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。

Firewall Device Manager 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 コンピューター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 以降：**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。

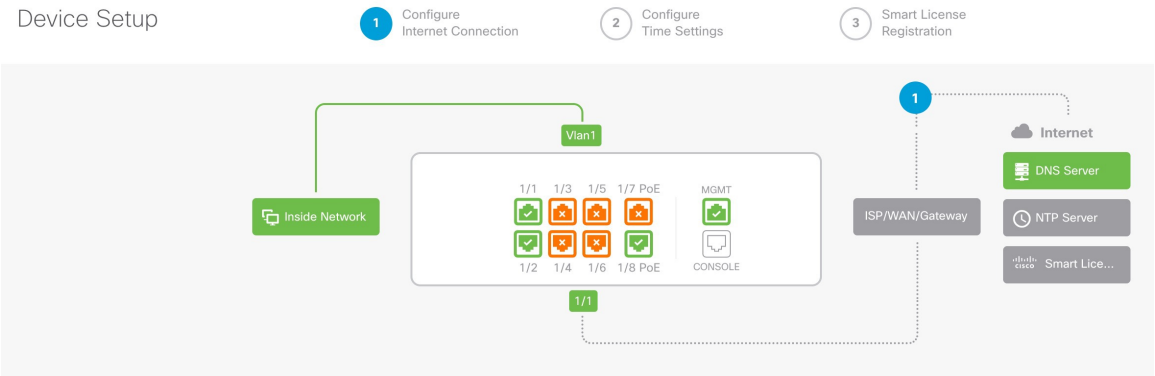
- 内部→外部トラフィックフロー
- 内部から外部へのすべての通信用のインターフェイス PAT。

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。

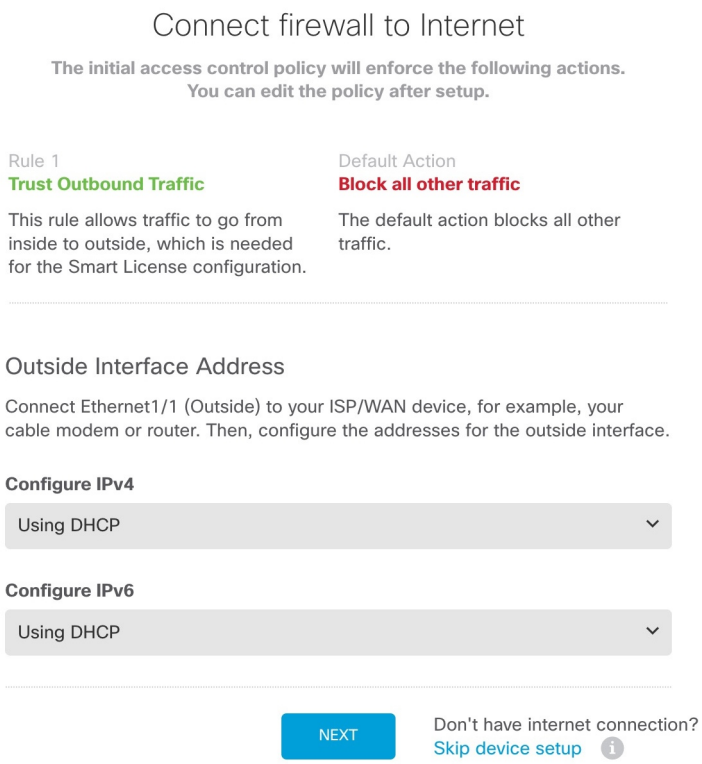
図 *1 : [デバイスの設定（Device Setup）]*



（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 *2*: 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。

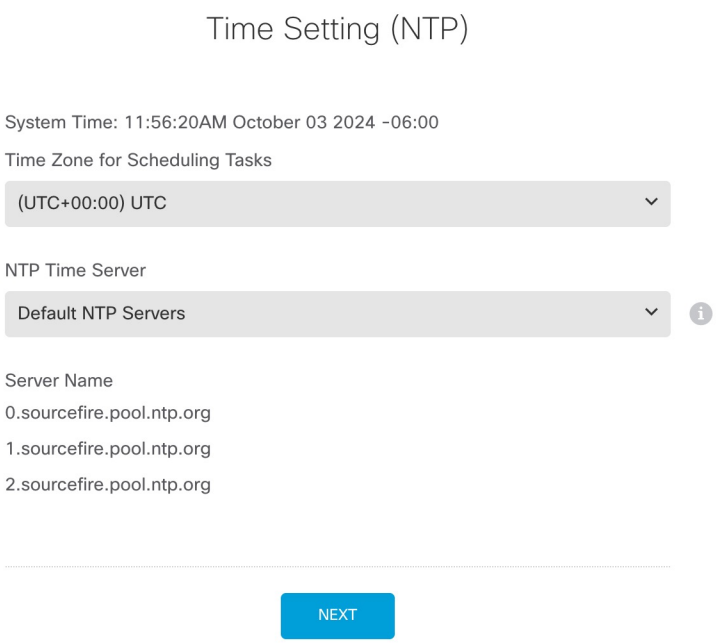
[**DNS Servers**]：デフォルトは OpenDNS パブリック DNS サーバーです。

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。

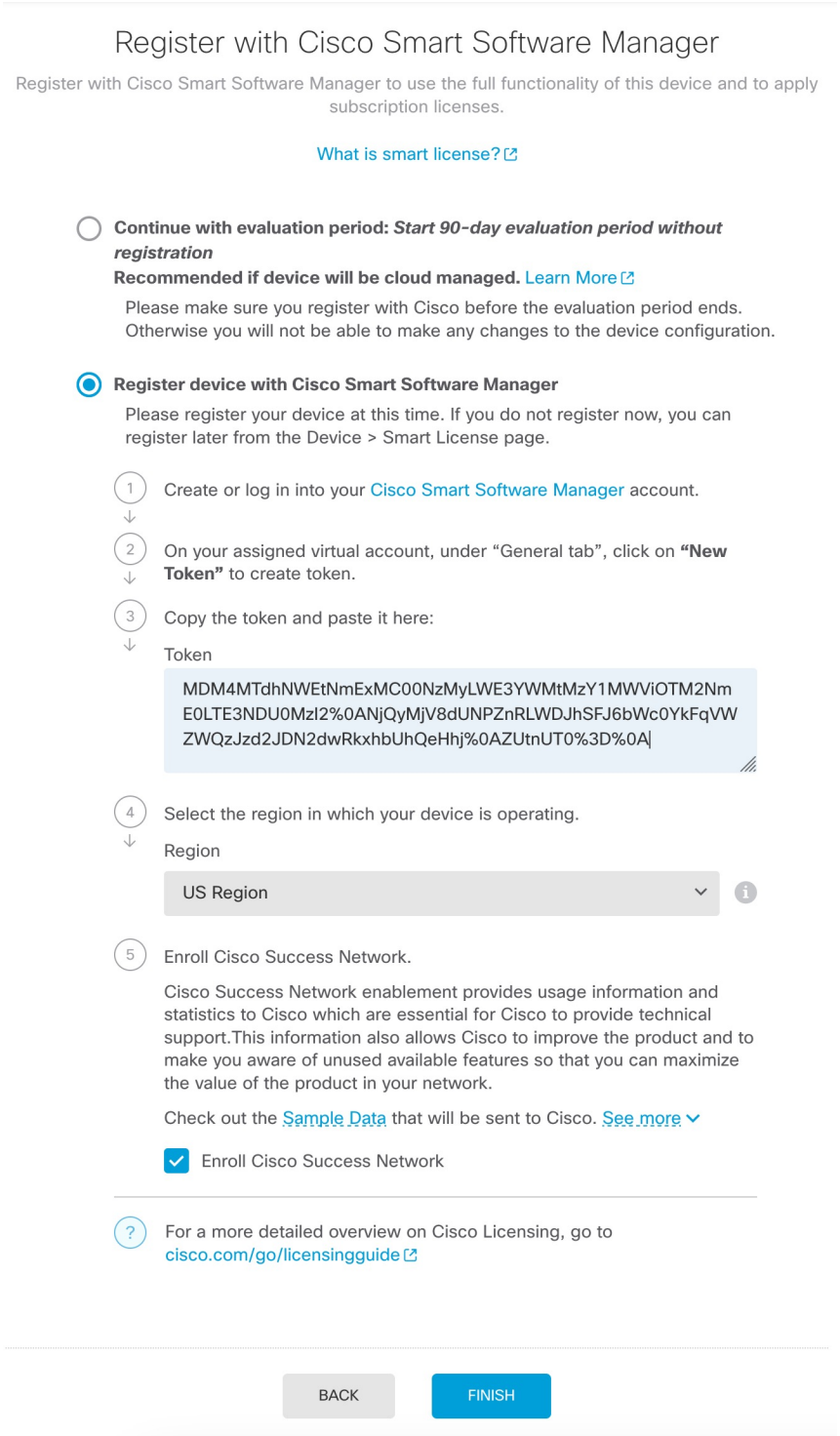
ステップ 3 システム時刻を設定します。

図 *3 :* 時刻設定（***NTP***）

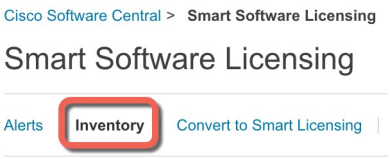


a) **タイム ゾーン**
b) [**NTP Time Server**]
c) [次へ（Next）] をクリックします。

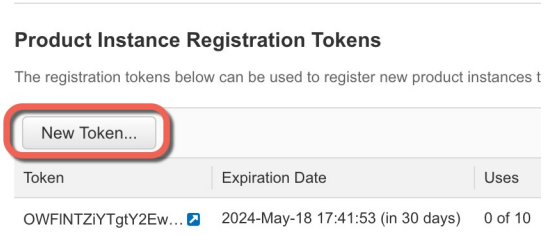
ステップ 4 スマート ライセンスを設定します。



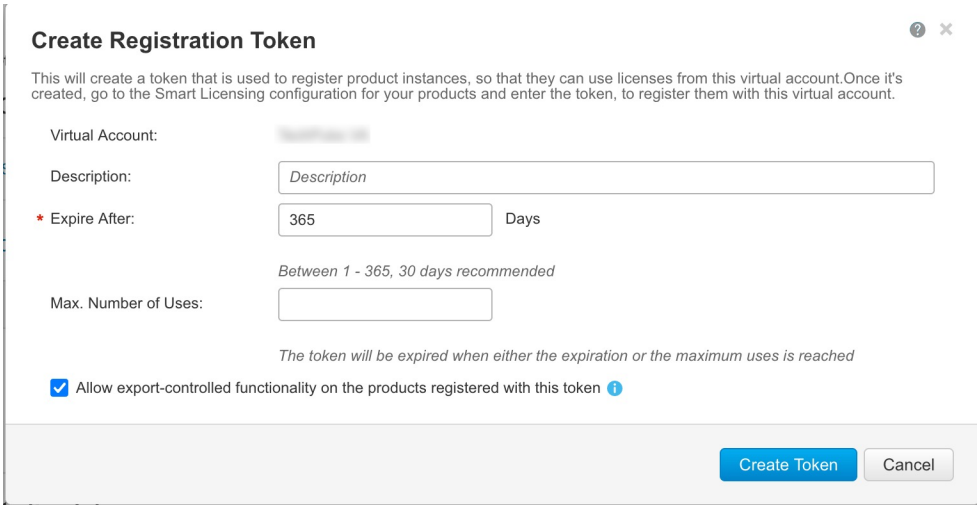
a) [**Register device with Cisco Smart Software Manager**] をクリックします。
b) [Cisco Smart Software Manager] リンクをクリックします。
c) [Inventory] をクリックします。



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 *4*: トークンの表示

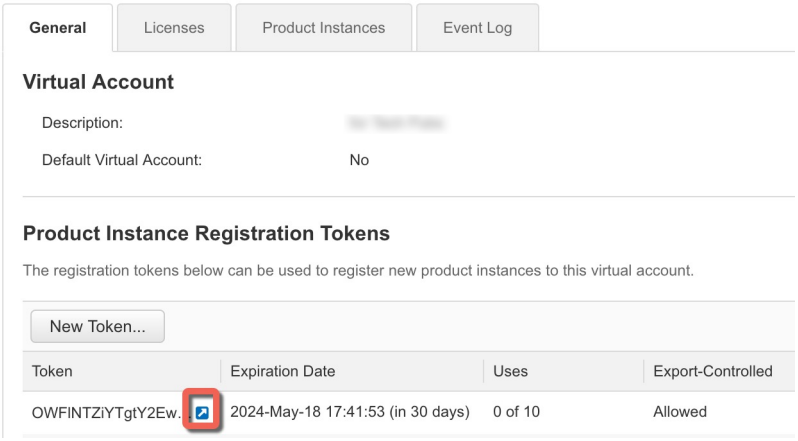
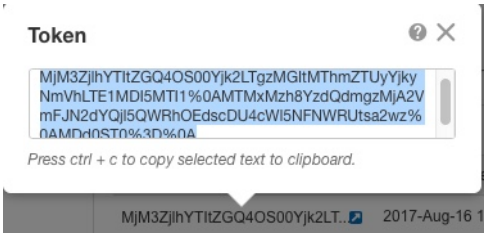


図 *5*: トークンのコピー

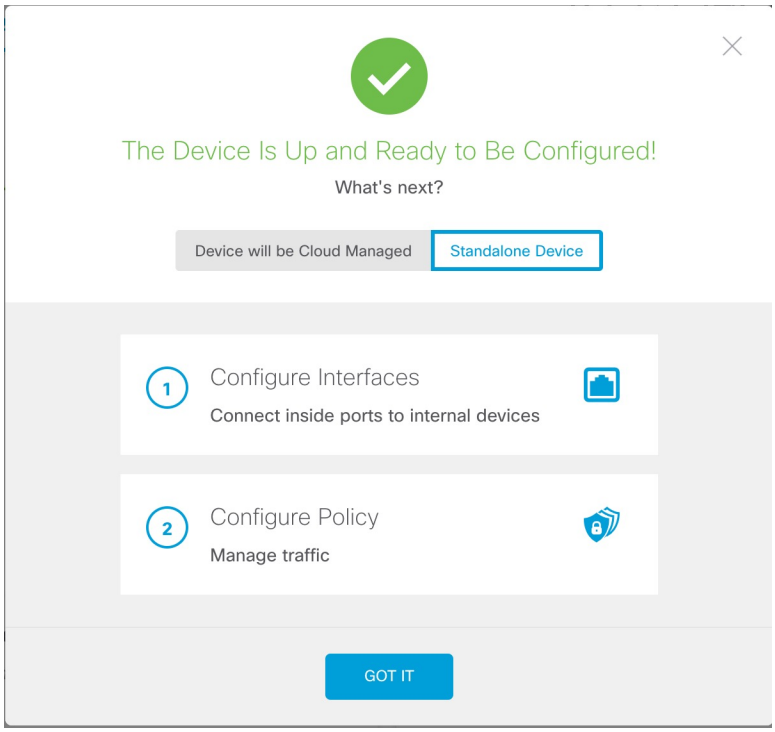


g) Firewall Device Manager で、トークンをトークンフィールドに貼り付けます。

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 *6*: 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。

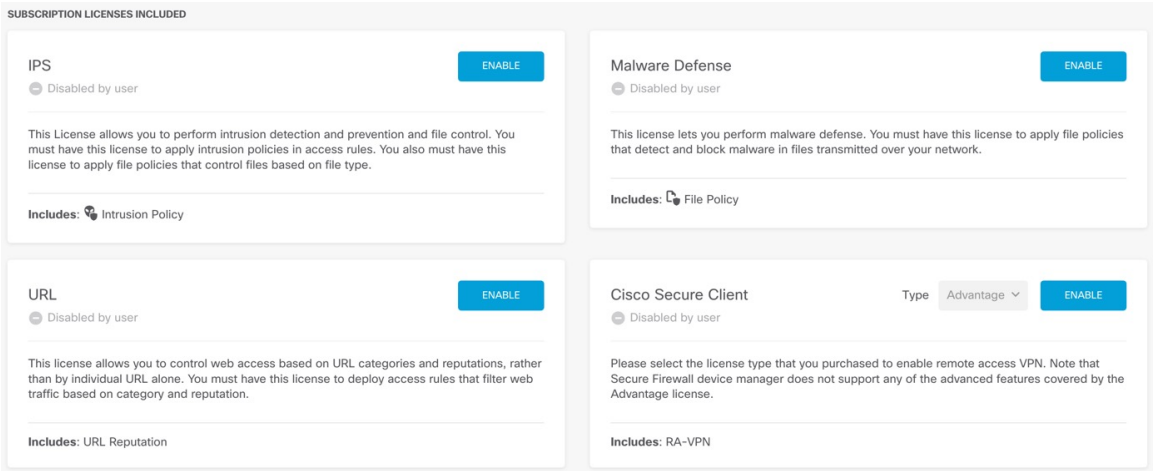
b) [**Configure Interfaces**] をクリックして [**Interfaces**] ページに直接移動するか、[**Configure Policy**] をクリックして [**Policies**] ページに移動するか、[**Got It**] をクリックして [**Device**] ページに移動します。

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 （9 ページ）」を参照してください。

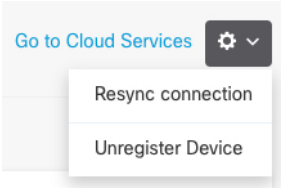
ステップ 6 機能ライセンスを有効化します。

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。

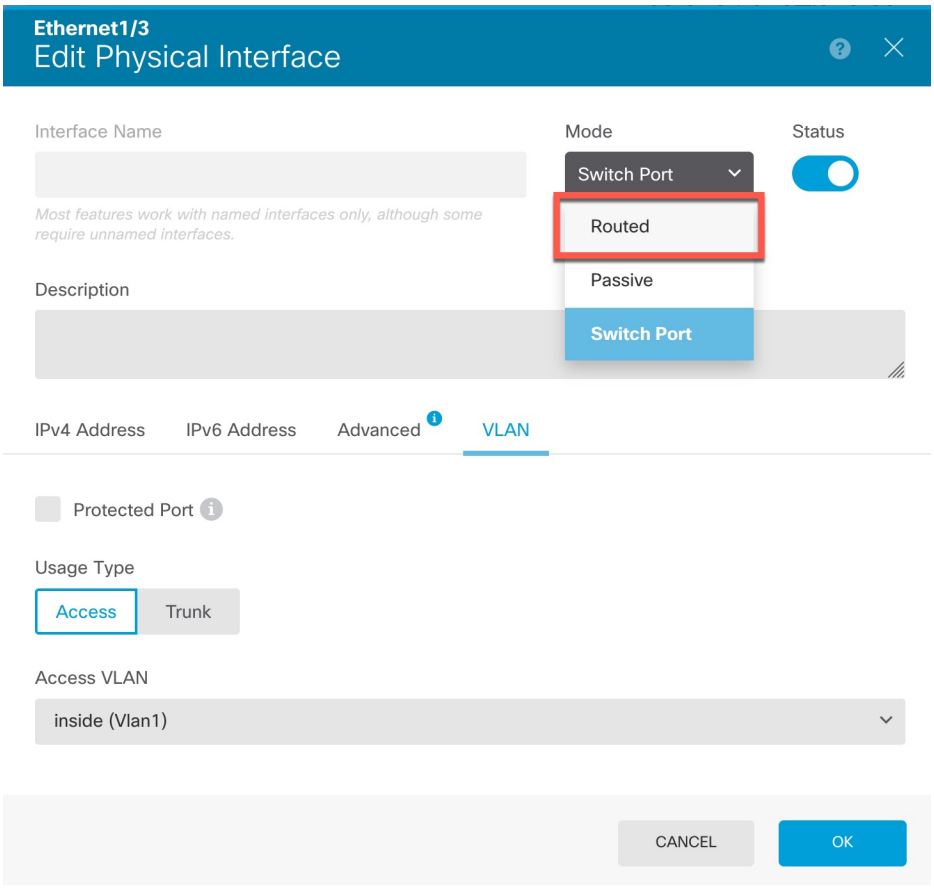
手順

ステップ 1 スイッチポートをファイアウォール インターフェイスに変換する場合は、[**Device**] を選択し、[**Interfaces**] の概要のリンクをクリックします。

a) スイッチポートの編集アイコン（）をクリックします。

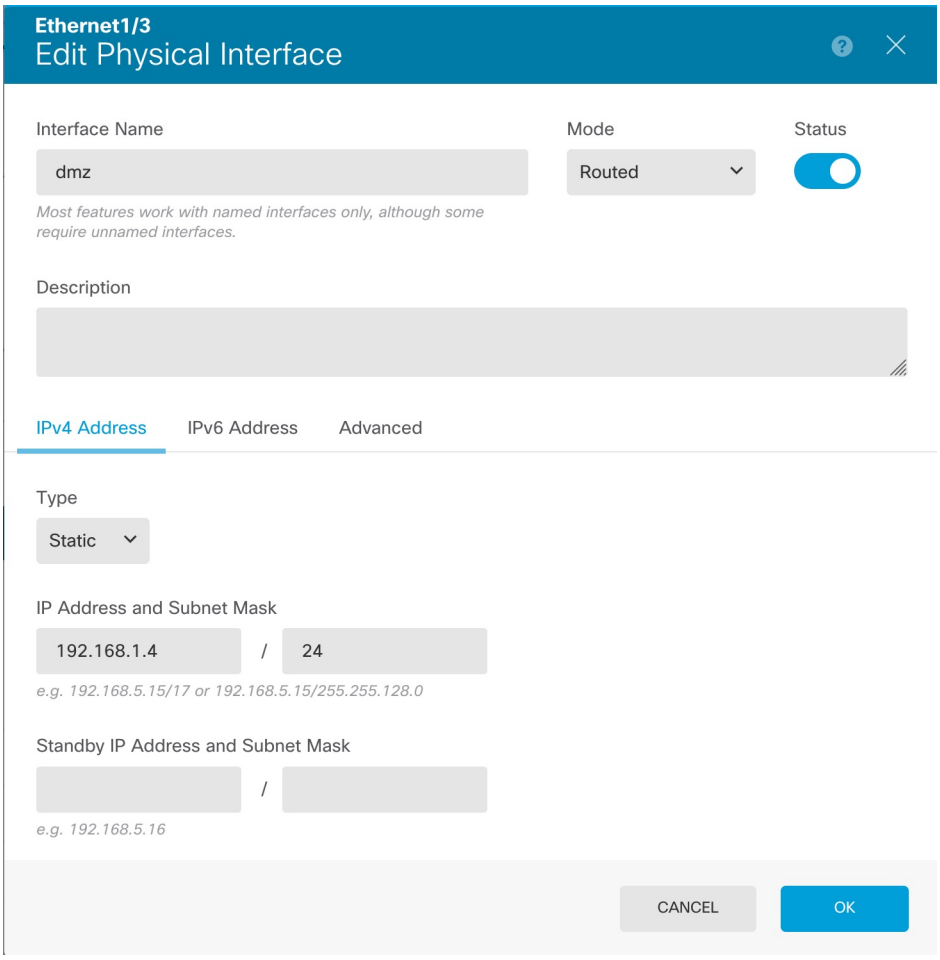
b) モードを [**Switch Port**] から [**Routed**]に変更します。

図 *7:* モードの変更



c) 名前と IP アドレスを設定します。

図 *8*:インターフェイスの編集



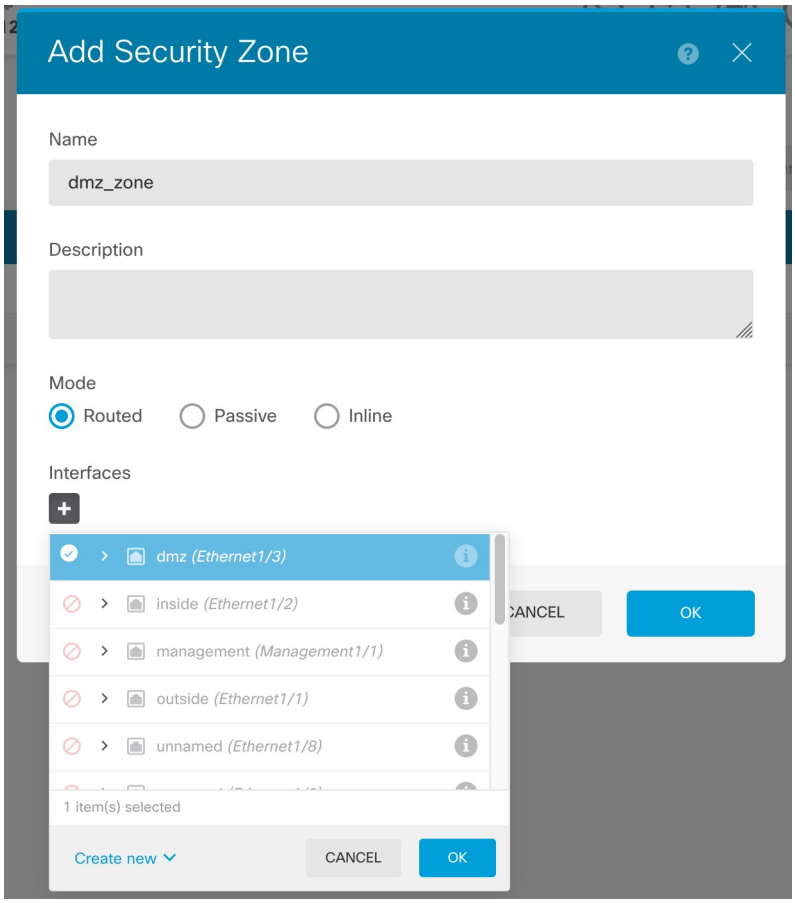
d) [OK] をクリックします。

ステップ 2 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。

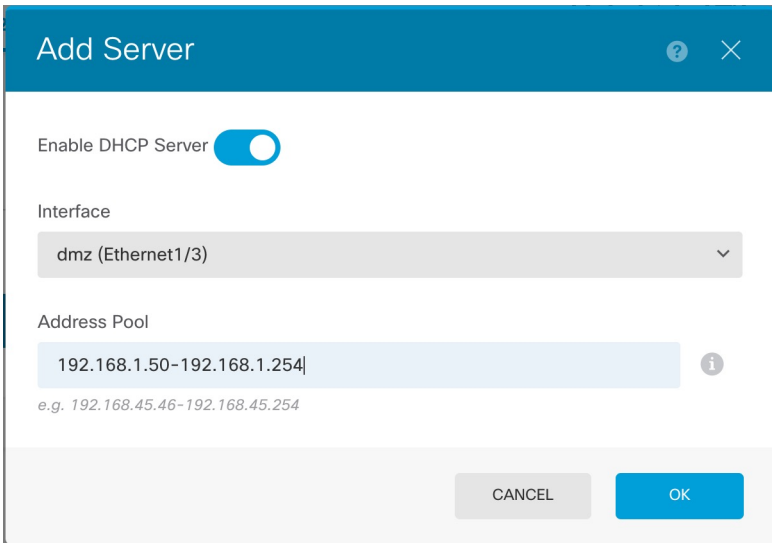
図 *9:* セキュリティ ゾーン オブジェクト



ステップ 3 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。

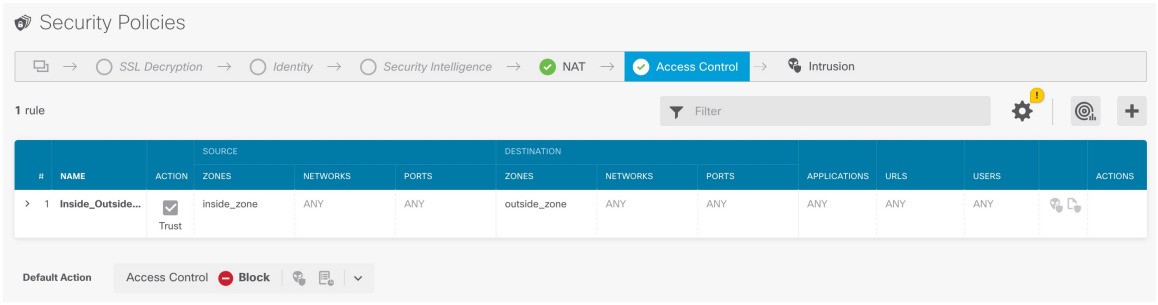
図 *10* : *DHCP* サーバー



ステップ 4 [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 *11* : 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。

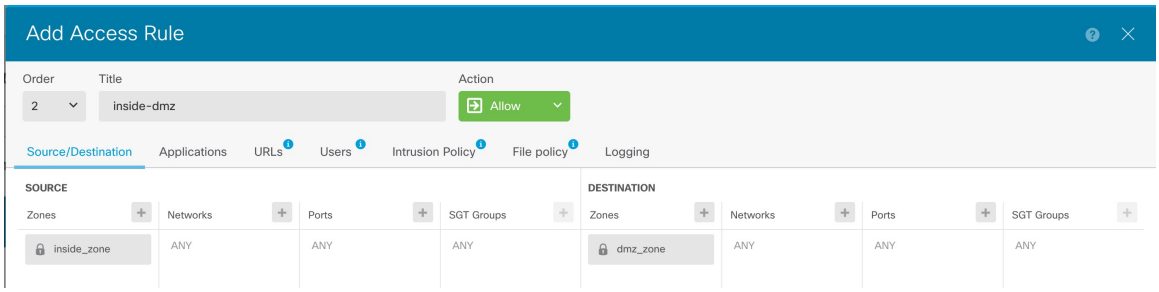
- [SSL復号（SSL Decryption）]：侵入、マルウェアなどについて暗号化された接続（HTTPS など）を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するには SSL 復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。
- [アイデンティティ（Identity）]：個々のユーザーにネットワーク アクティビティを関連付ける、またはユーザーまたはユーザー グループのメンバーシップに基づいてネットワーク アクセスを制御する場

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 *12*：アクセス コントロール ポリシー



ステップ 5 [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 6 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。