



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オペレーティングシステムとマネージャを確認するには、「[最適なオペレーティングシステムとマネージャを見つける方法](#)」を参照してください。この章は、中央の本社の Management Center を使用するリモート支社の脅威に対する防御 に適用されます。

各脅威に対する防御 は、トラフィックを制御、検査、監視、および分析して、管理 Management Center に報告します。Management Center は、サービスの管理、分析、レポートのタスクを実行できる Web インターフェイスを備えた集中管理コンソールを提供し、ローカルネットワークを保護します。

- 中央の本社の管理者が、CLI または Device Manager を使用して 脅威に対する防御 を事前設定してから、リモート支社に 脅威に対する防御 を送信します
- 支社の管理者が、脅威に対する防御 をケーブルで接続して電源をオンにします。
- 中央の管理者が、Management Center を使用して 脅威に対する防御 の設定を完了します。



(注) リモート支社への展開には、バージョン 6.7 以降が必要です。

ファイアウォールについて

ハードウェアでは、脅威に対する防御 ソフトウェアまたは ASA ソフトウェアを実行できません。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。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 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。

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、[Firepower 1000/2100 および Secure Firewall 3100 と Firepower Threat Defense の Cisco FXOS トラブルシューティング 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：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はありません。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せん。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 \(2 ページ\)](#)
- [はじめる前に \(4 ページ\)](#)
- [エンドツーエンドの手順 \(4 ページ\)](#)
- [中央の管理者による事前設定 \(6 ページ\)](#)
- [支社へのインストール \(20 ページ\)](#)
- [中央の管理者による事後設定 \(22 ページ\)](#)

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、管理インターフェイスの代わりに外部のインターフェイスを使用して Management Center を管理します。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 Management Center にアクセスして中央管理を行えるようにします。



- (注) マネージャアクセスには任意のデータインターフェイスを使用できます。たとえば、内部 Management Center がある場合は内部インターフェイスなどです。ただし、このガイドでは主に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、リモート支社で最も用いられる可能性が高いシナリオであるためです。

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。

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。

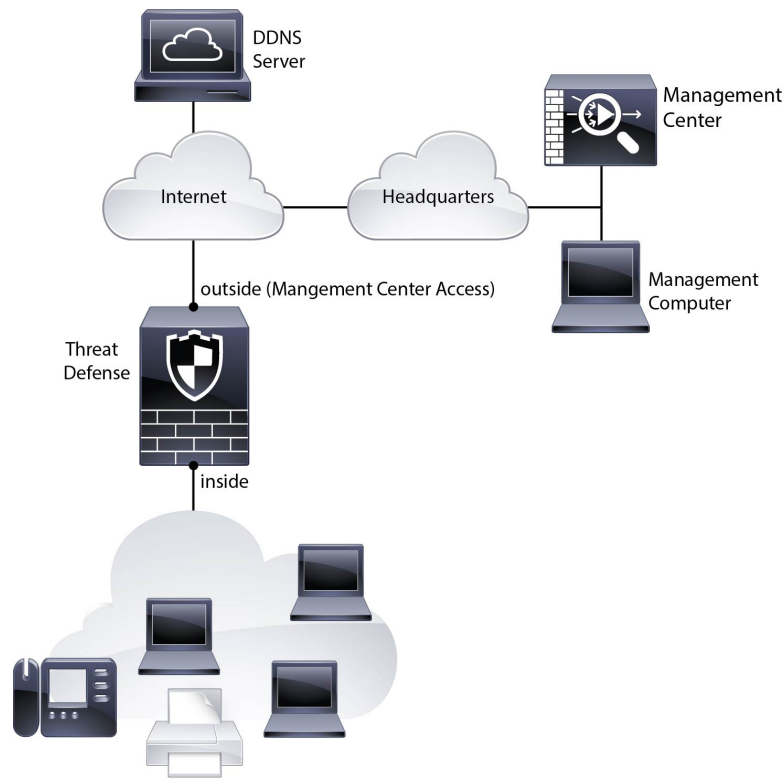
- マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。冗長性を目的として、Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
- このインターフェイスは管理専用にはできません。

- 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 モデムの上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。
- ハイアベイラビリティ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。

次の図は、中央の本社にある Management Center と外部インターフェイスでマネージャアクセスをもつ Threat Defense を示しています。

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:



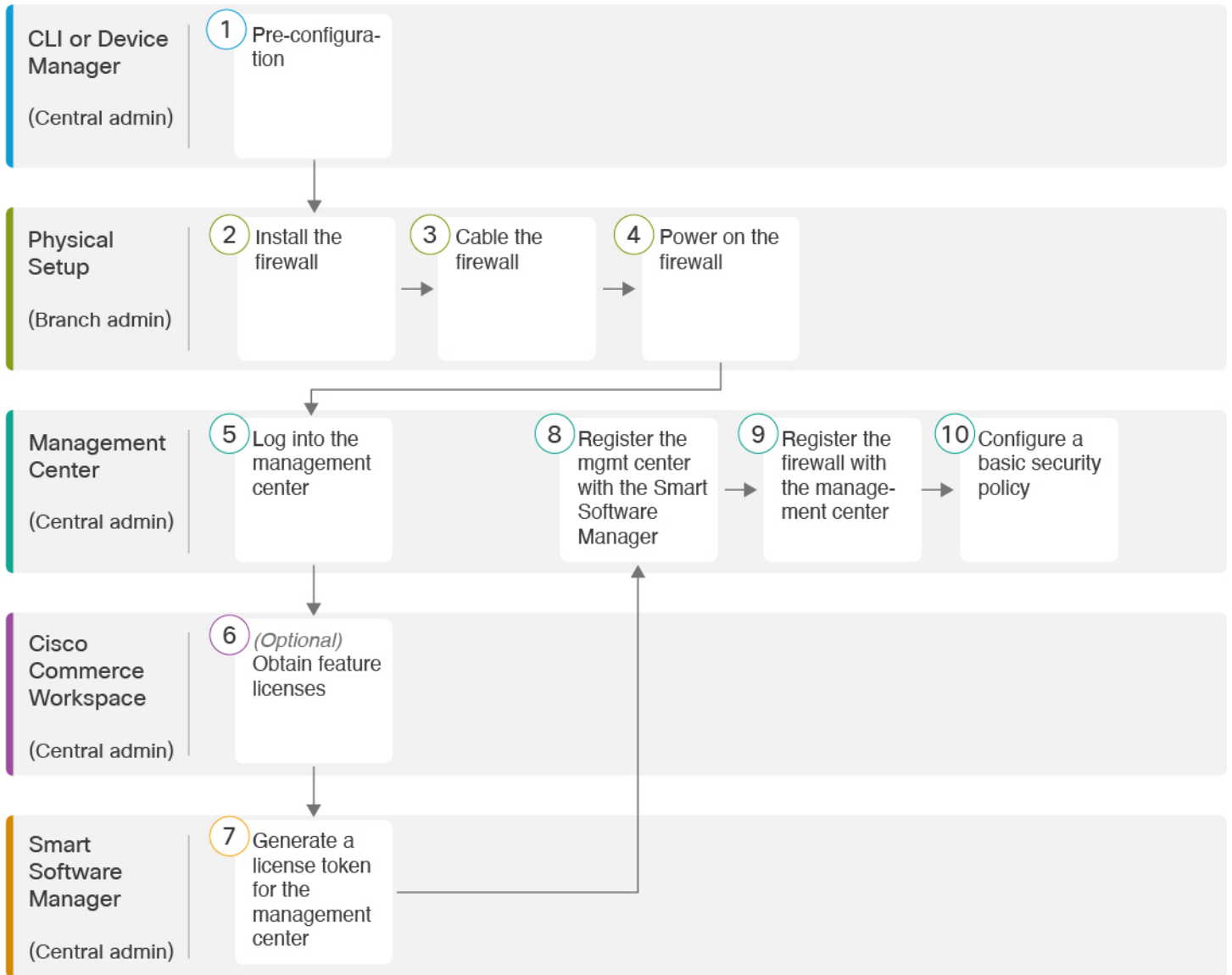
はじめる前に

Management Center の初期設定を展開して実行します。[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。

図 2: エンドツーエンドの手順 : 手動プロビジョニング



<p>①</p>	<p>CLI または Device Manager (中央の管理者)</p>	<ul style="list-style-type: none"> • (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) • Device Manager を使用した事前設定 (8 ページ) • CLI を使用した事前設定 (14 ページ)
<p>②</p>	<p>物理的なセットアップ (支社の管理者)</p>	<p>ファイアウォールをインストールします。 Cisco Firepower 2100 Series Hardware Installation Guideを参照してください。</p>

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 (20 ページ)。
④	物理的なセットアップ (支社の管理者)	デバイスの電源投入 (21 ページ)
⑤	Management Center (中央の管理者)	へのログイン Management Center。
⑥	Cisco Commerce Workspace (中央の管理者)	Management Center のライセンスの取得 (23 ページ) : 機能ライセンスを購入します。
⑦	Smart Software Manager (中央の管理者)	Management Center のライセンスの取得 (23 ページ) : Management Center のライセンストークンを生成します。
⑧	Management Center (中央の管理者)	Management Center のライセンスの取得 (23 ページ) : スマートライセンスサーバーに Management Center を登録します。
⑨	Management Center (中央の管理者)	Management Center への Threat Defense の登録 (25 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。

中央の管理者による事前設定

Threat Defense は、支社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](https://www.cisco.com/c/en/us/qa/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 CLI 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 \(40 ページ\)](#) を参照してください。この手順ではコンソールポートを使用していますが、代わりに SSH を使用することもできます。

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              7.2.0.65
```

7.2.0.65 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 Threat Defense 初期設定の実行の完了](#)」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。

Device Manager を使用した事前設定

Device Manager に接続して、Threat Defense の初期設定を実行します。Device Manager を使用して初期セットアップを実行すると、管理インターフェイスおよびマネージャアクセス設定に加えて、管理のために Management Center に切り替えたときに、Device Manager で完了したすべてのインターフェイス構成が保持されます。アクセスコントロールポリシーやセキュリティゾーンなどの他のデフォルト設定は保持されないことに注意してください。CLI を使用すると、管理インターフェイスとマネージャアクセス設定のみが保持されます（たとえば、デフォルトの内部インターフェイス構成は保持されません）。

始める前に

- 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](#)を参照してください。Threat Defense をセットアップする前に、Management Center の IP アドレスまたはホスト名を把握しておく必要があります。
- 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 管理コンピュータを内部（Ethernet 1/2）インターフェイスに接続します

ステップ 2 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 3 Device Manager にログインします。

- a) ブラウザに URL (<https://192.168.95.1>) を入力します。
- b) ユーザー名 **admin**、デフォルト パスワード **Admin123** を使用してログインします。

- c) エンドユーザー 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。

ステップ 4 初期設定を完了するには、最初に Device Manager 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。必要に応じて、ページの下部にある [デバイスの設定をスキップ (Skip device setup)] をクリックしてセットアップウィザードをスキップできます。

セットアップウィザードを完了すると、内部インターフェイス (Ethernet1/2) のデフォルト設定に加えて、Management Center の管理に切り替えるときに維持される外部 (Ethernet1/1) インターフェイスも設定できます。

- a) 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。

1. [外部インターフェイスアドレス (Outside Interface Address)]—このインターフェイスは通常インターネット ゲートウェイであり、マネージャ アクセス インターフェイスとして使用される場合があります。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。

マネージャアクセスに外部 (または内部) とは異なるインターフェイスを使用する場合は、セットアップウィザードの完了後に手動で設定する必要があります。

[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。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

[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。

2. [管理インターフェイス (Management Interface)]

CLI で初期設定を実行した場合、管理インターフェイスの設定は表示されません。

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。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。

[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。

- b) [時刻設定 (NTP) (Time Setting (NTP))] を設定し、[次へ (Next)] をクリックします。
1. [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。
 2. [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。
- c) [登録せずに 90 日間の評価期間を開始 (Start 90 day evaluation period without registration)] を選択します。
- Threat Defense を Smart Software Manager に登録しないでください。すべてのライセンスは Management Center で実行されます。
- d) [終了 (Finish)] をクリックします。
- e) [クラウド管理 (Cloud Management)] または [スタンドアロン (Standalone)] を選択するよう求められます。Management Center の管理については、[スタンドアロン (Standalone)] を選択してから、[Got It (了解)] を選択します。

ステップ 5 (必要に応じて) 管理インターフェイスを設定します。[デバイス (Device)] > [インターフェイス (Interfaces)] の管理インターフェイスを参照してください。

管理インターフェイスには、データインターフェイスに設定されたゲートウェイが必要です。デフォルトでは、管理インターフェイスは DHCP から IP アドレスとゲートウェイを受信します。DHCP からゲートウェイを受信しない場合 (たとえば、管理インターフェイスをネットワークに接続していない場合)、ゲートウェイはデフォルトでデータインターフェイスになり、何も設定する必要はありません。DHCP からゲートウェイを受信した場合は、代わりに管理インターフェイスに静的 IP アドレスを設定し、ゲートウェイをデータインターフェイスに設定する必要があります。

ステップ 6 マネージャアクセスに使用する外部または内部以外のインターフェイスを含む追加のインターフェイスを設定する場合は、[デバイス (Device)] を選択し、[インターフェイス (Interface)] のサマリーのリンクをクリックします。

Device Manager におけるインターフェイスの設定の詳細については、「[Device Manager でのファイアウォールの設定](#)」を参照してください。Management Center にデバイスを登録すると、Device Manager の他の設定は保持されません。

ステップ 7 [デバイス (Device)] [システム設定 (Device System Settings)] [中央管理 (Central Management)] [Management Center] [Management Center] [デバイス (Device)] [システム設定 (System Settings)] [中央管理 (Central Management)] [Management Center] の順に選択し、[続行 (Proceed)] をクリックして Management Center の管理を設定します。

ステップ 8 [Management Center/CDOの詳細 (Management Center/CDO Details)] を設定します。

図 3 : Management Center/CDO の詳細

Configure Connection to Management Center or CDO

Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes No

Threat Defense

10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64

→


Management Center/CDO

10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●● 

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup ▼

Management Center/CDO Access Interface

Data Interface

Please select an interface ▼

Management Interface [View details](#)

CANCEL CONNECT

- a) [Management Center/CDOのホスト名またはIPアドレスを知っていますか (Do you know the FMC hostname or IP address)] で、IP アドレスまたはホスト名を使用して Management Center に到達できる場合は [はい (Yes)] をクリックし、Management Center が NAT の背

後にあるか、パブリック IP アドレスまたはホスト名がない場合は[いいえ (No)]をクリックします。

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、少なくとも 1 台以上のデバイス (Management Center または Threat Defense デバイス) に到達可能な IP アドレスが必要です。

- b) [はい (Yes)] を選択した場合は、**管理センター/CDO のホスト名/IP アドレス**を入力します。
- c) **Management Center/CDO 登録キー**を指定します。

このキーは、Threat Defense デバイスを登録するとき Management Center でも指定する任意の 1 回限りの登録キーです。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 (-) があります。この ID は、Management Center に登録する複数のデバイスに使用できます。

- d) [NAT ID] を指定します。

この ID は、Management Center でも指定する任意の 1 回限りの文字列です。いずれかのデバイスの IP アドレスのみを指定する場合、このフィールドは必須です。両方のデバイスの IP アドレスがわかっている場合でも、NAT ID を指定することを推奨します。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 (-) 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。NAT ID は、正しいデバイスからの接続であることを確認するために IP アドレスと組み合わせて使用されます。IP アドレス/NAT ID の認証後にはのみ、登録キーがチェックされます。

ステップ 9 [接続の設定 (Connectivity Configuration)] を設定します。

- a) [FTD ホスト名 (FTD Hostname)] を指定します。

この FQDN は、外部インターフェイス、または **Management Center/CDO アクセスマスターフェイス**用に選択したインターフェイスに使用されます。

- b) [DNS サーバグループ (DNS Server Group)] を指定します。

既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

この設定により、データインターフェイス DNS サーバーが設定されます。セットアップウィザードで設定した管理 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。管理トラフィックとデータトラフィックの両方が外部インターフェイス経由で DNS サーバーに到達するため、管理に使用したものと同一 DNS サーバグループを選択する可能性があります。

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。

- c) **Management Center/CDO アクセスインターフェイス**については、[外部 (outside)]を選択します。

設定済みの任意のインターフェイスを選択できますが、このガイドでは外部を使用していることを前提としています。

ステップ 10 外部とは別のデータインターフェイスを選択した場合は、デフォルトルートを追加します。

インターフェイスを通過するデフォルトルートがあることを確認するように求めるメッセージが表示されます。外部を選択した場合は、セットアップウィザードの一環としてこのルートがすでに設定されています。別のインターフェイスを選択した場合は、Management Center に接続する前にデフォルトルートを手動で設定する必要があります。Device Manager におけるスタティックルートの設定の詳細については、「[Device Manager でのファイアウォールの設定](#)」を参照してください。

ステップ 11 [ダイナミック DNS (DDNS) 方式の追加 (Add a Dynamic DNS (DDNS) method)]をクリックします。

DDNS は、Threat Defense 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 Threat Defense に到達できるようにします。[デバイス (Device)]>[システム設定 (System Settings)]>[DDNS サービス (DDNS Service)]を参照して DDNS を設定します。

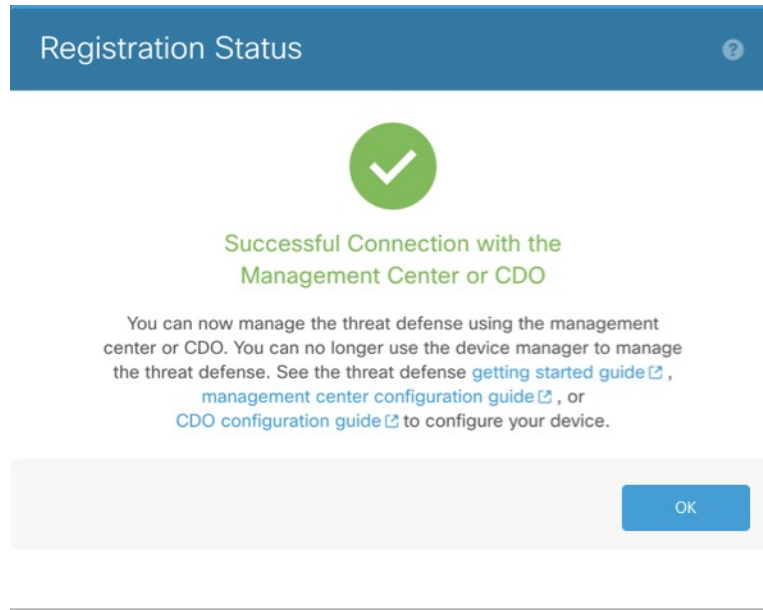
Threat Defense を Management Center に追加する前に DDNS を設定すると、Threat Defense は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、Threat Defense は HTTPS 接続の DDNS サーバー証明書を検証できます。Threat Defense は、DynDNS リモート API 仕様 (<https://help.dyn.com/remote-access-api/>) を使用するすべての DDNS サーバーをサポートします。

ステップ 12 [接続 (Connect)]をクリックします。[登録ステータス (Registration Status)]ダイアログボックスには、Management Center への切り替えに関する現在のステータスが表示されます。**[Management Center/CDO登録設定の保存 (Saving Management Center/CDO Registration Settings)]**のステップの後、Management Center に移動してファイアウォールを追加します。

Management Center への切り替えをキャンセルする場合は、[登録のキャンセル (Cancel Registration)]をクリックします。キャンセルしない場合は、**[Management Center/CDO登録設定の保存 (Saving Management Center/CDO Registration Settings)]**のステップが完了するまで Device Manager のブラウザウィンドウを閉じないでください。閉じた場合、プロセスは一時停止し、Device Manager に再接続した場合のみ再開されます。

[Management Center/CDO登録設定の保存 (Saving Management Center/CDO Registration Settings)]のステップの後に Device Manager に接続したままにする場合、その後**[Management CenterまたはCDOとの正常接続 (Successful Connection with Management Center or CDO)]**ダイアログボックスが表示され、Device Manager から切断されます。

図 4: 正常接続



CLI を使用した事前設定

Threat Defense CLI に接続して初期設定を行います。初期設定で CLI を使用すると、管理インターフェイスとマネージャ アクセス インターフェイスの設定のみが保持されます。Device Manager (7.1 以降) を使用して初期セットアップを実行すると、管理インターフェイスおよびマネージャアクセスインターフェイスの設定に加えて、管理のために Management Center に切り替えたときに、Device Manager で完了したすべてのインターフェイス設定が保持されます。アクセス コントロール ポリシーなどの他のデフォルト設定は保持されないことに注意してください。

始める前に

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 を参照してください。Threat Defense をセットアップする前に、Management Center の IP アドレスまたはホスト名を把握しておく必要があります。

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。

- [DHCP経由または手動でIPv4を設定しますか? (Configure IPv4 via DHCP or manually?)] : [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)] : ゲートウェイを [data-interfaces] 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。
- [ネットワーク情報が変更された場合は再接続が必要 (If your networking information has changed, you will need to reconnect)] : SSH で接続している場合は、接続が切断されます。管理コンピュータが管理ネットワーク上にある場合は、新しい IP アドレスとパスワードで再接続できます。(データインターフェイス経由で) デフォルトルートが変更されたため、リモートネットワークからはまだ再接続できません。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?)] : **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 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]:
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 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。
- 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://deanwinchester: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、少なくとも 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нта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 (-) があります。
- **nat_id** : Management Center でも指定する、任意で一意的の 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 (-) 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。

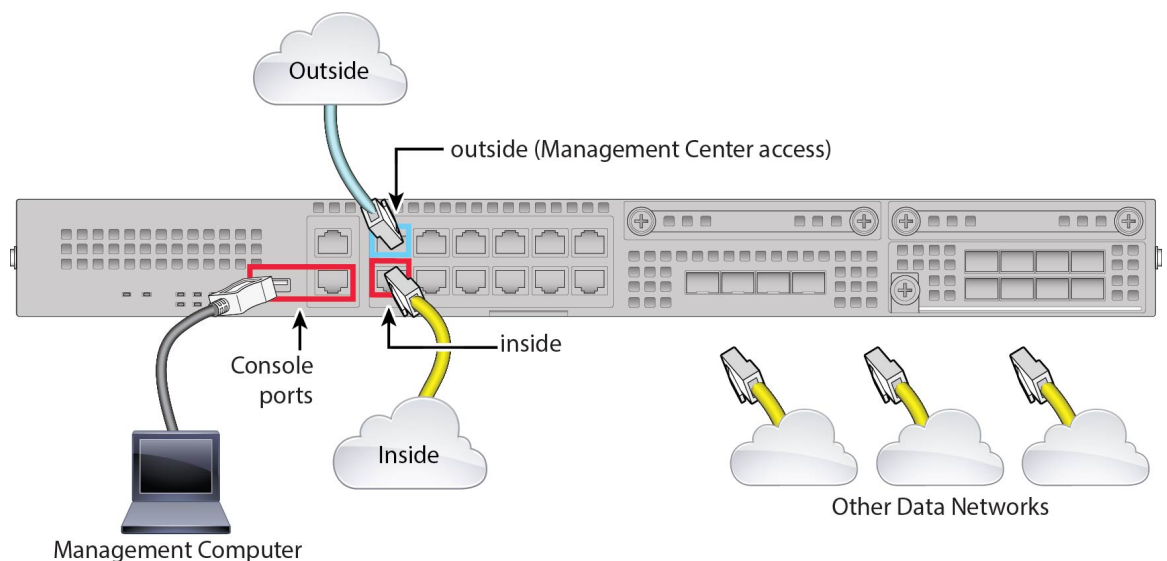
支社へのインストール

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。Firepower 2100 をケーブル配線するには、次の手順を参照してください。

図 5: リモート管理展開のケーブル接続



手順

- ステップ1 シャーシを取り付けます。Cisco Firepower 2100 Series Hardware Installation Guide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) 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。

デバイスの電源投入

電源スイッチは、シャーシの背面の電源モジュール1の左にあります。これはシステムへの電源を制御するトグルスイッチです。電源スイッチがスタンバイの位置にある場合は、3.3 V のスタンバイ電源ユニットのみが電源モジュールから有効化され、12 V の主電源はオフになります。スイッチがオンの位置にある場合は、12 V の主電源がオンになり、システムが起動します。



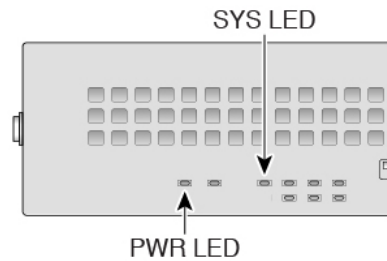
- (注) Threat Defense を初めて起動するときは、初期化に約 15 ~ 30 分かかります。

始める前に

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 デバイスの背面にある電源スイッチを押します。
- ステップ3 デバイスの前面にある PWR 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。



ステップ4 デバイスの前面にある SYS LED を確認します。緑色に点灯している場合は、電源投入時診断に合格しています。

(注) 電源スイッチをオフの位置に動かす前に、システムがグレースフルシャットダウンを実行できるように shutdown コマンドを使用します。終了するまでに数分かかる場合があります。グレースフルシャットダウンが完了すると、コンソールにはすぐに電源オフすると安全ですと表示されます。前面パネルの青いロケータ ビーコン LED が点灯し、システムの電源をオフにする準備ができています。これで、スイッチをオフの位置に移動できるようになりました。前面パネルの PWR LED が瞬間的に点滅し、消灯します。PWR LED が完全にオフになるまで電源を抜かないでください。

これらの shutdown コマンドの使用の詳細については、『[FXOS コンフィグレーションガイド](#)』を参照してください。

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。

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。オプションで、次の機能ライセンスを購入できます。

- **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** : 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** 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 6: 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。

• IPS、マルウェア防御、および URL ライセンスの組み合わせ：

- L-FPR2110T-TMC=
- L-FPR2120T-TMC=
- L-FPR2130T-TMC=
- L-FPR2140T-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-FPR2110T-TMC-1Y
- L-FPR2110T-TMC-3Y
- L-FPR2110T-TMC-5Y
- L-FPR2120T-TMC-1Y
- L-FPR2120T-TMC-3Y
- L-FPR2120T-TMC-5Y
- L-FPR2130T-TMC-1Y
- L-FPR2130T-TMC-3Y
- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

• Cisco Secure Client : 『[Cisco Secure Client 発注ガイド](#)』を参照してください。

• キャリアライセンス：

•

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。ロータッチプロビジョニングの場合は、Smart Software Manager に登録するとき、または登録した後に、**ロータッチプロビジョニングのクラウドアシスタンス**を有効にする必要があります。[システム (System)] > [ライセンス (Licenses)] > [スマートライセンス (Smart Licenses)] ページを参照してください。

Management Center への Threat Defense の登録

Threat Defense を Management Center に登録します。

始める前に

- Threat Defense の初期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。

The screenshot shows the 'Add Device' configuration window. It contains the following fields and options:

- Host:** ftd-1.cisco.com
- Display Name:** ftd-1.cisco.com
- Registration Key:** ****
- Group:** None (dropdown menu)
- Access Control Policy:** inside-outside (dropdown menu)
- Smart Licensing:**
 - Malware
 - Threat
 - URL Filtering
- Advanced:**
 - Unique NAT ID:** natid56
 - Transfer Packets

At the bottom, there are 'Cancel' and 'Register' buttons.

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一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 7: New Policy

New Policy

Name:
ftd-ac-policy

Description:

Select Base Policy:
None

Default Action:
 Block all traffic
 Intrusion Prevention
 Network Discovery

Cancel Save

- [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、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 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

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。

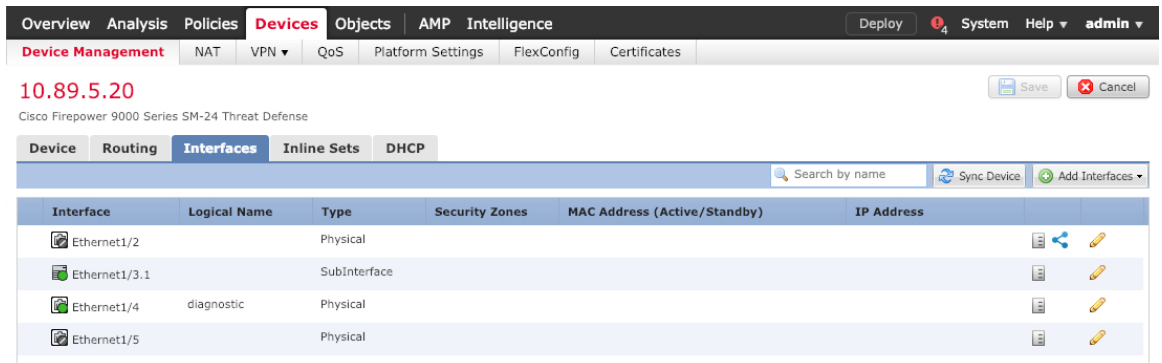
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

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

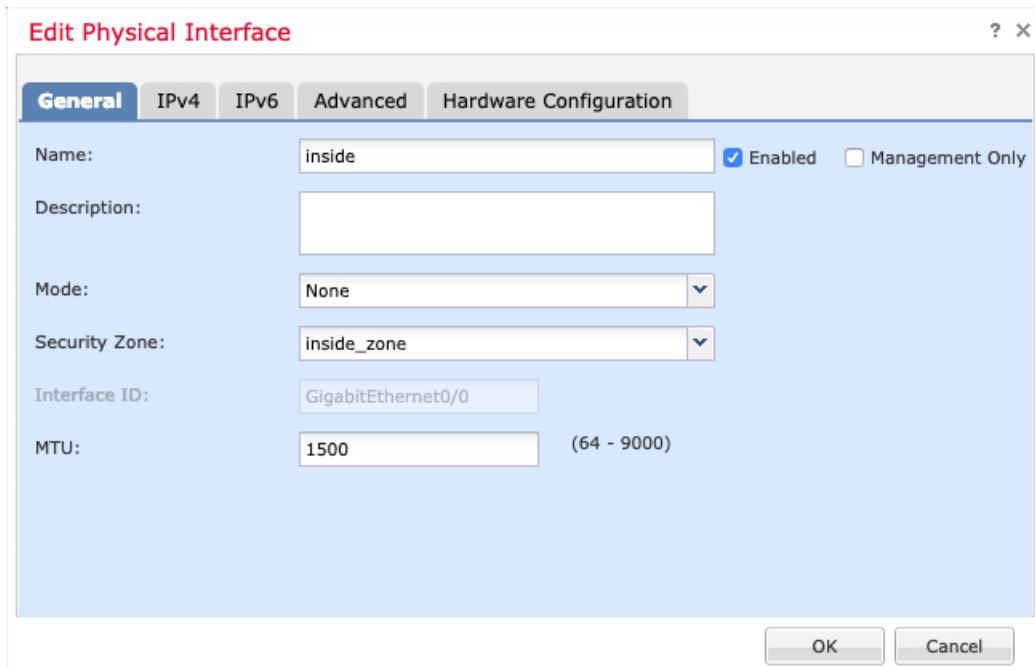
ステップ 1 [デバイス (Devices)]>[デバイス管理 (Device Management)] の順に選択し、ファイアウォールの をクリックします。

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せんが、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。

The screenshot shows the 'Edit Physical Interface' configuration window. The 'IPv4' tab is active. The 'IP Type' dropdown is set to 'Use Static IP'. The 'IP Address' field contains '192.168.1.1/24'. To the right of the IP address field, there is a small text example: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'.

- [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。

Edit Physical Interface ? x

General IPv4 IPv6 Advanced Hardware Configuration

Name: Enabled Management Only

Description:

Mode: ▼

Security Zone: ▼

Interface ID:

MTU: (64 - 9000)

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 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。

NAT の設定

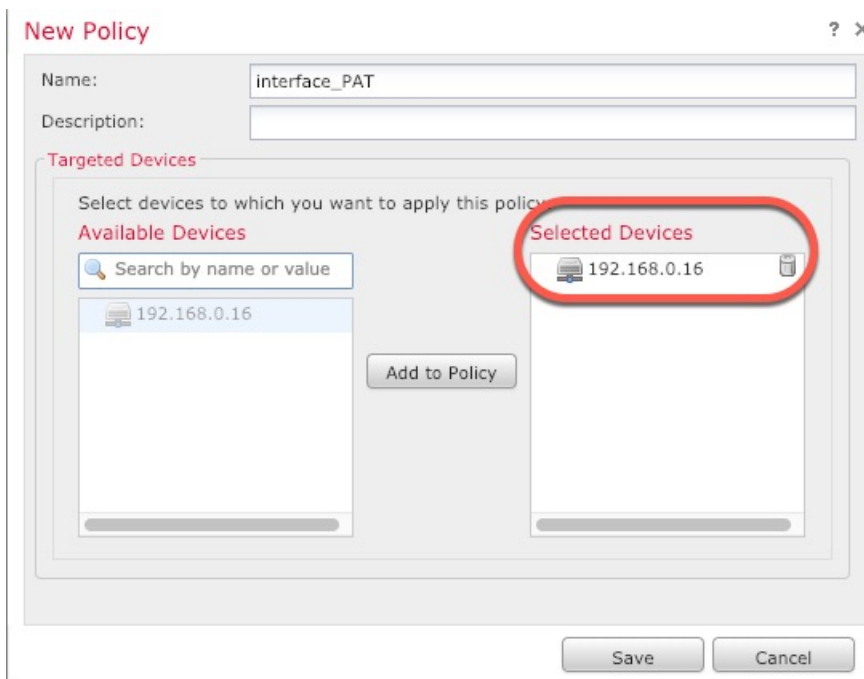
NAT の設定

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。

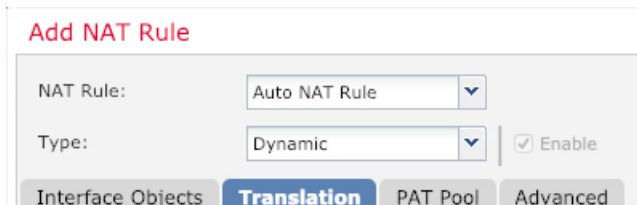


ポリシーが Management Center に追加されます。引き続き、ポリシーにルールを追加する必要があります。

ステップ 3 [ルール の追加 (Add Rule)] をクリックします。

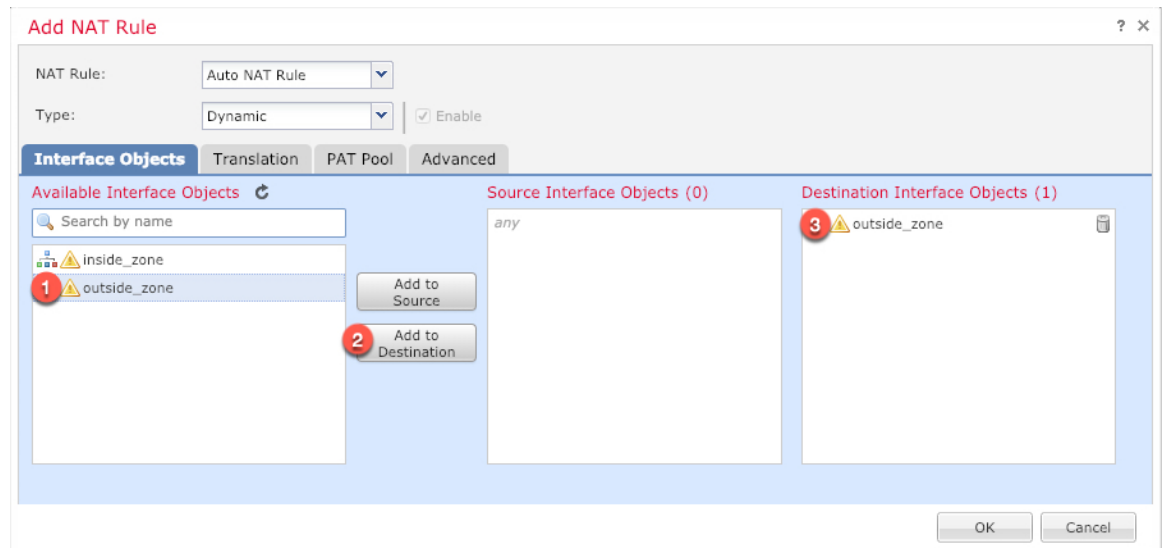
[NATルール の追加 (Add NAT Rule)] ダイアログボックスが表示されます。

ステップ 4 基本ルールのオプションを設定します。

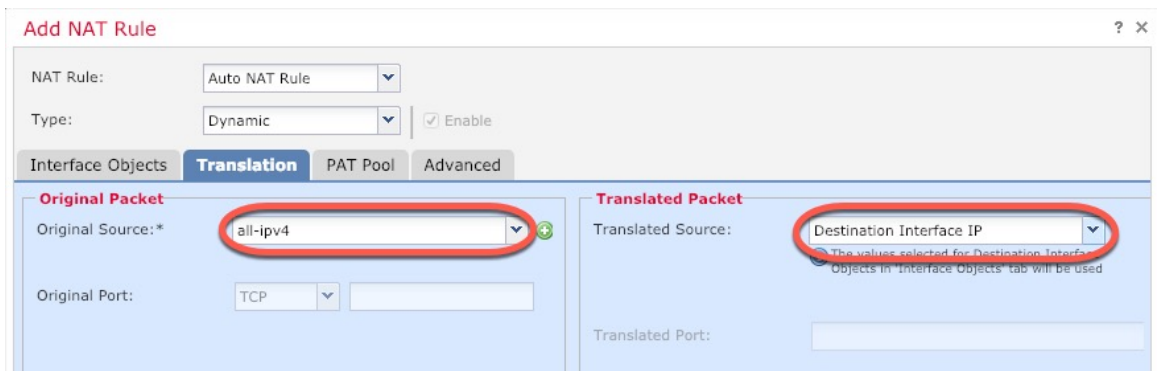


- [NATルール (NAT Rule)] : [自動NATルール (Auto NAT Rule)] を選択します。
- [タイプ (Type)] : [ダイナミック (Dynamic)] を選択します。

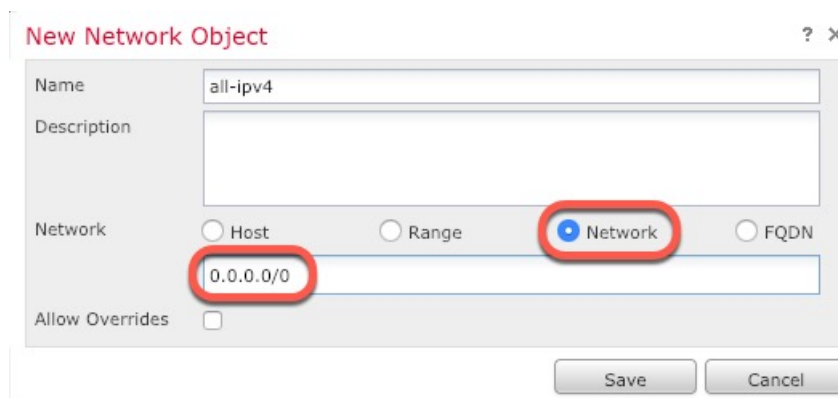
ステップ 5 [インターフェイスオブジェクト (Interface objects)] ページで、[使用可能なインターフェイスオブジェクト (Available Interface Objects)] 領域から [宛先インターフェイスオブジェクト (Destination Interface Objects)] 領域に外部ゾーンを追加します。



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。

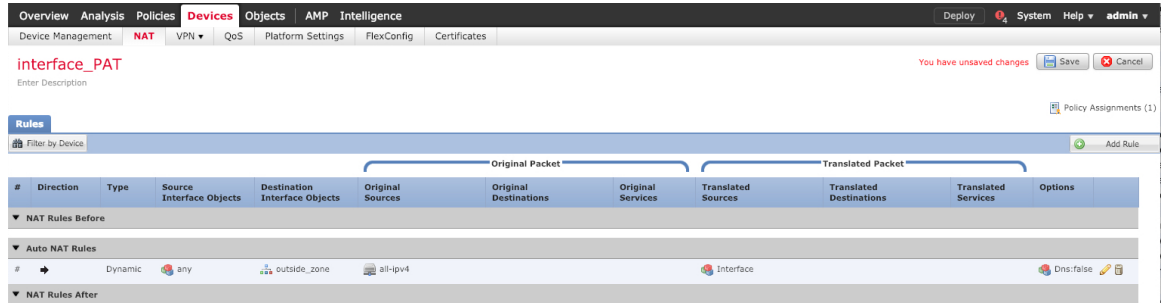


(注) 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [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。

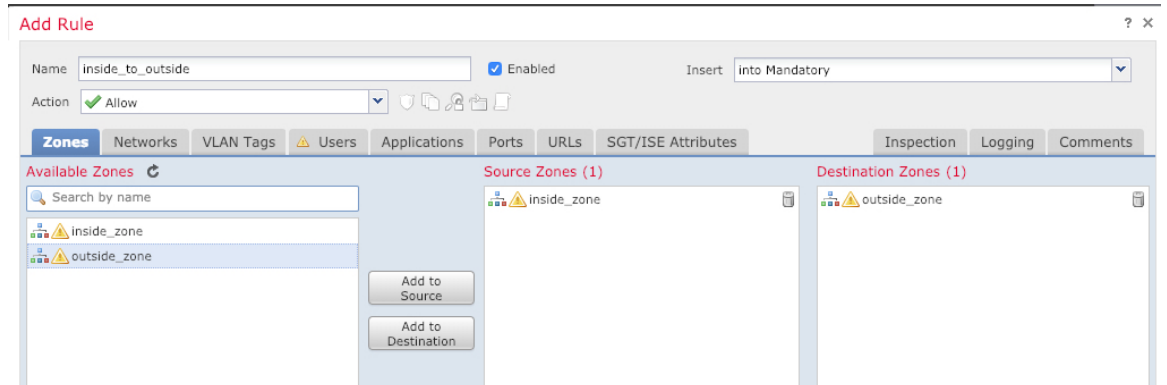
内部から外部へのトラフィックの許可

脅威に対する防衛 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、脅威に対する防衛 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。

The screenshot shows the Management Center interface for configuring a rule. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' section is active, showing 'Access Control' and 'Access Control' sub-sections. The rule name 'ftd_ac_policy' is entered in the 'Enter Description' field. Below this, there are fields for 'Prefilter Policy' (Default Prefilter Policy), 'SSL Policy' (None), and 'Identity Policy' (None). The 'Rules' section is expanded, showing a table with columns: #, Name, Source Zo..., Dest Zones, Source Ne..., Dest Netw..., VLAN Tags, Users, Applications, Source Po..., Dest Ports, URLs, ISE/SGT A..., and Action. A rule is listed with Name 'Mandatory - ftd_ac_policy (1-1)', Source 'inside_to_outside', Dest 'inside_zone', and Action 'Allow'. Below the table, there is a note: 'There are no rules in this section. Add Rule or Add Category'. The 'Default Action' is set to 'Access Control: Block All Traffic'.

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。SSH は診断論理インターフェイスに対してサポートされません。



- (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。



(注) SSH を介した 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、ルールに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 [セキュア シェル (Secure Shell)] 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。
- [セキュリティゾーン (Security Zones)] : 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、選択されたセキュリティゾーンの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。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 8: [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 9:すべて展開

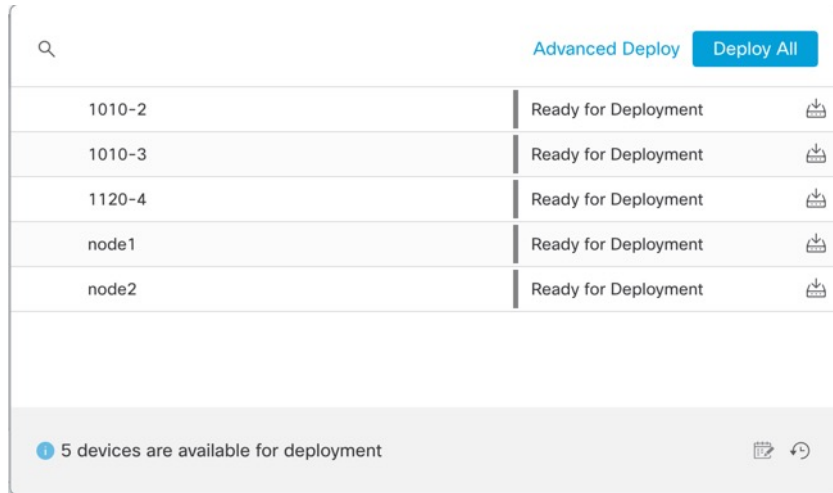
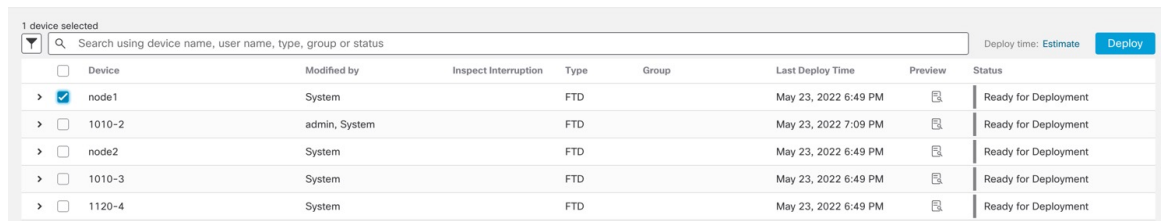
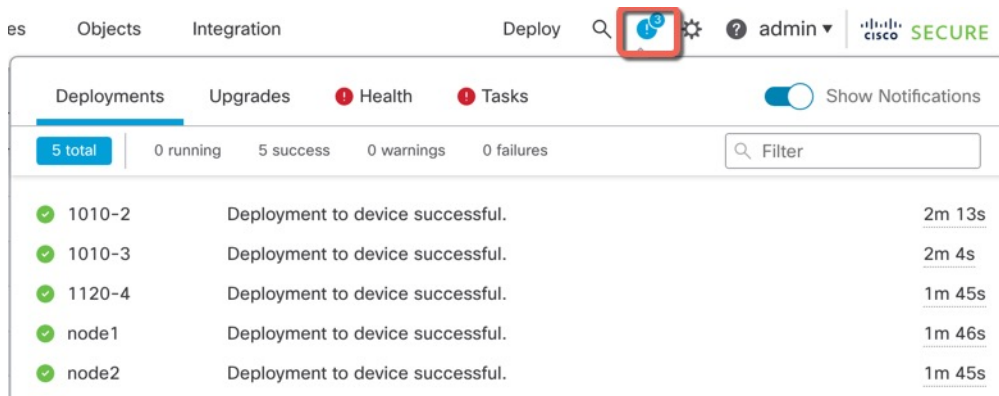


図 10:高度な展開



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 11: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。Firepower 2100 には DB-9 to RJ-45 シリアルケーブルが付属しているため、接続するためにはサードパーティ製のシリアル to USB ケーブルが必要です。お使い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#
```

データインターフェイスでの管理接続のトラブルシューティング

モデルのサポート：Threat Defense

専用の管理インターフェイスを使用する代わりに、Management Center にデータインターフェイスを使用する場合は、Management Center で脅威に対する防御のインターフェイスとネットワークの設定を変更するときに接続を中断しないように注意します。脅威に対する防御を Management Center に追加した後に管理インターフェイスタイプを変更する場合（データから管理へ、または管理からデータへ）、インターフェイスとネットワークの設定が正しく構成されていないと、管理接続が失われる可能性があります。

このトピックは、管理接続が失われた場合のトラブルシューティングに役立ちます。

管理接続ステータスの表示

Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] > [FMCアクセスの詳細 (FMC Access Details)] > [接続ステータス (Connection Status)] ページの順に選択して管理接続のステータスを確認します。

管理接続のステータスを表示するには、脅威に対する防御 CLI で、**sftunnel-status-brief** コマンドを入力します。**sftunnel-status** を使用して、より完全な情報を表示することもできます。

ダウン状態の接続の出力例を次に示します。ピアチャネルの「接続先」情報やハートビート情報が表示されていません。

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
```

```
Last disconnect reason : Both control and event channel connections with peer went
down
```

アップ状態の接続の出力例を次に示します。ピアチャネルとハートビート情報が表示されています。

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to
'10.10.17.202' via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Threat Defense ネットワーク情報の表示

脅威に対する防御 CLI で、管理および Management Center アクセス データ インターフェイスのネットワーク設定を表示します。

show network

```
> show network
===== [ System Information ] =====
Hostname           : 5516X-4
DNS Servers        : 208.67.220.220,208.67.222.222
Management port    : 8305
IPv4 Default route
  Gateway           : data-interfaces
IPv6 Default route
  Gateway           : data-interfaces

===== [ br1 ] =====
State              : Enabled
Link               : Up
Channels           : Management & Events
Mode               : Non-Autonegotiation
MDI/MDIX           : Auto/MDIX
MTU                : 1500
MAC Address        : 28:6F:7F:D3:CB:8D
----- [ IPv4 ] -----
Configuration      : Manual
Address            : 10.99.10.4
Netmask            : 255.255.255.0
Gateway            : 10.99.10.1
----- [ IPv6 ] -----
Configuration      : Disabled

===== [ Proxy Information ] =====
State              : Disabled
Authentication     : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers        :
Interfaces         : GigabitEthernet1/1

===== [ GigabitEthernet1/1 ] =====
State              : Enabled
```

```

Link                : Up
Name                : outside
MTU                 : 1500
MAC Address         : 28:6F:7F:D3:CB:8F
-----[ IPv4 ]-----
Configuration      : Manual
Address            : 10.89.5.29
Netmask            : 255.255.255.192
Gateway            : 10.89.5.1
-----[ IPv6 ]-----
Configuration      : Disabled

```

Management Center への Threat Defense の登録の確認

脅威に対する防御 CLI で、Management Center 登録が完了したことを確認します。このコマンドは、管理接続の現在のステータスを表示するものではないことに注意してください。

show managers

```

> show managers
Type                : Manager
Host                : 10.89.5.35
Registration        : Completed
>

```

Management Center に ping する

脅威に対する防御 CLI で、次のコマンドを使用して、データインターフェイスから Management Center に ping します。

ping fmc_ip

脅威に対する防御 CLI で、次のコマンドを使用して、管理インターフェイスから Management Center に ping します。これは、バックプレーンを介してデータインターフェイスにルーティングされます。

ping system fmc_ip

Threat Defense 内部インターフェイスでのパケットのキャプチャ

脅威に対する防御 CLI で、内部バックプレーンインターフェイス (nlp_int_tap) でパケットをキャプチャして、管理パケットが送信されているかどうかを確認します。

capture name interface nlp_int_tap trace detail match ip any any

show capture name trace detail

内部インターフェイスのステータス、統計、およびパケット数の確認

脅威に対する防御 CLI で、内部バックプレーンインターフェイス (nlp_int_tap) に関する情報を参照してください。

show interace detail

```

> show interface detail
[...]
```

```

Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
  (Full-duplex), (1000 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 0000.0100.0001, MTU 1500
  IP address 169.254.1.1, subnet mask 255.255.255.248
  37 packets input, 2822 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  5 packets output, 370 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  input queue (blocks free curr/low): hardware (0/0)
  output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
  37 packets input, 2304 bytes
  5 packets output, 300 bytes
  37 packets dropped
    1 minute input rate 0 pkts/sec,  0 bytes/sec
    1 minute output rate 0 pkts/sec,  0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
  Interface number is 14
  Interface config status is active
  Interface state is active

```

ルーティングと NAT の確認

脅威に対する防御 CLI で、デフォルトルート (S*) が追加されていること、および管理インターフェイス (nlp_int_tap) に内部 NAT ルールが存在することを確認します。

show route

```

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF

Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*      0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C       10.89.5.0 255.255.255.192 is directly connected, outside
L       10.89.5.29 255.255.255.255 is directly connected, outside

>

```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface
service tcp 8305 8305
   translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface service
tcp ssh ssh
   translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6 service tcp 8305 8305
   translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
   translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
   translate_hits = 0, untranslate_hits = 0
>
```

その他の設定の確認

次のコマンドを参照して、他のすべての設定が存在することを確認します。これらのコマンドの多くは、Management Center の [デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] > [FMCアクセスの詳細 (FMC Access Details)] > [CLI出力 (CLI Output)] ページでも確認できます。

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address fmc_ip

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
  preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.89.5.29(169.254.1.2):51231 outside 10.89.5.35:8305, idle 0:00:04,
bytes 86684, flags UxIO
TCP nlp_int_tap 10.89.5.29(169.254.1.2):8305 outside 10.89.5.35:52019, idle 0:00:02,
bytes 1630834, flags UIO
>
```

DDNS の更新が成功したかどうかを確認する

脅威に対する防御 CLI で、DDNS の更新が成功したかどうかを確認します。

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
```

```
DDNS: IDB SB total = 0
```

更新に失敗した場合は、**debug http** コマンドと **debug ssl** コマンドを使用します。証明書の検証が失敗した場合は、ルート証明書がデバイスにインストールされていることを確認します。

```
show crypto ca certificates trustpoint_name
```

DDNS の動作を確認するには :

```
show ddns update interface fmc_access_ifc_name
```

```
> show ddns update interface outside
```

```
Dynamic DNS Update on outside:
  Update Method Name Update Destination
  RBD_DDNS not available
```

```
Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Management Center ログファイルの確認

<https://cisco.com/go/fmc-reg-error> を参照してください。

Management Center の接続が失われた場合の構成のロールバック

Management Center で脅威に対する防御 のデータインターフェイスを使用し、ネットワーク接続に影響する Management Center からの構成の変更を展開する場合、脅威に対する防御 の構成を最後に展開した構成にロールバックして、管理接続を復元できます。その後、ネットワーク接続が維持されるように Management Center で構成設定を調整して再展開できます。ロールバック機能は、接続が失われていない場合でも使用でき、このトラブルシューティングの状況以外でも使用できます。

次のガイドラインを参照してください。

- 前回の展開のみ 脅威に対する防御 でローカルに使用できます。さらに以前の展開にロールバックすることはできません。
- ロールバックは、高可用性またはクラスタリングの導入ではサポートされていません。
- ロールバックは、Management Center で設定できる構成にのみ影響します。たとえば、ロールバックは、脅威に対する防御 CLI でのみ設定できる専用管理インターフェイスに関連するローカル構成には影響しません。**configure network management-data-interface** コマンドを使用した最後の Management Center 展開後にデータインターフェイス設定を変更し、**rollback** コマンドを使用すると、それらの設定は保持されないことに注意してください。最後に展開された Management Center 設定にロールバックされます。
- UCAPL/CC モードはロールバックできません。

- 以前の展開中に更新されたアウトオブバンド SCEP 証明書データはロールバックできません。
- ロールバック中に、現在の設定がクリアされるため、接続がドロップされます。

始める前に

モデルのサポート : Threat Defense

手順

ステップ 1 脅威に対する防御 CLI で、以前の構成へロールバックします。

configure policy rollback

ロールバック後、脅威に対する防御はロールバックが正常に完了したことを Management Center に通知します。Management Center では、構成がロールバックされたことを示すバナーが展開画面に表示されます。

ロールバックが失敗した場合、一般的な展開の問題について <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html> を参照してください。場合によっては、Management Center アクセスの復元後にロールバックが失敗することがあります。この場合、Management Center の構成の問題を解決して、Management Center から再展開できます。

例 :

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....
.....
>
```

ステップ 2 管理接続が再確立されたことを確認します。

Management Center で、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [デバイス (Device)] > [管理 (Management)] > [FMCアクセスの詳細 (FMC Access Details)] > [接続ステータス (Connection Status)] ページの順に選択して管理接続のステータスを確認します。

管理接続のステータスを表示するには、脅威に対する防御 CLI で、**sftunnel-status-brief** コマンドを入力します。

接続の再確立に 10 分以上かかる場合は、接続のトラブルシューティングを行う必要があります。データインターフェイスでの管理接続のトラブルシューティング (41 ページ) を参照してください。

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 [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 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 分間待つ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。

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 コンフィギュレーションガイド](#)」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。