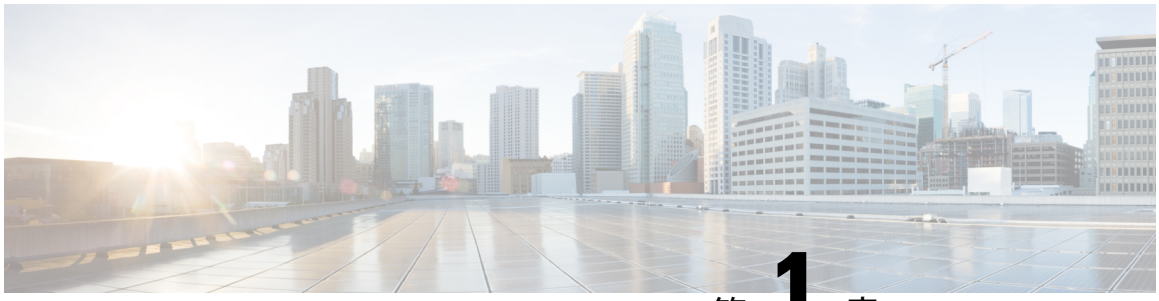
Secure Firewall 3100 Threat Defense スタートアップガイド：デバイスマネージャ

最終更新：2026 年 2 月 6 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/



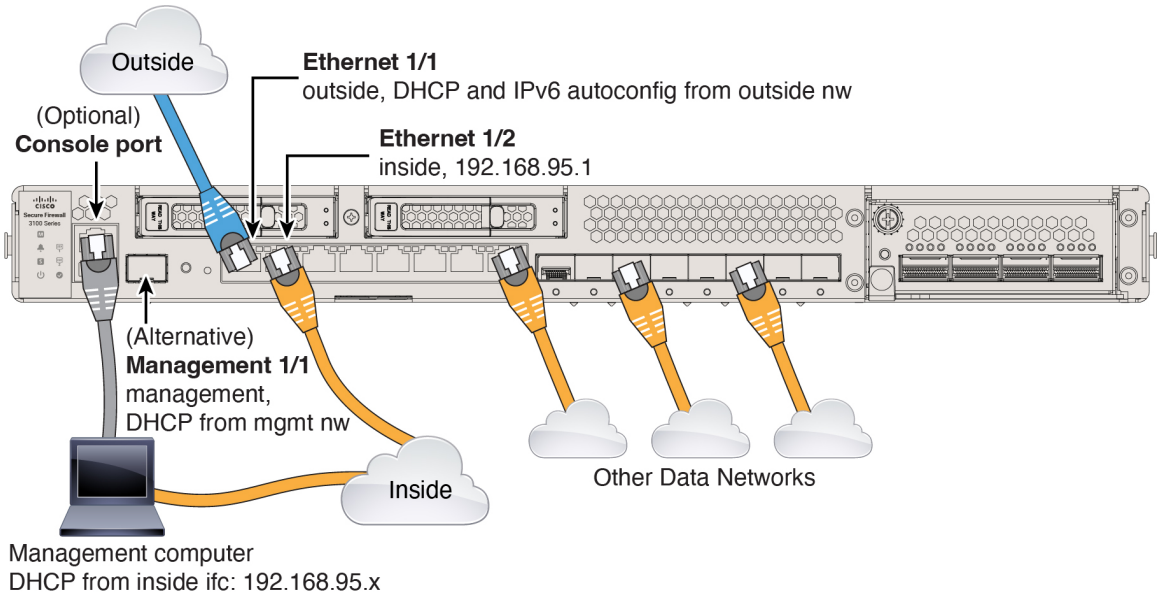
第 1 章

はじめる前に

ローカルの Secure Firewall Device Manager 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ケーブル接続

- （オプション）コンソールアダプタの取得：ファイアウォールには DB-9 to RJ-45 シリアルケーブルが付属しているため、接続するにはサードパーティの DB-9-to-USB シリアルケーブルの購入が必要になる場合があります。
- SFP/SFP+ モジュールをイーサネット 1/9 以降のポートに取り付けます。
- 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。



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

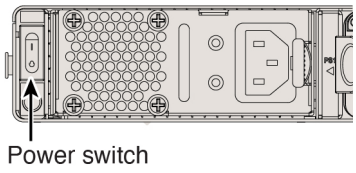
ファイアウォールに対して信頼性の高い電力を供給することが重要です（無停電電源装置（UPS）を使用するなど）。最初のシャットダウンを行わないで電力が失われると、重大なファイルシステムの損傷を引き起こす可能性があります。バックグラウンドでは常に多数のプロセスが実行されていて、電力が失われると、システムをグレースフルシャットダウンできません。

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。

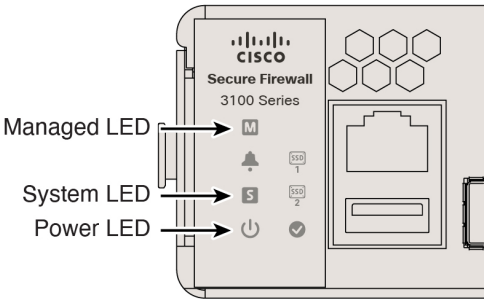
ステップ 2 シャーシの背面で、電源コードに隣接するロッカー電源スイッチを使用して電源をオンにします。

図 *1 :* 電源ボタン



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
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

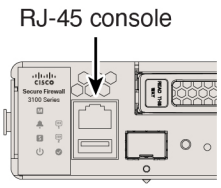
インストールされているアプリケーション（Firewall Threat Defense または ASA）の確認

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 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 （5 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。

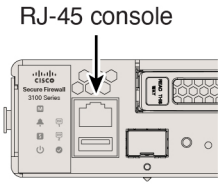
Firewall Threat Defense CLI へのアクセス

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 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。

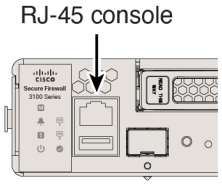
実行するバージョン

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 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。

（任意）CLI での管理ネットワーク設定の変更

デフォルトでは、次のいずれかのインターフェイスでファイアウォールを管理できます。

- イーサネット 1/2：192.168.95.1/24
- 管理 1/1：DHCP からの IP アドレス

デフォルトの IP アドレスを使用できない場合は、コンソールポートに接続し、CLI で初期セットアップを実行して管理 1/1 の IP アドレスを静的アドレスに設定できます。

手順

ステップ 1 コンソール ポートに接続します。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 （4 ページ）を参照してください。

ステップ 2 Firewall Threat Defense CLI に接続します。

connect ftd

例：

```
firepower# connect ftd
>
```

ステップ 3 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。

```
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]:
```

ガイダンス：静的 IP アドレスを設定するには [手動（manual）] を選択します。

```
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
```

ガイダンス：ゲートウェイの IP アドレスを設定します。

```
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

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]: yes

>
```

ガイダンス：Firewall Device Manager を使用する場合は、**yes** と入力します。

ステップ 4 新しい管理 IP アドレスで Firewall Device Manager にログインしてください。

ライセンスの取得

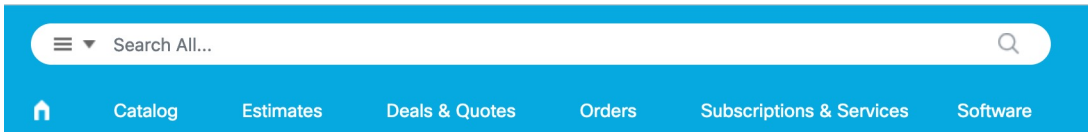
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。Smart Software Manager にアカウントがない場合は、リンクをクリック して新しいアカウントを設定します。

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

- 標準：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-FPR3110T-TMC=
  - L-FPR3120T-TMC=
  - L-FPR3130T-TMC=
  - L-FPR3140T-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-FPR3110T-TMC-1Y
  - L-FPR3110T-TMC-3Y
  - L-FPR3110T-TMC-5Y
  - L-FPR3120T-TMC-1Y
  - L-FPR3120T-TMC-3Y

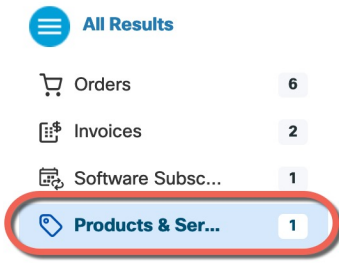
- L-FPR3120T-TMC-5Y
- L-FPR3130T-TMC-1Y
- L-FPR3130T-TMC-3Y
- L-FPR3130T-TMC-5Y
- L-FPR3140T-TMC-1Y
- L-FPR3140T-TMC-3Y
- L-FPR3140T-TMC-5Y

- 通信事業者：
  - L-FPR3K-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 & 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。

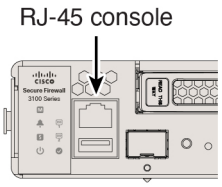
CLI におけるファイアウォールの電源の切断

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 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。

Device Manager を使用したファイアウォールの電源の切断

Firewall Device Manager 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（Device）] をクリックしてから、[システム設定（System Settings）] > [再起動/シャットダウン（Reboot/Shutdown）] リンクをクリックします。

b) [シャットダウン（Shut Down）] をクリックします。

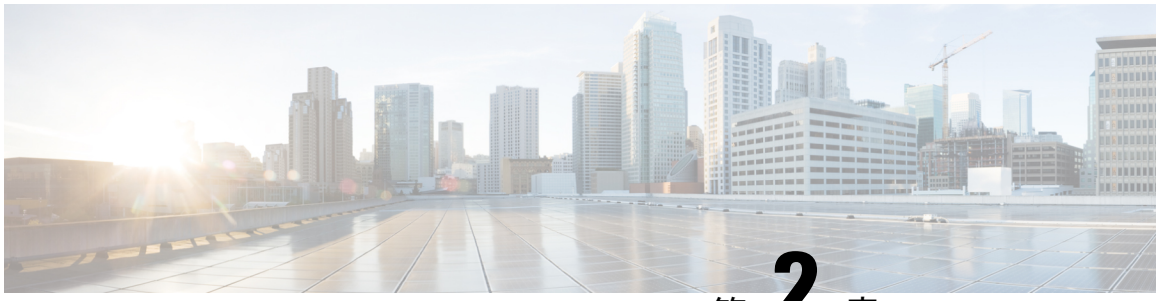
ステップ 2 コンソールからファイアウォールに接続している場合は、ファイアウォールがシャットダウンするときにシステムプロンプトをモニターします。シャットダウンが完了すると、次のプロンプトが表示されます。

```
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

基本ポリシーの設定

初期設定を完了してから、追加のインターフェイスとネットワークの設定、およびポリシーのカスタマイズを行います。

デバイスマネージャへのログイン

Firewall Device Manager にログインして Firewall Threat Defense を設定します。

手順

ステップ 1 コンピュータの接続先のインターフェイスに応じて、ブラウザに次の URL を入力します。

- イーサネット 1/2：**https://192.168.95.1**
- 管理 1/1：**https://***management_ip*（DHCP から）

ステップ 2 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。

初期設定の完了

初期設定を完了するには、最初に Firewall 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。セットアップウィザードの完了後、いくつかの基本ポリシーが適切に設定された、機能しているデバイスが必要です。

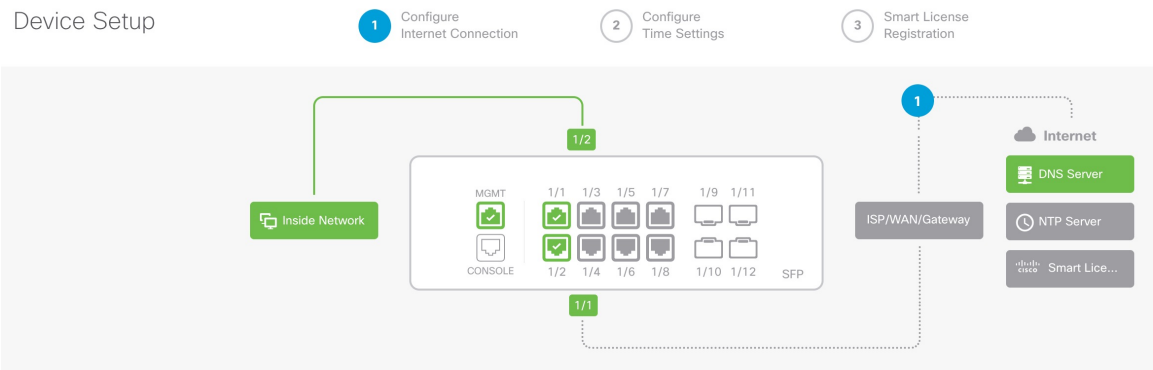
- 内部→外部トラフィックフロー
- 内部から外部へのすべての通信用のインターフェイス PAT。

手順

ステップ 1 一般条件に同意し、管理者パスワードを変更します。

[**Device Setup**] 画面が表示されます。

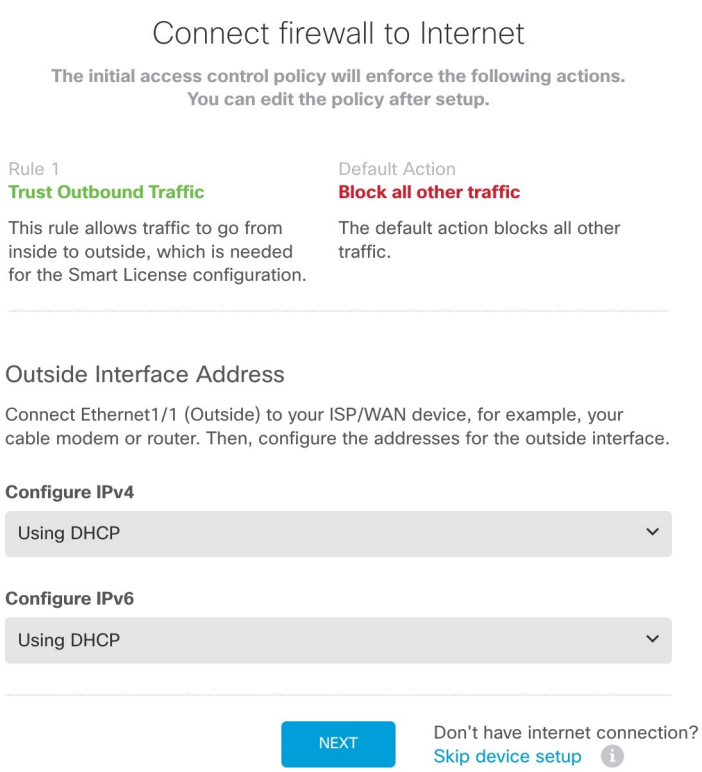
図 *9 : [デバイスの設定（Device Setup）]*



（注）
正確なポート設定は、モデルによって異なります。

ステップ 2 外部インターフェイスおよび管理インターフェイスのネットワーク設定を指定します。

図 *10* : インターネットへのファイアウォールの接続



a) [**Outside Interface**]：イーサネット 1/1。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。

[**Configure IPv4**]：PPPoE が必要な場合は、ウィザードの完了後に設定できます。

IPv6 を設定する

b) [**Management Interface**]：専用の管理 1/1 インターフェイスのパラメータを設定します。CLI で IP アドレスを変更した場合、これらの設定はすでに構成済みのため表示されません。

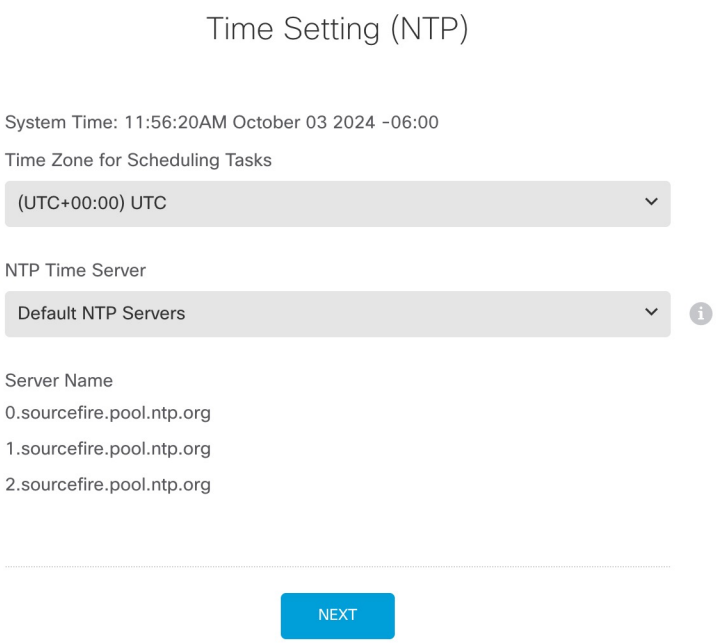
[**DNS Servers**]：デフォルトは OpenDNS パブリック DNS サーバーです。

ファイアウォールのホスト名

c) [次へ（Next）] をクリックします。

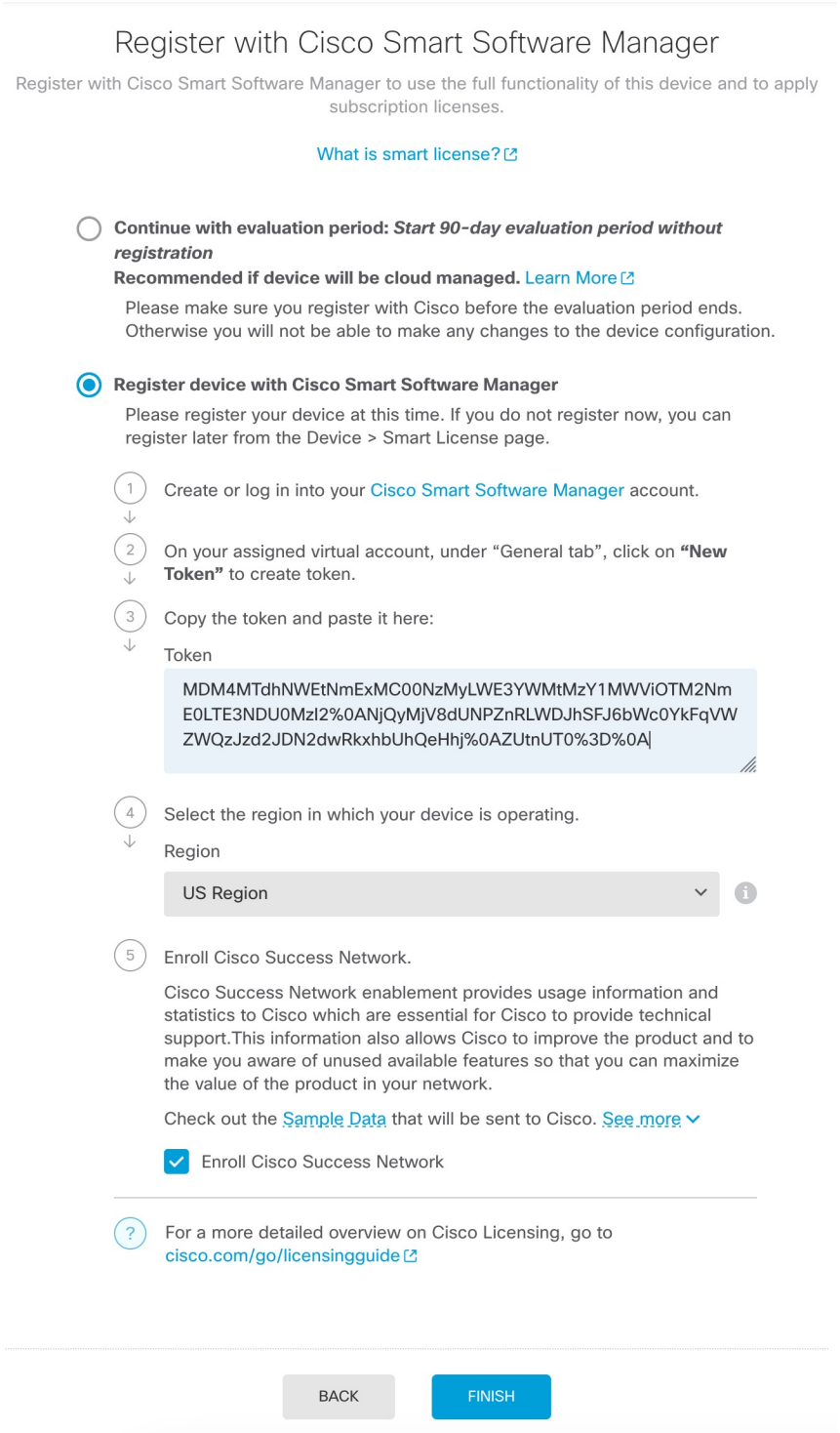
ステップ 3 システム時刻を設定します。

図 *11* : 時刻設定（***NTP***）

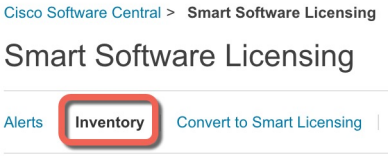


a) **タイム ゾーン**
b) [**NTP Time Server**]
c) [次へ（Next）] をクリックします。

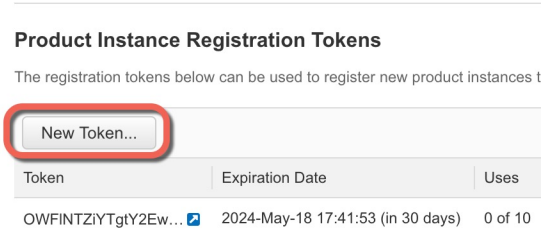
ステップ 4 スマート ライセンスを設定します。



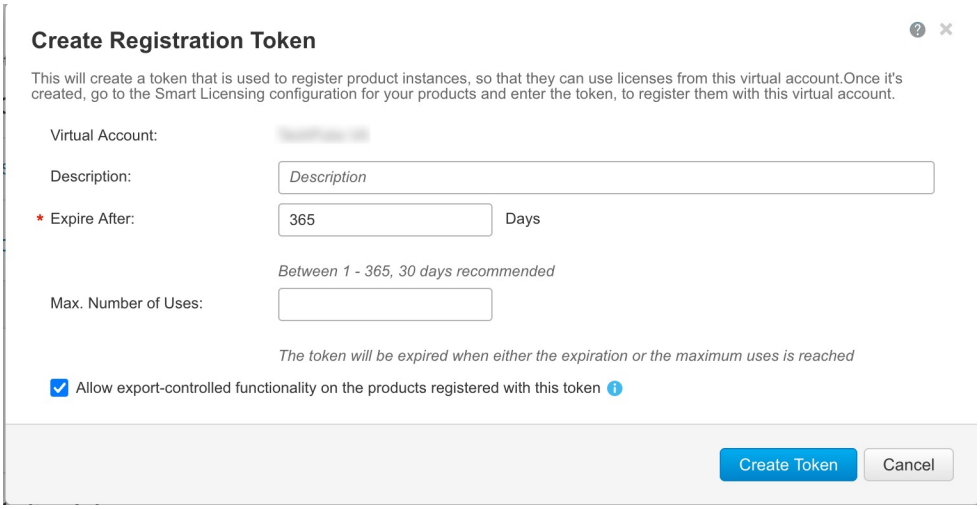
a) [**Register device with Cisco Smart Software Manager**] をクリックします。
b) [Cisco Smart Software Manager] リンクをクリックします。
c) [Inventory] をクリックします。



d) [General] タブで、[New Token] をクリックします。



e) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。



- **説明**
- [有効期限（Expire After）]：推奨値は 30 日です。
- 最大使用回数（Max. Number of Uses）
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：高度暗号化が許可されている国の場合は輸出コンプライアンスフラグを有効にします。 この機能を使用する予定の場合、このオプションをここで選択する必要があります。後でこの機能を有効にする場合は、デバイスを新しいプロダクトキーで再登録し、デバイスをリロードする必要があります。このオプションが表示されない場合、アカウントは輸出規制機能をサポートしていません。

トークンはインベントリに追加されます。

f) トークンの右側にある矢印アイコンをクリックして[トークン（Token）]ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。Firewall Threat Defense の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *12*：トークンの表示

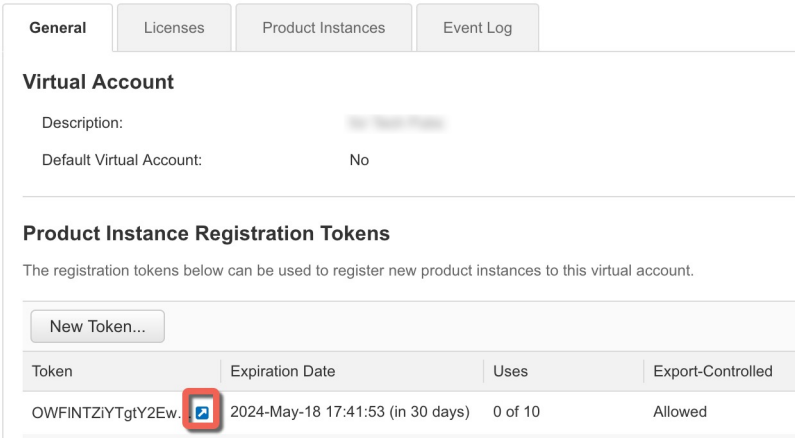
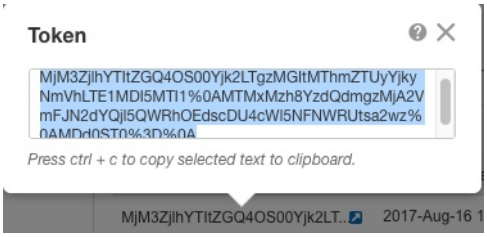


図 *13*：トークンのコピー

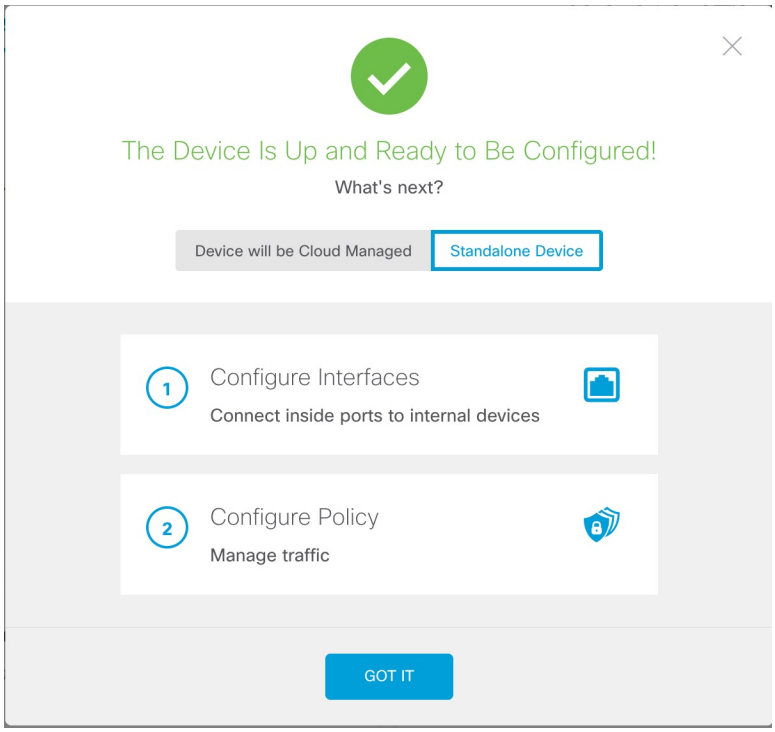


g) Firewall Device Manager で、トークンをトークンフィールドに貼り付けます。

h) その他のオプションを設定し、**[Finish]** をクリックします。

ステップ 5 セットアップウィザードを終了します。

図 *14* : 次のステップ



a) [**Standalone Device**] をクリックして Firewall Device Manager を使用します。

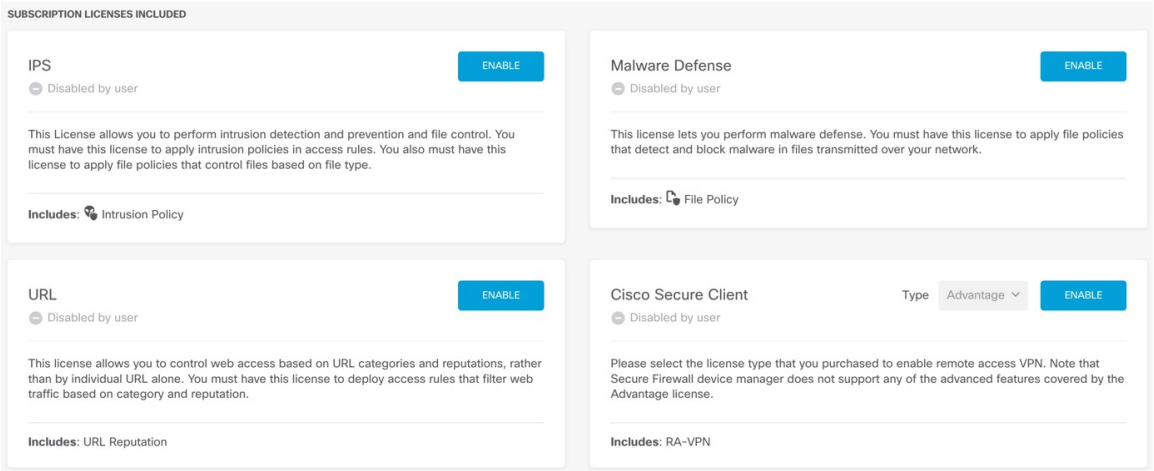
b) [**Configure Interfaces**] をクリックして [**Interfaces**] ページに直接移動するか、[**Configure Policy**] をクリックして [**Policies**] ページに移動するか、[**Got It**] をクリックして [**Device**] ページに移動します。

インターフェイスまたはポリシー設定については、「ネットワーク設定とポリシーの設定 （21 ページ）」を参照してください。

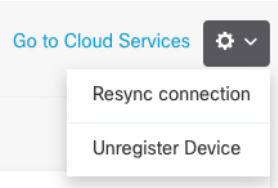
ステップ 6 機能ライセンスを有効化します。

a) [**Device**] ページから **[Smart License** > > **View Configuration]** の順にクリックします。

b) それぞれのオプションライセンスの [**Enable/Disable**] コントロールをクリックします。



c) 歯車ドロップダウンリストから [接続の再同期（Resync Connection）] を選択して、Cisco Smart Software Manager とライセンス情報を同期させます。



ネットワーク設定とポリシーの設定

追加のインターフェイス、DHCPサーバーを設定し、セキュリティポリシーをカスタマイズします。

手順

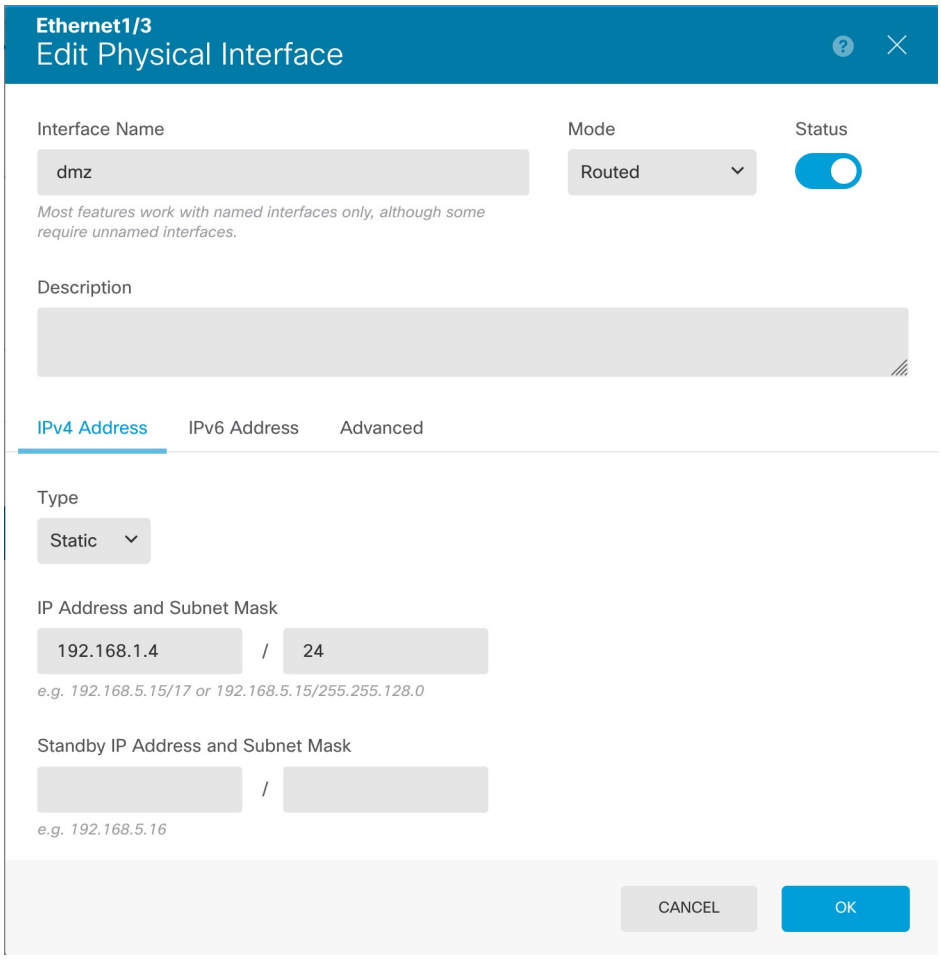
ステップ 1 （一部のモデルで使用可能な）40 Gb インターフェイスから 4 つの 10 Gb ブレークアウト インターフェイスを作成するには、[デバイス（Device）] を選択してから [インターフェイス（Interfaces）] のサマリーにあるリンクをクリックします。次に、インターフェイスのブレークアウトアイコンをクリックします。

ステップ 2 他のインターフェイスを有線接続する場合は、[**Device**] を選択し、[**Interfaces**] の概要のリンクをクリックします。

各インターフェイスの編集アイコン（）をクリックして、IP アドレスなどの設定を定義します。

次の例では、Web サーバーなどのパブリックアクセス可能な資産を配置する「緩衝地帯」（DMZ）として使用するためのインターフェイスを構成します。

図 *15* : インターフェイスの編集

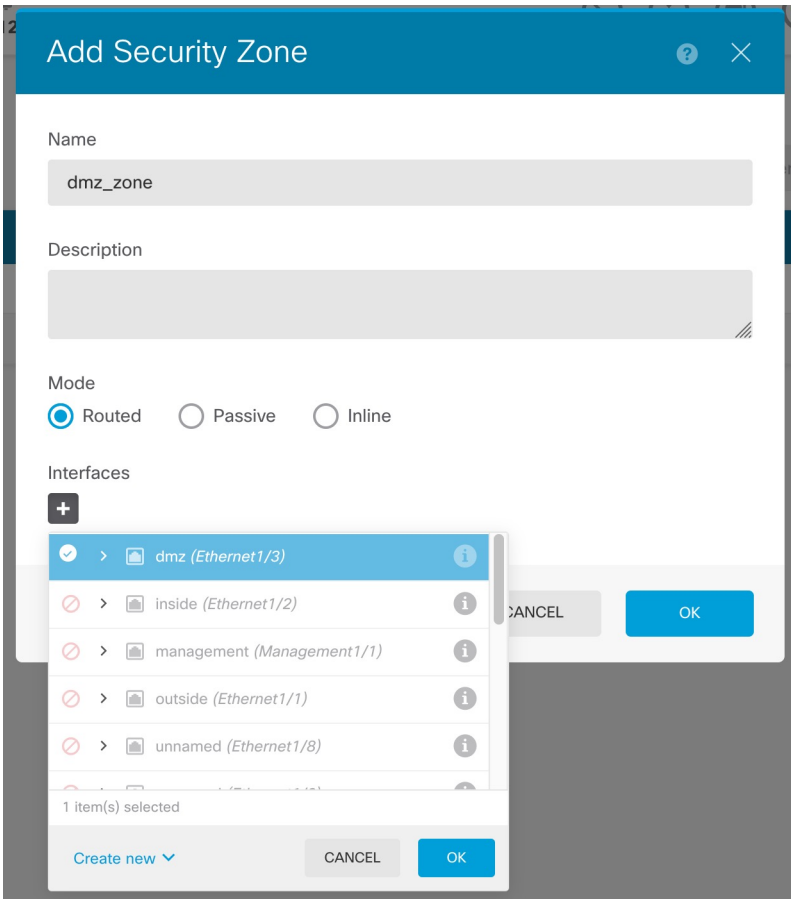


ステップ 3 新しいファイアウォールインターフェイスを構成する場合は、[**Objects**]、[**Security Zones**] の順に選択します。

必要に応じて新しいゾーンを編集または作成し、インターフェイスをそのゾーンに割り当てます。各インターフェイスは、ポリシーを設定するゾーンに属している必要があります。

次の例では、新しい dmz_zone を作成し、それに dmz インターフェイスを割り当てる方法を示します。

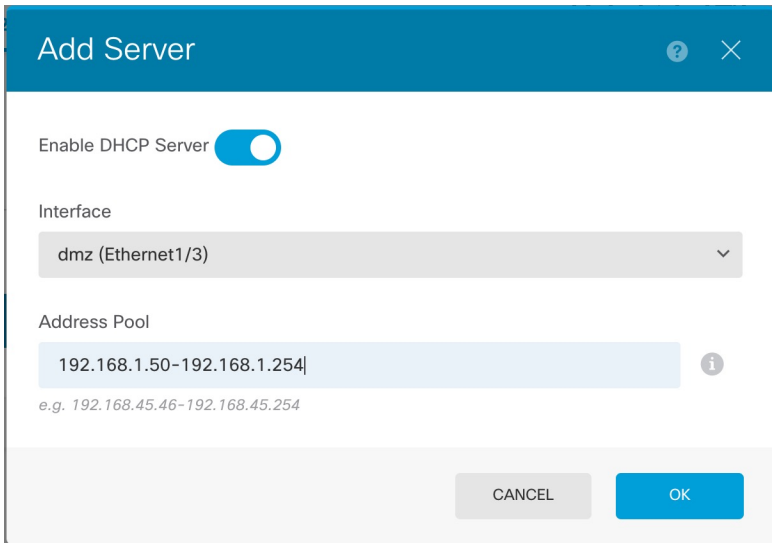
図 *16* : セキュリティ ゾーン オブジェクト



ステップ 4 内部クライアントで DHCP を使用してデバイスから IP アドレスを取得する場合は、**[Device > System Settings > DHCP Server]** の順に選択してから **[DHCP Servers]** タブを選択します。

すでに内部インターフェイス用に構成されている DHCP サーバーがあります。

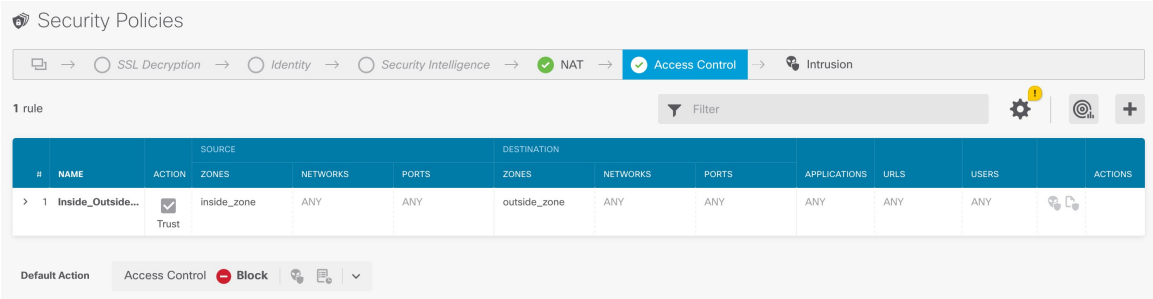
図 17 : DHCP サーバー



ステップ 5 [ポリシー（Policies）] を選択してネットワークのセキュリティ ポリシーを構成します。

デバイス セットアップ ウィザードでは、信頼ルールを使用して、inside_zone と outside_zone 間の通信フローを有効にできます。信頼ルールでは侵入ポリシーを適用しません。侵入を使用するには、ルールに対して許可アクションを指定します。ポリシーには、外部インターフェイスに向かうときのすべてのインターフェイスのインターフェイス PAT も含まれます。

図 18 : デフォルトのセキュリティポリシー



ただし、異なるゾーンにインターフェイスがある場合は、それらのゾーンとの間の通信を許可するアクセス制御ルールが必要です。

さらに、追加のサービスを提供するために他のポリシーを設定し、組織が必要とする結果を取得するためにNATおよびアクセスルールを調整することができます。ツールバーでポリシータイプをクリックすることで、次のポリシーを設定できます。

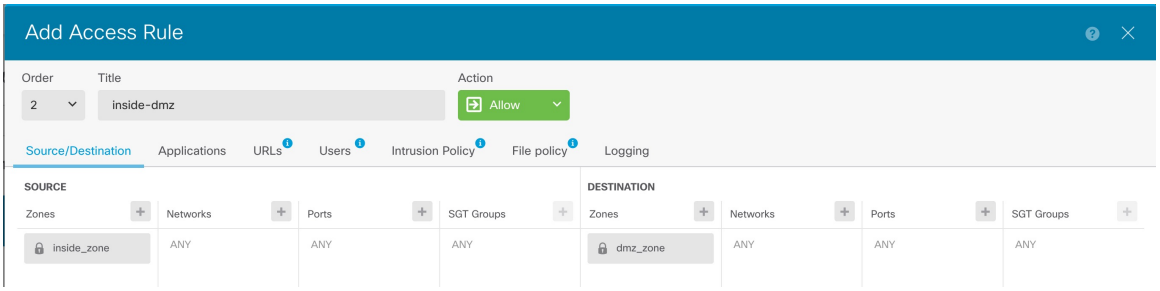
- [SSL復号（SSL Decryption）]：侵入、マルウェアなどについて暗号化された接続（HTTPS など）を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するには SSL 復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。
- [アイデンティティ（Identity）]：個々のユーザーにネットワーク アクティビティを関連付ける、またはユーザーまたはユーザー グループのメンバーシップに基づいてネットワーク アクセスを制御する場

合は、特定のソースIPアドレスに関連付けられているユーザーを判定するためにアイデンティティ ポリシーを使用します。

- [**Security Intelligence**]：（IPS ライセンスが必要）ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティ インテリジェンス ポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセス コントロール ポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティ インテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスやURLの定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。
- [NAT]（ネットワークアドレス変換）：内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。
- [アクセス制御（Access Control）]：ネットワーク上で許可する接続の決定にアクセス コントロール ポリシーを使用します。セキュリティ ゾーン、IPアドレス、プロトコル、ポート、アプリケーション、URL、ユーザーまたはユーザー グループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル（マルウェア）ポリシーを適用します。このポリシーを使用してURLフィルタリングを実装します。
- [侵入（Intrusion）]：侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。

次の例は、アクセス制御ポリシーで inside_zone と dmz_zone の間の通信を許可する方法を示しています。この例では、[接続の最後で（At End of Connection）] が選択されている場合、[ロギング（Logging）] を除いて他のいずれのタブでもオプションは設定されません。

図 *19*：アクセス コントロール ポリシー



ステップ 6 [デバイス（Device）] を選択してから、[更新（Updates）] グループで [設定の表示（View Configuration）] をクリックし、システムデータベースの更新スケジュールを設定します。

侵入ポリシーを使用している場合は、ルールとVDBのデータベースを定期的な更新を設定します。セキュリティ情報フィードを使用する場合は、それらの更新スケジュールを設定します。一致基準としてセキュリティポリシーで地理位置情報を使用する場合は、そのデータベースの更新スケジュールを設定します。

ステップ 7 メニューの [**Deploy**] ボタンをクリックし、[**Deploy Now**] ボタン（ ）をクリックして、変更内容をデバイスに展開します。

変更は、それらを展開するまでデバイスで有効になりません。

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。

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。