



Firepower 1100 Threat Defense スタートアップガイド：ローカル管理ネットワーク上の Management Center

最終更新：2026 年 9 月 10 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



第 1 章

はじめる前に

Cisco Firepower 1000 は、ビジネスの復元力、容易な管理、脅威に対する防御機能を提供します。優れたパフォーマンスを安定して確保しつつ、高度な脅威検出機能を有効にできます。Cisco Firepower 1000 シリーズは、小規模オフィスからリモートブランチまでさまざまなユースケースに対応します。

専用の管理ネットワークで Cisco Secure Firewall Management Center を使用してファイアウォールを管理します。

- [ファイアウォールの電源の投入](#) (1 ページ)
- [インストールされているアプリケーション \(Firewall Threat Defense または ASA\) の確認](#) (3 ページ)
- [Firewall Threat Defense CLI へのアクセス](#) (4 ページ)
- [バージョンの確認と再イメージ化](#) (5 ページ)
- [ライセンスの取得](#) (6 ページ)
- [\(必要な場合\) ファイアウォールの電源オフ](#) (7 ページ)

ファイアウォールの電源の投入

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。ロッカー電源スイッチは、ソフト通知を提供します。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) ファイアウォールを初めて起動するときは、Firewall Threat Defense の初期化に約 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

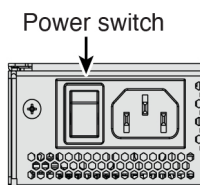
ロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

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。

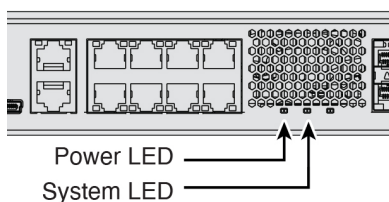
ステップ 2 シャーシの背面で、電源コードに隣接するロッカー電源スイッチを使用して電源をオンにします。

図 1: 電源スイッチ



ステップ 3 LED の現在のステータスを確認します。

図 2: LED



- 電源 LED : 緑色で点灯している場合は、ファイアウォールの電源がオンになっていることを意味します。
- システム (S) LED : 次の動作を参照してください。

表 1: システム (S) LED の動作

LED の動作	説明	デバイスの電源を入れた後の時間 (分: 秒)
緑色で高速点滅	起動中	01:00
オレンジ色で高速点滅 (エラー状態)	起動に失敗しました	01:00
緑色で点灯	アプリケーションがロードされました	15:00 ~ 30:00

LED の動作	説明	デバイスの電源を入れた後の時間（分：秒）
オレンジ色で点灯（エラー状態）	アプリケーションのロードに失敗しました	15:00 ～ 30:00

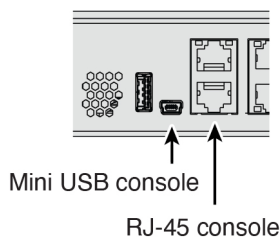
インストールされているアプリケーション（Firewall Threat Defense または ASA）の確認

Firewall Threat Defense と ASA の両方のアプリケーションが、ハードウェアでサポートされています。コンソールポートに接続し、出荷時にインストールされているアプリケーションを確認します。

手順

ステップ 1 いずれかのポートタイプを使用してコンソールポートに接続します。

図 3: コンソールポート



ステップ 2 CLI プロンプトを参照して、ファイアウォールで Firewall Threat Defense または ASA が実行されているかどうかを確認します。

Firewall Threat Defense

Firepower ログイン（FXOS）プロンプトが表示されます。ログインして新しいパスワードを設定せずに、切断することができます。ログインを完了する必要がある場合は、[Firewall Threat Defense CLI へのアクセス（4 ページ）](#)を参照してください。

```
firepower login:
```

ASA

ASA プロンプトが表示されます。

```
ciscoasa>
```

ステップ3 間違ったアプリケーションが実行されている場合は、[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。

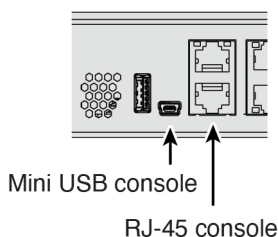
Firewall Threat Defense CLI へのアクセス

設定またはトラブルシューティングのためにCLIにアクセスする必要がある場合があります。

手順

ステップ1 いずれかのポートタイプを使用してコンソールポートに接続します。

図 4: コンソールポート



ステップ2 FXOS に接続します。ユーザー名 **admin** とパスワード（デフォルトは **Admin123**）を使用して CLI にログインします。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。

```
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3 Firewall Threat Defense CLI に変更します。

（注）

初期セットアップに Firewall Device Manager を使用する場合は、Firewall Threat Defense CLI にアクセスしないでください（アクセスすると、CLI セットアップが開始されます）。

connect ftd

Firewall Threat Defense CLI に初めて接続すると、初期セットアップを完了するように求められます。

例：

```
firepower# connect ftd
>
```

Firewall 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 プロンプトに戻ります。

例：

```
> exit
firepower#
```

バージョンの確認と再イメージ化

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。

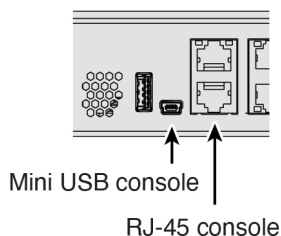
実行するバージョン

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> で説明されているリリース戦略を参照することもできます。

手順

ステップ1 いずれかのポートタイプを使用してコンソールポートに接続します。

図 5: コンソールポート



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) 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に静的 IP アドレスを設定する必要がある場合は、次のコマンドを入力します。

```
scope fabric-interconnect a
```

```
set out-of-band static ip ip netmask netmask gw gateway
```

```
commit-buffer
```

- 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。

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。

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。

ライセンスの取得

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。[Smart Software Manager](#) にアカウントがない場合は、リンクをクリックして[新しいアカウントを設定](#)します。

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

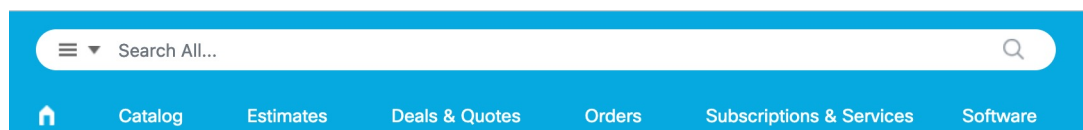
Firewall Threat Defense には次のライセンスがあります。

- Essentials : 必須
- IPS
- マルウェア防御

- URL フィルタリング
- Cisco Secure Client

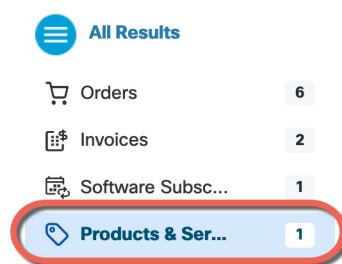
1. 自身でライセンスを追加する必要がある場合は、[Cisco Commerce Workspace](#) で [すべて検索 (Search All)] フィールドを使用します。

図 6: ライセンス検索



2. ライセンス PID を検索します。必要な PID については、発注ガイドを参照してください。
3. 結果から、[製品とサービス (Products & Services)] を選択します。

図 7: 結果



(必要な場合) ファイアウォールの電源オフ

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ません。

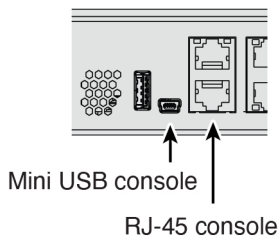
CLI におけるファイアウォールの電源の切断

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ファイアウォールの電源を切断できます。

手順

ステップ 1 いずれかのポートタイプを使用してコンソールポートに接続します。

図 8: コンソール ポート



ステップ 2 FXOS CLI でローカル管理モードに接続します。

```
firepower # connect local-mgmt
```

ステップ 3 システムをシャットダウンします。

```
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 4 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。シャットダウンが完了すると、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 5 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。

Firewall Management Center を使用したファイアウォールの電源切断

Firewall Management Center を使用してシステムを適切にシャットダウンします。

手順

ステップ 1 ファイアウォールをシャットダウンします。

- [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- 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。
- [デバイス (Device)] タブをクリックします。
- [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。

e) 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 2 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。シャットダウンが完了すると、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 3 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。



第 2 章

ファイアウォールのケーブル接続と登録

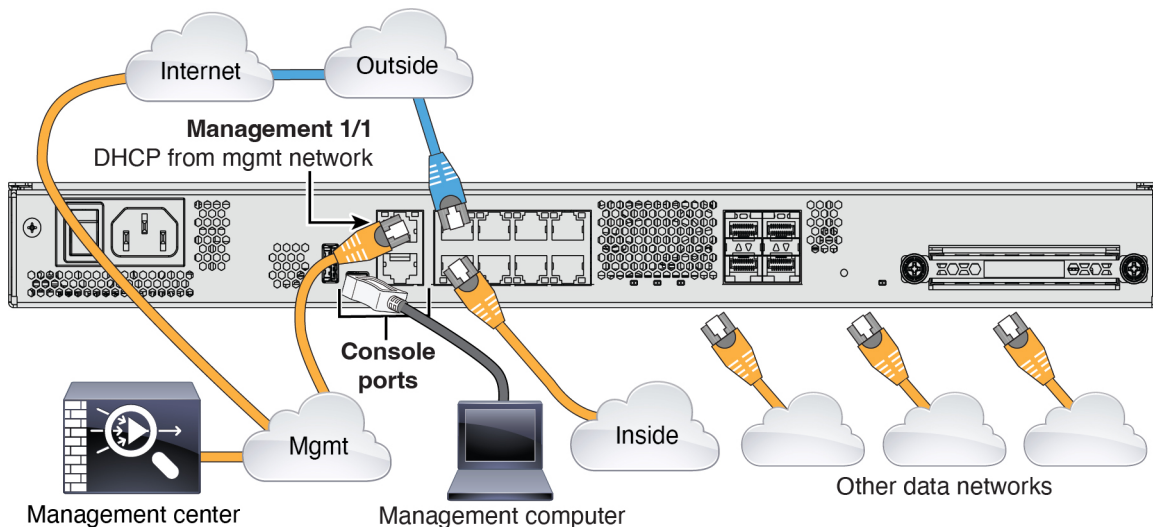
ファイアウォールをケーブル接続し、ファイアウォールを Firewall Management Center に登録します。

- [ファイアウォールのケーブル接続](#) (11 ページ)
- [初期設定の実行](#) (12 ページ)
- [Firewall Management Center でのファイアウォールの登録](#) (20 ページ)

ファイアウォールのケーブル接続

Firewall Management Center を専用の管理 1/1 インターフェイスに接続します。管理ネットワークには、更新のためのインターネットへのアクセスが必要です。たとえば、ファイアウォール自体を介して（たとえば、内部ネットワークに接続することによって）管理ネットワークをインターネットに接続できます。

詳細については、[ハードウェア設置ガイド](#)を参照してください。



(注)

正確なポート設定は、モデルによって異なります。

- a) 外部インターフェイスと管理インターフェイスを設定します。

図 10: インターネットへのファイアウォールの接続

Connect firewall to Internet

The initial access control policy will enforce the following actions.
You can edit the policy after setup.

Rule 1 Trust Outbound Traffic This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.	Default Action Block all other traffic The default action blocks all other traffic.
---	---

Outside Interface Address

Connect Ethernet1/1 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4

Using DHCP
 ▼

Configure IPv6

Using DHCP
 ▼

NEXT

Don't have internet connection?
[Skip device setup](#) ⓘ

1. [外部インターフェイスアドレス (Outside Interface Address)] : 高可用性の実装を予定している場合は、静的 IP アドレスを使用します。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。ウィザードの完了後に PPPoE を設定できます。
2. [管理インターフェイス (Management Interface)] : 管理インターフェイスの IP アドレスの設定はセットアップウィザードに含まれませんが、次のオプションを設定できます。静的 IP アドレスを使用する必要がある場合は、手順 [ステップ 4 \(15 ページ\)](#) を参照してください。

[DNSサーバ (DNS Servers)] : システムの管理アドレス用の DNS サーバ。デフォルトは OpenDNS パブリック DNS サーバです。

ファイアウォールのホスト名

- b) [時刻設定 (NTP) (Time Setting (NTP))] を設定し、[次へ (Next)] をクリックします。

図 11:時刻設定 (NTP)

Time Setting (NTP)

System Time: 11:56:20AM October 03 2024 -06:00

Time Zone for Scheduling Tasks

(UTC+00:00) UTC ▼

NTP Time Server

Default NTP Servers ▼ ⓘ

Server Name

0.sourcefire.pool.ntp.org

1.sourcefire.pool.ntp.org

2.sourcefire.pool.ntp.org

[NEXT](#)

- 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。

Register with Cisco Smart Software Manager

Register with Cisco Smart Software Manager to use the full functionality of this device and to apply subscription licenses.

[What is smart license? ⓘ](#)

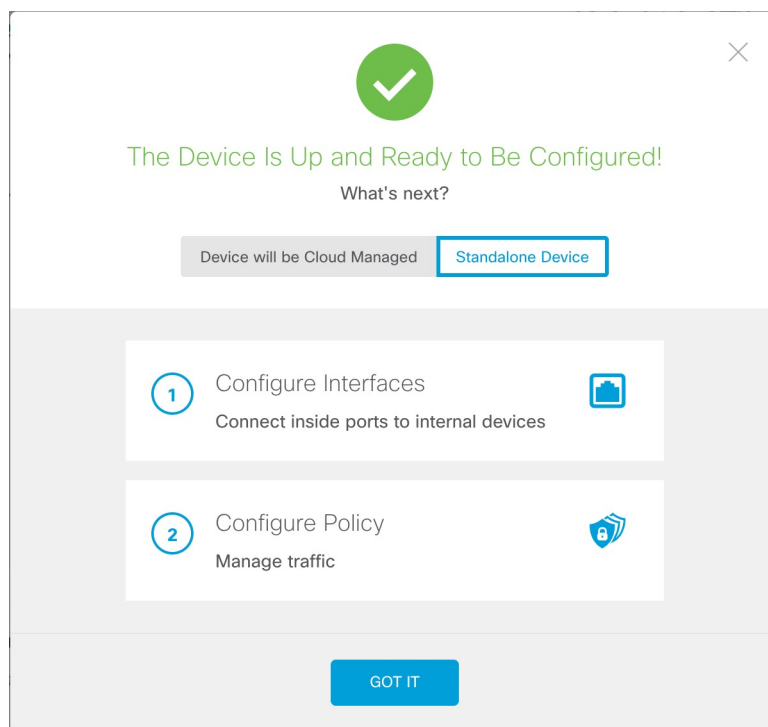
☐ **Continue with evaluation period: Start 90-day evaluation period without registration**
Recommended if device will be cloud managed. [Learn More ⓘ](#)

Please make sure you register with Cisco before the evaluation period ends.
 Otherwise you will not be able to make any changes to the device configuration.

Firewall 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 Firewall Management CenterSecurity Cloud Control で実行されます。

- d) [終了 (Finish)] をクリックします。

図 12: 次のステップ



e) [スタンドアロンデバイス (Standalone Device)] を選択し、[了解 (Got It)] を選択します。

ステップ 4 (任意) 管理インターフェイスに静的 IP アドレスを設定します。[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。

ステップ 5 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)] のサマリーにあるリンクをクリックします。

ステップ 6 [デバイス (Device)] > [システム設定 (System Settings)] > [集中管理 (Central Management)] の順に選択し、[続行 (Proceed)] をクリックして Firewall Management Center Security Cloud Control に登録します。

[Management Center/SCC/Details] を設定します。

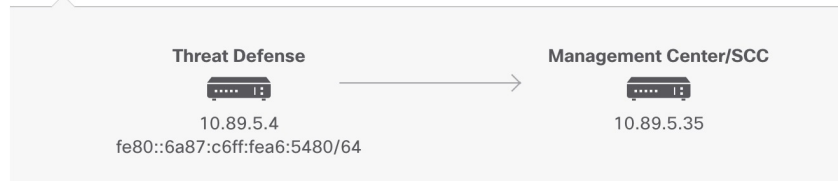
(注)

古いバージョンでは、「SCC」の代わりに「CDO」と表示されることがあります。

図 13 : Management Center/SCC の詳細

Management Center/SCC Details

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

☒ Yes ☐ No

Management Center/SCC Hostname or IP Address

10.89.5.35

Management Center/SCC Registration Key

....

NAT ID

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

11204

Connectivity Configuration

Threat Defense Hostname

1120-4

DNS Server Group

CustomDNSServerGroup

Management Center/SCC Access Interface

management (Management1/1)

Type: Static | IP Address: 10.89.5.4 / 255.255.255.192

[Edit](#)

CANCEL

CONNECT

- [Do you know the Management Center/SCC Hostname or IP address] に対し、IP アドレスまたはホスト名を使用して Firewall Management Center に到達できる場合は [Yes] を、Firewall Management Center が NAT の内側にあるか、パブリック IP アドレスまたはホスト名がない場合は [No] をクリックします。
- [Yes] を選択した場合は、[Management Center/SCC Hostname/IP Address] に入力します。
- [Management Center/SCC Registration Key] を指定します。

このキーは、ファイアウォールを登録するときに Firewall 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 2 ～ 36 文字である必要があります。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、Firewall Management Center に登録する複数のファイアウォールに使用できます。

d) [NAT ID] を指定します。

この識別子は、Firewall Management Center でも指定する任意の 1 回限りの文字列です。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 2 ～ 36 文字である必要があります。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、Firewall Management Center に登録する他のファイアウォールには使用「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で使用されます。IP アドレス/NAT ID の認証後にのみ、登録キーがチェックされます。

ステップ 7 [接続の設定（Connectivity Configuration）] を設定します。

a) [Threat Defenseのホスト名（Threat Defense Hostname）] を指定します。

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

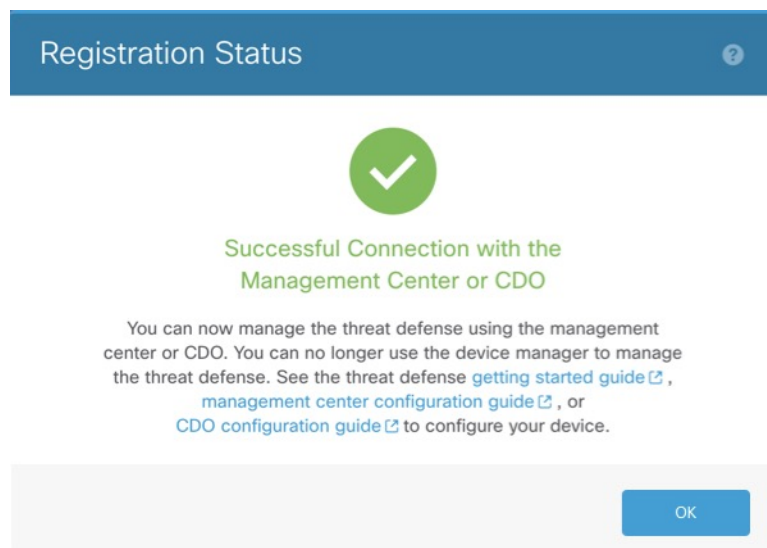
これはすでに設定していますが、既存のグループを選択するか、新しいグループを作成します。デフォルトの DNS グループは **CiscoUmbrellaDNSServerGroup** と呼ばれ、OpenDNS サーバーが含まれます。

c) [Management Center/SCC Access Interface] で [Management Interface] をクリックします。

ステップ 8 [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、Firewall Management CenterSecurity Cloud Control 登録の現在のステータスが表示されます。

図 14: 正常接続



ステップ 9 ステータス画面で [Saving Management Center/Registration Settings] の手順を実行したら Firewall Management CenterSecurity Cloud Control に移動し、ファイアウォールを追加します。Firewall Management Center でのファイアウォールの登録（20 ページ）を参照してください。

初期設定 : CLI

CLIセットアップスクリプトを使用して、専用の管理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 コンソールポートに接続して Firewall Threat Defense CLI にアクセスします。 [Firewall Threat Defense CLI へのアクセス \(4 ページ\)](#) を参照してください。

ステップ2 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を完了します。

(注)

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

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]
```

```
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
```

ガイダンス : これらのタイプのアドレスの少なくとも 1 つについて **y** を入力します。

```
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]: 10.10.10.1

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'

Manage the device locally? (yes/no) [yes]: no
```

ガイダンス : Firewall Management Center を使用する場合は、**no** と入力します。

```
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'
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 3 Firewall Management Center を指定します。

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

- {hostname | IPv4_address | IPv6_address | DONTRESOLVE}— Firewall Management Center の FQDN または IP アドレスを指定します。Firewall 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。この場合は、ファイアウォールが、到達可能な IP アドレスまたはホスト名を持っている必要があります。
- reg_key : Firewall Threat Defense を登録するときに Firewall 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 2 ～ 36 文字である必要があります。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 : Firewall 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。NAT ID は 2 ～ 36 文字である必要があります。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、Firewall 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.
```

Firewall Management Center でのファイアウォールの登録

基本設定用の登録キーと NAT ID による手動プロビジョニングを使用して、Firewall Management Center にデバイスを追加します。

ファイアウォールを Firewall Management Center に登録します。

手順

ステップ 1 Firewall Management Center にログインします。

a) 次の URL を入力します。

`https://fmc_ip_address`

b) ユーザー名とパスワードを入力します。

c) [ログイン (Log In)] をクリックします。

ステップ 2 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。

ステップ 3 [追加 (Add)] ドロップダウンメニューから、[デバイス (Device)] を選択します。

ステップ 4 [Registration Key]、[Basic]、[Next] の順にクリックします。

図 15: デバイスの登録方法

The screenshot shows the 'Add device' wizard in the Firewall Management Center. The wizard has three steps: 1. Device registration method, 2. Device details, and 3. Initial device configuration. The first step is active and highlighted with a blue border. It contains two options for registration: 'Registration key' and 'Serial number'. The 'Registration key' option is selected with a blue radio button. Below these options, there are two radio buttons for the initial device configuration method: 'Basic' (selected) and 'Device template'. The 'Basic' option is described as applying basic configuration, including the access control policy. The 'Device template' option is described as preconfiguring settings using a template, requiring a compatible template to exist. At the bottom of the wizard, there are 'Cancel' and 'Next' buttons.

Add device

1 Device registration method

2 Device details

3 Initial device configuration

Device registration method

Registration key
Identify the same one-time registration key on the device and in the management center.

Serial number
Identify the device by serial number. On the device, you don't have to configure anything (zero-touch provisioning).

Choose the initial device configuration method:

☒ **Basic**
Apply basic configuration, including the access control policy.

☐ **Device template**
Preconfigure settings using a template. A compatible **template** must exist (either a default template or one you added) before continuing.

Cancel Next

ステップ 5 デバイスの詳細を設定して **[Next]** をクリックします。

図 16: デバイスの詳細

Add device

✓ Device registration method

2 Device details

3 Initial device configuration

Device details

Domain *

Global/Leaf1

Hostname or IP address

10.89.5.41

e.g. server.example.com or 192.168.1.1

Display name *

3110-1

Registration key *

....

Enter the same registration key you set on the device. This key doesn't have to be unique per device. Use alphanumeric characters (A-Z, a-z, 0-9) and the hyphen (-), between 2 and 36 characters.

Unique NAT ID ⓘ

31101

Enter the same NAT ID if you set one on the device. This key needs to be unique per device. Use alphanumeric characters (A-Z, a-z, 0-9) and the hyphen (-), between 2 and 36 characters.

☐ **Analytics-only management center**

When using Security Cloud Control as your primary manager, you can use an On-Prem management center for analytics.

Cancel

Back Next

- **[Domain]** : マルチドメイン環境で、リーフドメインを選択します。
- **[Device group]** : 単一ドメイン環境で、デバイスを **[Device group]** に追加します。
- **[Hostname or IP address]** : 追加するデバイスの IP アドレスまたはホスト名を入力します。デバイスの IP アドレスが不明な場合は (NAT の背後にある場合など)、このフィールドを空欄のままにします。
- **[Display name]** : Firewall Management Center に表示するデバイスの名前を入力します。この名前は変更できません。
- **[Registration key]** : 初期構成と同じ登録キーを入力します。
- **[Unique NAT ID]** : 初期設定と同じ識別子を入力します。
- **[Analytics-only management center]** : 。

ステップ 6 デバイスの初期設定を行います。

図 17: デバイスの初期設定

Add device

- Device registration method
- Device details
- Initial device configuration**

Initial device configuration

Access control policy *
Default Access Control Policy ⓘ +

Smart licensing
Ensure that your smart licensing account has the required licenses.

Is this device physical or virtual?
☒ Physical device ☐ Virtual device

License type	Includes
☒ Essentials	Base firewall capabilities
☒ Carrier	GTP/GPRS, Diameter, SCTP, M3UA
☒ IPS	Intrusion Policy
☒ Malware Defense	File Policy
☒ URL Filtering	URL Reputation
☒ RA VPN Premier ⓘ	RA VPN

☒ **Transfer packets**
For each intrusion event, the device sends event information and the packet that triggered the event to the management center for inspection. If you disable it, only event information will be sent to the management center; the packet will not be sent.

[Cancel](#) [Back](#) [Add device](#)

- [アクセスコントロールポリシー（Access control policy）]：登録時にデバイスに展開する最初のポリシーを選択するか、新しいポリシーを作成します。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き、[[追加（Add）]（+）]、[すべての通信をブロック（Block all traffic）]の順に選択します。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。
- [スマートライセンス（Smart licensing）]：ライセンスを選択します。
 - このデバイスは物理と仮想のどちらですか？：[物理デバイス（Physical device）]
 - [ライセンスタイプ（License type）]：デバイスに割り当てる各ライセンスのタイプを確認します。

デバイスを追加した後、ライセンスを適用することもできます。

- [パケットの転送（Transfer packets）]：このオプションを有効にすると、侵入イベントが発生するたびに、デバイスが検査のためにパケットを Firewall Management Center に転送します。

侵入イベントごとに、デバイスは、イベント情報とイベントをトリガーしたパケットを検査のために Firewall 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 Firewall Management Center に送信され、パケットは送信されません。

ステップ 7 [Add device] をクリックします。

Firewall Management Center がデバイスのハートビートを確認して通信を確立するまでに、最大 2 分かかる場合があります。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。デバイスの登録に失敗した場合は、次の項目を確認してください。

- **ping** : デバイスの CLI にアクセスし、次のコマンドを使用して Firewall 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。デバイスの IP アドレスを変更する必要がある場合は、**configure network {ipv4 | ipv6} manual** コマンドを使用します。

- 登録キー、NAT ID、および Firewall 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、デバイスで登録キーと 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。



第 3 章

基本ポリシーの設定

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します。

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

セキュリティポリシーをカスタマイズして、より高度な検査を含めることもできます。

- [インターフェイスの設定 \(25 ページ\)](#)
- [DHCP サーバーの設定 \(31 ページ\)](#)
- [デフォルトルートの追加 \(32 ページ\)](#)
- [NAT の設定 \(35 ページ\)](#)
- [アクセスコントロールルールの設定 \(39 ページ\)](#)
- [設定を展開する \(42 ページ\)](#)

インターフェイスの設定

初期設定に Firewall Device Manager を使用する場合、次のインターフェイスが事前設定されます。

- イーサネット 1/1：「外部」、DHCP からの IP アドレス、IPv6 自動設定
- イーサネット 1/2：「内部」、192.168.95.1/24
- デフォルトルート：外部インターフェイスで DHCP を介して取得

Firewall Management Center に登録する前に Firewall Device Manager 内で追加のインターフェイス固有の設定を実行した場合、その設定は保持されます。

次の例では、静的アドレスを持つルーテッドモードの内部インターフェイスと、DHCPを使用するルーテッドモードの外部インターフェイスを設定します。また、内部 Web サーバー用の DMZ インターフェイスも追加します。

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 18: インターフェイス

Device Routing Interfaces Inline Sets DHCP VTEP								
					Q Search by name	Sync Device	Add Interfaces ▼	
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
● Management0/0	management	Physical				Disabled	Global	Q < >
✎ GigabitEthernet0/0		Physical				Disabled		✎
✎ GigabitEthernet0/1		Physical				Disabled		✎
✎ GigabitEthernet0/2		Physical				Disabled		✎
✎ GigabitEthernet0/3		Physical				Disabled		✎
✎ GigabitEthernet0/4		Physical				Disabled		✎
✎ GigabitEthernet0/5		Physical				Disabled		✎
✎ GigabitEthernet0/6		Physical				Disabled		✎
✎ GigabitEthernet0/7		Physical				Disabled		✎

ステップ 3 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。

図 19: [General] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:
inside

☒ Enabled
☐ Management Only

Description:

Mode:
None

Security Zone:
inside_zone

Interface ID:
GigabitEthernet0/1

MTU:
1500
(64 - 9000)

Priority:
0 (0 - 65535)

Propagate Security Group Tag: ☐

NVE Only:
☐

- a) [セキュリティゾーン (SecurityZone)] 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。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、内部ゾーンから外部ゾーンへのトラフィックは有効にするが外部ゾーンから内部ゾーンへのトラフィックは有効にしないアクセスコントロールポリシーを設定します。

内部インターフェイスが事前に設定されている場合、これらのフィールドの残りの部分はオプションです。

- b) 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。
- c) [有効 (Enabled)] チェックボックスをオンにします。
- d) [モード (Mode)] は [なし (None)] に設定したままにします。
- e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]: 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 20: [IPv4] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

IP Type:
Use Static IP

IP Address:
192.168.1.1/24
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。

図 21: [IPv6] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configur

Basic Address Prefixes Settings DHCP

Enable IPV6: ☐

Enforce EUI 64: ☐

Link-Local address:

Autoconfiguration: ☒

Obtain Default Route: ☐

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の [編集 (Edit)] (🔗) をクリックします。

図 22: [General] タブ

Edit Physical Interface

General	IPv4	IPv6	Path Monitoring	Hardware
Name: outside				
☒ Enabled ☐ Management Only				
Description:				
Mode: None				
Security Zone: outside_zone				
Interface ID: GigabitEthernet0/0				
MTU: 1500 (64 - 9000)				
Priority: 0 (0 - 65535)				
Propagate Security Group Tag: ☐				
NVE Only: ☐				

- a) [セキュリティゾーン (SecurityZone)] 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。

外部インターフェイスが事前に設定されている場合、これらのフィールドの残りの部分はオプションです。

- b) 48 文字までの [名前 (Name)] を入力します。

たとえば、インターフェイスに「outside」という名前を付けます。

- c) [有効 (Enabled)] チェックボックスをオンにします。
 d) [モード (Mode)] は [なし (None)] に設定したままにします。
 e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4] : [DHCPの使用 (Use DHCP)] を選択し、次のオプションのパラメータを設定します。
 - [DHCP を使用してデフォルトルートを取得 (Obtain default route using DHCP)] : DHCP サーバーからデフォルトルートを取得します。

- [DHCPルートメトリック (DHCP route metric)] : アドミニストレーティブ ディスタンスを学習したルートに割り当てます (1 ~ 255)。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。

図 23: [IPv4] タブ

Edit Physical Interface

General IPv4 IPv6 Path Mc

IP Type:
Use DHCP

Obtain default route using DHCP: ☒

DHCP route metric:
1
(1 - 255)

- [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 24: [IPv6] タブ

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configu

Basic Address Prefixes Settings DHCP

Enable IPV6: ☐

Enforce EUI 64: ☐

Link-Local address:

Autoconfiguration: ☒

Obtain Default Route: ☐

f) [OK] をクリックします。

ステップ 5 たとえば、Web サーバーをホストするように DMZ インターフェイスを設定します。

- 使用するインターフェイスの [編集 (Edit)] (🔗) をクリックします。
- [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 DMZ 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、**dmz_zone** という名前のゾーンを追加します。

- 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 **dmz** という名前を付けます。

- [有効 (Enabled)] チェックボックスをオンにします。
- [モード (Mode)] は [なし (None)] に設定したままにします。

- f) 必要に応じて、[IPv4] タブと [IPv6] タブのいずれかまたは両方をクリックし、IP アドレスを設定します。
- g) [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 を使用してファイアウォールから IP アドレスを取得するようにする場合、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 25: DHCPサーバー

The screenshot displays the DHCP Server configuration interface. The top navigation bar includes tabs for Device, Routing, Interfaces, Inline Sets, DHCP (active), VTEP, and SNMP. A left-hand menu lists DHCP Server, DHCP Relay, and DDNS. The main configuration area includes:

- Ping Timeout: 50 (range 10 - 10000 ms)
- Lease Length: 3600 (range 300 - 10,48,575 sec)
- Auto-Configuration: unchecked checkbox
- Interface: dropdown menu
- Override Auto Configured Settings:
 - Domain Name: text input
 - Primary DNS Server and Secondary DNS Server: dropdown menus
 - Primary WINS Server and Secondary WINS Server: dropdown menus

 At the bottom, there are tabs for Server (highlighted with a red box) and Advanced. A + Add button (also highlighted with a red box) is located in the top right of the configuration area. Below the tabs is a table with headers Interface, Address Pool, and Enable DHCP Server. The table currently shows 'No records to display'.

ステップ 3 [サーバー (Server)] エリアで、[追加 (Add)] をクリックし、以下のオプションを設定します。

図 26: サーバーの追加

Add Server ⓘ

Interface*
inside ▼

Address Pool*
192.168.1.2-192.168.1.55
(2.2.2.10-2.2.2.20)

☒ Enable DHCP Server

Cancel OK

- [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名を選択します。
- [アドレスプール (Address Pool)] : IP アドレスの範囲を設定します。IP アドレスは、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
- [DHCPサーバーを有効にする (Enable DHCP Server)] : 選択したインターフェイスの DHCP サーバーを有効にします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存 (Save)] をクリックします。

デフォルトルートの追加

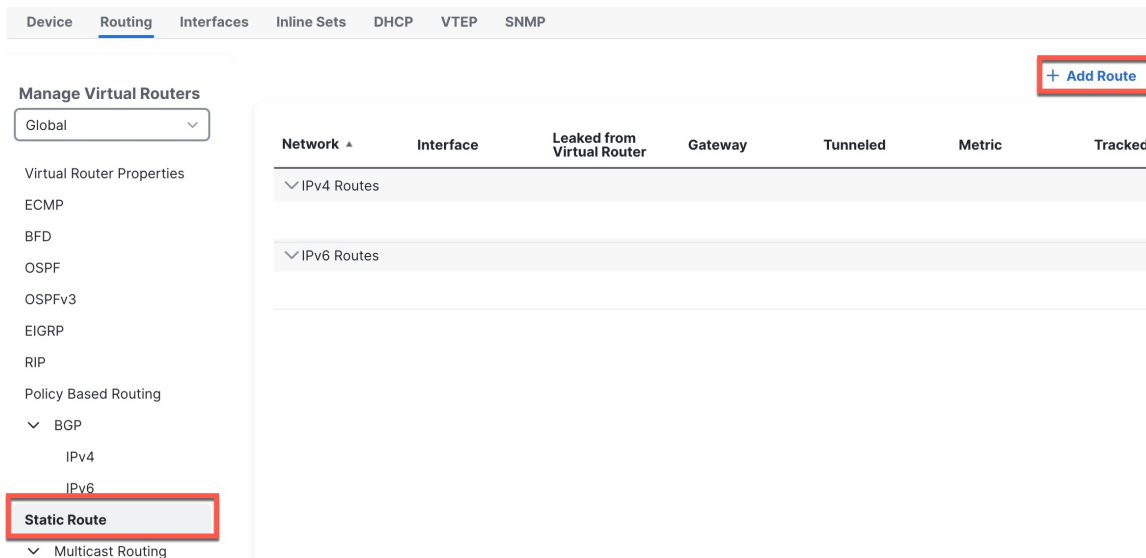
デフォルトルートは通常、外部インターフェイスから到達可能なアップストリームルータを指し示します。DHCPから外部アドレスを取得した場合は、デバイスがすでにデフォルトルートを受信している可能性があります。手動でルートを追加する必要がある場合は、次の手順を実行します。

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 [ルーティング (Routing)] > [静的ルート (Static Routes)] を選択します。

図 27: 静的ルート



DHCP サーバーからデフォルトルートを受信した場合は、このテーブルに表示されます。

ステップ 3 [ルートを追加 (Add route)] をクリックして、次のオプションを設定します。

図 28: 静的ルート追加の設定

Add Static Route Configuration

Type: ☒ IPv4 ☐ IPv6

Interface*
outside

(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Search

- any-ipv4
- gateway
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8

Add

Selected Network

- any-ipv4

Gateway*
gateway +

Metric:
1
(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:
+

Cancel OK

- [タイプ (Type)] : 追加するスタティックルートのタイプに応じて、[IPv4] または [IPv6] オプションボタンをクリックします。
- [インターフェイス (Interface)] : 出力インターフェイスを選択します。通常は外部インターフェイスです。
- [使用可能なネットワーク (Available Network)] : IPv4 デフォルトルートの場合は [any-ipv4] を選択し、IPv6 デフォルトルートの場合は [any-ipv6] を選択し、[追加 (Add)] をクリックして [選択したネットワーク (Selected Network)] リストに移動させます。
- [ゲートウェイ (Gateway)] または [IPv6ゲートウェイ (IPv6 Gateway)] : このルートのネクストホップであるゲートウェイルータを入力または選択します。IP アドレスまたはネットワーク/ホストオブジェクトを指定できます。

ステップ 4 [OK] をクリックします。

ルートがスタティックルートテーブルに追加されます。

ステップ 5 [保存 (Save)] をクリックします。

NAT の設定

この手順では、内部クライアントが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する NAT ルールを作成します。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] の順に選択し、[新しいポリシー (New Policy)] 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 29:新しいポリシー

New Policy

Name:
FTD_policy

Description:

Targeted Devices
Select devices to which you want to apply this policy.

Available Devices and Templates
Search by name or value

192.168.0.124
192.168.0.155

Selected Devices and Templates

192.168.0.124
192.168.0.155

Add to Policy

Cancel Save

ポリシーが Firewall 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 30: NAT ポリシー

FTD_Policy

Show Warnings Save Cancel

Enter Description

Rules NAT Exemptions Policy Assignments (1)

Filter by Device Filter Rules Add Rule

	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
						Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
NAT Rules Before												
Auto NAT Rules												
NAT Rules After												

ステップ 3 [ルールの追加 (Add Rule)] をクリックします。

ステップ 4 基本ルールのおプションを設定します。

図 31: 基本ルールのおプション

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

☒ Enable

Interface Objects **Translation**

- [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 32: インターフェイス オブジェクト

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

Search by name

inside

1 outside

Add to Source

2 Add to Destination

Source Interface Objects (0)

any

Destination Interface Objects (1)

3 outside

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 33: 変換

Interface Objects	Translation	PAT Pool	Advanced
Original Packet		Translated Packet	
Original Source:* all-ipv4 +		Translated Source: Destination Interface IP	
Original Port: TCP		Translated Port: 	

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

- [元の送信元 (Original Source)] : [追加 (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 34: 新しいネットワークオブジェクト

New Network Object

Name

Description

Network
☐ Host ☐ Range ☒ Network ☐ FQDN

☐ Allow Overrides

Cancel Save

(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。

アクセスコントロールルールの設定

ファイアウォールを登録したときに、基本の [すべての通信をブロック (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、ファイアウォールを通過する通信を許可するためのルールをポリシーに追加する必要があります。アクセス コントロール ポリシーには、順番に評価される複数のルールを含めることができます。

次の手順では、内部ゾーンから外部ゾーンへのすべてのトラフィックを許可するアクセス制御ルールを作成します。

手順

ステップ 1 [ポリシー (Policies)] > [セキュリティポリシー (Security policies)] > [アクセス制御 (Access Control)] を選択し、デバイス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。

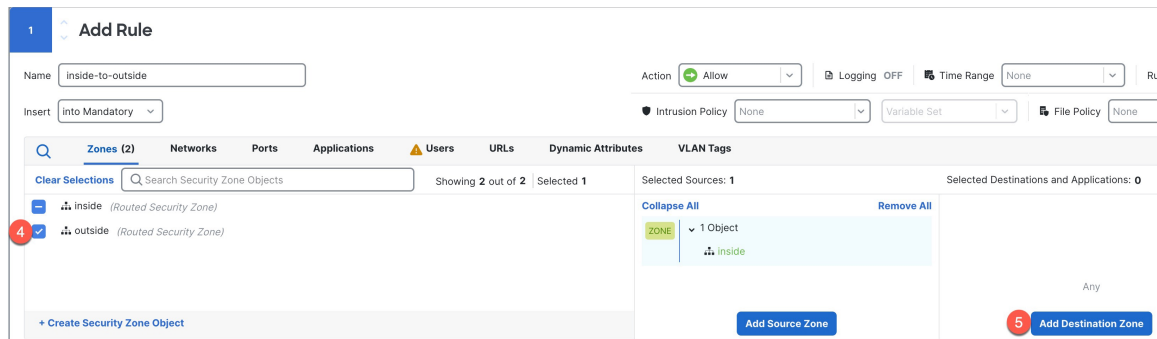
ステップ 2 [ルールを追加 (Add Rule)] をクリックし、次のパラメータを設定します。

図 35: 送信元ゾーン (Source Zone)

The screenshot shows the 'Add Rule' configuration page. The 'Name' field is set to 'inside-to-outside'. The 'Action' is set to 'Allow'. The 'Intrusion Policy' is set to 'None'. The 'Zones' tab is selected, showing a list of zones: 'inside (Routed Security Zone)' and 'outside (Routed Security Zone)'. The 'inside' zone is selected. A red circle with the number '1' is next to the 'Name' field, a red circle with the number '2' is next to the 'inside' zone selection, and a red circle with the number '3' is next to the 'Add Source Zone' button.

1. このルールに名前を付けます (たとえば、**inside-to-outside**)。
2. [ゾーン (Zones)] から内部ゾーンを選択します。
3. [送信元ゾーンの追加 (Add Source Zone)] をクリックします。

図 36:宛先ゾーン (Destination Zone)



4. [ゾーン (Zones)] から外部ゾーンを選択します。

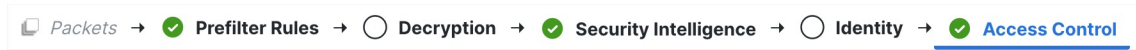
5. [宛先ゾーンを追加 (Add Destination Zone)] をクリックします。

他の設定はそのままにしておきます。

ステップ 3 (任意) パケットフロー図でポリシータイプをクリックして、関連付けられたポリシーをカスタマイズします。

[プレフィルタ (Prefilter)]、[復号 (Decryption)]、[セキュリティインテリジェンス (Security Intelligence)]、および[アイデンティティ (Identity)] ポリシーは、アクセス制御ルールの前に適用されます。これらのポリシーをカスタマイズする必要はありませんが、ネットワークのニーズを把握した後、信頼できるトラフィックに fastpath を適用 (処理をバイパス) したりトラフィックをブロックしてその後の処理が不要になるようにすることで、ネットワークのパフォーマンスを向上させることができます。

図 37: アクセス制御の前に適用されるポリシー



- [プレフィルタルール (Prefilter Rules)] : デフォルトのプレフィルタポリシーは、他のルールが適用される (分析する) すべてのトラフィックを通過させます。デフォルトポリシーに加えることができる唯一の変更は、トンネルトラフィックを「ブロックする」ことです。それ以外では、新しいプレフィルタポリシーを作成して、分析 (通過) 、fastpath 処理 (以降のチェックをバイパス) 、またはブロックできるアクセス コントロール ポリシーに関連付けることができます。

プレフィルタを使用すると、ブロックまたは fastpath 処理のいずれかによって、トラフィックがさらに進む前に処理することで、パフォーマンスを向上させることができます。新しいポリシーでは、「トンネル」ルールと「プレフィルタ」ルールを追加できます。トンネルルールを使用すると、プレーンテキスト (非暗号化) のパススルートンネルを fastpath 処理、ブロック、または再ゾーン化できます。プレフィルタルールを使用すると、IP アドレス、ポート、およびプロトコルで識別される非トンネルトラフィックを fastpath 処理またはブロックできます。

たとえば、ネットワーク上のすべての FTP トラフィックをブロックし、管理者からの SSH トラフィックを高速パスする場合は、新しいプレフィルタ ポリシーを追加できます。

- [復号 (Decryption)] : デフォルトでは、復号は適用されません。復号は、ネットワークトラフィックをディープインスペクションに公開する方法です。ほとんどの場合、トラフィックを復号する必要はなく、法的に許可されている場合にのみ復号できます。ネットワークを最大限に保護するために、重

要なサーバーへのトラフィックや、信頼できないネットワークセグメントからのトラフィックには、復号ポリシーを使用することをお勧めします。

- [セキュリティ インテリジェンス (Security Intelligence)] : (IPS ライセンスが必要) セキュリティ インテリジェンスはデフォルトで有効になっています。セキュリティ インテリジェンスは、悪意のあるアクティビティに対するもう 1 つの早期防御で、さらなる処理のために接続をアクセス コントロール ポリシーに渡す前に適用されます。セキュリティ インテリジェンスは、レピュテーション インテリジェンスを使用して、シスコの脅威インテリジェンス組織である Talos が提供する IP アドレス、URL、およびドメイン名との接続を迅速にブロックします。必要に応じて、IP アドレス、URL、ドメインを追加または削除できます。

(注)

IPS ライセンスがない場合、このポリシーは、アクセス コントロール ポリシーで有効と表示されていても展開されません。

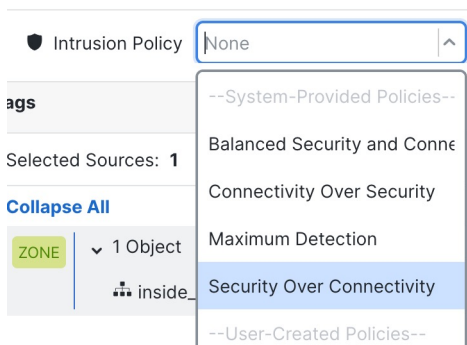
- [アイデンティティ (Identity)] : アイデンティティはデフォルトでは適用されません。アクセス コントロール ポリシーによるトラフィックの処理を許可する前に、ユーザーに認証を要求できます。

ステップ 4 (任意) アクセス制御ルールの後に適用される侵入ポリシーを追加します。

侵入ポリシーは、トラフィックのセキュリティ違反を検査する定義済みの一連の侵入検出および侵入防止設定です。Firewall Management Center には、多数のシステム提供のポリシーが含まれており、そのまま有効にすることもカスタマイズすることもできます。この手順では、システム提供のポリシーを有効にします。

- a) [侵入ポリシー (Intrusion Policy)] ドロップダウンリストをクリックします。

図 38: システム提供の侵入ポリシー



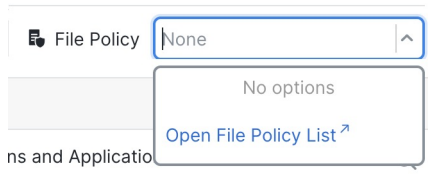
- b) リストからシステム提供のポリシーを 1 つ選択します。

ほとんどのユースケースでは、[バランスのとれたセキュリティと接続 (Balanced Security and Connections)] を推奨しています。

ステップ 5 (任意) アクセス制御ルールの後に適用されるファイルポリシーを追加します。

- a) [ファイルポリシー (File Policy)] ドロップダウンリストをクリックし、既存のポリシーを選択するか、[ファイルポリシーリストを開く (Open File Policy List)] を選択してポリシーを追加します。

図 39: ファイルポリシー (File Policy)



新しいポリシーの場合は、[[ポリシー (Policies)] > [セキュリティポリシー (Security policies)] > [マルウェアとファイル (Malware & File)] ページが別のタブで開きます。

- b) ポリシーの作成の詳細については、[Cisco Secure Firewall Device Manager コンフィギュレーション ガイド](#)を参照してください。
- c) [ルールを追加 (Add Rule)] ページに戻り、ドロップダウンリストから新しく作成したポリシーを選択します。

ステップ 6 [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 7 [保存 (Save)] をクリックします。

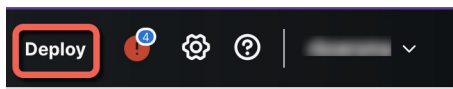
設定を展開する

設定の変更をデバイスに展開します。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

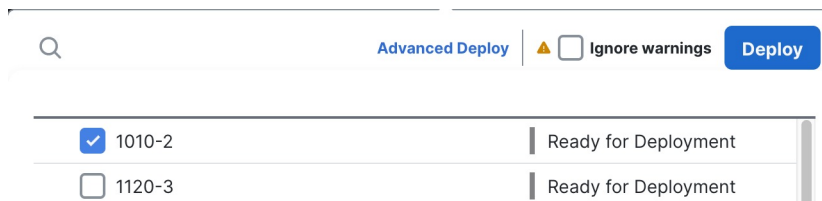
ステップ 1 右上の [展開 (Deploy)] をクリックします。

図 40: 展開



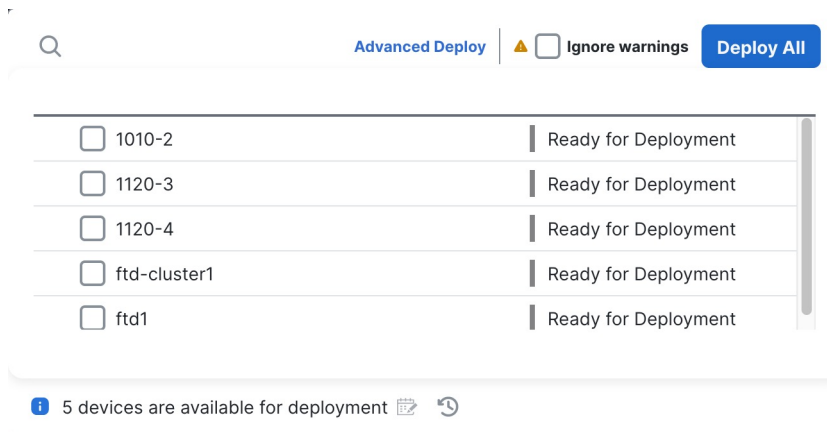
ステップ 2 迅速な展開の場合は、特定のデバイスのチェックボックスをオンにして [展開 (Deploy)] をクリックします。

図 41: 選択したものを展開



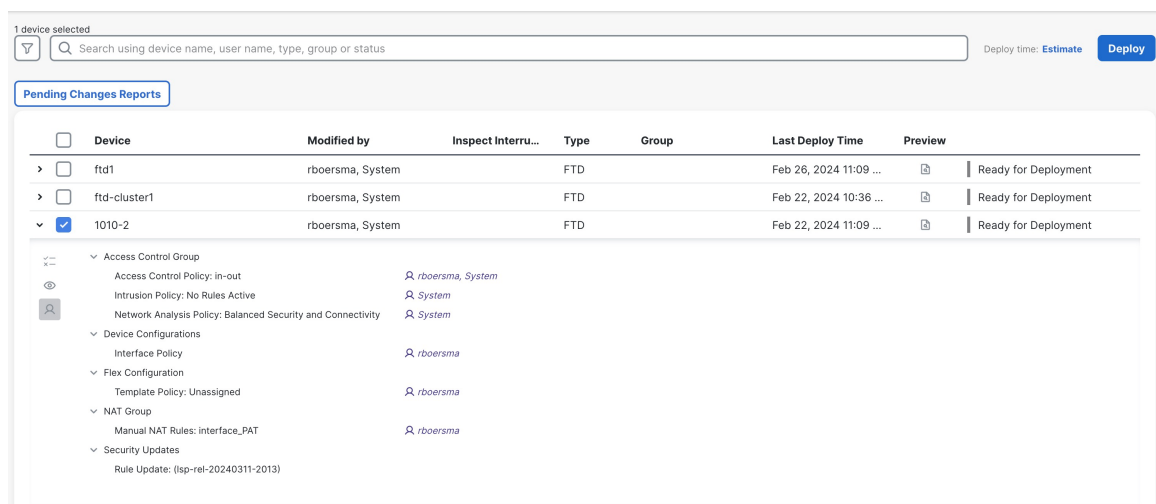
または、[すべて展開（Deploy All）] をクリックしてすべてのデバイスに展開します。

図 42: すべて展開



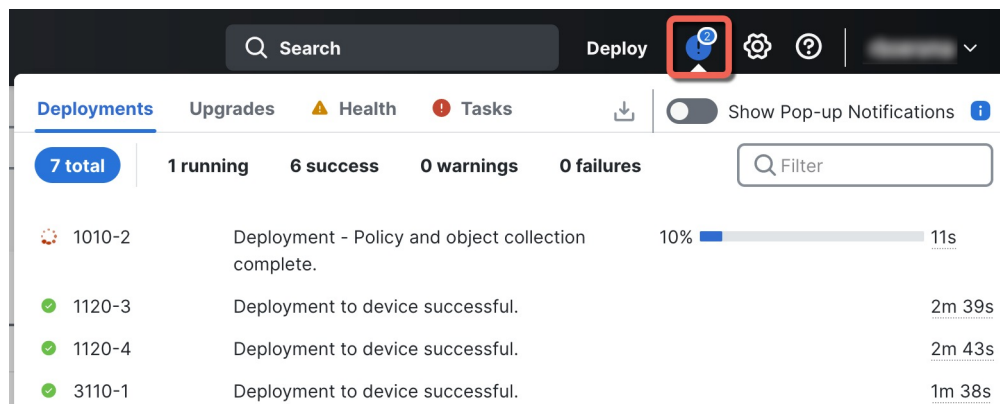
それ以外の場合は、追加の展開オプションを設定するために、[高度な展開（Advanced Deploy）] をクリックします。

図 43: 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 44: 展開ステータス



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。