination Zone）]** 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 [Apply] 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。

マネージャ アクセス データ インターフェイスでの SSH の設定

外部インターフェイスなどの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は、この手順に従ってそのインターフェイスで SSH を有効にする必要があります。ここでは、Threat Defense で 1 つ以上のデータインターフェイスに対して SSH 接続を有効にする方法について説明します。

（注） SSH は管理インターフェイス上でデフォルトで有効になっていますが、この画面は管理 SSH アクセスに影響しません。

管理インターフェイスは、デバイスの他のインターフェイスとは分離されています。Management Centerにデバイスを設定し、登録するために使用されます。データ インターフェイスの SSH は、管理インターフェイスの SSH と内部および外部ユーザ リストを共有します。その他の設定は個別に設定されます。データ インターフェイスでは、この画面を使用して SSH とアクセス リストを有効にします。データ インターフェイスの SSH トラフィックは通常のルーティング設定を使用し、設定時に設定されたスタティック ルートや CLI で設定されたスタティック ルートは使用しません。

管理インターフェイスの場合、SSH アクセスリストを構成するには Cisco Secure Firewall Threat Defense コマンドリファレンス の **configure ssh-access-list** コマンドを参照してください。スタティック ルートを設定するには、**configure network static-routes** コマンドを参照してください。デフォルトでは、初期設定時に管理インターフェイスからデフォルト ルートを設定します。

SSH を使用するには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。

SSH は、到達可能なインターフェイスにのみ使用できます。SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。

SSH は、次の暗号およびキー交換をサポートしています。

- 暗号化：aes128-cbc、aes192-cbc、aes256-cbc、aes128-ctr、aes192-ctr、aes256-ctr
- 完全性：hmac-sha2-256
- キー交換：dh-group14-sha256

（注） SSH を使用した CLI へのログイン試行が 3 回連続して失敗すると、デバイスの SSH 接続は終了します。

始める前に

- SSH 内部ユーザーは、**configure user add** コマンドを使用して CLI でのみ設定できます。。デフォルトでは、初期設定時にパスワードを設定した**Admin**ユーザーが存在します。LDAP または RADIUS 上の外部ユーザーは、プラットフォーム設定で [外部認証（External Authentication）] を設定することによっても設定できます。
- デバイスへの SSH 接続を許可するホストまたはネットワークを定義するネットワーク オブジェクトが必要です。オブジェクトをプロシージャの一部として追加できますが、IP アドレスのグループを特定するためにオブジェクト グループを使用する場合は、ルールで必要なグループがすでに存在することを確認します。**[オブジェクト（Objects）]**>**[オブジェクト管理（Object Management）]** を選択して、オブジェクトを設定します。

（注） システムが提供する **any** ネットワーク オブジェクトは使用できません。代わりに、**any-ipv4** または **any-ipv6** を使用します。

手順

ステップ 1 **[デバイス（Devices）]**>**[プラットフォーム設定（Platform Settings）]** を選択し、Threat Defense ポリシーを作成または編集します。

ステップ 2 **[SSHアクセス（SSH Access）]** を選択します。

ステップ 3 SSH 接続を許可するインターフェイスと IP アドレスを指定します。

この表を使用して、SSH接続を受け入れるインターフェイス、およびそれらの接続を許可されるクライアントの IP アドレスを制限します。個々の IP アドレスはなく、ネットワーク アドレスを使用できます。

a) [追加（Add）]をクリックして新しいルールを追加するか、[編集（Edit）]をクリックして既存のルールを編集します。

b) ルールのプロパティを設定します。

- [IP Address]：SSH 接続を許可するホストまたはネットワークを特定するネットワーク オブジェクトまたはグループ。オブジェクトをドロップダウンメニューから選択するか、または [+] をクリックして新しいネットワークオブジェクトを追加します。
- **[使用可能なゾーン/インターフェイス（Available Zones/Interfaces）]**：SSH 接続を許可するインターフェイスを含むゾーンを追加します。ゾーンにないインターフェイスでは、**[選択したゾーン/インターフェイス（Selected Zones/Interfaces）]** リストの下のフィールドにインターフェイス名を入力し、[追加（Add）] をクリックします。 ループバック インターフェイスを追加することもできます。選択されているインターフェイスまたはゾーンがデバイスに含まれているときにのみ、これらのルールがデバイスに適用されます。

c) [OK] をクリックします。

ステップ 4 **[Save（保存）]** をクリックします。

これで、**[展開（Deploy）]** > **[展開（Deployment）]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更はポリシーを展開するまで有効になりません。

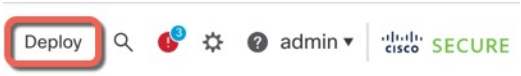
設定の展開

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 *23 :* 展開



ステップ 2 迅速な展開の場合は、特定のデバイスのチェックボックスをオンにして [展開（Deploy）] をクリックするか、[すべて展開（Deploy All）] をクリックしてすべてのデバイスを展開します。それ以外の場合は、追加の展開オプションを設定するために、[高度な展開（Advanced Deploy）] をクリックします。

図 *24 :* すべて展開

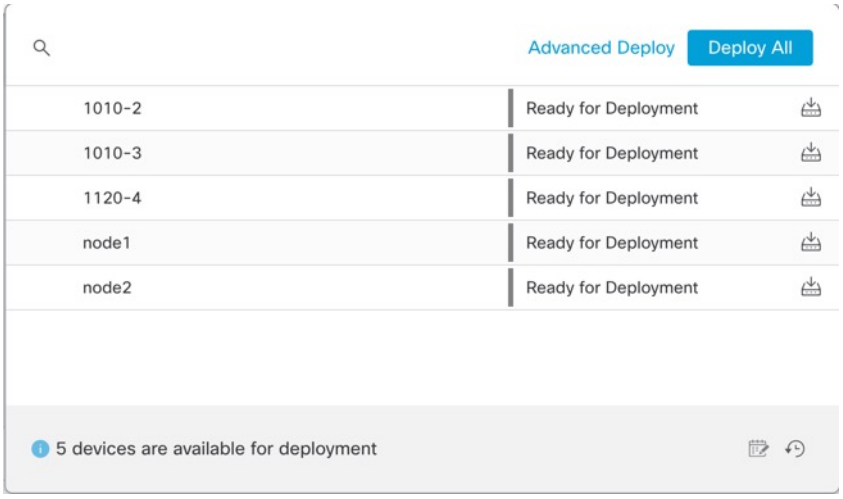
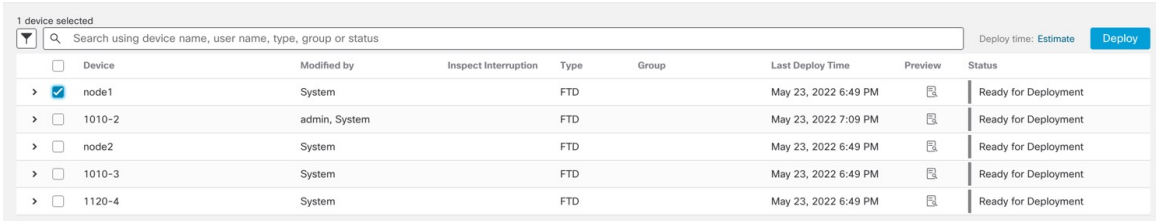
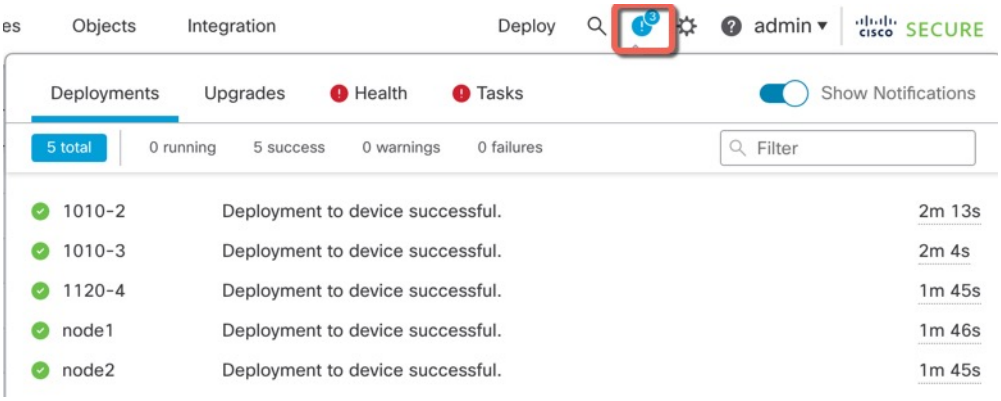


図 *25* : 高度な展開



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 *26* : 展開ステータス



Threat Defense および FXOS 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。

トラブルシューティングのためにも FXOS CLI にアクセスできます。

（注） または、Threat Defense デバイスの管理インターフェイスに SSH で接続できます。コンソールセッションとは異なり、SSH セッションはデフォルトで Threat Defense CLI になり、**connect fxos** コマンドを使用して FXOS CLI に接続できます。SSH 接続用のインターフェイスを開いている場合、後でデータインターフェイス上のアドレスに接続できます。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。この手順では、デフォルトで FXOS CLI となるコンソールポートアクセスについて説明します。

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。デフォルトでは Cisco Secure Firewall 4200 にコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。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。コンソール ポートはデフォルトで FXOS CLI になります。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

FXOS CLI に接続します。ユーザー名 **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 CLI にログインします（デフォルトは **Admin123**）。

例：

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

ステップ 2 Threat Defense CLI にアクセスします。

connect ftd

例：

```
firepower# connect ftd
>
```

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用方法については、『Cisco Secure Firewall Threat Defense コマンドリファレンス』を参照してください。

ステップ 3 Threat Defense CLI を終了するには、**exit** または **logout** コマンドを入力します。

このコマンドにより、FXOS CLI プロンプトに戻ります。FXOS CLI で使用可能なコマンドについては、**?** を入力してください。

例：

```
> exit
firepower#
```

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。

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、FXOS 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。

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 **[デバイス（Devices）]** > **[デバイス管理（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（Edit）]**（ ） 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（Shut Down Device）]**（ ）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 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。

```
System is stopped.
It is safe to power off now.

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

コンソールから接続していない場合は、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。

ステップ 7 必要に応じて電源スイッチをオフにし、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

FXOS CLI を使用すると、システムを安全にシャットダウンしてデバイスの電源を切断できます。CLI には、コンソールポートに接続してアクセスします。Threat Defense および FXOS CLI へのアクセス （35 ページ）を参照してください。

手順

ステップ 1 FXOS CLI で local-mgmt に接続します。

firepower # **connect local-mgmt**

ステップ 2 **shutdown** コマンドを発行します。

firepower(local-mgmt) # **shutdown**

例：

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

ステップ 3 ファイアウォールのシャットダウン時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。

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

ステップ 4 必要に応じて電源スイッチをオフにし、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。

次のステップ

Threat Defense の設定を続行するには、「Cisco Secure Firewall Threat Defense ドキュメントにアクセス」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、「Cisco Secure Firewall Management Center デバイス構成ガイド」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。