



Cisco Secure Firewall 4200 Threat Defense スタートアップガイド ド：クラウド提供型 Firewall Management Center

最終更新：2025 年 3 月 7 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

分散拠点にファイアウォールをインストールし、Security Cloud Control（旧称、Cisco Defense Orchestrator）を使用して外部インターフェイスで管理します。



(注) 外部管理は、クラスタリングではサポートされません。この場合は、Security Cloud Control アクセスに管理インターフェイスを使用します。このガイドでは、特に外部管理について説明しますが、管理インターフェイスを使用した管理については、[Cisco Security Cloud Control のクラウド提供型 Firewall Management Center](#) を使用した [Firewall Threat Defense の管理](#) を参照してください。マルチインスタンス展開についても、そのガイドを参照してください。

- [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（Threat Defense または ASA）の確認](#)（3 ページ）
- [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）
- [ライセンスを取得する](#)（7 ページ）
- [（必要な場合）ファイアウォールの電源の切断](#)（8 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、Threat Defense の初期化に約 15 ～ 30 分かかります。

始める前に

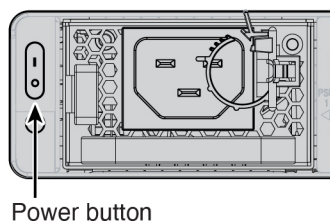
ファイアウォールに対して信頼性の高い電力を供給することが重要です（無停電電源装置（UPS）を使用するなど）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

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。

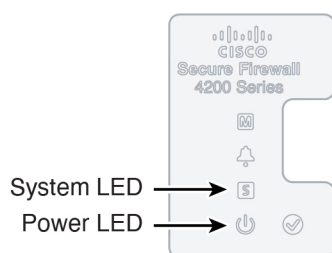
ステップ 2 シャーシの背面で、電源コードに隣接するロッカー電源スイッチを使用して電源をオンにします。

図 1: 電源ボタン



ステップ 3 ファイアウォールの背面にある電源LEDを確認します。緑色に点灯している場合は、ファイアウォールの電源が入っています。

図 2: システムおよび電源 LED



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

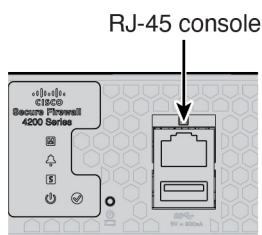
インストールされているアプリケーション（Threat Defense または ASA）の確認

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 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 Threat Defense または ASA が実行されているかどうかを確認します。

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、[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。

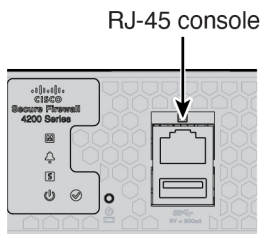
Threat Defense CLI へのアクセス

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 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 Threat Defense CLI に変更します。

（注）

初期セットアップに Device Manager を使用する場合は、ゼロタッチプロビジョニングを使用する場合は、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

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
>
```

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。

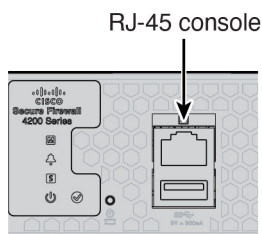
実行するバージョン

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 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

(注)

次のエラーが発生する場合は、変更をコミットする前に DHCP を無効にする必要があります。DHCP を無効にするには、次の手順に従います。

```
firepower /fabric-interconnect* # commit-buffer
Error: Update failed: [Management ipv4 address (IP <ip> / net mask <netmask> ) is not
in the same network of current DHCP server IP range <ip - ip>].
Either disable DHCP server first or config with a different ipv4 address.]
firepower /fabric-interconnect* # exit
firepower* # scope system
firepower /system* # scope services
firepower /system/services* # disable dhcp-server
firepower /system/services* # 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。

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

- d) ファイアウォールをシャットダウンします。 [\(必要な場合\) ファイアウォールの電源の切断 \(8 ページ\)](#) を参照してください。

ライセンスを取得する

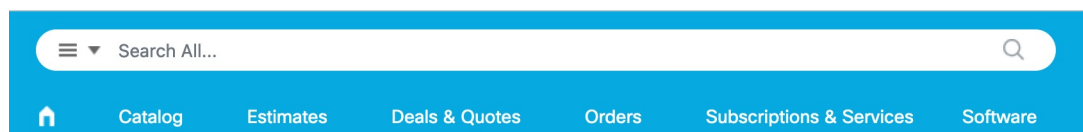
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートソフトウェアライセンシングアカウントにリンクされています。[Smart Software Manager](#) にアカウントがない場合は、リンクをクリックして[新しいアカウントを設定します](#)。

まだの場合は、[Smart Software Manager](#) に [Security Cloud Control](#) 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。詳しい手順については、[Security Cloud Control のマニュアル](#)を参照してください。

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
 - キャリア (Diameter、GTP/GPRS、M3UA、SCTP)
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. 次のライセンス PID を検索します。



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

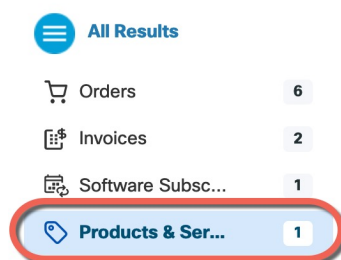
- Essentials :
 - 自動的に含める
- IPS、マルウェア防御、および URL の組み合わせ :
 - L-FPR4215T-TMC=
 - L-FPR4225T-TMC=
 - L-FPR4245T-TMC=

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

- L-FPR4215T-TMC-1Y
 - L-FPR4215T-TMC-3Y
 - L-FPR4215T-TMC-5Y
 - L-FPR4225T-TMC-1Y
 - L-FPR4225T-TMC-3Y
 - L-FPR4225T-TMC-5Y
 - L-FPR4245T-TMC-1Y
 - L-FPR4245T-TMC-3Y
 - L-FPR4245T-TMC-5Y
- 通信事業者 :
 - L-FPR4200-FTD-CAR=
 - Cisco Secure Client : 『[Cisco Secure Client Ordering Guide](#)』を参照してください。

3. 結果から、[製品とサービス (Products and 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。

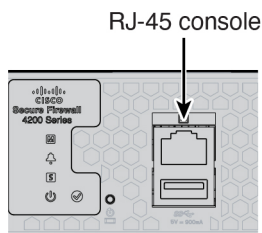
CLI におけるファイアウォールの電源の切断

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 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。

Management Center を使用したファイアウォールの電源の切断

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。

- a) **[デバイス (Devices)] > [デバイス管理 (Device Management)]** を選択します。
- b) 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。
- c) **[デバイス (Device)]** タブをクリックします。
- d) **[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分間待ってシステムがシャットダウンしたことを確認します。

ステップ 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

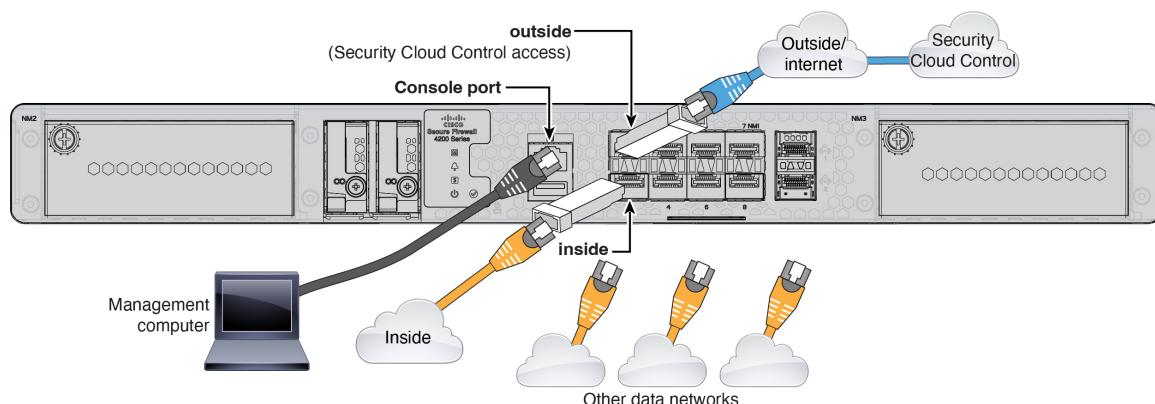
ファイアウォールのケーブル接続とオンボード

ファイアウォールをケーブル接続し、Security Cloud Control にオンボードします。

- [ファイアウォールのケーブル接続](#) (11 ページ)
- [手動プロビジョニングによるファイアウォールをオンボード](#) (12 ページ)
- [初期設定 : CLI](#) (14 ページ)

ファイアウォールのケーブル接続

- コンソールケーブルを入手します。デフォルトではファイアウォールにコンソールケーブルが付属していないため、サードパーティの USB-to-RJ-45 シリアルケーブルなどを購入する必要があります。
- データ インターフェイス ポートに SFP を取り付けます。組み込みポートは、SFP/SFP+/SFP28 モジュールを必要とする 1/10/25 Gb SFP28 ポートです。
- 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。



手動プロビジョニングによるファイアウォールをオンボード

CLI 登録キーを使用してファイアウォールをオンボードします。

手順

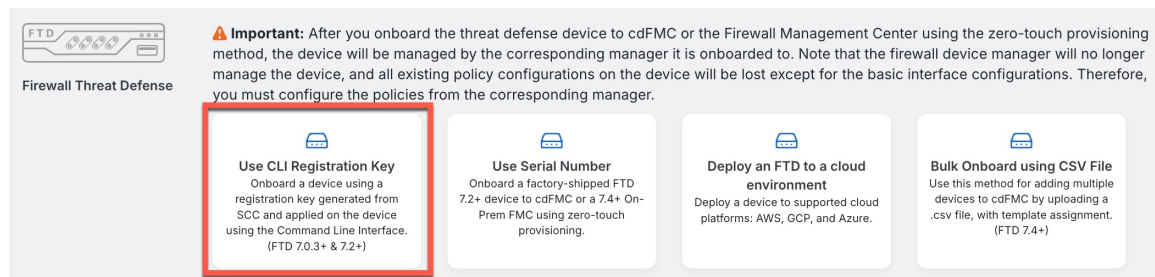
ステップ 1 Security Cloud Control のナビゲーションウィンドウで **セキュリティデバイス** をクリックし、青色のプラスボタン () をクリックしてデバイスを [オンボード (Onboard)] します。

ステップ 2 [FTD] タイルをクリックします。

ステップ 3 [管理モード] で、[FTD] が選択されていることを確認します。

ステップ 4 オンボーディング方法として [CLI登録キーを使用 (Use CLI Registration Key)] を選択します。

図 9: CLI 登録キーを使用



ステップ 5 [デバイス名 (Device Name)] を入力して、[次へ (Next)] をクリックします。

図 10: デバイス名

ステップ 6 [ポリシー割り当て (Policy Assignment)] については、ドロップダウンメニューを使用して、デバイスのアクセスコントロールポリシーを選択します。ポリシーが設定されていない場合は、[デフォルトのアクセスコントロールポリシー (Default Access Control Policy)] を選択します。

図 11: アクセス コントロール ポリシー

2 Policy Assignment

Access Control Policy

Default Access Control Policy ▼

Next

ステップ 7 [サブスクリプションライセンス (Subscription License)] については、[物理 FTD デバイス (Physical FTD Device)] ラジオ ボタンをクリックし、有効にする各機能ライセンスをチェックします。[Next] をクリックします。

図 12: サブスクリプションライセンス

3 Subscription License

Please indicate if this FTD is physical or virtual:

☒ Physical FTD Device

☐ Virtual FTD Device

License Type	Includes
☒ Essentials	Base Firewall Capabilities
☒ Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
☒ IPS	Intrusion Policy
☒ Malware Defense	File Policy
☒ URL	URL Reputation
☒ RA VPN	RA VPN

Next

ステップ 8 [CLI登録キー (CLI Registration Key)] については、Security Cloud Control は、登録キーとその他のパラメータを使用してコマンドを生成します。このコマンドをコピーして、Threat Defense の初期設定で使用する必要があります。

図 13: CLI 登録キー

4 CLI Registration Key

1 Ensure the device's initial configuration is complete before trying to apply the registration key. [Learn more](#)

2 Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cisco-security-docs.app.us.cdo.cisco.com
BanyI2oaT0ew1JTpC0P2w3xEBnVVkfZv x7R7dwcM43JCMzwGY3ZzCfoFmZhw97my cisco-security-
docs.app.us.cdo.cisco.com
```

Next

configure manager add Security Cloud Control_hostname registration_key nat_id display_name

スタートアップスクリプトを完了した後、Threat Defense CLI でこのコマンドをコピーします。初期設定 : CLI (14 ページ) を参照してください。

例 :

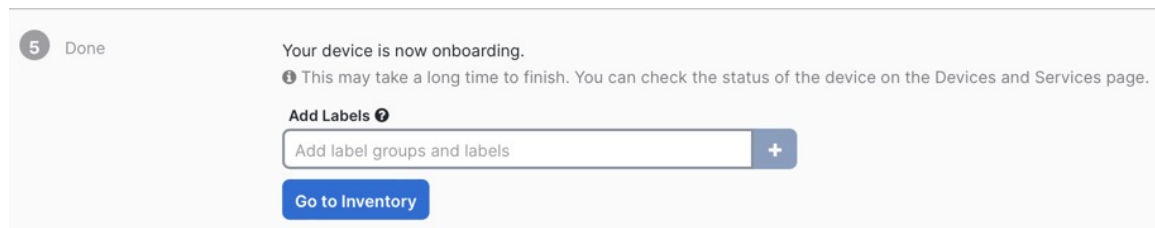
CLI セットアップのサンプルコマンド:

```
configure manager add account1.app.us.scc.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
LzmlHOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.scc.cisco.com
```

ステップ 9 オンボーディングウィザードで [次へ (Next)] をクリックして、デバイスの登録を開始します。

ステップ 10 (任意) [セキュリティデバイス (Security Devices)] ページの並べ替えとフィルタ処理に役立つラベルをデバイスに追加します。ラベルを入力し、青いプラスボタン (+) を選択します。ラベルは、Security Cloud Control への導入準備後にデバイスに適用されます。

図 14: 終了



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 Threat Defense CLI にアクセスします。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。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。

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

ガイダンス : [手動 (manual)] を選択します。マネージャアクセスに外部インターフェイスを使用する場合、DHCP はサポートされません。ルーティングの問題を防ぐために、このインターフェイスがマネージャアクセス インターフェイスとは異なるサブネット上にあることを確認してください。

```
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]:
```

ガイダンス : ゲートウェイを **data-interfaces** に設定します。この設定は、外部インターフェイスを通じてルーティングできるように、バックプレーンを介して管理トラフィックを転送します。

```
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
```

ガイダンス : 管理インターフェイスの DNS サーバーを設定します。これらは、両方とも外部インターフェイスからアクセスされるため、後で設定する外部インターフェイスの DNS サーバーと一致する可能性があります。

```
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'
```

```
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'
```

ガイダンス : **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。

```
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 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。

手動 IP アドレス

```
> 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
```

ガイダンス：登録後に外部 DNS サーバーを保持するには、Management Center で DNS プラットフォーム設定を再設定する必要があります。

```
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.
```

```
>
```

DHCP からの IP アドレス

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
```

```

IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

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

Setting IPv4 network configuration.
Network settings changed.

>

```

ステップ 4 Security Cloud Control が生成した **configure manager add** コマンドを使用して、この Threat Defense を管理する Security Cloud Control を識別します。コマンドの生成については、[手動プロビジョニングによるファイアウォールをオンボード（12 ページ）](#) を参照してください。

例 :

```

> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnjlV5ha2q5Rf8pKFX9E
LzmlHOynhVUWhXYWz2swmkj2ZWsn3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.

```

ステップ 5 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。



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 \(19 ページ\)](#)
- [DHCP サーバーの設定 \(24 ページ\)](#)
- [NAT の設定 \(25 ページ\)](#)
- [アクセス制御ルールの設定 \(29 ページ\)](#)
- [外部インターフェイスでの SSH の有効化 \(32 ページ\)](#)
- [設定の展開 \(33 ページ\)](#)

インターフェイスの設定

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 15: 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 40 Gb 以上のインターフェイスからブレイクアウトポートを作成するには、インターフェイスの **[ブレイク (Break)]** アイコンをクリックします。

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

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

図 16 : [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。

- 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 17: [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 18: [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 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 19: [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 (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。

他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。

- b) [OK] をクリックします。

ステップ 6 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。

- a) 使用するインターフェイスの [編集 (Edit)] (🔗) をクリックします。
- b) [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。

- c) 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。
- d) [有効 (Enabled)] チェックボックスをオンにします。
- e) [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 7 [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は、DHCP サーバーを有効にします。

手順

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

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

図 20: DHCP サーバー

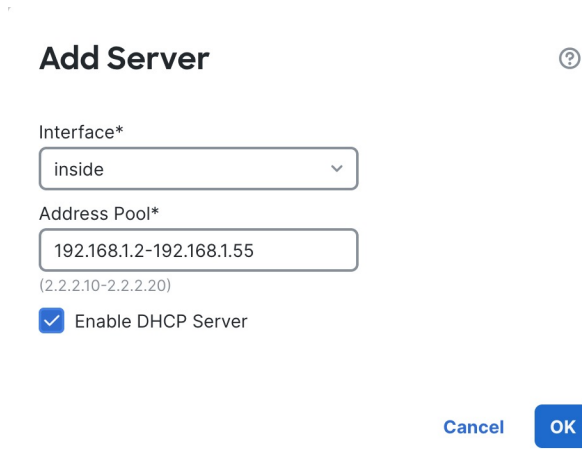
The screenshot displays the DHCP configuration interface. On the left, a sidebar lists 'DHCP Server', 'DHCP Relay', and 'DDNS'. The main area is titled 'DHCP' and contains several settings:

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

At the bottom, there is a 'Server' tab (highlighted with a red box) and an 'Advanced' tab. A '+ Add' button (also highlighted with a red box) is located in the bottom right corner. Below the tabs is a table with columns 'Interface', 'Address Pool', and 'Enable DHCP Server'. The table is currently empty, showing '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 21: サーバーの追加



- [インターフェイス (Interface)] : ドロップダウンリストからインターフェイス名を選択します。
- [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。

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 22: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 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 23: NAT ポリシー

FTD_Policy

Enter Description

Show Warnings Save Cancel

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 24: 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 25: 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 26: 変換

Interface Objects	Translation	PAT Pool	Advanced
Original Packet		Translated Packet	
Original Source:* all-ipv4		Translated Source: Destination Interface IP	
Original Port: TCP		The values selected for Destination Interface Objects in 'Interface Objects' tab will be used	
		Translated Port: 	

- [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 27: 新しいネットワークオブジェクト

New Network Object

Name

all-ipv4

Description

Network

☐ Host
 ☐ Range
 ☒ Network
 ☐ FQDN

0.0.0.0/0

☐ 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。

アクセス制御ルールの設定

デバイスを登録したときに、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。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 (Policy)] > [アクセスポリシー (Access Policy)] > [アクセスポリシー (Access Policy)] の順に選択し、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。

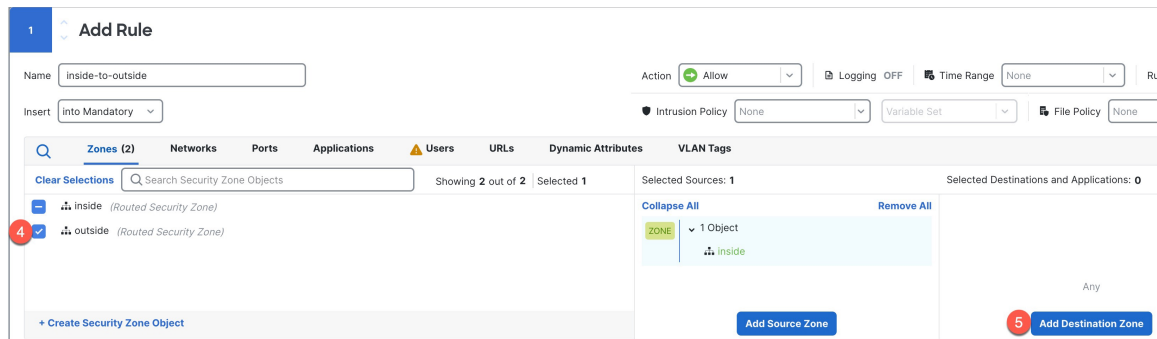
ステップ 2 [ルールを追加 (Add Rule)] をクリックし、次のパラメータを設定します。

図 28: 送信元ゾーン (Source Zone)

The screenshot shows the 'Add Rule' configuration page. The 'Name' field is 'inside-to-outside'. The 'Action' is 'Allow'. The 'Intrusion Policy' is '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 '2' highlights the 'inside' zone selection. A red circle with the number '3' highlights the 'Add Source Zone' button at the bottom right.

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 29: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。

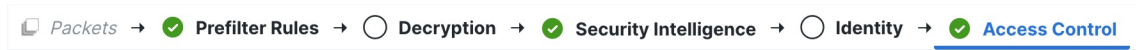
5. [宛先ゾーンを追加 (Add Destination Zone)] をクリックします。

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 30: 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。

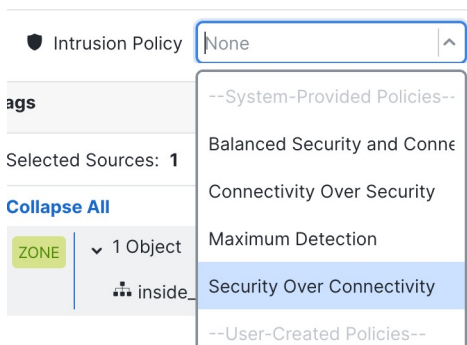
- [アイデンティティ (Identity)] : アイデンティティはデフォルトでは適用されません。アクセス コントロール ポリシーによるトラフィックの処理を許可する前に、ユーザーに認証を要求できます。

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。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。

- [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 31: システム提供の侵入ポリシー

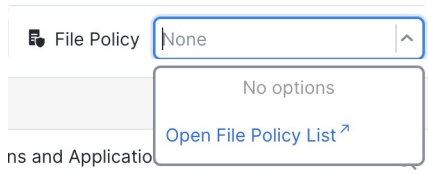


- リストからシステム提供のポリシーを 1 つ選択します。

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。

- [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 32: 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)] > [マルウェア&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 Configuration Guide](#)を参照してください。
- c) [ルール の追加 (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。

外部インターフェイスでの SSH の有効化

ここでは、外部インターフェイスへの SSH 接続を有効にする方法について説明します。

デフォルトでは、初期設定時にパスワードを設定した **admin** ユーザーを使用できます。

手順

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

ステップ 2 [SSHアクセス (SSH Access)] を選択します。

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

- a) [追加 (Add)] をクリックして新しいルールを追加するか、[編集 (Edit)] をクリックして既存のルールを編集します。
- b) ルールのプロパティを設定します。
 - [IP Address]: SSH 接続を許可するホストまたはネットワークを特定するネットワークオブジェクトまたはグループ。オブジェクトをドロップダウンメニューから選択するか、または[+]をクリックして新しいネットワークオブジェクトを追加します。
 - [使用可能なゾーン/インターフェイス (Available Zones/Interfaces)]: [選択したゾーン/インターフェイス (Selected Zones/Interfaces)] リストの下フィールドに外部ゾーンを追加するか「外部」インターフェイス名を入力し、[追加 (Add)] をクリックします。

図 33: 外部インターフェイスでの SSH の有効化

Edit Secure Shell Configuration

IP Address*
any-ipv4 +

Available Zones/Interfaces ↺ Selected Zones/Interfaces

Search Add

DMZ
inside
outside

outside Add

Cancel OK

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。

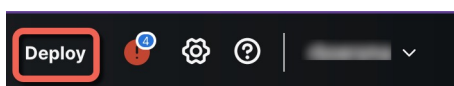
設定の展開

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

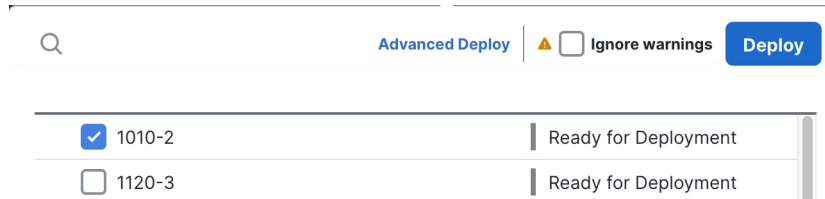
ステップ 1 右上の [展開 (Deploy)] をクリックします。

図 34: 展開



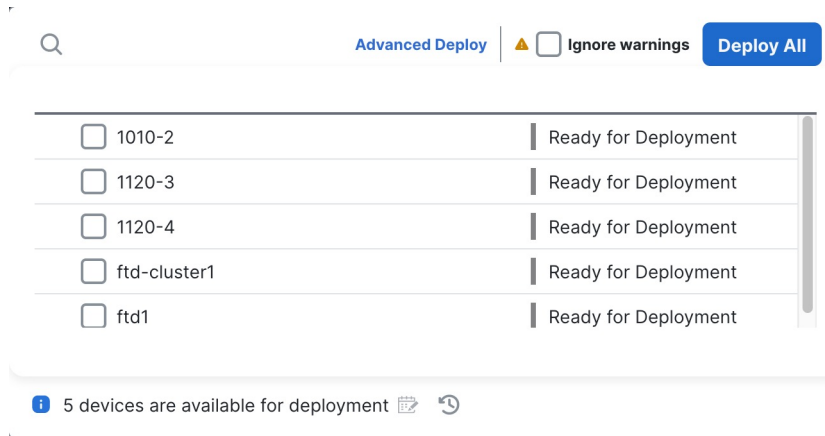
ステップ 2 迅速な展開の場合は、特定のデバイスのチェックボックスをオンにして [展開 (Deploy)] をクリックします。

図 35: 選択したものを展開



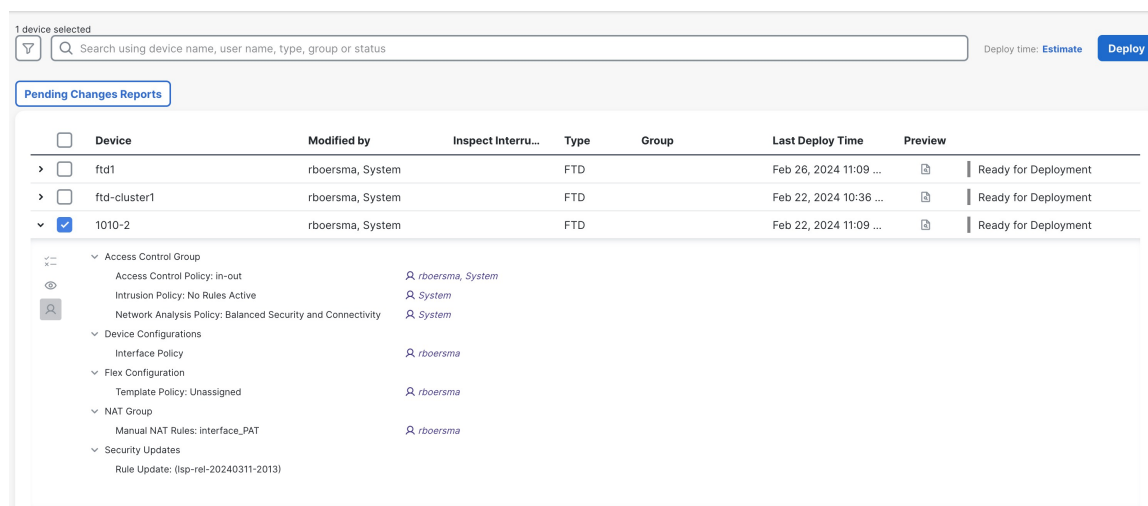
または、[すべて展開 (Deploy All)] をクリックしてすべてのデバイスに展開します。

図 36: すべて展開



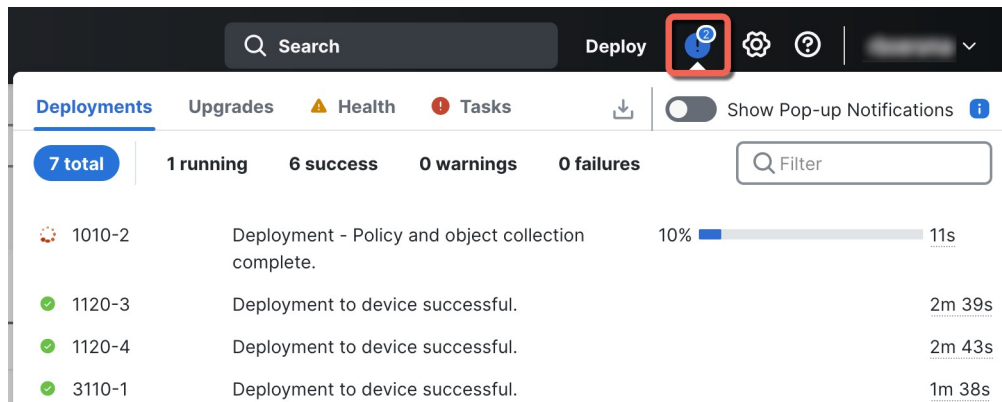
それ以外の場合は、追加の展開オプションを設定するために、[高度な展開 (Advanced Deploy)] をクリックします。

図 37: 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 38: 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。