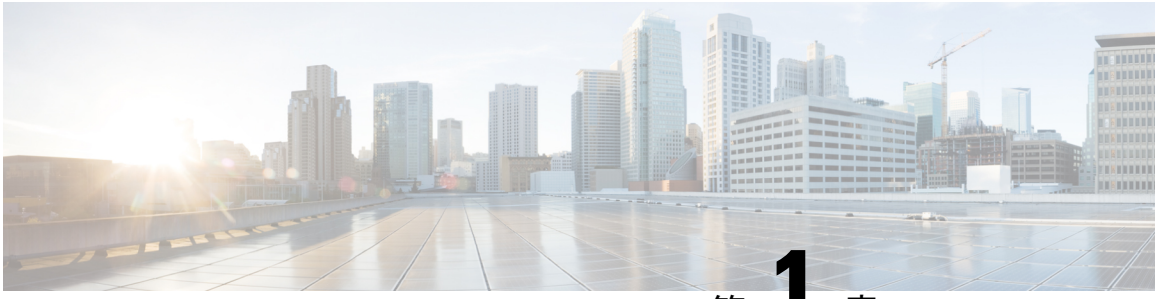
Cisco Firepower 9300 スタートアップガイド

初版：2019 年 3 月 5 日

最終更新：2023 年 1 月 23 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

最適なアプリケーションとマネージャを見つける方法

ハードウェアプラットフォームは、2 つのアプリケーションのいずれかを実行できます。アプリケーションごとに、マネージャを選択できます。この章では、アプリケーションとマネージャの選択肢について説明します。

アプリケーション

ハードウェア プラットフォームでは、Cisco Secure Firewall ASA または Secure Firewall Threat Defense（旧 Firepower Threat Defense） アプリケーションを使用できます。

- ASA：ASA は、従来の高度なステートフル ファイアウォールおよび VPN コンセントレータです。

  Threat Defense の高度な機能が必要ない場合、または Threat Defense ではまだ使用できない ASA 専用の機能が必要な場合は、ASA の使用が適しています。シスコでは、ASA から Threat Defense への移行ツールを提供しています。このツールは、ASA の使用を開始し、後に Threat Defense に再イメージ化する場合に、ASA を Threat Defense に変換するのに役立ちます。

- Threat Defense —脅威防御は、高度なステートフル ファイアウォール、VPN コンセントレータ、および次世代 IPS を組み合わせた次世代ファイアウォールです。つまり、Threat Defense は ASA の機能を最大限に活用し、最適な次世代ファイアウォールと IPS 機能を融合させます。

  Threat Defense には ASA の主要な機能の大部分に加えて、次世代ファイアウォールと IPS 機能が追加されているため、ASA よりも FTD を使用することをお勧めします。

マネージャ

Threat Defense と ASA は複数のマネージャをサポートします。

Threat Defense マネージャ

表 1 : *Threat Defense* マネージャ

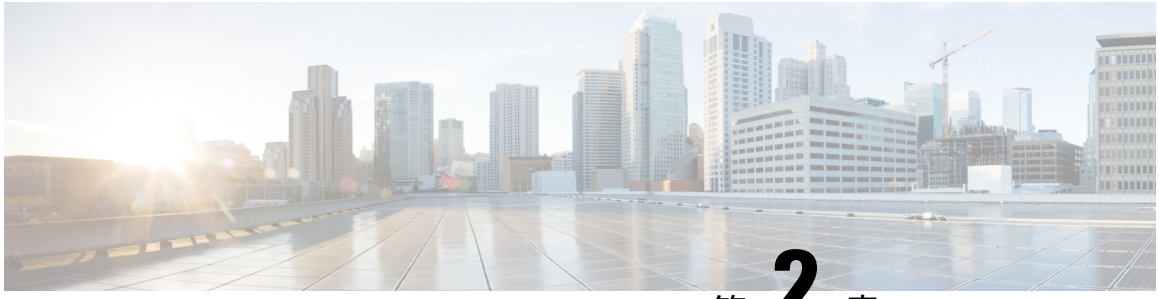
マネージャ	説明
Secure Firewall Management Center（旧 Firepower Management Center）	Management Center は強力な Web ベースのマルチデバイスマネージャです。独自のサーバーハードウェア上で、またはハイパーバイザ上の仮想デバイスとして稼働します。マルチデバイスマネージャを必要とし、Threat Defense のすべての機能が必要な場合は、Management Center を使用する必要があります。Management Center は、トラフィックとイベントの強力な分析とモニタリングも提供します。 （注） Management Center は Threat Defense 設定を持ち、Management Center をバイパスして Threat Defense を直接設定することはできないため、Management Center は他のマネージャとの互換性がありません。 Management Center を開始する前に、「Firepower 9300 シャーシの初期設定 （5 ページ）」に従ってシャーシをセットアップします。また、「Management Center での Threat Defense の展開 （35 ページ）」を参照してください。
Secure Firewall Device Manager （旧 Firepower Device Manager）	Device Manager は、Web ベースのシンプルなオンデバイスマネージャです。簡素化されているため、一部の Threat Defense 機能は Device Manager では使用できません。少数のデバイスのみを管理し、マルチデバイスマネージャを必要としない場合は、Device Manager を使用するのに適しています。 （注） FDM モードの Device Manager と CDO の両方でファイアウォールの設定を検出できるため、Device Manager と CDO を使用して同じファイアウォールを管理することが可能です。Management Center は他のマネージャと互換性がありません。 Device Manager を開始する前に、「Firepower 9300 シャーシの初期設定 （5 ページ）」に従ってシャーシをセットアップします。また、「Device Manager での Threat Defense の展開 （65 ページ）」を参照してください。

マネージャ	説明
Cisco Defense Orchestrator（CDO）	CDO には 2 つの管理モードがあります。 • （7.2 以降）オンプレミスの管理センターのすべての設定機能を備えたクラウド提供型の管理センターモード。分析機能については、クラウド内の Secure Cloud Analytics またはオンプレミスの管理センターのいずれかを使用できます。 • （既存の CDO ユーザーのみ）ユーザーエクスペリエンスが簡素化されたデバイスマネージャモード。このモードは、すでに CDO を使用してデバイスマネージャモードで Threat Defense を管理しているユーザーのみが使用できます。このモードについては、このガイドでは説明していません。 CDO はクラウドベースであるため、独自のサーバーで CDO を実行する必要はありません。CDO は ASA などの他のセキュリティデバイスも管理するため、すべてのセキュリティデバイスに単一のマネージャを使用できます。 CDO プロビジョニングを開始するには、CDO での Threat Defense の展開 （97 ページ）を参照してください。
Cisco Secure Firewall Threat Defense REST API	Threat Defense REST API を使用すると、Threat Defense の直接設定を自動化できます。Device Manager と CDO はどちらもファイアウォールで設定を検出できるため、この API はそれらの両方と互換性があります。Management Center を使用して Threat Defense を管理している場合は、この API を使用できません。 このガイドでは、Threat Defense REST API について説明しません。詳細については、Cisco Secure Firewall Threat Defense REST API ガイドを参照してください。
Secure Firewall Management Center REST API	Management Center REST API を使用すると、管理対象の Threat Defense に適用可能な Management Center ポリシーの設定を自動化できます。この API は、Threat Defense を直接管理しません。 このガイドでは、Management Center REST API について説明しません。詳細については、Cisco Secure Firewall Management Center REST API クイックスタートガイドを参照してください。

ASA マネージャ

表 *2 : ASA* マネージャ

マネージャ	説明
Adaptive Security Device Manager（ASDM）	ASDM は Java ベースのオンデバイスマネージャであり、ASA のすべての機能を提供します。CLI よりも GUI を使用することを好み、管理が必要な ASA が少数の場合は、ASDM の使用が適しています。ASDM はファイアウォールの設定を検出できるため、ASDM で CLI、CDO、または CSM を使用することも可能です。 ASDM を開始する前に、Firepower 9300 シャーシの初期設定 （5 ページ）に従ってシャーシをセットアップします。また、ASDM を使用した ASA の展開（129 ページ）を参照してください。
CLI	GUI よりも CLI を使用することを好む場合は、ASA CLI を使用してください。 CLI については、このガイドでは取り上げていません。詳細については、『ASA 構成ガイド』を参照してください。
CDO	CDO は、シンプルなクラウドベースのマルチデバイスマネージャです。シンプル化されているため、一部の ASA 機能は CDO では使用できません。シンプルな管理エクスペリエンスを提供するマルチデバイスマネージャが必要な場合、CDO を使用するのに適しています。また、CDO はクラウドベースであるため、独自のサーバーで CDO を実行する必要はありません。CDO は Threat Defense などの他のセキュリティデバイスも管理するため、すべてのセキュリティデバイスに単一のマネージャを使用できます。CDO はファイアウォールの設定を検出できるため、CLI や ASDM を使用することも可能です。 CDO については、このガイドでは取り上げていません。CDO を使用する前に、CDO のホームページを参照してください。
Cisco Security Manager（CSM）	CSM は、独自のサーバーハードウェア上で動作する強力なマルチデバイスマネージャです。多数の ASA を管理する必要がある場合、CSM を使用するのに適しています。CSM はファイアウォールの設定を検出できるため、CLI や ASDM を使用することも可能です。CSM は Threat Defense の管理をサポートしていません。 CSM については、このガイドでは取り上げていません。詳細については、『CSM ユーザーガイド』を参照してください。
ASA REST API	ASA REST API を使用すると、ASA の設定を自動化できます。ただし、API にはすべての ASA 機能が搭載されておらず、拡張されることもありません。 ASA REST API については、このガイドでは取り上げていません。詳細については、Cisco ASA REST API クイック スタート ガイドを参照してください。



第 2 章

Firepower 9300 シャーシの初期設定

この章の対象読者

この章では、Cisco Firepower 9300 シャーシの初期設定の方法について、ASA および 脅威に対する防御 論理デバイスで使用するためのインターフェイスの設定を含めて説明します。

このガイドの対象読者

このガイドでは、ASA および/または 脅威に対する防御 アプリケーションで使用するために Firepower 9300 シャーシを設定する方法について説明します。このガイドでは、次の展開について説明します。

- Management Center を使用したネイティブまたはコンテナインスタンス（マルチインスタンス機能）としてのスタンドアロン 脅威に対する防御
- Device Manager を使用したスタンドアロン 脅威に対する防御

（注） Device Manager はマルチインスタンスをサポートしていません。

- CDO を使用したスタンドアロン 脅威に対する防御

（注） CDO はマルチインスタンスをサポートしていません。

- ASDM を使用したスタンドアロン ASA

このガイドでは以下の展開については取り上げていませんので、FXOS、ASA、FDM、CDO、および FMC のコンフィギュレーション ガイドを参照してください。

- ハイ アベイラビリティ/フェールオーバー
- クラスタリング（ASA、または Management Center のみを使用した 脅威に対する防御 ）
- マルチインスタンス（Management Center のみを使用した 脅威に対する防御 ）
- Radware DefensePro デコレータ アプリケーション
- CLI 設定（ASA または FXOS のみ）

このガイドでは、基本的なセキュリティ ポリシーの設定手順についても説明します。より高度な要件がある場合は、コンフィギュレーション ガイドを参照してください。

Firepower 9300 シャーシについて

Firepower 9300 シャーシは、ネットワークおよびコンテンツ セキュリティ ソリューションの次世代プラットフォームです。Firepower 9300 シャーシには、スーパバイザと、論理デバイスをインストールできる最大 3 つのセキュリティ モジュールが含まれています。また、複数の高パフォーマンス ネットワーク モジュールも組み込むことができます。

論理デバイスの動作方法：Firepower 4100/9300

Firepower 4100/9300 は、Firepower eXtensible Operating System（FXOS）という独自のオペレーティング システムをスーパバイザ上で実行します。オンボックスの シャーシマネージャ では、シンプルな GUI ベースの管理機能を利用できます。シャーシマネージャ を使用して、ハードウェア インターフェイスの設定、スマートライセンシング（ASA 用）、およびその他の基本的な操作パラメータをスーパバイザ上で設定します。FXOS CLI を使用する場合は、『FXOS CLI コンフィグレーション ガイド』を参照してください。

論理デバイスでは、1 つのアプリケーション インスタンスおよび 1 つのオプション デコレータ アプリケーションを実行し、サービス チェーンを形成できます。論理デバイスを導入すると、スーパバイザは選択されたアプリケーション イメージをダウンロードし、デフォルト設定を確立します。その後、アプリケーションのオペレーティング システム内でセキュリティ ポリシーを設定できます。

論理デバイスは互いにサービスチェーンを形成できず、バックプレーンを介して相互に通信することはできません。別の論理デバイスに到達するために、すべてのトラフィックが 1 つのインターフェイス上のシャーシから出て、別のインターフェイスに戻る必要があります。コンテ

ナインスタンスの場合、データインターフェイスを共有できます。この場合にのみ、複数の論理デバイスがバックプレーンを介して通信できます。

（注） 異なるアプリケーションタイプをシャーシ内の別個のモジュールにインストールすることができます。別個のモジュールでは、異なるリリースのアプリケーションタイプも実行できます。

サポートされるアプリケーション

次のアプリケーション タイプを使用して、シャーシに論理デバイスを展開できます。

Threat Defense

脅威に対する防御 は、ステートフル ファイアウォール、ルーティング、VPN、Next-Generation Intrusion Prevention System（NGIPS）、Application Visibility and Control（AVC）、URL フィルタリング、マルウェア防御などの次世代ファイアウォールサービスを提供します。

脅威に対する防御 は、次のいずれかのマネージャを使用して管理できます。

- Management Center：別のサーバ上で実行されるフル機能のマルチデバイス マネージャ。
- Device Manager ：デバイスに含まれるシンプルな単独のデバイスマネージャ。
- CDO：クラウドベースのマルチデバイスマネージャ。

ASA

ASA は、高度なステートフル ファイアウォールと VPN コンセントレータの機能を 1 つの装置に組み合わせたものです。次のいずれかのマネージャを使用して ASA を管理できます。

- ASDM：デバイスに含まれるシンプルな単独のデバイス マネージャ。このガイドでは、*ASDM* を使用して *ASA* を管理する方法について説明します。
- CLI
- CDO：クラウドベースのマルチデバイスマネージャ。
- CSM：別のサーバー上のマルチデバイスマネージャ。

Radware DefensePro （デコレータ）

Radware DefensePro（vDP）をインストールし、デコレータアプリケーションとして ASA または 脅威に対する防御 の目の前で実行することができます。vDP は、Firepower 4100/9300 に分散型サービス妨害（DDoS）の検出と緩和機能を提供する KVM ベースの仮想プラットフォームです。ネットワークからのトラフィックは、ASA または 脅威に対する防御 に到達する前に、まず vDP を通過する必要があります。

vDP を展開するには、『FXOS コンフィグレーション ガイド』を参照してください。

論理デバイスのアプリケーションインスタンス：コンテナとネイティブ

論理デバイスのアプリケーション インスタンスは次の展開タイプで実行されます。

- ネイティブ インスタンス：ネイティブ インスタンスはセキュリティ モジュールのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブ インスタンスを 1 つのみインストールできます。
- コンテナ インスタンス：コンテナ インスタンスでは、セキュリティ モジュールのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。
  注：マルチインスタンス機能は、脅威に対する防御 でのみサポートされています。ASA または vDP との組み合わせではサポートされていません。

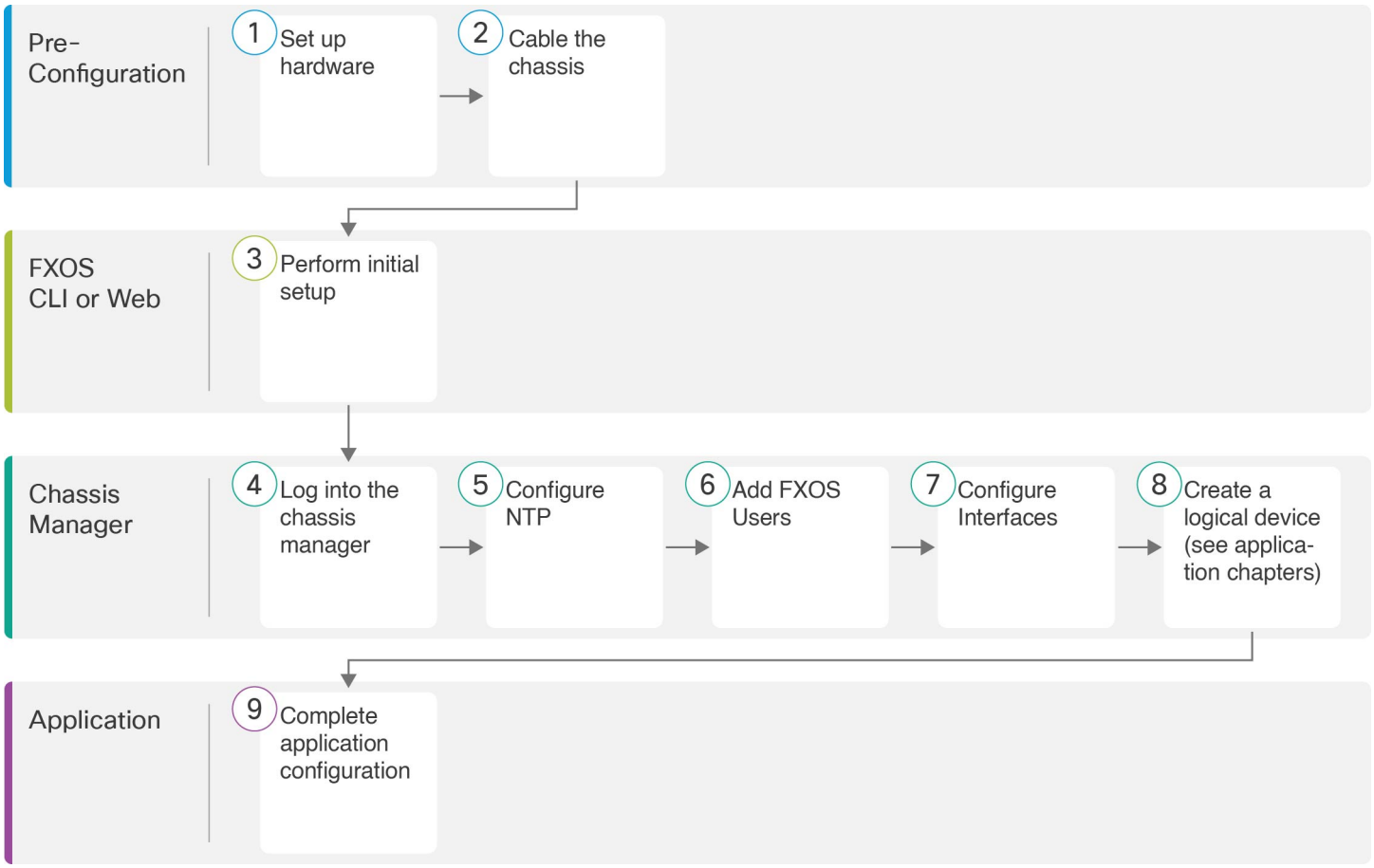
一部のモジュールでネイティブ インスタンスを使用し、その他のモジュールでコンテナ インスタンスを使用することができます。

モデルごとの最大コンテナ インスタンス数

- Firepower 9300 SM-24 セキュリティ モジュール：7
- Firepower 9300 SM-36 セキュリティ モジュール：11
- Firepower 9300 SM-40 セキュリティ モジュール：13
- Firepower 9300 SM-44 セキュリティ モジュール：14
- Firepower 9300 SM-48 セキュリティ モジュール：15
- Firepower 9300 SM-56 セキュリティ モジュール：18

エンドツーエンドの手順

Firepower 9300 シャーシを設定し、シャーシに論理デバイスを展開するには、次のタスクを参照してください。



1	事前設定	Firepower 9300 ハードウェアをセットアップします。『Firepower 9300 ハードウェアガイド』を参照してください。
2	事前設定	シャーシのケーブル接続 （10 ページ）。
3	FXOS CLI または Web	シャーシの初期セットアップの実行 （15 ページ）。
4	Chassis Manager	Chassis Manager へのログイン （20 ページ）。
5	Chassis Manager	NTP の設定 （20 ページ）。
6	Chassis Manager	FXOS ユーザーの追加 （22 ページ）。
7	Chassis Manager	インターフェイスの設定 （24 ページ）。

8	Chassis Manager	論理デバイスを作成します。 • Management Center を使用した Threat Defense ：Management Center での Threat Defense の展開 （35 ページ）を参照してください。 • Device Manager を使用した Threat Defense ：Device Manager での Threat Defense の展開 （65 ページ）を参照してください。 • CDO を使用した Threat Defense ：CDO での Threat Defense の展開 （97 ページ）を参照してください。 • ASA：ASDM を使用した ASA の展開 （129 ページ） を参照してください。 （注） 同じシャーシ上の 脅威に対する防御 と ASA の両方のサポートが FXOS 2.6.1/脅威に対する防御 6.4/ASA 9.12(1) で追加されました。 （注） Device Manager を使用した 脅威に対する防御 のサポートが FXOS 2.7.1/脅威に対する防御 6.5 で追加されました。
9	アプリケーション	アプリケーション構成を完了します。 • Management Center を使用した Threat Defense ：Management Center での Threat Defense の展開 （35 ページ）を参照してください。 • Device Manager を使用した Threat Defense ：Device Manager での Threat Defense の展開 （65 ページ）を参照してください。 • CDO を使用した Threat Defense ：CDO での Threat Defense の展開 （97 ページ）を参照してください。 • ASA：ASDM を使用した ASA の展開 （129 ページ） を参照してください。

シャーシのケーブル接続

シャーシの初期設定、継続的なモニタリング、論理デバイスの使用には、次のインターフェイスにケーブルを配線します。

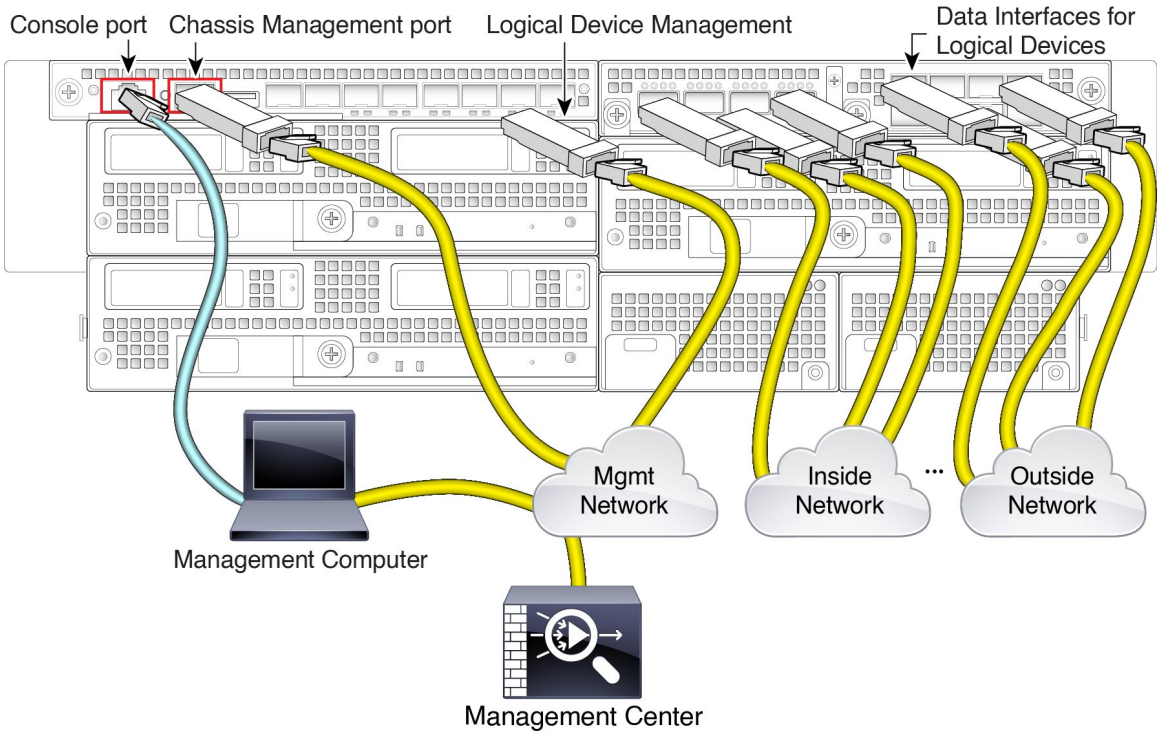
- コンソールポート：（オプション）シャーシ管理ポートで初期セットアプを実行しない場合は、管理コンピュータをコンソールポートに接続して、シャーシの初期セットアップを実行します。Firepower 9300 には、RS-232 - RJ-45 シリアルコンソールケーブルが付属しています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。

- シャーシ管理ポート：シャーシ管理ポートを管理ネットワークに接続し、シャーシの設定と継続的な管理を行います。この管理ポートで DHCP サーバーから IP アドレスを受信する場合は、このポートで初期セットアップを実行できます。
- 論理デバイス管理インターフェイス: 1 つ以上のインターフェイスを使用して論理デバイスを管理します。このガイドでは、独自のインターネットアクセスを持つ別の管理ネットワークがあることを前提としています。シャーシ管理ポート以外は、シャーシ上の任意のインターフェイスを選択できます。シャーシ管理ポートは、FXOS 管理用に予約されています。管理インターフェイスを論理デバイス間で共有できます。また、論理デバイスごとに別のインターフェイスを使用することもできます。通常は、管理インターフェイスをすべての論理デバイスと共有します。または、別個のインターフェイスを使用する場合は、それらを単一の管理ネットワークに配置します。ただし、正確なネットワーク要件は場合によって異なります。Threat Defense の場合、管理インターフェイスはデータインターフェイスとは別のインターフェイスであり、独自のネットワーク設定があります。6.7 以降では、管理インターフェイスを使用する代わりに、必要に応じて、データインターフェイスをマネージャアクセス用に設定できます。この場合でも、内部のアーキテクチャ上の理由から管理インターフェイスを論理デバイスに割り当てる必要がありますが、ケーブル接続は必要ありません。Management Center の場合、データインターフェイスからのマネージャアクセスは、高可用性またはクラスタリング展開ではサポートされません。詳細については、『FTD command reference』の **configure network management-data-interface** コマンドを参照してください。
- データインターフェイス：データインターフェイスを論理デバイスデータネットワークに接続します。物理インターフェイス、EtherChannel、VLAN サブインターフェイス（コンテナインスタンスの場合のみ）、およびブレイクアウトポートを設定して、大容量のインターフェイスを分割できます。ネットワークのニーズに応じて、複数の論理デバイスを同じネットワークまたは異なるネットワークにケーブル接続できます。コンテナインスタンスの場合、データインターフェイスを共有できます。この場合にのみ、複数の論理デバイスがバックプレーンを介して通信できます。それ以外の場合は、別の論理デバイスに到達するために、すべてのトラフィックが 1 つのインターフェイス上のシャーシから出て、別のインターフェイスに戻る必要があります。共有インターフェイスの制限事項とガイドラインの詳細については、『FXOS コンフィグレーション ガイド』を参照してください。

（注） コンソール ポート以外のすべてのインターフェイスには、SFP/SFP+/QSFP のトランシーバーが必要です。サポートされているトランシーバーについては、『Cisco Firepower 9300 ハードウェア設置ガイド』を参照してください。

（注） このガイドでは説明していませんが、ハイアベイラビリティの場合は、フェールオーバー/ステートリンクにデータインターフェイスを使用します。シャーシ間クラスタリングの場合は、シャーシで定義されている EtherChannel をクラスタ タイプのインターフェイスとして使用します。

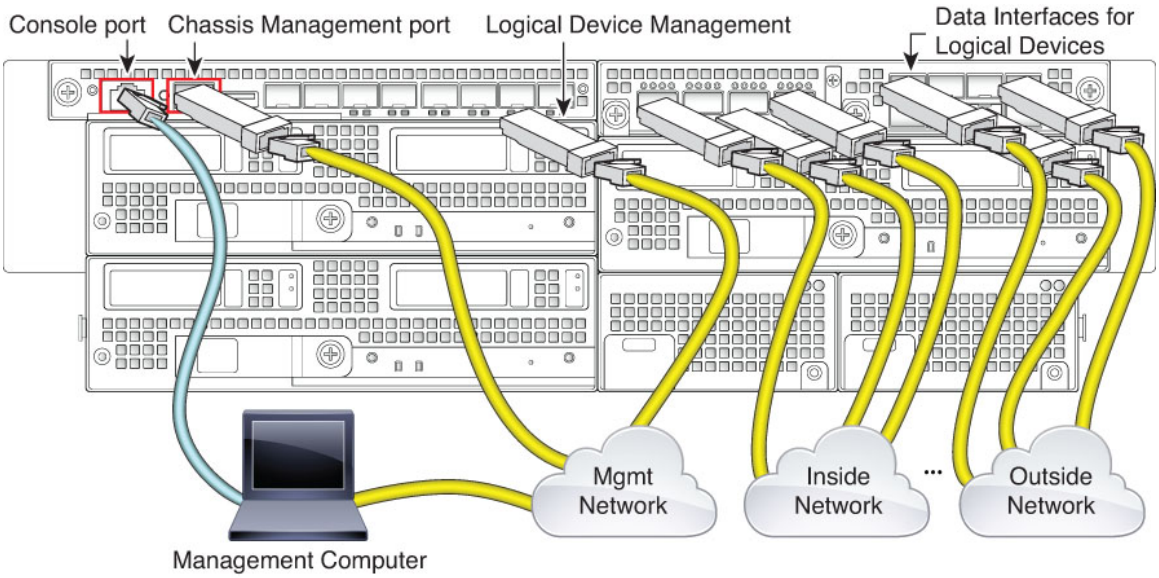
Threat Defense と Management Center のケーブル接続



このガイドでは、独自のインターネットアクセスを持つ別の管理ネットワークがあることを前提としています。デフォルトでは、管理インターフェイスは展開時に事前設定されていますが、データインターフェイスは後で設定する必要があります。

論理デバイス管理ネットワークにManagement Centerを配置（またはアクセス可能に）します。脅威に対する防御 およびManagement Centerは、更新およびライセンシングのために管理ネットワークを介してインターネットにアクセスする必要があります。6.7以降では、管理インターフェイスの代わりに、必要に応じて、データインターフェイスを Management Center の管理用に設定できます。データインターフェイスからの Management Center アクセスは、高可用性またはクラスタリング展開ではサポートされません。Management Center アクセス用のデータインターフェイスの設定の詳細については、FTD コマンドリファレンス [英語] の **configure network management-data-interface** コマンドを参照してください。

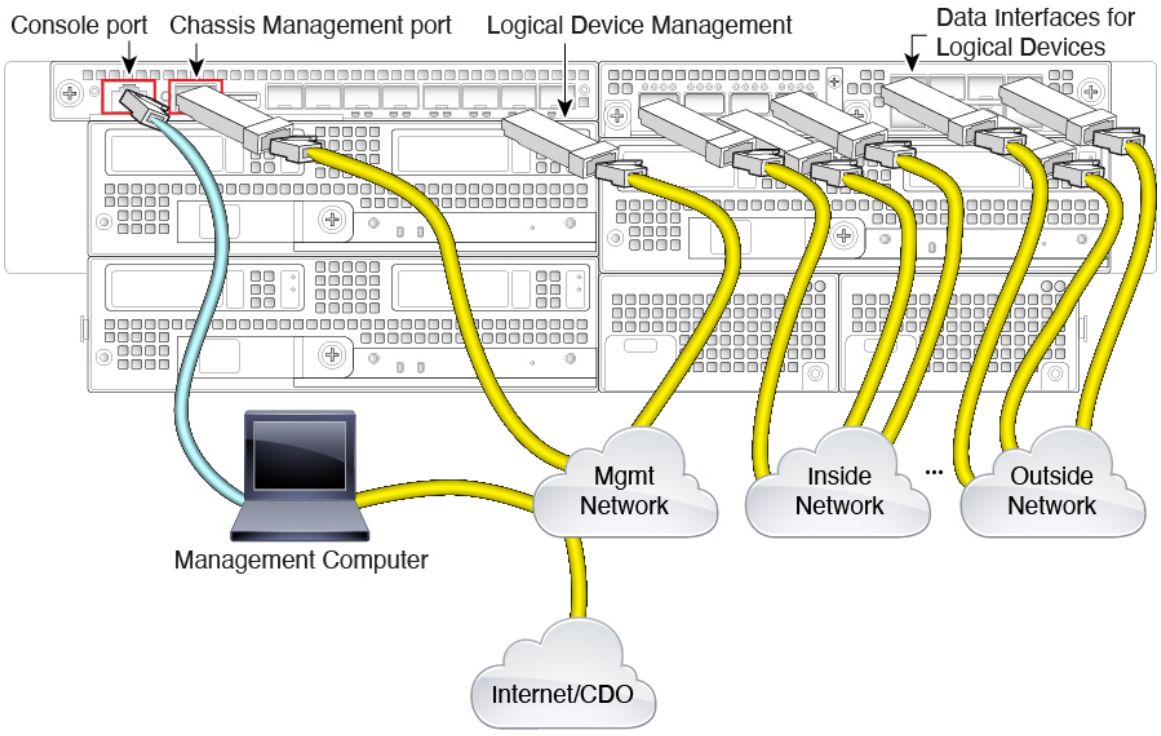
Threat Defense と Device Manager のケーブル接続



このガイドでは、独自のインターネットアクセスを持つ別の管理ネットワークがあることを前提としています。デフォルトでは、管理インターフェイスは展開時に事前設定されていますが、データインターフェイスは後で設定する必要があります。

論理デバイスの管理インターフェイスで 脅威に対する防御 の初期設定を実行します。脅威に対する防御 では、ライセンシング、更新、およびCDOの管理のためにインターネットアクセスが必要です。デフォルトの動作では、脅威に対する防御 の展開時に指定したゲートウェイIPアドレスに管理トラフィックがルーティングされます。後で、任意のデータインターフェイスから Device Manager の管理を有効にできます。

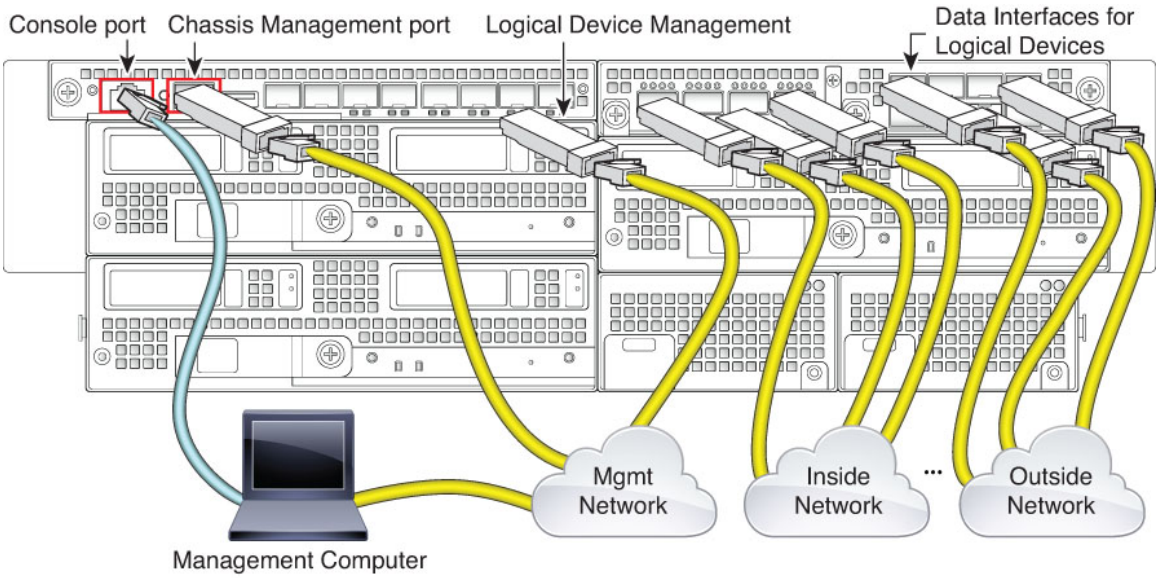
Threat Defense と CDO のケーブル接続



このガイドでは、独自のインターネットアクセスを持つ別の管理ネットワークがあることを前提としています。デフォルトでは、管理インターフェイスは展開時に事前設定されていますが、データインターフェイスは後で設定する必要があります。

論理デバイスの管理ネットワークからインターネットにアクセスできることを確認します。脅威に対する防御 は、CDO の管理、更新、およびライセンシングのために、管理ネットワーク経由でインターネットにアクセスする必要があります。管理インターフェイスの代わりに、必要に応じて、データインターフェイスを CDO の管理用に設定できます。マネージャアクセス用のデータインターフェイスの設定の詳細については、FTD コマンドリファレンス [英語] の **configure network management-data-interface** コマンドを参照してください。

ASA のケーブル接続



このガイドでは、独自のインターネットアクセスを持つ別の管理ネットワークがあることを前提としています。デフォルトでは、管理インターフェイスは展開時に事前設定されていますが、データインターフェイスは後で設定する必要があります。

論理デバイスの管理インターフェイスで ASA の初期設定を実行します。後で、任意のデータインターフェイスから管理を有効にすることができます。

シャーシの初期セットアップの実行

システムの設定と管理に Chassis Manager を使用する前に、いくつかの初期設定タスクを実行する必要があります。初期設定は、コンソールポートで FXOS CLI を使用するか、またはシャーシ管理ポートへの SSH セッションを使用するか、あるいはシャーシ管理ポートで HTTPS を使用して実行できます。

ブラウザを使用したシャーシの初期セットアップの実行

シャーシ管理ポートは、DHCP を使用して IP アドレスを取得します。初期設定では、Web ブラウザを使用してシャーシの基本設定を行うことができます。DHCP サーバーがない場合は、初期セットアップにコンソールポートを使用する必要があります。

（注） 初期セットアップを繰り返すには、CLIから次のコマンドを使用して既存の設定をすべて消去する必要があります。

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

始める前に

セットアップ スクリプトで使用する次の情報を収集します。

- 新しい管理者パスワード
- 管理 IP アドレスおよびサブネット マスク
- ゲートウェイ IP アドレス
- HTTPS と SSH アクセスを許可するサブネット
- ホスト名とドメイン名
- DNS サーバの IP アドレス

手順

ステップ 1 DHCP サーバーを設定してシャーシ管理ポートに IP アドレスを割り当てます。

シャーシからの DHCP クライアント要求には次の情報が含まれています。

- 管理インターフェイスの MAC アドレス。
- DHCP オプション 60（vendor-class-identifier）：「FPR9300」に設定します。
- DHCP オプション 61（dhcp-client-identifier）：シャーシのシリアル番号に設定します。このシリアル番号は、シャーシの引き出しタブで確認できます。

ステップ 2 シャーシの電源を入れます。

ステップ 3 ブラウザで次の URL を入力します。

https://*ip_address***/api**

DHCP サーバーによってシャーシ管理ポートに割り当てられた IP アドレスを指定します。

ステップ 4 ユーザー名とパスワードの入力を求められたら、それぞれ **install** と *chassis_serial_number* を入力してログインします。

chassis_serial_number は、シャーシのプルアウトタブで確認できます。

ステップ 5 プロンプトに従ってシステム設定を行います。

- 強力なパスワード適用ポリシー。
- admin アカウントのパスワード。
- システム名。
- スーパーバイザ管理の IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス。
- デフォルト ゲートウェイの IPv4 アドレスまたは IPv6 アドレス。
- SSH アクセスが許可されているホスト/ネットワーク アドレスおよびネットマスク/プレフィックス。
- HTTPS アクセスが許可されるホスト/ネットワークアドレスとネットマスク/プレフィックス。
- DNS サーバの IPv4 または IPv6 アドレス。
- デフォルト ドメイン名。

ステップ 6 **[送信（Submit）]** をクリックします。

CLI でのシャーシの初期セットアップの実行

コンソールで FXOS CLI に初めてアクセスするか、またはシャーシ管理ポートに対して SSH セッションを使用すると、セットアップウィザードによって基本的なネットワーク設定を求めるプロンプトが表示され、シャーシ管理ポートから Chassis Manager（HTTPS を使用）または FXOS CLI（SSH を使用）にアクセスできるようになります。

シャーシ管理ポートは、DHCP を使用して IP アドレスを取得します。DHCP サーバーがない場合は、初期セットアップにコンソールポートを使用する必要があります。

（注） 初期設定を繰り返すには、次のコマンドを使用して既存の設定をすべて消去する必要があります。

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

始める前に

セットアップ スクリプトで使用する次の情報を収集します。

- 新しい管理者パスワード
- 管理 IP アドレスおよびサブネット マスク

- ゲートウェイ IP アドレス
- HTTPS および SSH アクセスを許可するサブネット
- ホスト名とドメイン名
- DNS サーバの IP アドレス

手順

ステップ 1 シャーシの電源を入れます。

ステップ 2 ターミナルエミュレータを使用してシリアルコンソールポートに接続するか SSH を使用してシャーシ管理ポートに接続します。

Firepower 9300 には、RS-232 - RJ-45 シリアルコンソールケーブルが付属しています。接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。次のシリアルパラメータを使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

ステップ 3 ユーザー名とパスワードの入力を求められたら、それぞれ **admin** と **cisco123** を入力してログインします。

ステップ 4 プロンプトに従ってシステム設定を行います。

例：

```
           ---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.


You have chosen to setup a new Security Appliance.
      Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name:  firepower-9300
```

```
  Supervisor Mgmt IP address : 10.80.6.12

  Supervisor Mgmt IPv4 netmask : 255.255.255.0

  IPv4 address of the default gateway : 10.80.6.1

  The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

  Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

  SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

  SSH Mgmt Access IPv4 netmask: 255.0.0.0

  Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

  Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

  HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

  HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

  Configure the DNS Server IP address? (yes/no) [n]: y

    DNS IP address : 10.164.47.13

  Configure the default domain name? (yes/no) [n]: y

    Default domain name : cisco.com

  Following configurations will be applied:

    Switch Fabric=A
    System Name=firepower-9300
    Enforced Strong Password=no
    Supervisor Mgmt IP Address=10.89.5.14
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    DNS Server=72.163.47.11
    Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
  Applying configuration. Please wait...  Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#
```

ステップ 5 使用している場合はコンソールポートから切断したり、SSHセッションを終了することができます。

Chassis Manager へのログイン

Chassis Manager を使用して、インターフェイスの有効化や論理デバイスの展開など、シャーシの設定を行います。

始める前に

- サポートされるブラウザの詳細については、使用しているバージョンのリリース ノートを参照してください（http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html を参照）。
- 最初のシャーシのセットアップ時に指定した範囲内の IP アドレスを持つ管理コンピュータからのみ、Chassis Manager にアクセスできます。

手順

ステップ 1 サポートされているブラウザを使用して、次の URL を入力します。

https://*chassis_mgmt_ip_address*

- *chassis_mgmt_ip_address*：初期設定時に入力したシャーシ管理ポートの IP アドレスまたはホスト名です。

ステップ 2 ユーザー名 **admin** と新しいパスワードを入力します。

FXOS ユーザーの追加 （22 ページ） に従って、後でさらにユーザーを追加できます。

ステップ 3 [ログイン（Login）] をクリックします。
ログインすると Chassis Manager が開き、[概要（Overview）] ページが表示されます。

NTP の設定

手動で時刻を設定することもできますが、NTP サーバーを使用することを推奨します。ASA および 脅威に対する防御 と Device Manager のスマート ソフトウェア ライセンシングには正しい時刻が必要です。脅威に対する防御 と Management Center の場合は、シャーシと Management Center の間で時刻が一致している必要があります。この場合は、Management Center の場合と同じ NTP サーバーをシャーシで使用することを推奨します。Management Center 自身を NTP サーバーとして使用しないでください。この方法はサポートされていません。

始める前に

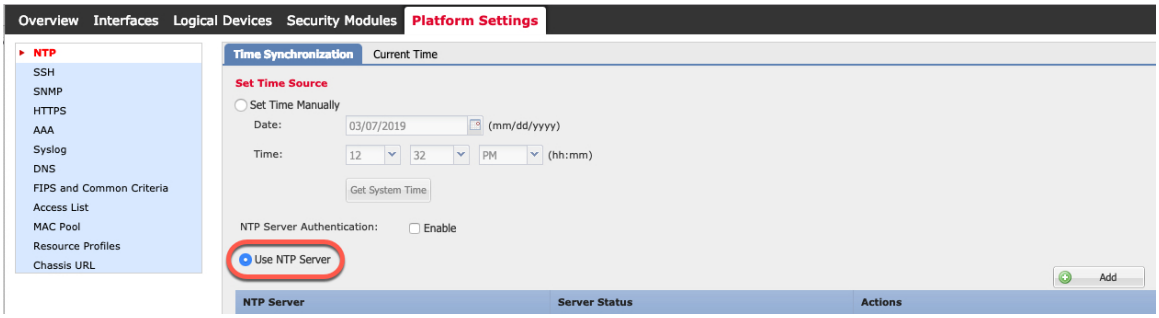
NTP サーバーのホスト名を使用する場合は、DNS サーバーを設定する必要があります（最初のセットアップで未実施の場合）。**[プラットフォーム設定（Platform Settings）]** > **[DNS]** を参照してください。

手順

ステップ 1 **[プラットフォーム設定（Platform Settings）]** > **[NTP]** を選択します。

[時間同期（Time Synchronization）] ページがデフォルトで選択されています。

ステップ 2 [NTPサーバーを使用する（Use NTP Server）] オプション ボタンをクリックします。

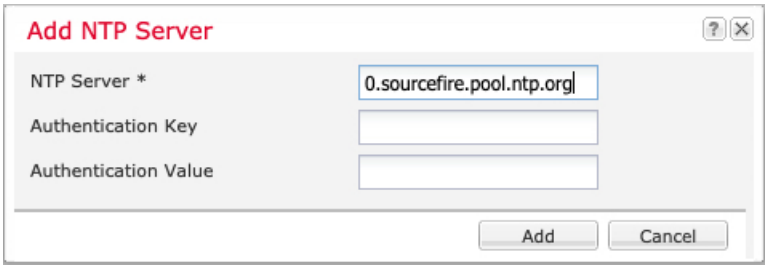


ステップ 3 （任意） NTP サーバーで認証が必要な場合は、[NTPサーバー認証：有効（NTP Server Authentication: Enable）] チェックボックスをオンにします。

NTP 認証を有効にすることが求められます。すべての NTP サーバー エントリで認証キーの ID と値を必要とする場合は、[Yes] をクリックします。

NTP サーバー認証では SHA1 のみがサポートされます。

ステップ 4 [追加（Add）] をクリックし、次のパラメータを設定します。



- [NTPサーバー（NTP Server）]：NTP サーバーの IP アドレスまたはホスト名
- [認証キー（Authentication key）] および [認証値（authentication VALUE）]：NTP サーバーからキー ID と値を取得します。たとえば、OpenSSL がインストールされた NTP サーババージョン 4.2.8 p8 以降で SHA1 キーを生成するには、**ntp-keygen -M** コマンドを入力して ntp. keys ファイルでキー ID と値を確認します。このキーは、クライアントとサーバの

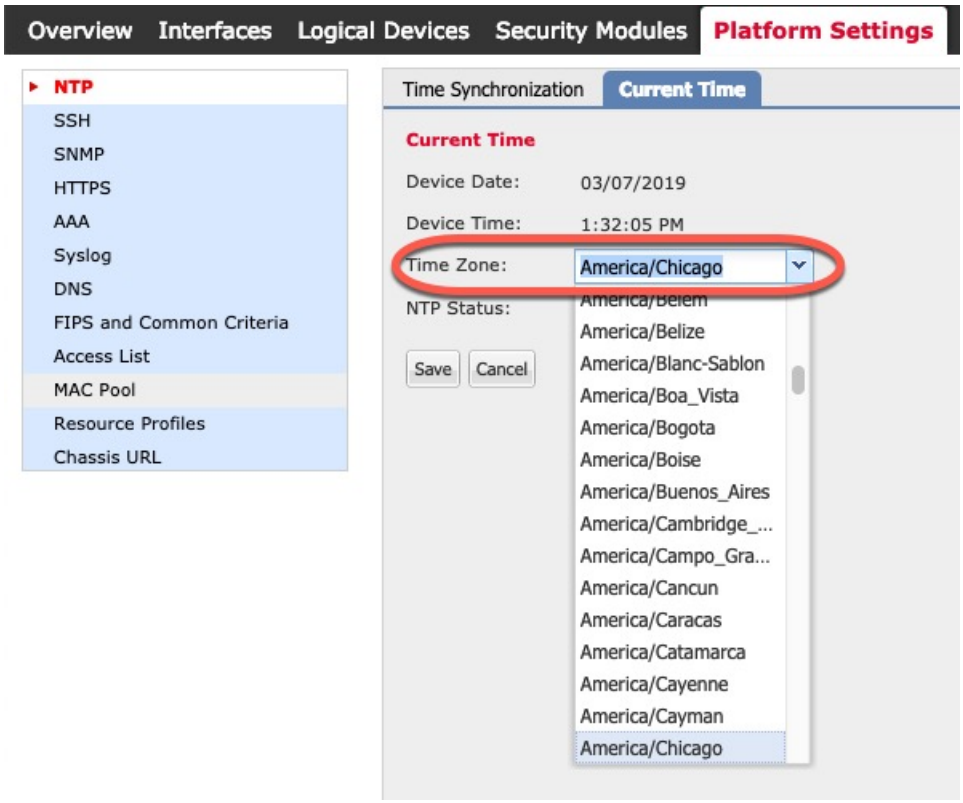
両方に対して、メッセージダイジェストの計算時に使用するキー値を通知するために使用します。

ステップ 5 [追加（Add）] をクリックしてサーバーを追加します。

NTP サーバーは最大 4 つまで追加できます。

ステップ 6 [保存（Save）] をクリックしてサーバーを保存します。

ステップ 7 [現在時刻（Current Time）] をクリックし、[タイムゾーン（Time Zone）] ドロップダウンリストからシャーシに適したタイム ゾーンを選択します。



ステップ 8 [保存（Save）] をクリックします。

（注） システム時刻の変更に 10 分以上かかると、自動的にログアウトされ、Chassis Manager への再ログインが必要になります。

FXOS ユーザーの追加

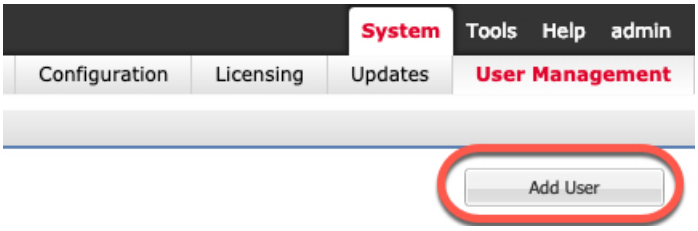
Chassis Manager および FXOS CLI ログインのローカルユーザーを追加します。

手順

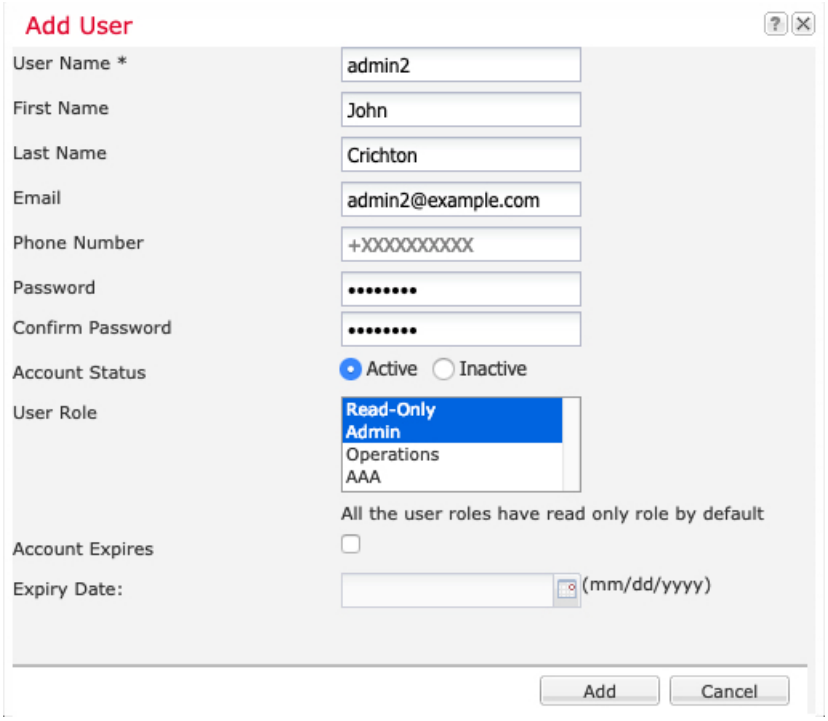
ステップ 1 **[システム（System）] > [ユーザー管理（User Management）]** を選択します。

ステップ 2 [ローカルユーザー（Local Users）] をクリックします。

ステップ 3 [ユーザの追加（Add User）] をクリックして [ユーザの追加（Add User）] ダイアログボックスを開きます。



ステップ 4 ユーザに関して要求される情報を使用して、次のフィールドに値を入力します。



- [ユーザー名（User Name）]：最大 32 文字のユーザー名を設定します。ユーザを保存した後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。
- （任意）[名（First name）]：ユーザーの名前を最大 32 文字で設定します。
- （任意）[姓（Last name）]：ユーザーの姓を最大 32 文字で設定します。
- （任意）[電子メール（Email）]：ユーザーの電子メール アドレスを設定します。
- （任意）[電話番号（Phone Number）]：ユーザーの電話番号を設定します。

- [パスワード（Password）]および[パスワードの確認（Confirm Password）]：このアカウントに関連付けられているパスワードを設定します。パスワード強度チェックを有効にした場合は、ユーザーパスワードを強固なものにする必要があります。FXOSは強度チェック要件を満たしていないパスワードを拒否します。強力なパスワードのガイドラインについては、『FXOS コンフィグレーション ガイド』を参照してください。
- [アカウントステータス（Account status）]：ステータスを[アクティブ（Active）]または[非アクティブ（Inactive）]に設定します。
- [ユーザーロール（User Role）]：ユーザーアカウントに割り当てる権限を表すロールを設定します。すべてのユーザーはデフォルトでは [読み取り専用（Read-Only）] ロールが割り当てられます。このロールは選択解除できません。別のロールを割り当てるには、ウィンドウ内のロール名をクリックして、そのロールが強調表示されるようにします。次のユーザー ロールのいずれかを使用できます。
  - [管理（Admin）]：システム全体に対する完全な読み取りと書き込みのアクセス権。
  - [読み取り専用（Read-Only）]：システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。
  - [運用（Operations）]：NTP の設定、Smart Licensing のための Smart Call Home の設定、システム ログ（syslog サーバーとエラーを含む）に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。
  - [AAA管理者（AAA Administrator）]：ユーザー、ロール、および AAA 設定に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。
- （任意）[アカウント有効期限（Account expires）]：このアカウントの有効期限を設定します。アカウントは、[有効期限（Expiry Date）] フィールドで指定された日付の後には使用できません。ユーザアカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、使用できる最新の有効期限日付でアカウントを設定することは可能です。デフォルトでは、ユーザー アカウントの有効期限はありません。
- （任意）[有効期限（Expiry Date）]：アカウントが期限切れになる日付。日付の形式は *yyyy-mm-dd* です。このフィールドの終端にあるカレンダー アイコンをクリックするとカレンダーが表示され、それを使用して期限日を選択できます。

ステップ 5 [追加（Add）] をクリックします。

インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。FXOS では、インターフェイスを有効にし、EtherChannels を追加して、VLAN サブインターフェイスを追加し、インターフェイスプロパティを編集できます。インターフェイスを使用するには、インターフェイスを FXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

ブレイクアウト ポートを設定するには、『FXOS コンフィグレーション ガイド』を参照してください。

インターフェイス タイプ

各インターフェイスは、次のいずれかのタイプになります。

- Data：通常のデータに使用します。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- Data-sharing：通常のデータに使用します。コンテナインスタンスでのみサポートされ、これらのデータインターフェイスは 1 つまたは複数の論理デバイス/コンテナインスタンス（脅威に対する防御 Management Center 専用）で共有できます。 各コンテナ インスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バックプレーン経由で通信できます。共有インターフェイスは、展開可能なコンテナインスタンスの数に影響することがあります。共有インターフェイスは、ブリッジグループ メンバーインターフェイス（トランスペアレントモードまたはルーテッドモード）、インラインセット、パッシブインターフェイス、クラスタ、またはフェールオーバーリンクではサポートされません。
- Mgmt：アプリケーション インスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。アプリケーションと管理によっては、後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。

（注） 管理インターフェイスを変更すると、論理デバイスが再起動します。たとえば、e1/1 から e1/2 に1回変更すると、論理デバイスが再起動して新しい管理が適用されます。

- Eventing： Management Center デバイスを使用した 脅威に対する防御 のセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、脅威に対する防御 CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。詳細については、管理センター構成ガイドを参照してください。Eventing インターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスはこのインターフェイスを介してインターフェイスを共有する他の倫理デバイスと通信することはできません。 後で管理用のデータインターフェイスを設定する場合は、別のイベントインターフェイスを使用できません。

（注） 各アプリケーションインスタンスのインストール時に、仮想イーサネットインターフェイスが割り当てられます。アプリケーションがイベントインターフェイスを使用しない場合、仮想インターフェイスは管理上ダウンの状態になります。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster：クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。クラスタタイプは、EtherChannel インターフェイスのみでサポートされます。 マルチインスタンスクラスタリングの場合、デバイス間でクラスタタイプのインターフェイスを共有することはできません。各クラスタが別個のクラスタ制御リンクを使用でできるように、クラスタ EtherChannel に VLAN サブインターフェイスを追加できます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。Device Manager および CDO はクラスタリングをサポートしていません。

論理デバイスを展開する前に、管理インターフェイスと少なくとも 1 つのデータ（またはデータ共有）インターフェイスを設定する必要があります。

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスを FXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

始める前に

すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。インターフェイスを EtherChannel に追加する前に、設定を行ってください。

手順

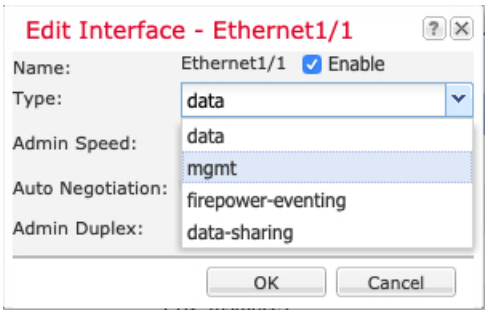
ステップ 1 [インターフェイス（Interfaces）] をクリックします。

[すべてのインターフェイス（All Interfaces）] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 編集するインターフェイスの をクリックし、[インターフェイスを編集（Edit Interface）] ダイアログボックスを開きます。

ステップ 3 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 4 インターフェイスの [タイプ（Type）] を次から選択します。**Data**、**Data-sharing**、**Mgmt**、または **Firepower-eventing**



（注） データ共有タイプのインターフェイスを使用する場合は、制限があります。詳細については、『FXOS コンフィグレーション ガイド』を参照してください。

Firepower-eventing については、Firepower Management Center コンフィギュレーション ガイドを参照してください。

ステップ 5 （任意）インターフェイスの [速度（Speed）] を選択します。

ステップ 6 （任意）インターフェイスで [自動ネゴシエーション（Auto Negotiation）] がサポートされている場合は、[はい（Yes）] または [いいえ（No）] オプション ボタンをクリックします。

ステップ 7 （任意）インターフェイスの [デュプレックス（Duplex）] を選択します。

ステップ 8 [OK] をクリックします。

EtherChannel（ポート チャネル）の追加

EtherChannel（ポートチャネルとも呼ばれる）は、同じメディアタイプと容量の最大 16 個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1 GB インターフェイスと 10 GB インターフェイスなど）を混在させることはできません。

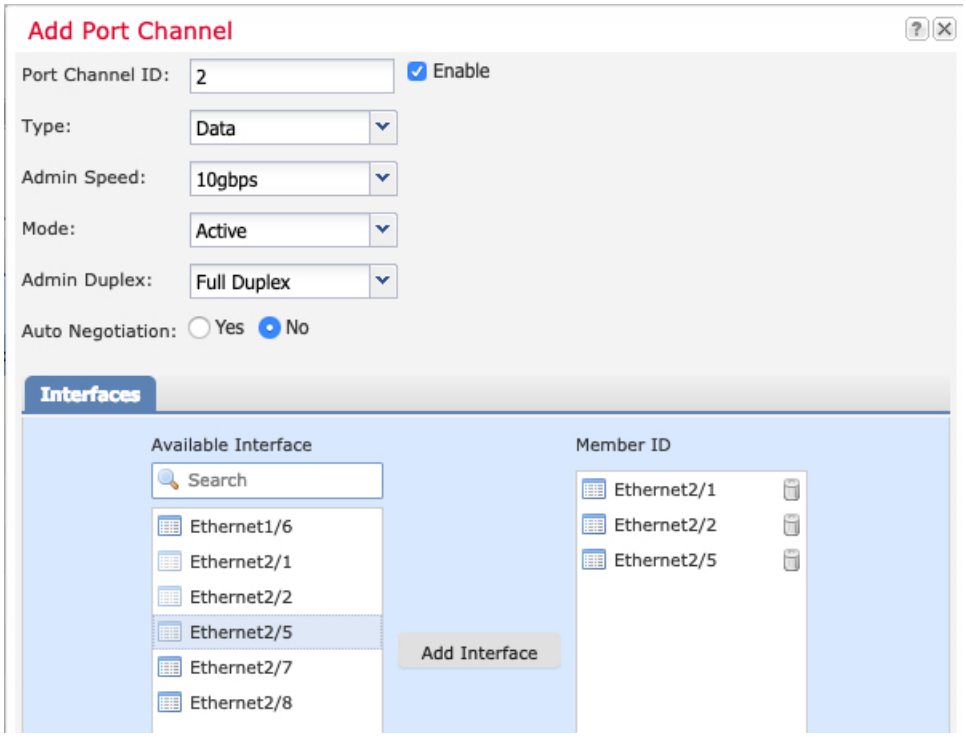
（注） シャーシが EtherChannel を作成すると、EtherChannel は [一時停止（Suspended）] 状態（Active LACP モードの場合）または [ダウン（Down）] 状態（On LACP モードの場合）になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。

手順

ステップ 1 [インターフェイス（Interfaces）] をクリックします。

[すべてのインターフェイス（All Interfaces）] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 **[新規追加（Add New）] > [ポートチャネル（Port Channel）]** をクリックします。



ステップ 3 [ポートチャネルID（Port Channel ID）] に、1 ～ 47 の値を入力します。

ステップ 4 **[有効（Enable）]** チェックボックスをオンにします。

ステップ 5 インターフェイスの [タイプ（Type）] を選択します。

- **データ**
- [データ共有（Data-sharing）]：コンテナインスタンスのみ。
- **管理**
- [Firepower-eventing]：Threat Defense のみ。
- [クラスタ（Cluster）]：クラスタリングの場合のみ。

（注） データ共有タイプのインターフェイスを使用する場合は、制限があります。詳細については、『FXOS コンフィグレーション ガイド』を参照してください。

Firepower-eventing については、Firepower Management Center コンフィギュレーション ガイドを参照してください。

ステップ 6 ドロップダウン リストでメンバ インターフェイスの [Admin Speed] を設定します。

ステップ 7 データまたはデータ共有インターフェイスに対して、LACP ポートチャネル [Mode]、[Active] または [On] を選択します。

非データまたはデータ共有インターフェイスの場合、モードは常にアクティブです。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。

ステップ 8 ドロップダウン リストから [管理デュプレックス（Admin Duplex）] を設定します。

ステップ 9 インターフェイスをポート チャネルに追加するには、[使用可能なインターフェイス（Available Interface）] リストでインターフェイスを選択し、[インターフェイスの追加（Add Interface）] をクリックして、そのインターフェイスを [メンバID（Member ID）] リストに移動します。

最大 16 個のインターフェイスを追加できます。

ヒント 一度に複数のインターフェイスを追加できます。複数の個別インターフェイスを選択するには、**Ctrl** キーを押しながら目的のインターフェイスをクリックします。一連のインターフェイスを選択するには、その範囲の最初のインターフェイスを選択し、**Shift** キーを押しながら最後のインターフェイスをクリックして選択します。

ステップ 10 ポート チャネルからインターフェイスを削除するには、[メンバID（Member ID）] リストのインターフェイスの右側にある をクリックします。

ステップ 11 [OK] をクリックします。

コンテナ インスタンスの VLAN サブインターフェイスの追加

シャーシには最大500個のサブインターフェイスを追加できます。サブインターフェイスはコンテナ インスタンスでのみサポートされます。詳細については、論理デバイスのアプリケーション インスタンス：コンテナとネイティブ （8 ページ） を参照してください。

マルチインスタンス クラスタリングの場合、クラスタタイプのインターフェイスにサブインターフェイスを追加するだけです。データインターフェイス上のサブインターフェイスはサポートされません。

インターフェイスごとの VLAN ID は一意である必要があります。コンテナ インスタンス内では、VLAN ID は割り当てられたすべてのインターフェイス全体で一意である必要があります。異なるコンテナ インターフェイスに割り当てられている限り、VLAN ID を別のインターフェイス上で再利用できます。ただし、同じ ID を使用していても、各サブインターフェイスが制限のカウント対象になります。

アプリケーション内にサブインターフェイスを追加することもできます。FXOS サブインターフェイスとアプリケーションサブインターフェイスを使用するタイミングの詳細については、「FXOS コンフィグレーション ガイド」を参照してください。

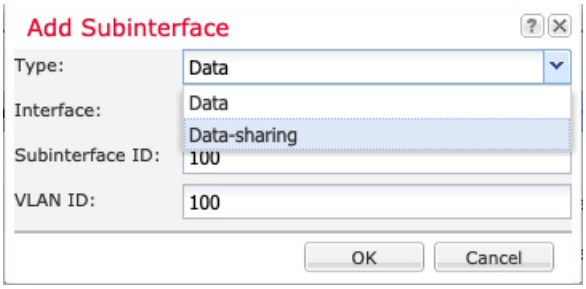
手順

ステップ 1 [インターフェイス（Interfaces）] をクリックします。

[すべてのインターフェイス（All Interfaces）] ページでは、上部に現在インストールされているインターフェイスが視覚的に表示され、下部の表にそれらのリストが表示されます。

ステップ 2 **[Add New** > **Subinterface]** をクリックして [Add Subinterface] ダイアログボックスを開きます。

ステップ 3 インターフェイスの [タイプ（Type）] を選択します。



- **データ**
- **データ共有**
- [クラスタ（Cluster）]：クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタに使用できません。

データインターフェイスおよびデータ共有インターフェイスの場合：タイプは、親インターフェイスのタイプに依存しません。たとえば、データ共有の親とデータサブインターフェイスを設定できます。

データ共有タイプのインターフェイスを使用する場合は、制限があります。詳細については、『FXOS コンフィグレーション ガイド』を参照してください。

ステップ 4 ドロップダウン リストから親**インターフェイス**を選択します。

現在論理デバイスに割り当てられている物理インターフェイスにサブインターフェイスを追加することはできません。親の他のサブインターフェイスが割り当てられている場合、その親インターフェイス自体が割り当てられていない限り、新しいサブインターフェイスを追加できます。

ステップ 5 [Subinterface ID] を 1 ～ 4294967295 で入力します。

この ID は、*interface_id.subinterface_id* のように親インターフェイスの ID に追加されます。たとえば、サブインターフェイスを ID 100 でイーサネット 1/1 に追加する場合、そのサブインターフェイス ID はイーサネット 1/1.100 になります。利便性を考慮して一致するように設定することができますが、この ID は VLAN ID と同じではありません。

ステップ 6 1 ～ 4095 の間で [VLAN ID] を設定します。

ステップ 7 [OK] をクリックします。

親インターフェイスを展開し、その下にあるすべてのサブインターフェイスを表示します。

ソフトウェア イメージのシャーシへのアップロード

この手順では、FXOS イメージのアップグレード方法だけでなく、新しい FXOS およびアプリケーション イメージをアップロードする方法について説明します。事前にインストールされたイメージが必要なバージョンではない場合は、新しいイメージのアップロードが必要になることがあります。

始める前に

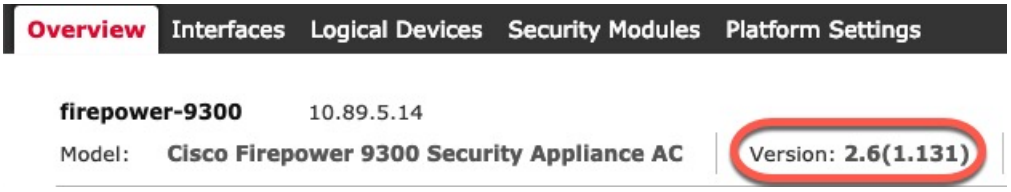
- FXOS 互換性ガイド [英語] で、FXOS、ASA、および 脅威に対する防御 バージョン間の互換性を確認します。
- アップロードするイメージがローカル コンピュータで使用可能であることを確認します。Firepower 9300 の FXOS およびアプリケーション ソフトウェアを取得するには、次を参照してください。

  http://www.cisco.com/go/firepower9300-software
- HTTPS セッション中にアップロードが成功するようにするには、FXOS CLI で絶対タイムアウトを変更する必要があることがあります。絶対タイムアウトは60分（最大）であり、大規模なアップロードには 60 分以上かかる場合があります。絶対タイムアウトを無効にするには、次のように入力します。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set absolute-session-timeout 0
Firepower-chassis /security/default-auth* # commit-buffer
```

手順

ステップ 1 現在の FXOS のバージョンを確認するには、[概要（Overview）] ページを参照してください。



次のステップで、シャーシで現在使用可能なアプリケーション イメージを表示できます。

ステップ 2 **[システム（System）] > [更新（Updates）]** を選択します。

[使用可能な更新（Available Updates）] ページに、FXOS のプラットフォーム バンドルのイメージやアプリケーションのイメージのリストが表示されます。

ステップ 3 [イメージのアップロード（Upload Image）] をクリックして、[イメージのアップロード（Upload Image）] ダイアログボックスを開きます。

ステップ 4 [Browse] をクリックし、アップロードするイメージまで移動して選択します。

ステップ 5 [Upload] をクリックします。選択したイメージがシャーシにアップロードされます。

[イメージのアップロード（Upload image）] ダイアログボックスに経過表示バーが表示され、イメージのアップロードが完了すると、[成功（Success）] ダイアログボックスが表示されます。

ステップ 6 FXOS イメージをアップグレードするには、以下を実行します。

a) アップグレードする FXOS プラットフォーム バンドルの アップグレードアイコン（）をクリックします。

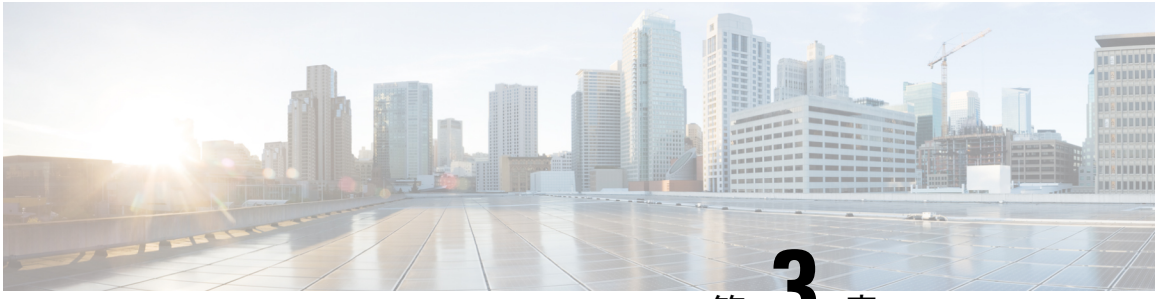
b) [はい（Yes）] をクリックして、インストールを続行することを確認します。

シャーシがリロードします。アップグレード プロセスには通常 20 ～ 30 分かかります。

FXOS の履歴

機能名	バージョン	機能情報
コンテナインスタンスで使用される VLAN サブインターフェイス	2.4.1	柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。 （注） Threat Defense バージョン 6.3 以降が必要です。 新規/変更された画面： **[Interfaces] > [All Interfaces] > [Add New]** ドロップダウン メニュー **> [Subinterface]** 新規/変更された Management Center 画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）]** アイコン **> [インターフェイス（Interfaces）]**
コンテナインスタンスのデータ共有インターフェイス	2.4.1	柔軟な物理インターフェイスの使用を可能にするため、複数のインスタンス間でインターフェイスを共有することができます。 （注） Threat Defense バージョン 6.3 以降が必要です。 新規/変更された画面： **[Interfaces] > [All Interfaces] > [Type]**

機能名	バージョン	機能情報
オンモードでのデータ EtherChannel のサポート	2.4.1	データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオン モードに設定できるようになりました。Etherchannel の他のタイプはアクティブ モードのみをサポートします。 新規/変更された画面： **[Interfaces] > [All Interfaces] > [Edit Port Channel] > [Mode]**
Threat Defense インラインセットでの EtherChannel のサポート	2.1.1	Threat Defense インラインセットで EtherChannel を使用できるようになりました。
Threat Defense のインライン セット リンク ステート伝達サポート	2.0(1)	Threat Defense アプリケーションでインライン セットを設定し、リンク ステート伝達を有効にすると、Threat Defense はインライン セット メンバーシップを FXOS シャーシに送信します。リンク ステート伝達により、インライン セットのインターフェイスの 1 つが停止した場合、シャーシは、インライン インターフェイス ペアの 2 番目のインターフェイスも自動的に停止します。 新規/変更されたコマンド：**show fault |grep link-down**、**show interface detail**
ハードウェアバイパス ネットワーク モジュールのサポート Threat Defense	2.0(1)	ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。 新規/変更された Management Center 画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]**
Threat Defense の Firepower-eventing タイプインターフェイス	1.1.4	Threat Defense で使用するために、Firepower イベントとしてインターフェイスを指定できます。このインターフェイスは、Threat Defense デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、Threat Defense CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント（Web イベントなど）から管理トラフィックを分類できます。Management Center 構成ガイドのシステム設定の章にある「管理インターフェイス」のセクションを参照してください。 新規/変更された Chassis Manager 画面： **[Interfaces] > [All Interfaces] > [Type]**



第 3 章

Management Center での Threat Defense の展開

この章の対象読者

この章では、Management Center を使用してスタンドアロンの 脅威に対する防御 論理デバイスを展開する方法について説明します。高可用性ペアかクラスタを展開する場合は、『Firepower Management Center コンフィギュレーション ガイド』を参照してください。

大規模ネットワークの一般的な導入では、複数の管理対象デバイスがネットワークセグメントにインストールされます。各デバイスは、トラフィックを制御、検査、監視、および分析して、管理 Management Center に報告します。Management Center は、サービスの管理、分析、レポートのタスクを実行できる Web インターフェイスを備えた集中管理コンソールを提供し、ローカルネットワークを保護します。

単一またはごく少数のデバイスのみが含まれるネットワークでは、Management Center のような高性能の多機能デバイスマネージャを使用する必要がなく、一体型の Device Manager を使用できます。Device Manager の Web ベースのデバイス セットアップ ウィザードを使用して、小規模ネットワークの導入に最もよく使用されるソフトウェアの基本機能を設定できます。

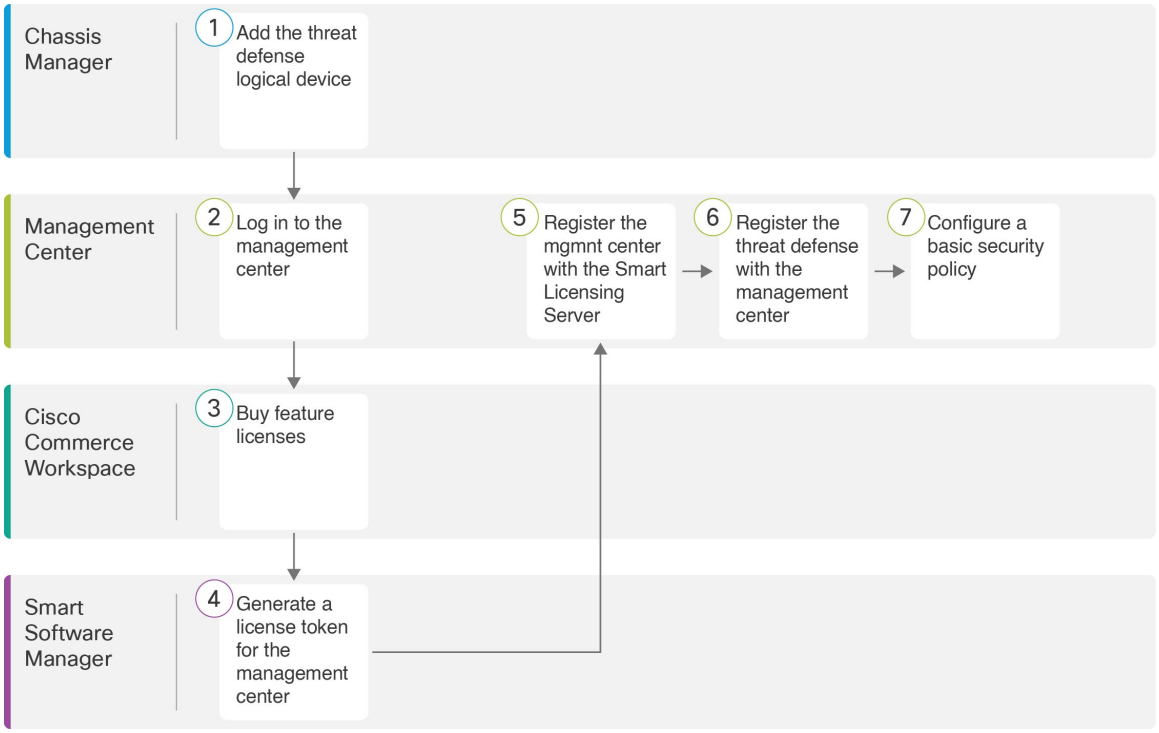
プライバシー収集ステートメント：Firepower 9300 には個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザー名などの設定では、個人識別情報を使用できます。この場合、設定作業時やSNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

はじめる前に

Management Center の初期設定を展開して実行します。Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation GuideまたはCisco Secure Firewall Management Center Virtual 入門ガイドを参照してください。

エンドツーエンドの手順

シャーシで 脅威に対する防御 を展開して設定するには、次のタスクを参照してください。



	ワークスペース	手順
1	Chassis Manager	Chassis Manager：Threat Defense 論理デバイスの追加 （37 ページ）。
2	Management Center	Management Center へのログイン （43 ページ）。
3	Cisco Commerce Workspace	Management Center のライセンスの取得 （43 ページ）：機能ライセンスを購入します。
4	Smart Software Manager	Management Center のライセンスの取得 （43 ページ）：Management Center のライセンストークンを生成します。

	ワークスペース	手順
5	Management Center	Management Center のライセンスの取得 （43 ページ）：スマート ライセンシング サーバーに Management Center を登録します。
6	Management Center	Management Center への Threat Defense の登録 （45 ページ）。
7	Management Center	基本的なセキュリティポリシーの設定 （48 ページ）。

Chassis Manager：Threat Defense 論理デバイスの追加

Threat Defense をネイティブまたはコンテナいずれかのインスタンスとして Firepower 9300 から展開できます。セキュリティ モジュール ごとに複数のコンテナ インスタンスを展開できますが、ネイティブ インスタンスは 1 つだけです。モデルごとの最大コンテナ インスタンス数については、論理デバイスのアプリケーション インスタンス：コンテナとネイティブ （8 ページ） を参照してください。 一部のモジュールでネイティブ インスタンスを使用し、その他のモジュールでコンテナ インスタンスを使用することができます。

高可用性ペアかクラスタを追加する場合は、『Firepower Management Center コンフィギュレーション ガイド』を参照してください。

この手順では、アプリケーションで使用されるブートストラップ設定を含む、論理デバイスの特性を設定できます。

始める前に

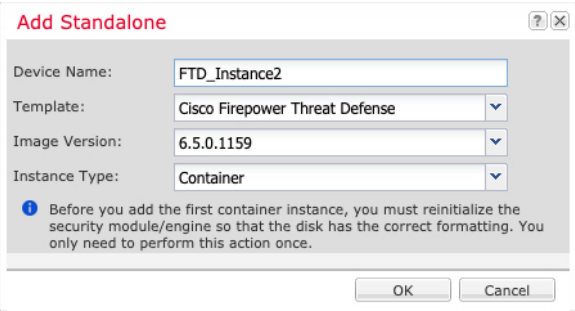
- Threat Defense と一緒に使用する管理インターフェイスを設定します。インターフェイスの設定 （24 ページ） を参照してください。管理インターフェイスが必要です。 6.7 以降では、後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。この管理インターフェイスは、シャーシの管理のみに使用される（[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示される）シャーシ管理ポートと同じではありません。
- また、少なくとも 1 つのデータ インターフェイスを設定する必要があります。
- コンテナ インスタンスの場合、最小リソースを使用するデフォルト プロファイルを使用しない場合は、 **[プラットフォーム設定（Platform Settings）]** > **[リソースプロファイル（Resource Profiles）]** でリソース プロファイルを追加します。
- コンテナ インスタンスの場合、最初にコンテナ インスタンスをインストールする前に、ディスクが正しいフォーマットになるように セキュリティ モジュール を再度初期化する必要があります。このアクションが必要な場合は、論理デバイスを保存できません。**[セキュリティモジュール（Security Modules）]** を選択し、[再初期化（Reinitialize）] アイコン（ ） をクリックします。

- 次の情報を用意します。
  - このデバイスのインターフェイス Id
  - 管理インターフェイス IP アドレスとネットワークマスク
  - ゲートウェイ IP アドレス
  - Management Center 選択した IP アドレス/NAT ID
  - DNS サーバの IP アドレス

手順

ステップ 1 Chassis Manager で、[論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[追加（Add）]** > **[スタンドアロン（Standalone）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

この名前は、シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

b) [Template] では、[Cisco Firepower Threat Defense] を選択します。

c) [Image Version] を選択します。

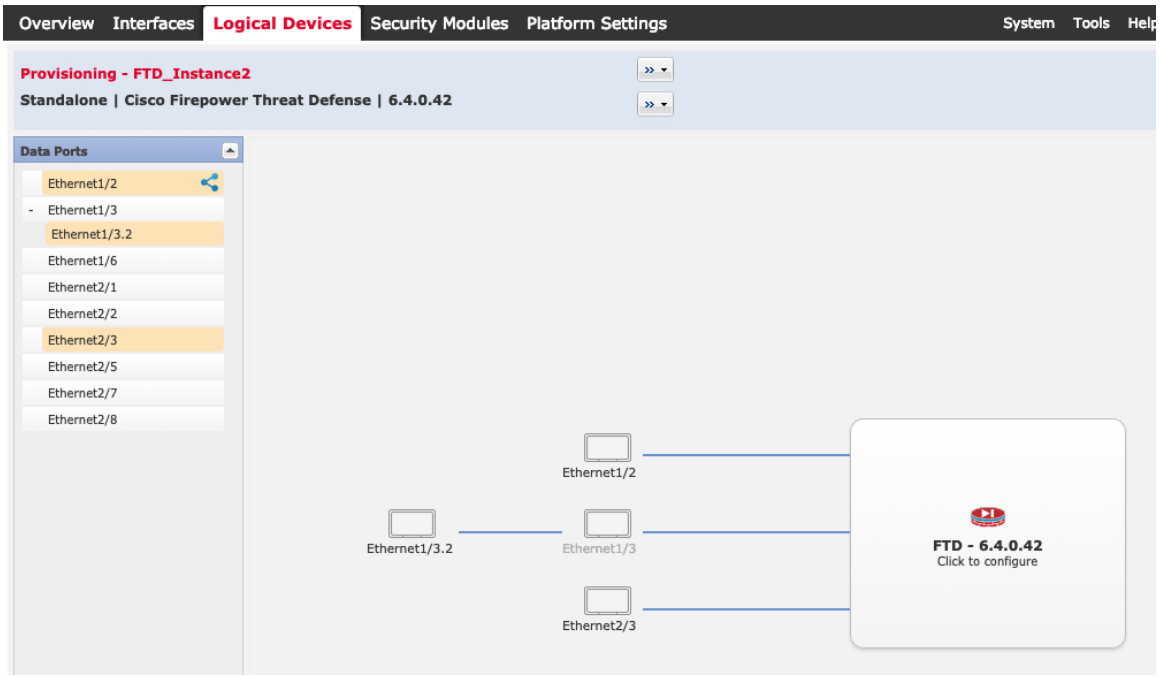
d) [インスタンスタイプ（Instance Type）] : [コンテナ（Container）] または [ネイティブ（Native）] を選択します。

ネイティブインスタンスはセキュリティモジュール/エンジンのすべてのリソース（CPU、RAM、およびディスク容量）を使用するため、ネイティブ インスタンスを 1 つのみインストールできます。コンテナ インスタンスでは、セキュリティ モジュール/エンジンのリソースのサブセットを使用するため、複数のコンテナインスタンスをインストールできます。

e) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。



[インターフェイス（Interfaces）]ページで以前に有効にしたデータ インターフェイスとデータ共有インターフェイスのみを割り当てることができます。後で Management Center でこれらのインターフェイスを有効にして設定します。これには、IP アドレスの設定も含まれます。

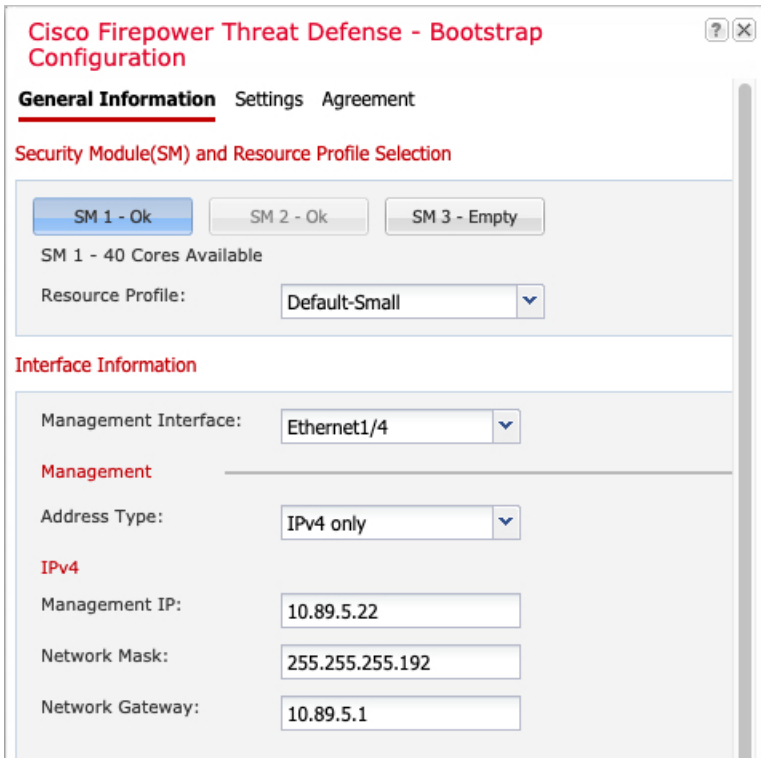
コンテナ インスタンスごとに最大 10 のデータ共有インターフェイスを割り当てることができます。また、各データ共有インターフェイスは、最大 14 個のコンテナ インスタンスに割り当てることができます。データ共有インターフェイスは[Sharing]アイコン（ ）で示されます。

ハードウェア バイパス 対応のポートは次のアイコンで表示されます：。特定のインターフェイスモジュールでは、インライン セット インターフェイスに対してのみハードウェアバイパス機能を有効にできます（インラインセットの詳細については、『Firepower Management Center コンフィギュレーション ガイド』を参照）。ハードウェア バイパスは、停電時にトラフィックがインラインインターフェイスペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。ハードウェアバイパスペアの両方のインターフェイスとも割り当てられていない場合、割り当てが意図的であることを確認する警告メッセージが表示されます。ハードウェア バイパス 機能を使用する必要はないため、単一のインターフェイスを割り当てることができます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [一般情報（General Information）] ページで、次の手順を実行します。



a) [セキュリティモジュールの選択（Security Module Selection）] の下で、この論理デバイスに使用するセキュリティ モジュールをクリックします。

b) コンテナのインスタンスでは、**リソースのプロファイル**を指定します。

後でさまざまなリソースプロファイルを割り当てると、インスタンスがリロードされ、この操作に約 5 分かかることがあります。確立されたハイ アベイラビリティ ペアまたはクラスタの場合に、異なるサイズのリソースプロファイルを割り当てるときは、すべてのメンバのサイズが同じであることをできるだけ早く確認してください。

c) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

d) 管理インターフェイスを選択します。[アドレスタイプ（Address Type）]：[IPv4のみ（IPv4 only）]、[IPv6のみ（IPv6 only）]、または [IPv4およびIPv6（IPv4 and IPv6）]。

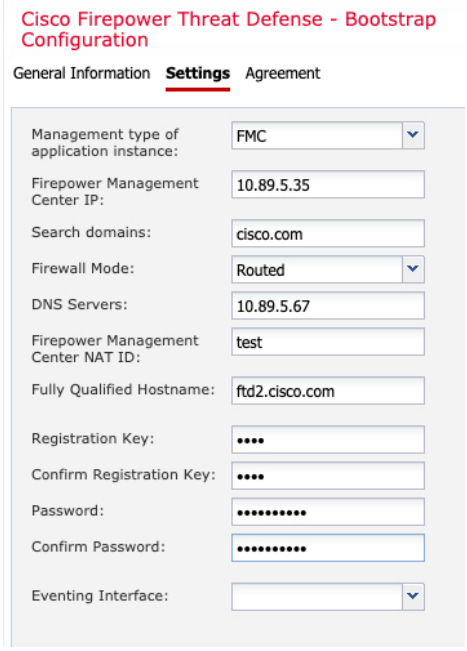
e) [Management IP] アドレスを設定します。

このインターフェイスに一意の IP アドレスを設定します。

f) [Network Mask] または [Prefix Length] に入力します。

g) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [設定（Settings）] タブで、次の項目を入力します。



a) ネイティブ インスタンスの場合は、[アプリケーションインスタンスの管理タイプ（Management type of application instance）] ドロップダウン リストで [FMC] を選択します。

ネイティブインスタンスは、マネージャとしての Device Manager もサポートしています。論理デバイスを展開した後にマネージャ タイプを変更することはできません。

b) 管理 Management Center の [Firepower Management Center IP] またはホスト名を入力します。Management Center の IP アドレスがわからない場合は、このフィールドを空白のままにして、[Firepower Management Center NAT ID] フィールドにパスフレーズを入力します。

c) **FTD SSH セッションからエキスパート モード**、[**Yes**]、または [**No**] を許可します。エキスパートモードでは、高度なトラブルシューティングに Threat Defense シェルからアクセスできます。

このオプションで [はい（Yes）] を選択すると、SSH セッションからコンテナインスタンスに直接アクセスするユーザーがエキスパートモードを開始できます。[いいえ（No）] を選択した場合、FXOS CLI からコンテナインスタンスにアクセスするユーザーのみがエキスパートモードを開始できます。インスタンス間の分離を増やすには、[No] を選択することをお勧めします。

マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパート モードを使用します。このモードを開始するには、Threat Defense CLI で **expert** コマンドを使用します。

d) カンマ区切りリストとして [検索ドメイン（Search Domains）] を入力します。

e) [Firewall Mode] を [Transparen] または [Routed] に選択します。

ルーテッド モードでは、Threat Defense はネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、

トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォール モードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

f) [DNS Servers] をカンマ区切りのリストとして入力します。

たとえば、Management Centerのホスト名を指定する場合、Threat Defense は DNS を使用します。

g) Threat Defense の [Fully Qualified Hostname] を入力します。

h) 登録時に Management Center とデバイス間で共有する [Registration Key] を入力します。

このキーには、1 ～ 37 文字の任意のテキスト文字列を選択できます。Threat Defense を追加するときに、Management Center に同じキーを入力します。

i) CLI アクセス用の Threat Defense 管理ユーザの [Password] を入力します。

j) イベントの送信に使用する [イベンティングインターフェイス（Eventing Interface）] を選択します。指定しない場合は、管理インターフェイスが使用されます。

このインターフェイスは、Firepower-eventing インターフェイスとして定義する必要があります。

k) コンテナインスタンスの場合は、[ハードウェア暗号化（Hardware Crypto）] を [有効（Enabled）] または [無効（Disabled）] に設定します。

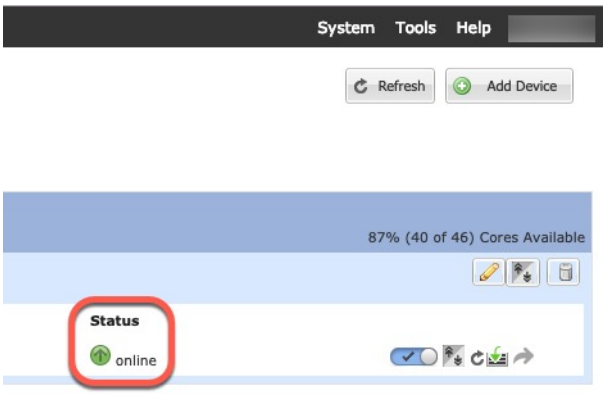
この設定により、ハードウェアの TLS 暗号化アクセラレーションが有効になり、特定タイプのトラフィックのパフォーマンスが向上します。詳細については、Firepower Management Center コンフィギュレーション ガイドを参照してください。この機能はネイティブ インスタンスではサポートされていません。このインスタンスに割り当てられているハードウェア暗号化リソースの割合を表示するには、**show hw-crypto** コマンドを入力します。

ステップ 7 [利用規約（Agreement）] タブで、エンドユーザ ライセンス（EULA）を読んで、同意します。

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



Management Center へのログイン

Management Center を使用して、Threat Defense を設定および監視します。

始める前に

サポートされているブラウザの詳細については、使用するバージョンのリリースノート（https://www.cisco.com/go/firepower-notes）を参照してください。

手順

ステップ 1 サポートされているブラウザを使用して、次の URL を入力します。

https://*fmc_ip_address*

ステップ 2 ユーザー名とパスワードを入力します。

ステップ 3 [ログイン（Log In）] をクリックします。

Management Center のライセンスの取得

すべてのライセンスは、Management Center によって 脅威に対する防御 に提供されます。次のライセンスを購入できます。

- **IPS**：セキュリティインテリジェンスと次世代 IPS
- **マルウェア防御**：マルウェア防御
- **URL**：URL フィルタリング

- **Cisco Secure Client**：Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

始める前に

- Smart Software Manager にマスターアカウントを持ちます。

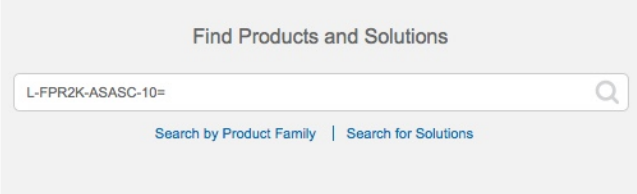
  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用のスマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

手順

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *1*: ライセンス検索



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

- IPS、マルウェア防御、および URL ライセンスの組み合わせ：
  - L-FPR9K-40T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-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-FPR9K-40T-TMC-1Y

- L-FPR9K-40T-TMC-3Y
- L-FPR9K-40T-TMC-5Y
- L-FPR9K-48T-TMC-1Y
- L-FPR9K-48T-TMC-3Y
- L-FPR9K-48T-TMC-5Y
- L-FPR9K-56T-TMC-1Y
- L-FPR9K-56T-TMC-3Y
- L-FPR9K-56T-TMC-5Y

- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。
- キャリアライセンス：
  - L-FPR9K-FTD-CAR=

ステップ 2 まだ設定していない場合は、スマート ライセンシング サーバーに Management Center を登録します。

登録を行うには、Smart Software Manager で登録トークンを生成する必要があります。詳細な手順については、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。

Management Center への Threat Defense の登録

各論理デバイスを同じ Management Center に個別に登録します。

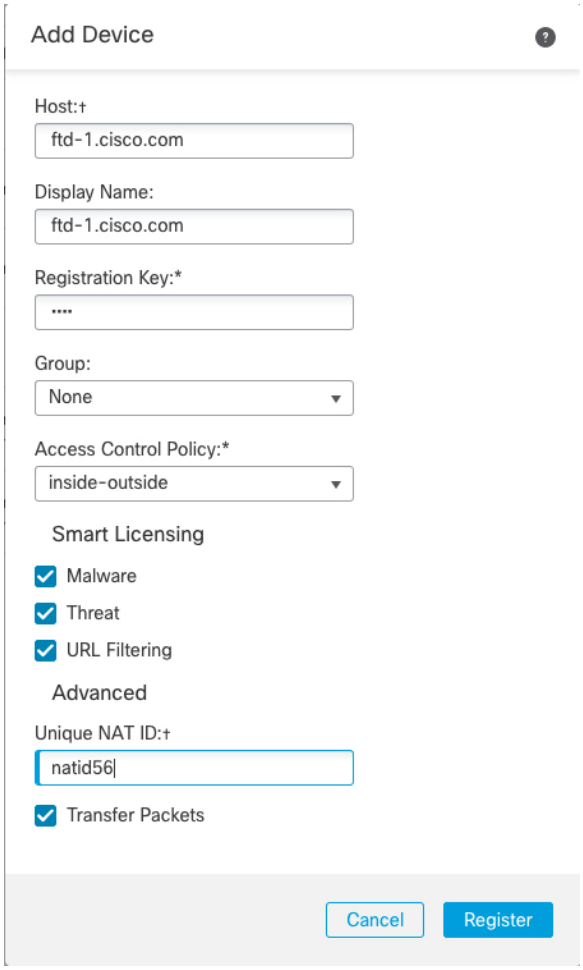
始める前に

- Chassis Manager の [論理デバイス（Logical Devices）] ページで、Threat Defense 論理デバイスの [ステータス（Status）] が [オンライン（online）] になっていることを確認します。
- Threat Defense の最初のブートストラップ設定で設定した次の情報を収集します（「Chassis Manager：Threat Defense 論理デバイスの追加 （37 ページ）」を参照）。
  - Threat Defense の管理 IP アドレスまたはホスト名、および NAT ID
  - Management Center の登録キー
- 6.7 以降で管理にデータインターフェイスを使用する場合は、Threat Defense CLI で **configure network management-data-interface** コマンドを使用します。詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

手順

ステップ 1 Management Center で、[デバイス（Devices）] > [デバイス管理（Device Management）] の順に選択します。

ステップ 2 [追加（Add）] ドロップダウン リストから、[デバイスの追加（Add Device）] を選択します。



次のパラメータを設定します。

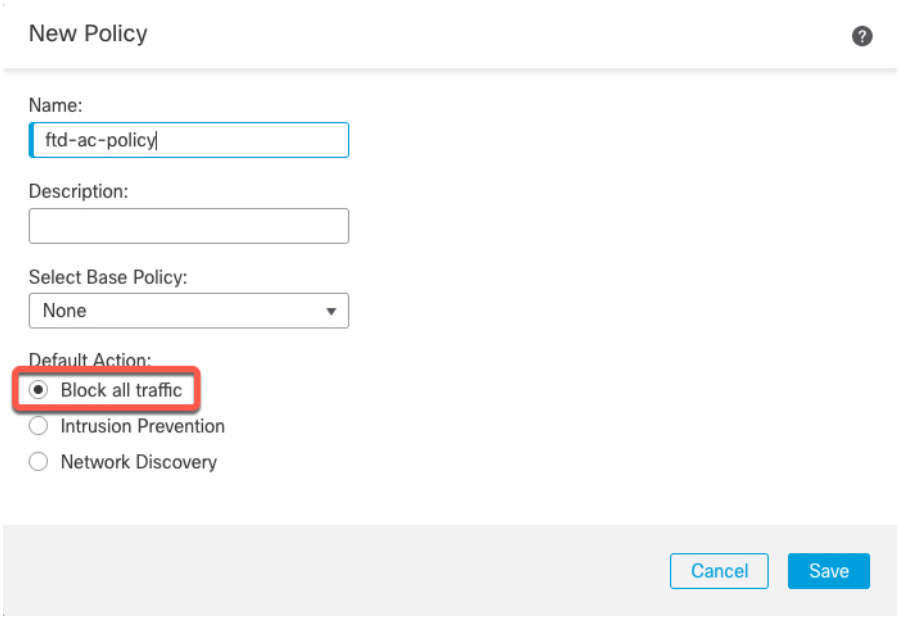
- [ホスト（Host）]：追加する Threat Defense の IP アドレスかホスト名を入力します。Threat Defense の最初のブートストラップ設定で Management Center の IP アドレスと NAT ID の両方を指定した場合は、このフィールドを空のままにしておくことができます。

  （注） HA 環境では、両方の Management Center が NAT の背後にある場合、プライマリ Management Center のホスト IP または名前なしで Threat Defense を登録できます。ただし、Threat Defense をセカンダリ Management Center に登録するには、Threat Defense の IP アドレスかホスト名を指定する必要があります。

- [表示名（Display Name）] フィールドに、Management Center に表示する Threat Defense の名前を入力します。

- [登録キー（Registration key）]：Threat Defense の最初のブートストラップ設定で指定したものと同じ登録キーを入力します。
- [ドメイン（Domain）]：マルチドメイン環境を使用している場合は、デバイスをリーフドメインに割り当てます。
- [グループ（Group）]：グループを使用している場合は、デバイスグループに割り当てます。
- [アクセスコントロールポリシー（Access Control Policy）]：初期ポリシーを選択します。使用する必要があることがわかっているカスタマイズ済みのポリシーがすでにある場合を除いて、[新しいポリシーの作成（Create new policy）] を選択し、[すべてのトラフィックをブロック（Block all traffic）] を選択します。後でこれを変更してトラフィックを許可することができます。「内部から外部へのトラフィックの許可 （58 ページ）」を参照してください。

図 *2 : New Policy*



- [スマートライセンス（Smart Licensing）]：展開する機能に必要なスマートライセンスとして、[マルウェア（Malware）]（マルウェアインスペクションを使用する予定の場合）、[脅威（Threat）]（侵入防御を使用する予定の場合）、および [URL]（カテゴリベースの URL フィルタリングを実行する予定の場合）を割り当てます。**注**：デバイスを追加した後、**[システム（System）]** > **[ライセンス（Licenses）]** > **[スマートライセンス（Smart Licenses）]** ページから セキュアクライアント リモートアクセス VPN のライセンスを適用できます。
- [一意のNAT ID（Unique NAT ID）]：Threat Defense の最初のブートストラップ設定で指定した NAT ID を指定します。
- [パケットの転送（Transfer Packets）]：デバイスから Management Center へのパケット転送を許可します。このオプションを有効にして IPS や Snort などのイベントがトリガーされ

た場合は、デバイスが検査用としてイベントメタデータ情報とパケットデータをManagement Centerに送信します。このオプションを無効にした場合は、イベント情報だけがManagement Center に送信され、パケットデータは送信されません。

ステップ 3 [登録（Register）]（別のデバイスを追加する場合は [別のデバイスを登録して追加（Register and Add Another）]）をクリックし、登録が成功したことを確認します。

登録が成功すると、デバイスがリストに追加されます。失敗した場合は、エラーメッセージが表示されます。Threat Defense が登録に失敗した場合は、次の項目を確認してください。

- ping：Threat Defense CLI（Threat Defense CLI へのアクセス （61 ページ））にアクセスし、次のコマンドを使用して Management Center IP アドレスへの ping を実行します。

  ping system *ip_address*

  ping が成功しない場合は、**show network** コマンドを使用してネットワーク設定を確認します。Threat Defense 管理 IP アドレスを変更するには、**configure network {ipv4 | ipv6} manual** コマンドを使用します。 Management Center アクセス用にデータインターフェイスを設定した場合は、**configure network management-data-interface** コマンドを使用します。

- NTP：Firepower 9300 の NTP サーバーが [システム（System）] > [設定（Configuration）] > [時刻の同期（Time Synchronization）] ページで設定した Management Center サーバーと一致していることを確認します。

- 登録キー、NAT ID、および Management Center IP アドレス：両方のデバイスで同じ登録キーを使用していることを確認し、使用している場合は NAT ID を使用していることを確認します。**configure manager add** コマンドを使用して、Management Center で登録キーと NAT ID を設定することができます。

トラブルシューティングの詳細については、https://cisco.com/go/fmc-reg-error を参照してください。

基本的なセキュリティポリシーの設定

ここでは、次の設定を使用して基本的なセキュリティポリシーを設定する方法について説明します。

- 内部インターフェイスと外部インターフェイス：内部インターフェイスにスタティック IP アドレスを割り当て、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。

基本的なセキュリティ ポリシーを設定するには、次のタスクを実行します。

1	インターフェイスの設定 （49 ページ）。
2	DHCP サーバーの設定 （53 ページ）。
3	デフォルトルートの追加 （54 ページ）。
4	NAT の設定 （55 ページ）。
5	内部から外部へのトラフィックの許可 （58 ページ）。
6	設定の展開 （59 ページ）。

インターフェイスの設定

脅威に対する防御 インターフェイスを有効にし、それらをセキュリティゾーンに割り当てて IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。これらのインターフェイスの一部は、Web サーバーなどのパブリックアクセスが可能なアセットを配置する「緩衝地帯」（DMZ）となる場合があります。

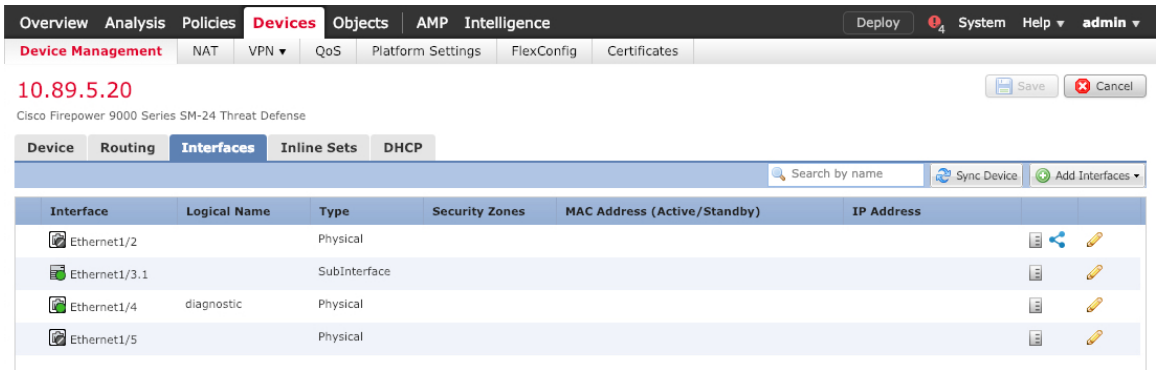
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCP によるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して、ルーテッドモードの内部インターフェイスを設定します。

手順

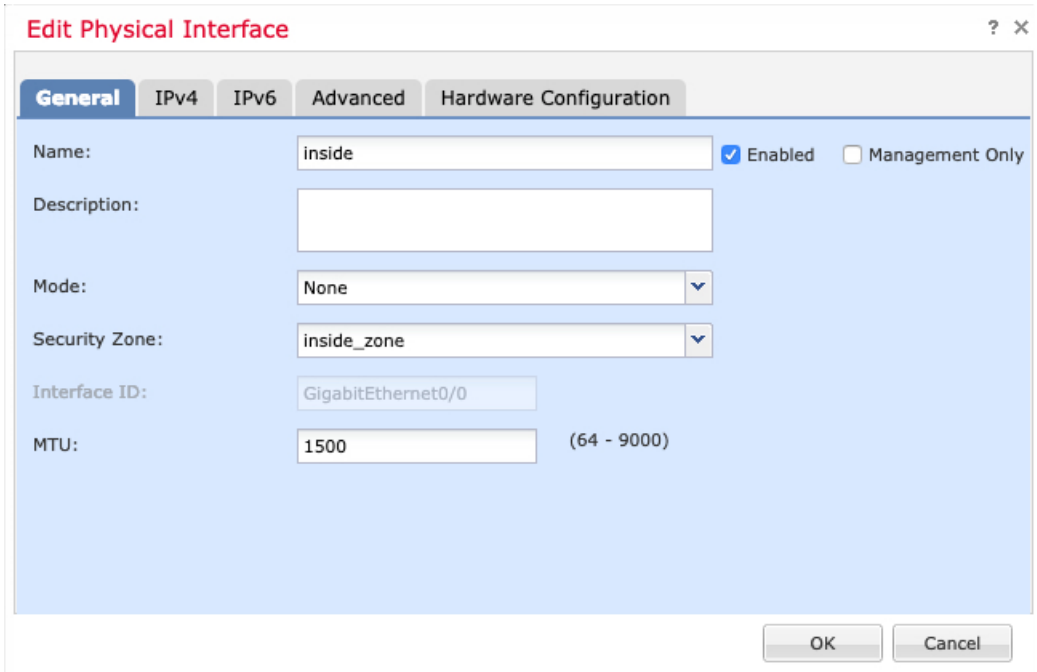
ステップ 1 [デバイス（Devices）]>[デバイス管理（Device Management）] の順に選択し、ファイアウォールの をクリックします。

ステップ 2 [インターフェイス（Interfaces）] をクリックします。



ステップ 3 内部に使用するインターフェイスの をクリックします。

[全般（General）] タブが表示されます。



a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに **inside** という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

c) [モード（Mode）] は [なし（None）] に設定したままにします。

d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

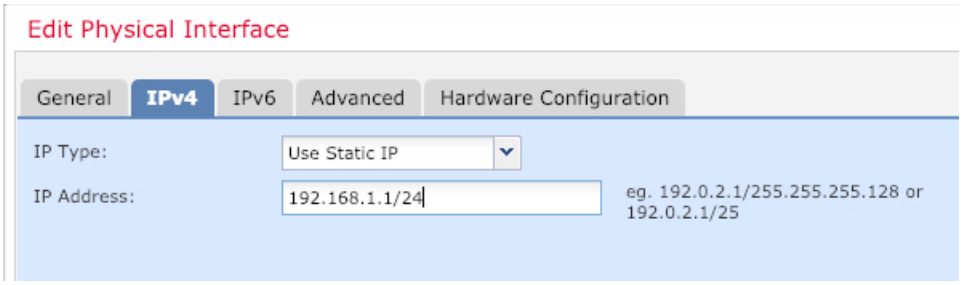
たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てる必要があります。インターフェイスは、1 つのセキュリティゾーンにのみ属することも、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシー

を適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみサポートしています。NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーで、ゾーンまたはインターフェイスグループを使用できます。

e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：ドロップダウンリストから [スタティックIPを使用する（Use Static IP）] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

  たとえば、**192.168.1.1/24** などと入力します。

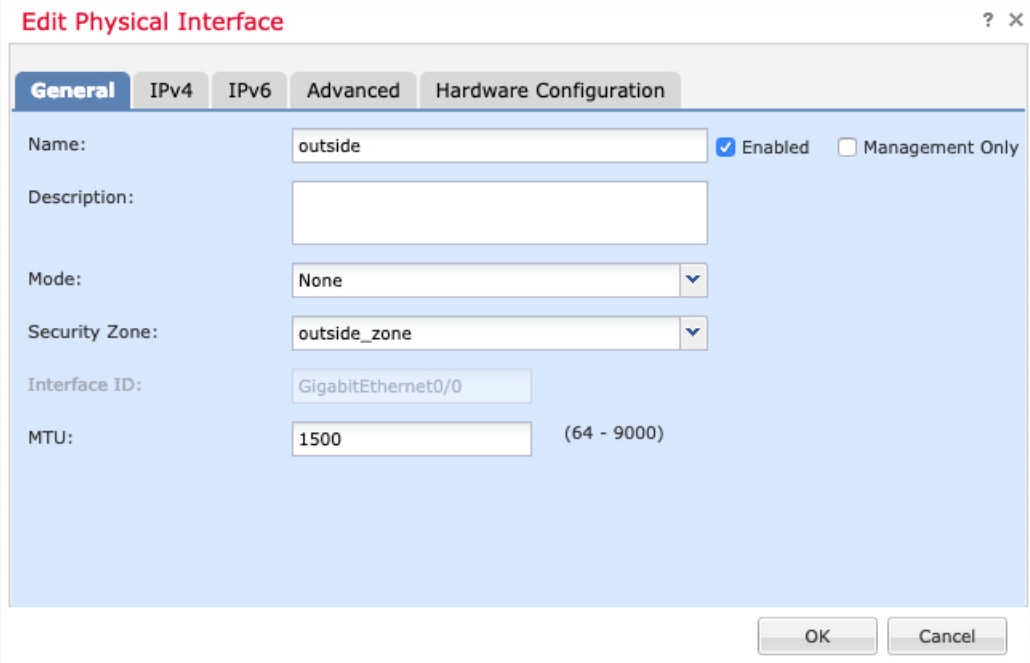


- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 4 「外部」に使用するインターフェイスをクリックします。

[全般（General）] タブが表示されます。



（注） 管理アクセス用にこのインターフェイスを事前に設定している場合、インターフェイスにはすでに名前が付けられており、有効化とアドレス指定が完了しています。これらの基本設定は変更しないでください。変更すると、Management Center の管理接続が中断されます。この画面でも、通過トラフィックポリシーのセキュリティゾーンを設定できます。

a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに「outside」という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

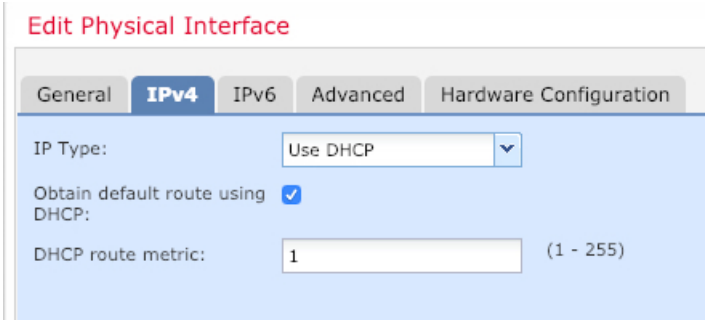
c) [モード（Mode）] は [なし（None）] に設定したままにします。

d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の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。

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。



- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

DHCP サーバーの設定

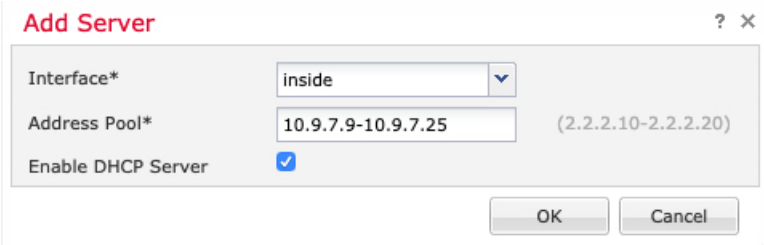
クライアントで DHCP を使用して 脅威に対する防御 から IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

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

ステップ 3 **[サーバー（Server）]** ページで、**[追加（Add）]** をクリックして、次のオプションを設定します。



- [インターフェイス（Interface）]：ドロップダウンリストからインターフェイスを選択します。
- [アドレスプール（Address Pool）]：DHCP サーバーが使用する IP アドレスの最下位から最上位の間の範囲を設定します。IPアドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。

- [DHCPサーバーを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバーを有効にします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

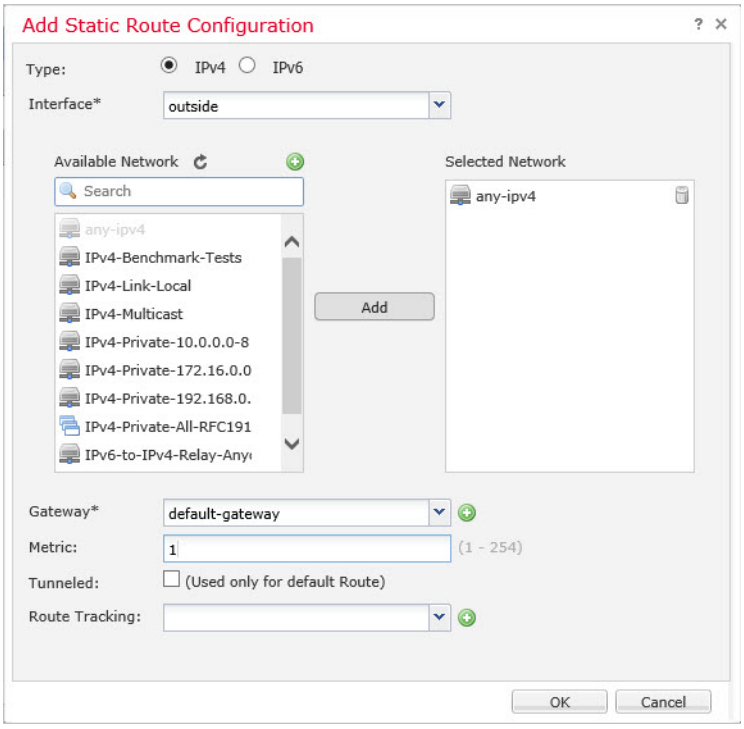
デフォルトルートの追加

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。外部インターフェイスに DHCP を使用する場合は、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。DHCP サーバーからデフォルトルートを受信した場合は、**[デバイス（Devices）] > [デバイス管理（Device Management）] > [ルーティング（Routing）] > [スタティックルート（Static Route）]**ページの [IPv4ルート（IPv4 Routes）] または [IPv6ルート（IPv6 Routes）] テーブルに表示されます。

手順

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

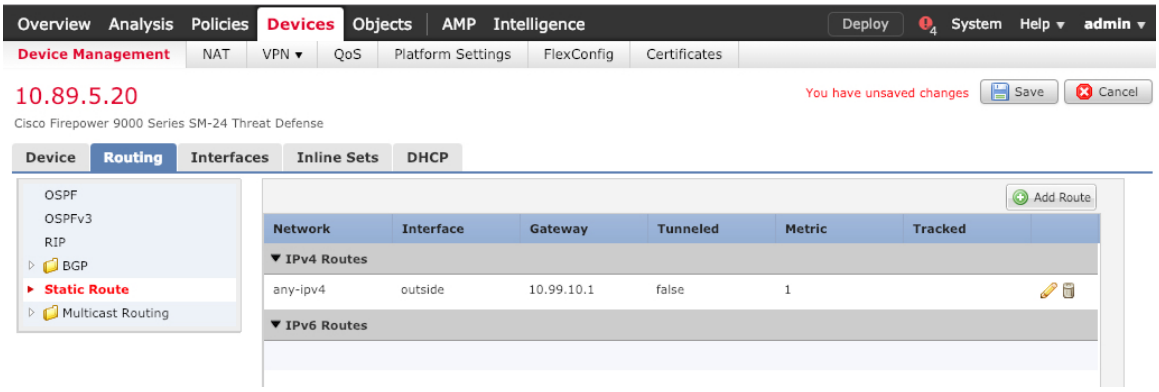
ステップ 2 **[ルーティング（Routing）] > [スタティックルート（Static route）]** を選択し、[ルートを追加（Add route）] をクリックして、次のように設定します。



- [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 [ipv4] を選択し、IPv6 デフォルト ルートの場合は [any] 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。
- [メトリック（Metric）]：宛先ネットワークへのホップの数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。

ステップ 3 [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 4 [保存（Save）] をクリックします。

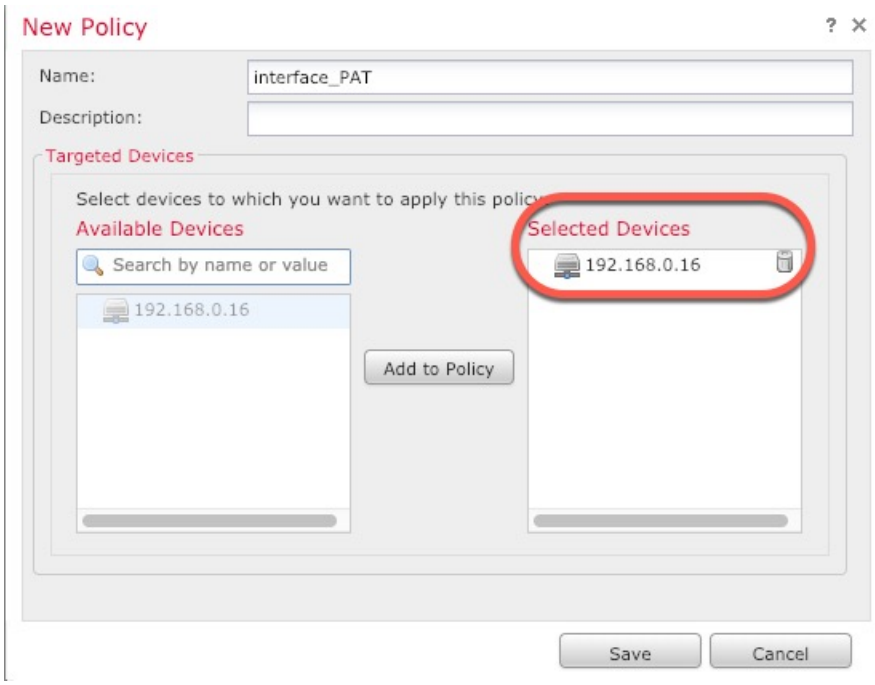
NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。

手順

ステップ 1 **[デバイス（Devices）]** > **[NAT]** をクリックし、**[新しいポリシー（New Policy）]** > **[Threat Defense NAT]** をクリックします。

ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。



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

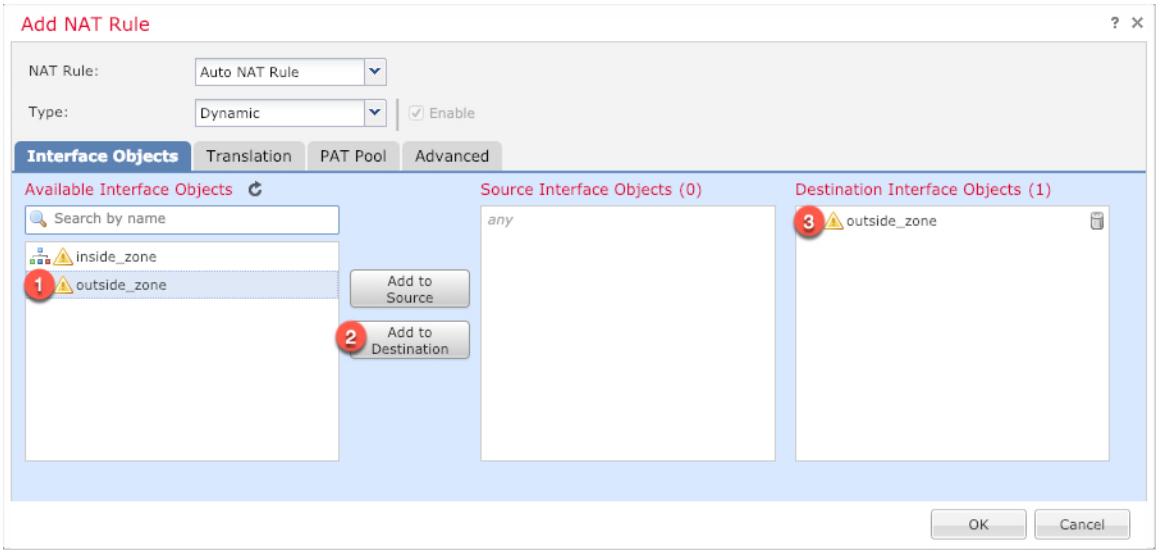
ステップ 3 [ルールの追加（Add Rule）] をクリックします。

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

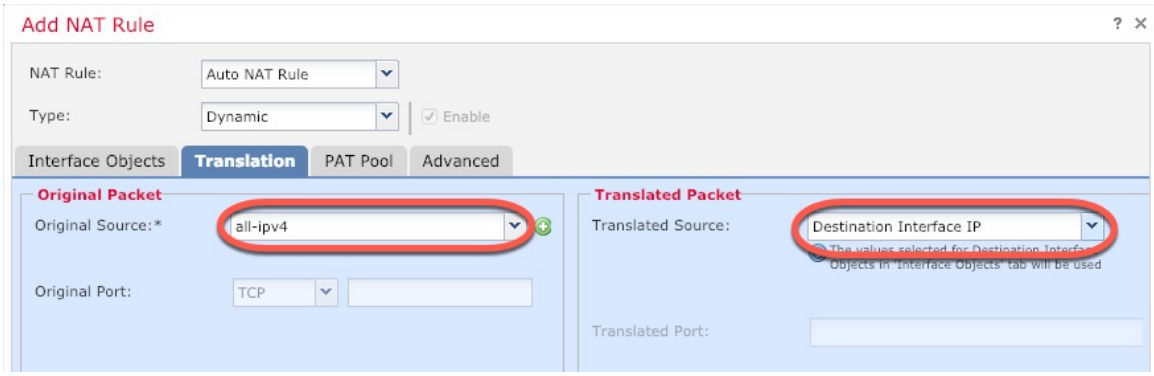
ステップ 4 基本ルールのオプションを設定します。

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

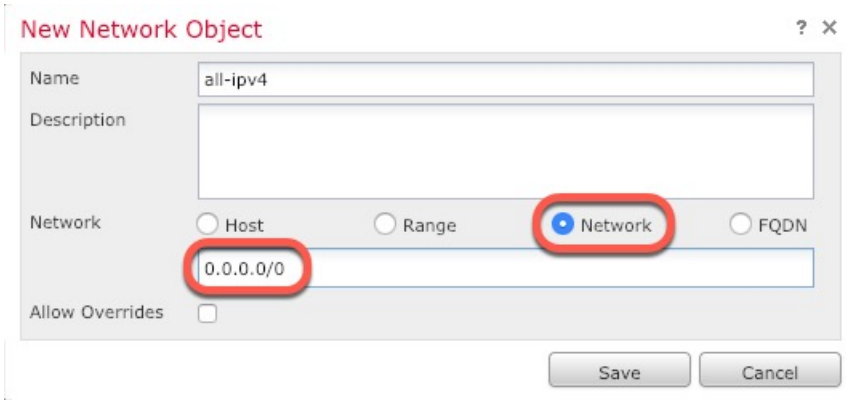
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。



ステップ 6 [変換（Translation）] ページで、次のオプションを設定します。



- [元の送信元（Original Source）]：をクリックして、すべての IPv4 トラフィック（0.0.0.0/0）のネットワークオブジェクトを追加します。

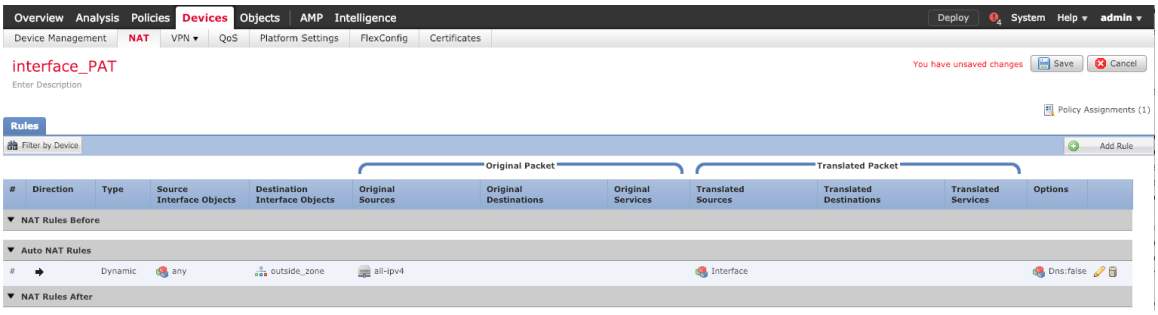


（注） 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元（Translated Source）]：[宛先インターフェイスIP（Destination Interface IP）] を選択します。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ルールが [ルール（Rules）] テーブルに保存されます。



ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

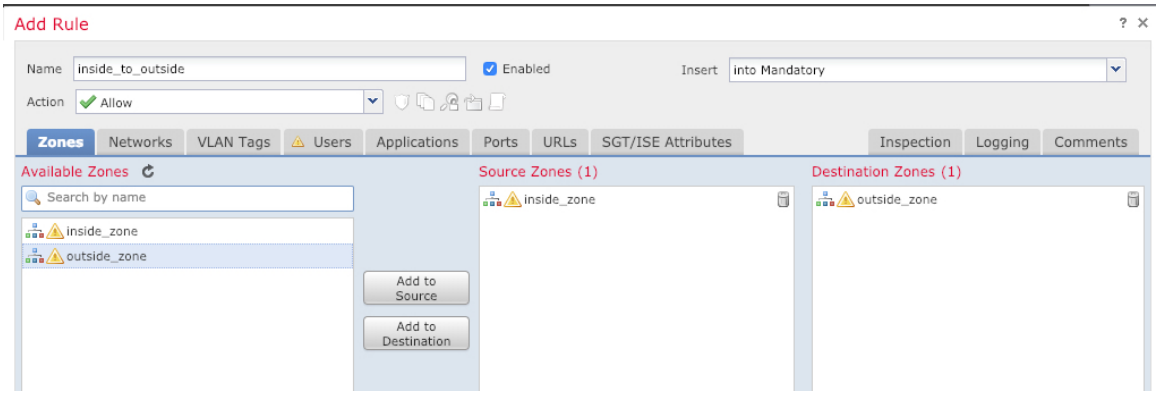
内部から外部へのトラフィックの許可

脅威に対する防御 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、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

手順

ステップ 1 **[ポリシー（Policy）] > [アクセスポリシー（Access Policy）] > [アクセスポリシー（Access Policy）]**を選択し、脅威に対する防御 に割り当てられているアクセス コントロール ポリシーの をクリックします。

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

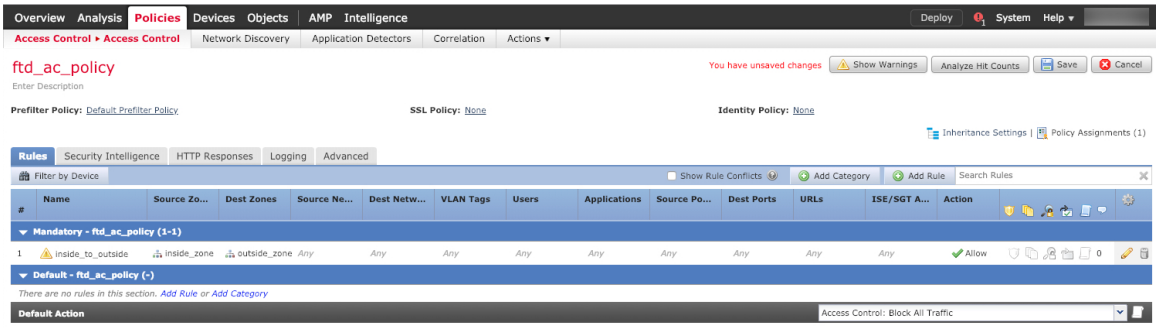


- [名前（Name）]：このルールに名前を付けます（たとえば、**inside_to_outside**）。
- [送信元ゾーン（Source Zones）]：[使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。
- [宛先ゾーン（Destination Zones）]：[使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

他の設定はそのままにしておきます。

ステップ 3 [追加（Add）] をクリックします。

ルールが [ルール（Rules）] テーブルに追加されます。



ステップ 4 [保存（Save）] をクリックします。

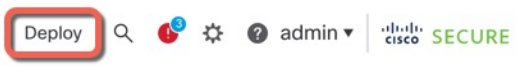
設定の展開

設定の変更を 脅威に対する防御 に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

手順

ステップ 1 右上の [展開（Deploy）] をクリックします。

図 *3 : [*展開（*Deploy***）*]***



ステップ 2 [すべて展開（Deploy All）] をクリックしてすべてのデバイスに展開するか、[高度な展開（Advanced Deploy）] をクリックして選択したデバイスに展開します。

図 *4*: すべて展開

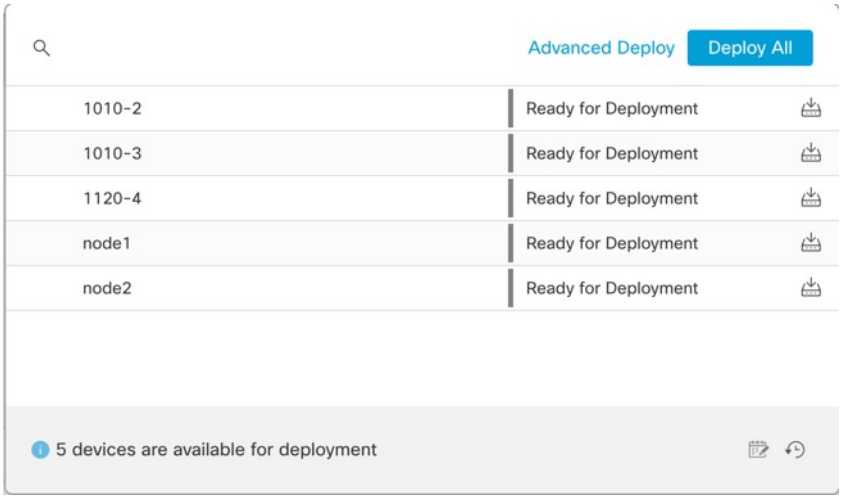
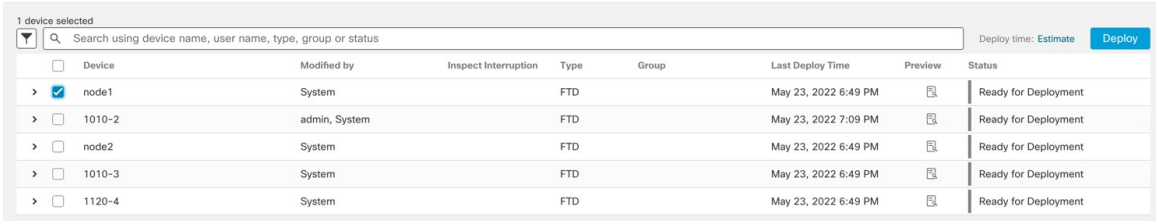
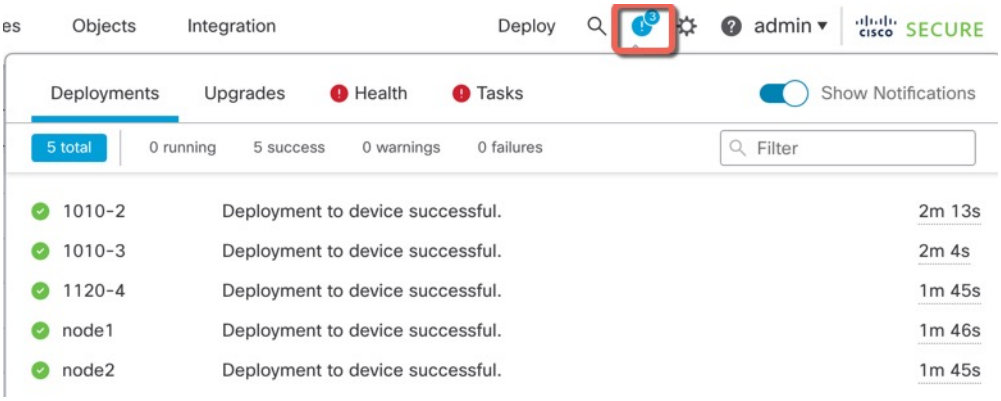


図 *5*: 高度な展開



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 *6*: 展開ステータス



Threat Defense CLI へのアクセス

脅威に対する防御 CLI を使用して、管理インターフェイスパラメータを変更したり、トラブルシューティングを行ったりできます。CLI にアクセスするには、管理インターフェイスへの SSH を使用するか、FXOS CLI から接続します。

手順

ステップ 1 （オプション 1）脅威に対する防御 管理インターフェイスの IP アドレスに直接 SSH 接続します。

管理 IP アドレスは、論理デバイスを展開したときに設定したものです。初期展開時に設定した「admin」アカウントとパスワードを使用して 脅威に対する防御 にログインします。

パスワードを忘れた場合は、シャーシマネージャ で論理デバイスを編集して変更できます。

ステップ 2 （オプション 2）コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

a) セキュリティ モジュール に接続します。

connect module *slot_number* {**console** | **telnet**}

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 脅威に対する防御 コンソールに接続します。

connect ftd *name*

複数のアプリケーションインスタンスがある場合は、インスタンスの名前を指定する必要があります。インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect ftd FTD_Instance1

============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
```

```
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
==========================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to
bootCLI
>
```

c) **exit** と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

（注） 6.3 より前のバージョンの場合は、**Ctrl-a, d** と入力します。

d) FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了するには、以下を実行します。

1. ~ と入力

   Telnet アプリケーションに切り替わります。

2. Telnet アプリケーションを終了するには、次を入力します。

   telnet>**quit**

Telnet セッションを終了するには、以下を実行します。

Ctrl-], . と入力

例

次に、セキュリティモジュール 1 の 脅威に対する防御 に接続してから、FXOS CLI のスーパバイザレベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
```

```
'connect module <slot> telnet' to connect to the security module.
==================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

次のステップ

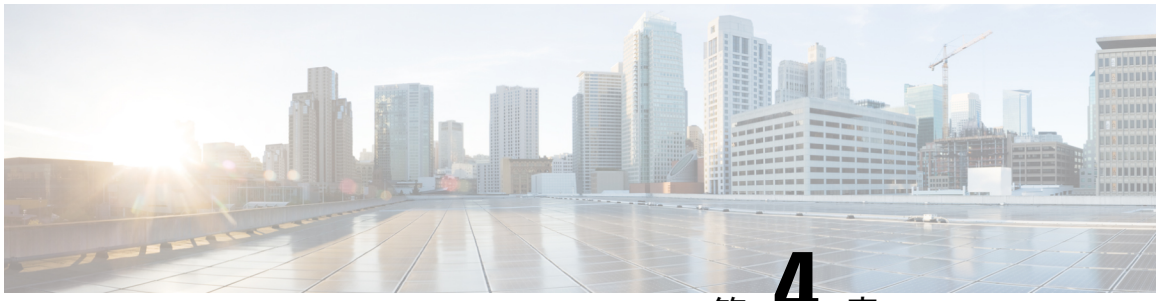
Threat Defense の設定を続行するには、「Cisco Firepower ドキュメント一覧」にあるお使いのソフトウェアバージョンのマニュアルを参照してください。

Management Center の使用に関する情報については、「Firepower Management Center コンフィギュレーション ガイド」を参照してください。

Threat Defense と Management Center の履歴

機能名	バージョン	機能情報
ASA および 脅威に対する防御 を同じ Firepower 9300 の別のモジュールでサポート	6.4	ASA および 脅威に対する防御 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 （注） FXOS 2.6.1 が必要です。

機能名	バージョン	機能情報
Firepower 4100/9300 上の Threat Defense のマルチインスタンス機能	6.3.0	単一のセキュリティエンジンまたはモジュールに、それぞれ Threat Defense コンテナインスタンスがある複数の論理デバイスを展開できるようになりました。以前は、単一のネイティブ アプリケーション インスタンスを展開できるだけでした。 柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。リソース管理では、各インスタンスのパフォーマンス機能をカスタマイズできます。 2 台の個別のシャーシ上でコンテナ インスタンスを使用して高可用性を使用できます。クラスタリングはサポートされません。 （注） マルチインスタンス機能は、実装は異なりますが、ASA マルチ コンテキスト モードに似ています。Threat Defense ではマルチコンテキストモードは使用できません。 新規/変更された Management Center 画面： • **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[編集（Edit）]** アイコン > **[インターフェイス（Interfaces）]** タブ 新規/変更された Chassis Manager 画面： • **[概要（Overview）]** > **[デバイス（Devices）]** • **[インターフェイス（Interfaces）]**> **[すべてのインターフェイス（All Interfaces）]**> **[新規追加（Add New）]** ドロップダウン メニュー > [サブインターフェイス（Subinterface）] • **[インターフェイス（Interfaces）]**> **[すべてのインターフェイス（All Interfaces）]**> **[タイプ（Type）]** • **[論理デバイス（Logical Devices）]** > **[デバイスの追加（Add Device）]** • **[プラットフォームの設定（Platform Settings）]** > **[Macプール（Mac Pool）]** • **[プラットフォームの設定（Platform Settings）]** > **[リソースのプロファイル（Resource Profiles）]**



第 4 章

Device Manager での Threat Defense の展開

この章の対象読者

この章では、Device Manager を使用してスタンドアロンの 脅威に対する防御 論理デバイスを展開する方法について説明します。高可用性ペアを展開する場合は、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

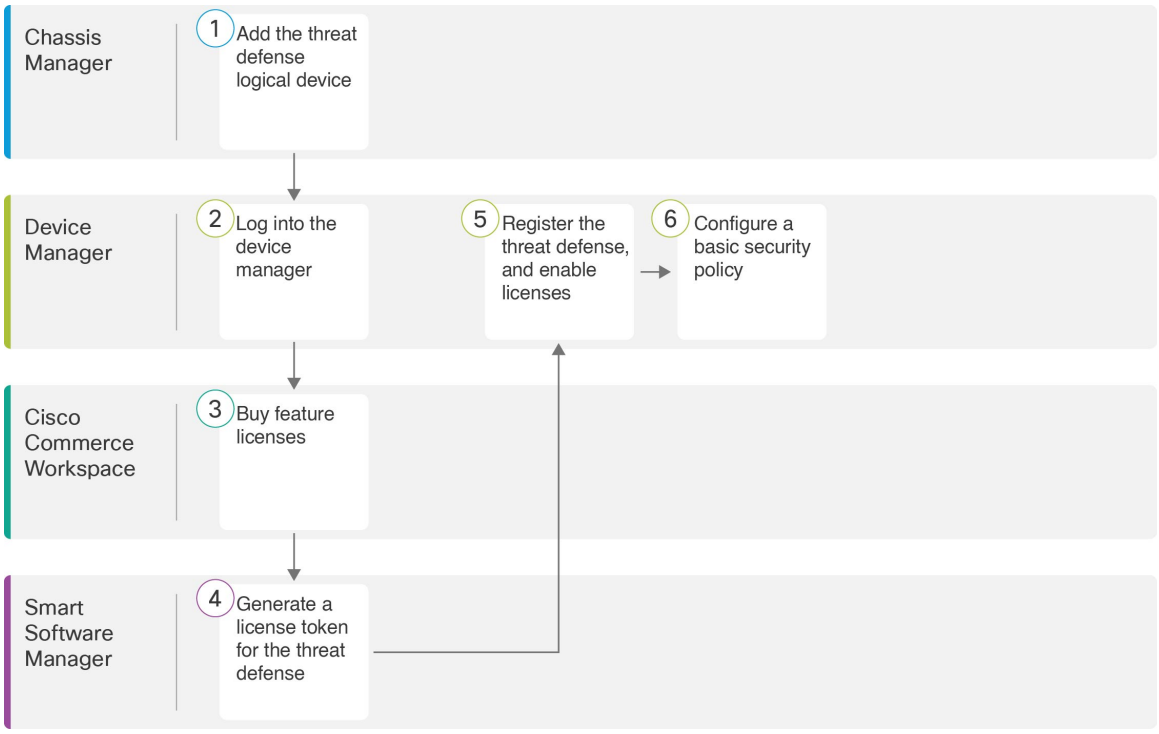
Device Manager では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Device Manager デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

多数のデバイスを管理している場合、または 脅威に対する防御 で許可される、より複雑な機能や設定を使用する場合は、代わりに Management Center を使用します。

プライバシー収集ステートメント：Firepower 9300 には個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザー名などの設定では、個人識別情報を使用できます。この場合、設定作業時やSNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

エンドツーエンドの手順

シャーシで 脅威に対する防御 を展開して設定するには、次のタスクを参照してください。



	ワークスペース	手順
1	Chassis Manager	Chassis Manager：Threat Defense 論理デバイスの追加 （66 ページ）。
2	Device Manager	Device Manager へのログイン （71 ページ）。
3	Cisco Commerce Workspace	ライセンスの設定 （71 ページ）：機能ライセンスを購入します。
4	Smart Software Manager	ライセンスの設定 （71 ページ）：Device Manager のライセンストークンを生成します。
5	Device Manager	ライセンスの設定 （71 ページ）：Device Manager をスマート ライセンシング サーバーに登録し、機能ライセンスを有効にします。
6	Device Manager	基本的なセキュリティポリシーの設定 （78 ページ）。

Chassis Manager：Threat Defense 論理デバイスの追加

Threat Defense をネイティブインスタンスとして Firepower 9300 から展開できます。コンテナインスタンスはサポートされていません。

高可用性ペアを追加するには、Cisco Secure Firewall Device Manager Configuration Guideを参照してください。

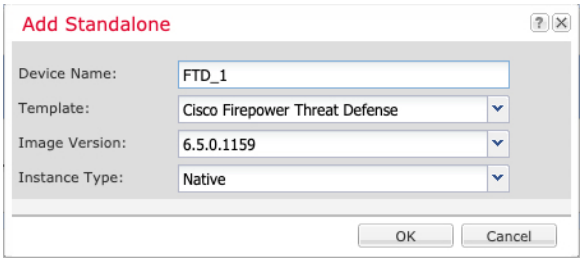
始める前に

- Threat Defense と一緒に使用する管理インターフェイスを設定します。インターフェイスの設定 （24 ページ） を参照してください。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用される（[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示される）シャーシ管理ポートと同じではありません。
- また、少なくとも 1 つのデータ インターフェイスを設定する必要があります。
- 次の情報を用意します。
  - このデバイスのインターフェイス Id
  - 管理インターフェイス IP アドレスとネットワークマスク
  - ゲートウェイ IP アドレス
  - DNS サーバの IP アドレス
  - Threat Defense ホスト名とドメイン名

手順

ステップ 1 Chassis Manager で、[論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[追加（Add）]** > **[スタンドアロン（Standalone）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

この名前は、シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

b) [Template] では、[Cisco Firepower Threat Defense] を選択します。

c) [Image Version] を選択します。

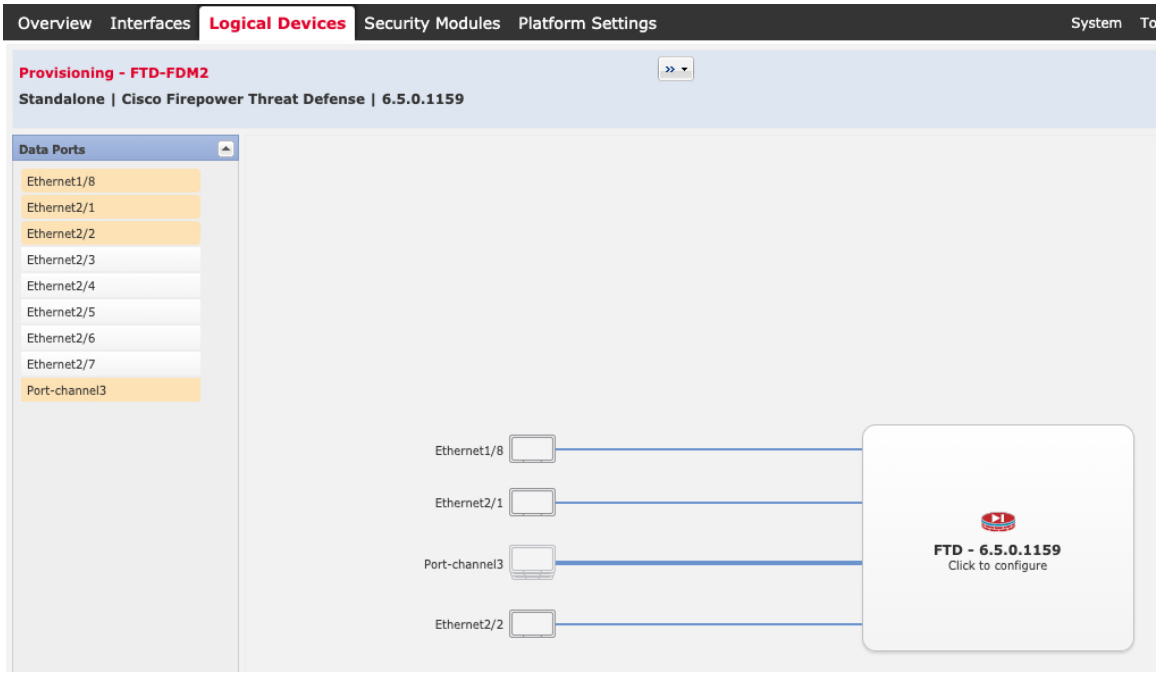
d) [Instance Type] で [Native] を選択します。

コンテナインスタンスは Device Manager ではサポートされていません。

e) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。

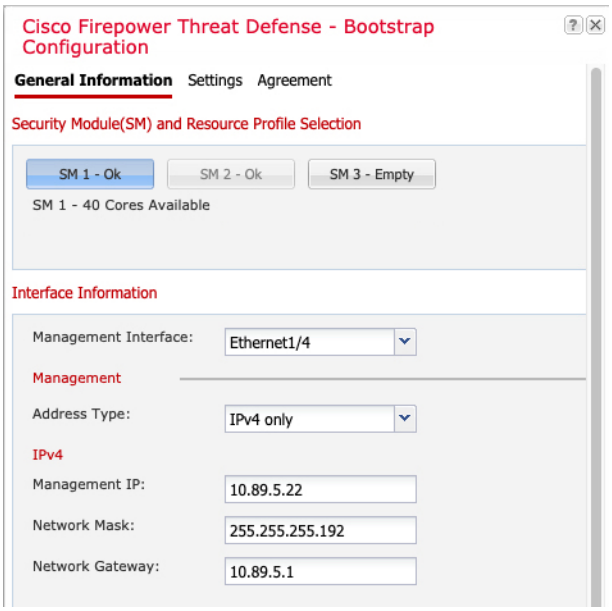


以前に[インターフェイス（Interfaces）]ページで有効にしたデータインターフェイスのみを割り当てることができます。後で Device Manager でこれらのインターフェイスを有効にして設定します。これには、IP アドレスの設定も含まれます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [一般情報（General Information）] ページで、次の手順を実行します。



a) （Firepower 9300 の場合）[セキュリティモジュールの選択（Security Module Selection）] の下で、この論理デバイスに使用するセキュリティモジュールをクリックします。

b) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

c) 管理インターフェイスを選択します。[アドレスタイプ（Address Type）]：[IPv4のみ（IPv4 only）]、[IPv6のみ（IPv6 only）]、または [IPv4およびIPv6（IPv4 and IPv6）]。

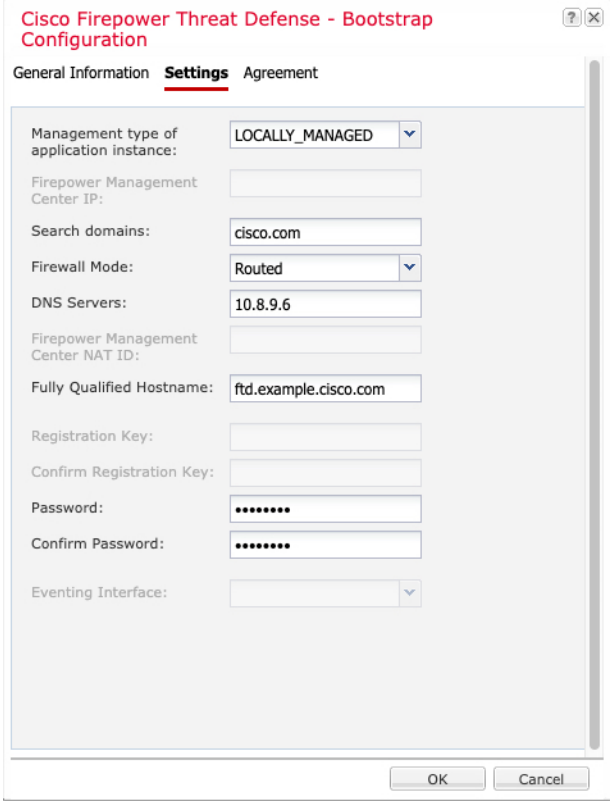
d) [Management IP] アドレスを設定します。

このインターフェイスに一意の IP アドレスを設定します。

e) [Network Mask] または [Prefix Length] に入力します。

f) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [Settings] タブで、次の手順を実行します。



a) [Management type of application instance] ドロップダウンリストで、[LOCALLY_MANAGED] を選択します。

ネイティブインスタンスは、マネージャとしての Management Center もサポートしています。論理デバイスの展開後にマネージャを変更すると、設定が消去され、デバイスが再初期化されます。

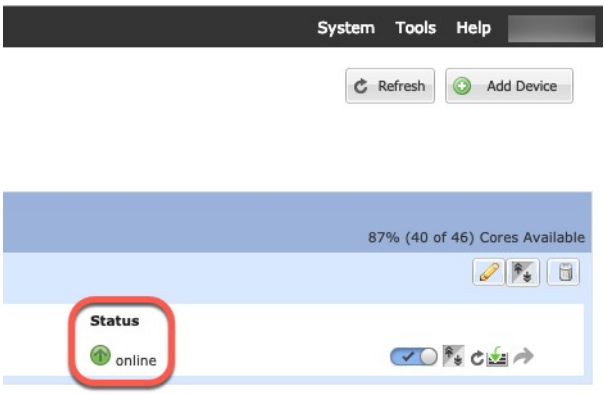
b) カンマ区切りリストとして [検索ドメイン（Search Domains）] を入力します。
c) [Firewall Mode] では [Routed] モードのみサポートされています。
d) [DNS Servers] をカンマ区切りのリストとして入力します。
e) 脅威に対する防御 の [Fully Qualified Hostname] を入力します。
f) CLI アクセス用の 脅威に対する防御 管理ユーザの [Password] を入力します。

ステップ 7 [利用規約（Agreement）] タブで、エンドユーザライセンス（EULA）を読んで、同意します。

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



Device Manager へのログイン

Device Manager にログインして 脅威に対する防御 を設定します。

始める前に

- Firefox、Chrome、Safari、Edge、または Internet Explorer の最新バージョンを使用します。
- Chassis Manager の [論理デバイス（Logical Devices）] ページで、Threat Defense 論理デバイスの [ステータス（Status）] が [オンライン（online）] になっていることを確認します。

手順

ステップ 1 ブラウザに次の URL を入力します。

- 管理：**https://***management_ip*。ブートストラップ設定に入力したインターフェイスの IP アドレスを入力します。

ステップ 2 ユーザー名 **admin**、Threat Defense の展開時に設定したパスワードを使用してログインします。

ステップ 3 90 日間の評価ライセンスに同意するように求められます。

ライセンスの設定

Threat Defense は、ライセンスの購入およびライセンスプールの一元管理が可能なスマート ソフトウェア ライセンシングを使用します。

シャーシを登録すると、Smart Software Manager はシャーシと Smart Software Manager 間の通信用の ID 証明書を発行します。また、適切な仮想アカウントにシャーシが割り当てられます。

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

Essentials ライセンスは自動的に含まれます。スマートライセンスでは、まだ購入していない製品の機能を使用できます。Smart Software Manager に登録すると、すぐにライセンスの使用を開始できます。また、後でライセンスを購入することもできます。これによって、機能の展開および使用が可能になり、発注書の承認による遅延がなくなります。次のライセンスを確認してください。

- **IPS**：セキュリティインテリジェンスと次世代 IPS
- **マルウェア防御**：マルウェア防御
- **URL**：URL フィルタリング
- **Cisco Secure Client**：Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ

始める前に

- Smart Software Manager にマスターアカウントを持ちます。

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

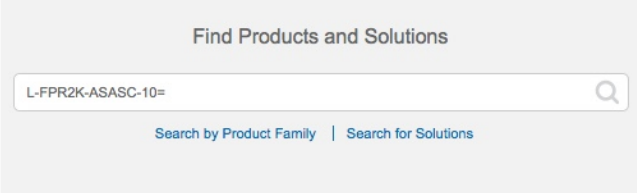
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用のスマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

手順

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 7: ライセンス検索



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

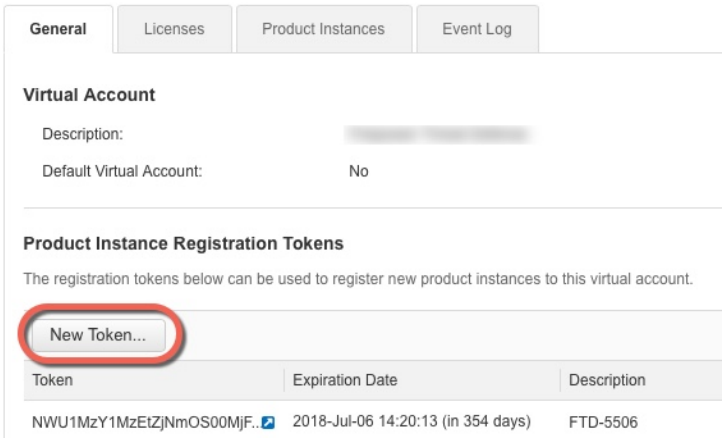
- IPS、マルウェア防御、および URL ライセンスの組み合わせ：
  - L-FPR9K-40T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-TMC=

  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-FPR9K-40T-TMC-1Y
  - L-FPR9K-40T-TMC-3Y
  - L-FPR9K-40T-TMC-5Y
  - L-FPR9K-48T-TMC-1Y
  - L-FPR9K-48T-TMC-3Y
  - L-FPR9K-48T-TMC-5Y
  - L-FPR9K-56T-TMC-1Y
  - L-FPR9K-56T-TMC-3Y
  - L-FPR9K-56T-TMC-5Y
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。

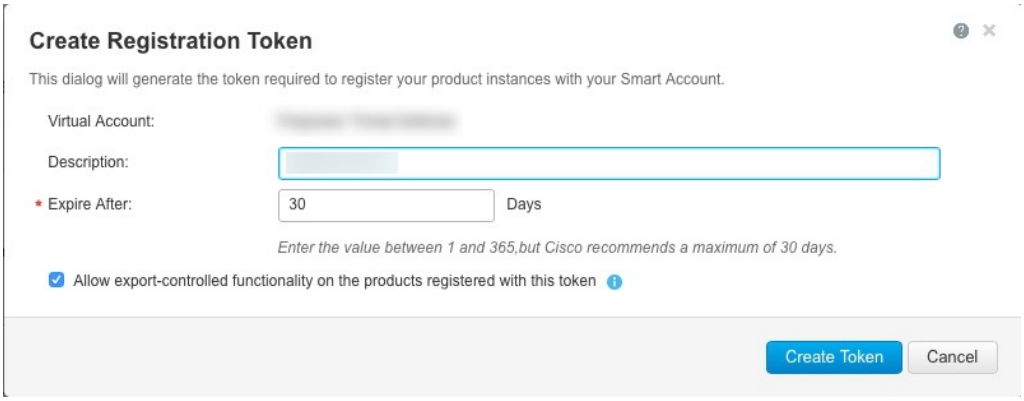
ステップ 2 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

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



c) [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（Description）]**
- [有効期限（Expire After）]：推奨値は 30 日です。
- [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。

d) 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。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 *8*：トークンの表示

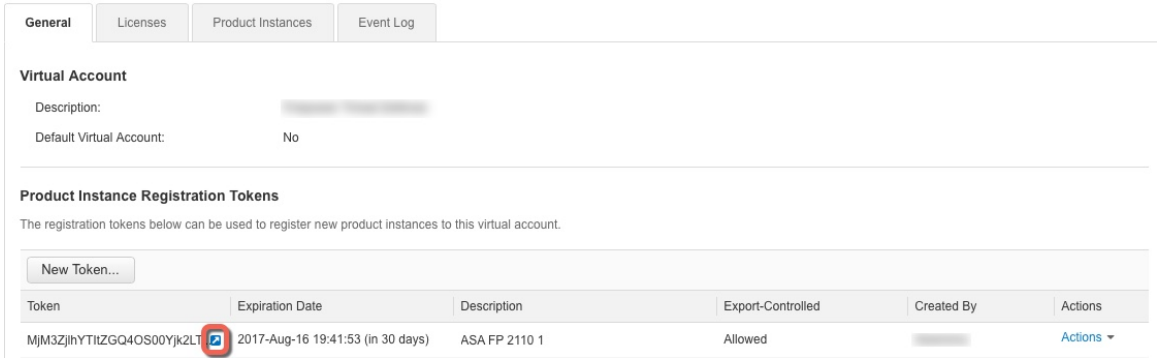
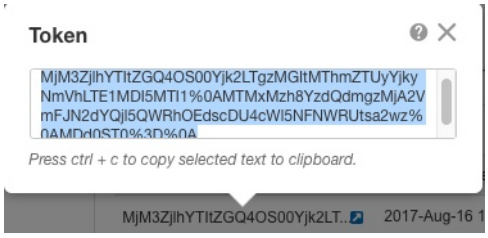


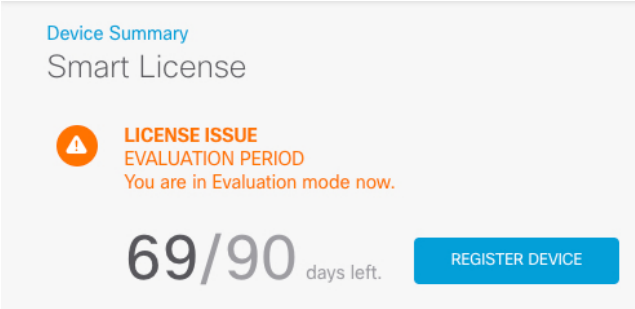
図 *9*：トークンのコピー



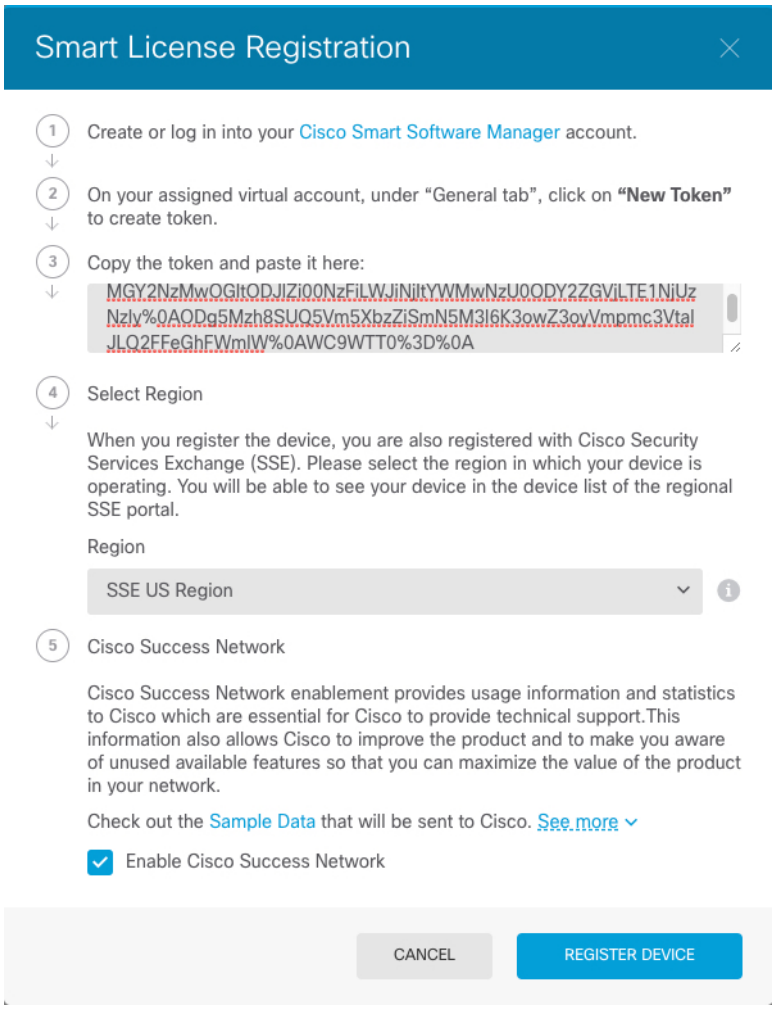
ステップ 3 Device Manager で、[デバイス（Device）] をクリックし、[スマートライセンス（Smart License）] のサマリーで [設定の表示（View Configuration）] をクリックします。

[スマート ライセンス（Smart License）] ページが表示されます。

ステップ 4 [デバイスの登録（Register Device）] をクリックします。

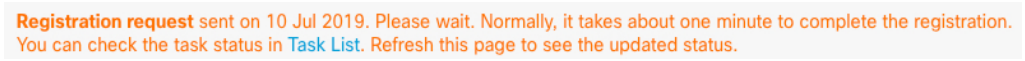


次に、[スマートライセンスの登録（Smart License Registration）] ダイアログボックスの指示に従って、トークンに貼り付けます。

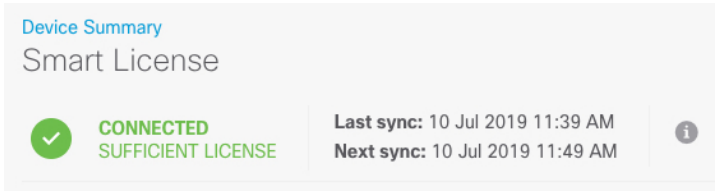


ステップ 5 [デバイスの登録（Register Device）] をクリックします。

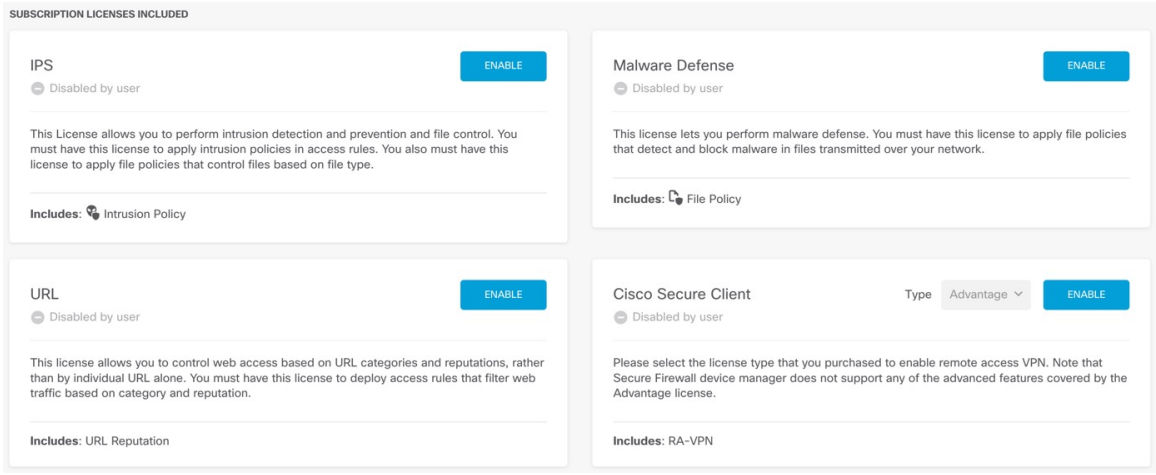
[スマート ライセンス（Smart License）] ページに戻ります。デバイス登録中は次のメッセージが表示されます。



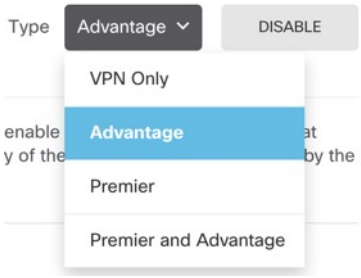
デバイスが正常に登録され、ページが更新されると、次のように表示されます。



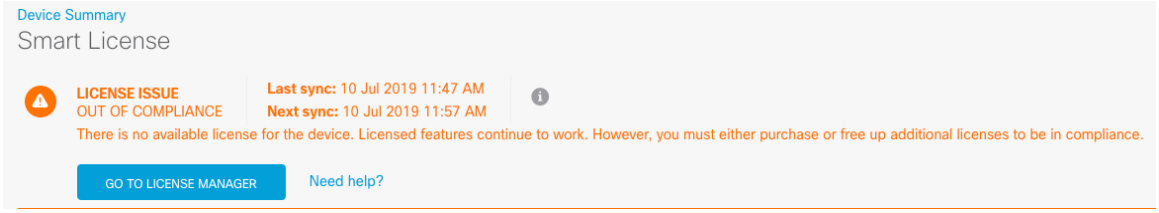
ステップ 6 必要に応じて、それぞれのオプション ライセンスの [有効化/無効化（Enable/Disable）] コントロールをクリックします。



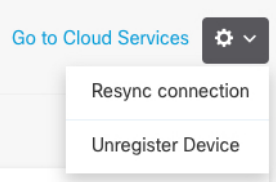
- [有効化（Enable）]：Cisco Smart Software Manager アカウントにライセンスを登録し、制御された機能が有効になります。ライセンスによって制御されるポリシーを設定し、展開できます。
- [無効化（Disable）]：Cisco Smart Software Manager アカウントのライセンスを登録解除し、制御された機能が無効になります。新しいポリシーの機能の設定も、その機能を使用するポリシーの展開もできません。
- [Cisco Secure Client] [RA VPN] ライセンスを有効にした場合は、使用するライセンスのタイプ（[Advantage]、[Plus]、[Premier]、[Apex]、[VPN専用（VPN Only）、または [Premier とAdvantage（Premier and Advantage）] [Apex and Plus（Apex and Plus）] を選択します。



機能を有効にすると、アカウントにライセンスがない場合はページを更新した後に次の非準拠メッセージが表示されます。



ステップ 7 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。



基本的なセキュリティポリシーの設定

基本的なセキュリティ ポリシーを設定するには、次のタスクを実行します。

1	インターフェイスの設定 （79 ページ）。 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。
2	セキュリティゾーンへのインターフェイスの追加 （81 ページ）。 アクセス制御に必要な内部および外部のセキュリティゾーンに、内部インターフェイスと外部インターフェイスを追加します。
3	デフォルトルートの追加 （83 ページ）。 外部DHCPサーバーからデフォルトルートを受け取らない場合は、手動で追加する必要があります。
4	NAT の設定 （85 ページ）。 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。
5	内部から外部へのトラフィックの許可 （87 ページ）。 内部から外部へのトラフィックを許可します。
6	（任意）DHCP サーバーの設定 （88 ページ）。 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。
7	（任意）管理ゲートウェイの設定とデータインターフェイスの管理の許可 （91 ページ）。 管理ゲートウェイを変更するか、データインターフェイスからの管理を許可します。
8	設定の展開 （92 ページ）。

インターフェイスの設定

脅威に対する防御 インターフェイスを有効にし、IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。これらのインターフェイスの一部は、Web サーバーなどのパブリックアクセスが可能なアセットを配置する「緩衝地帯」（DMZ）となる場合があります。

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

次の例では、DHCP によるスタティックアドレスと外部インターフェイスを使用して、内部インターフェイスを設定します。

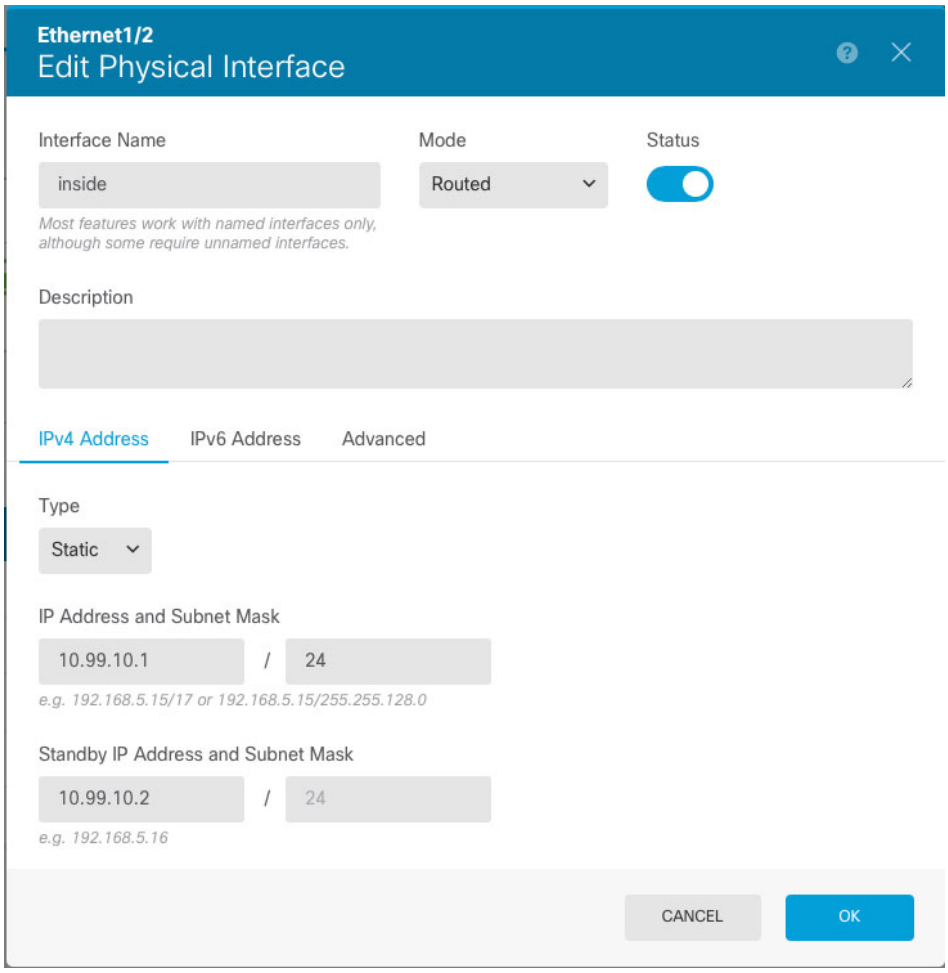
手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにあるリンクをクリックします。

[インターフェイス（Interfaces）] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 外部用に使用するインターフェイスの編集アイコン（）をクリックします

ステップ 3 次の設定を行います。



a) [インターフェイス名（Interface Name）] を設定します。

インターフェイスの名前（最大 48 文字）を設定します。英字は小文字にする必要があります。例、[inside] または [outside]。名前を設定しないと、インターフェイスの残りの設定は無視されます。サブインターフェイスを設定する場合を除き、インターフェイスには名前が必要です。

b) [モード（Mode）] を [ルーテッド（Routed）] に設定します。

パッシブインターフェイスを使用する場合は、Cisco Secure Firewall Device Manager Configuration Guideを参照してください。

c) [ステータス（Status）] スライダを [有効（enabled）] 設定（）に設定します。

重要 また、FXOS でインターフェイスを有効にする必要があります。

d) （任意）[説明（Description）] を設定します。

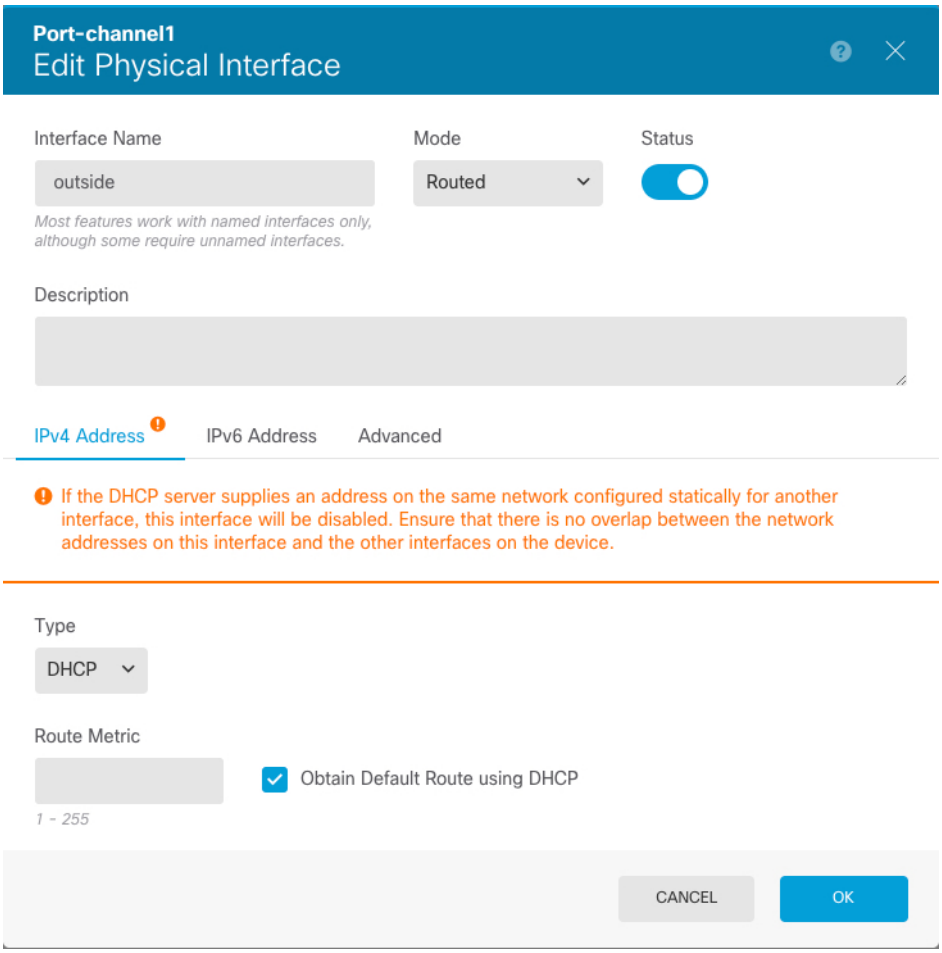
説明は 200 文字以内で、改行を入れずに 1 行で入力します。

e) [IPv4アドレス（IPv4 Address）] ページで、スタティック IP アドレスを設定します。

f) （任意）[IPv6アドレス（IPv6 Address）] をクリックし、IPv6 を設定します。

ステップ 4 [OK] をクリックします。

ステップ 5 外部用に使用するインターフェイスの編集アイコン（）をクリックし、内部の場合と同じフィールドを設定します。このインターフェイスでは、IPv4 アドレスに [DHCP] を選択します。



（注） スタティック IP アドレスを使用する場合、または DHCP からデフォルトルートを受信しない場合は、デフォルトルートを手動で設定する必要があります。Cisco Secure Firewall Device Manager Configuration Guideを参照してください。

セキュリティゾーンへのインターフェイスの追加

セキュリティゾーンとはインターフェイスのグループ分けです。ゾーンは、トラフィックの管理と分類に役立つようにネットワークをセグメントに分割します。複数のゾーンを定義できますが、所与のインターフェイスは単一のゾーンの中にのみ存在できます。

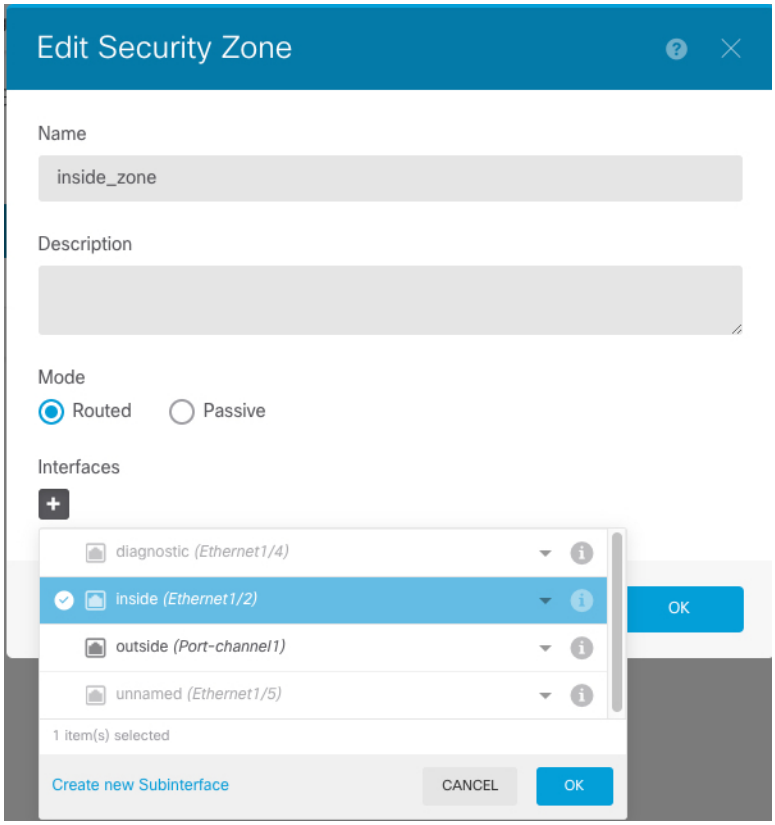
この手順では、次の事前設定ゾーンにインターフェイスを追加する方法について説明します。

- [inside_zone]：このゾーンは、内部ネットワークを表します。
- [outside_zone]：このゾーンは、インターネットなどの制御不可能な外部ネットワークを表します。

手順

ステップ 1 [オブジェクト（Objects）] を選択し、次に目次から [セキュリティゾーン（Security Zones）] を選択します。

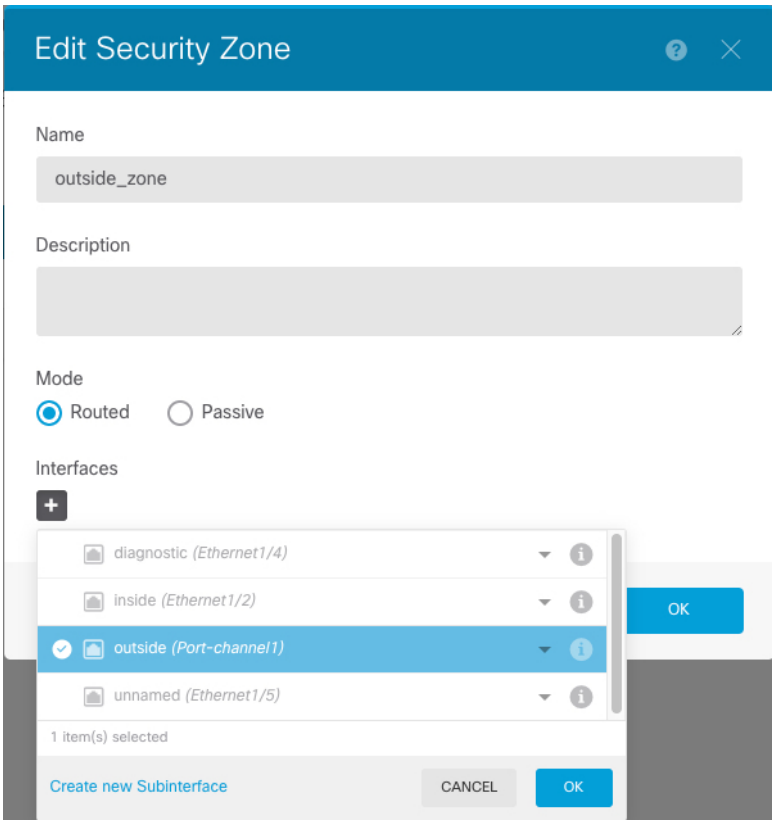
ステップ 2 [inside_zone] の [編集（edit）] アイコン（）をクリックします。



ステップ 3 [インターフェイス（Interfaces）] リストで、をクリックし、ゾーンに追加する内部インターフェイスを選択します。

ステップ 4 [OK] をクリックして変更を保存します。

ステップ 5 外部インターフェイスを [outside_zone] に追加するには、これらの手順を繰り返します。



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。外部インターフェイスにDHCPを使用する場合は、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。DHCP サーバーからデフォルトルートを受信した場合は、**[デバイスの概要（Device Summary）]**>**[スタティックルーティング（Static Routing）]**ページに表示されます。

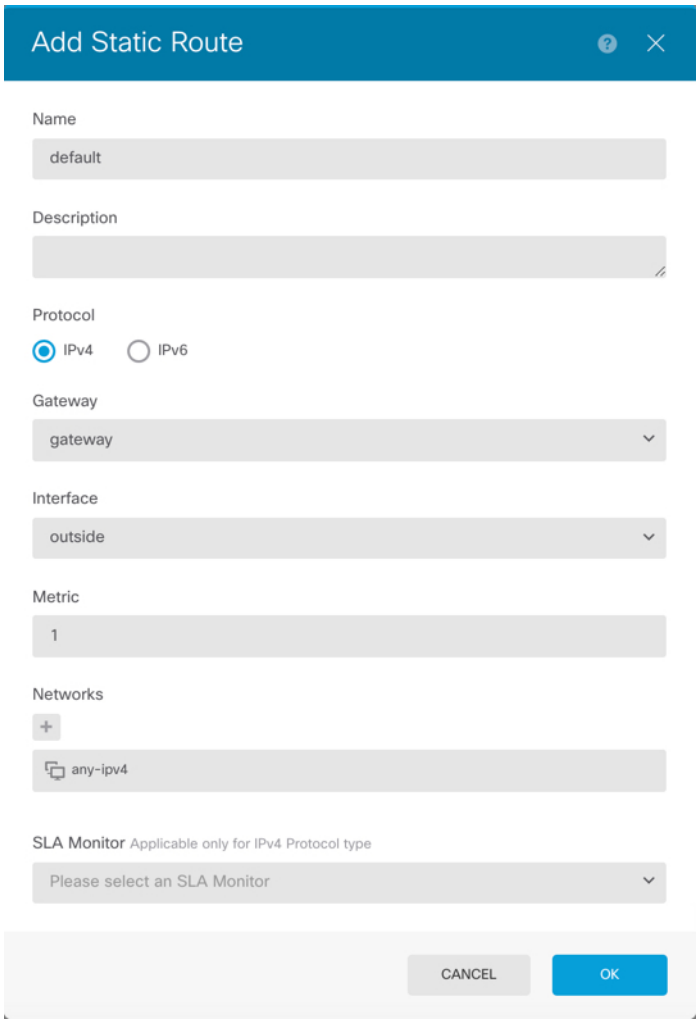
手順

ステップ 1 [デバイス（Device）] をクリックしてから、[ルーティング（Routing）] サマリーにあるリンクをクリックします。

[スタティックルーティング（Static Routing）] ページが表示されます。

ステップ 2 + または [スタティックルートの作成（Create Static Route）] をクリックします。

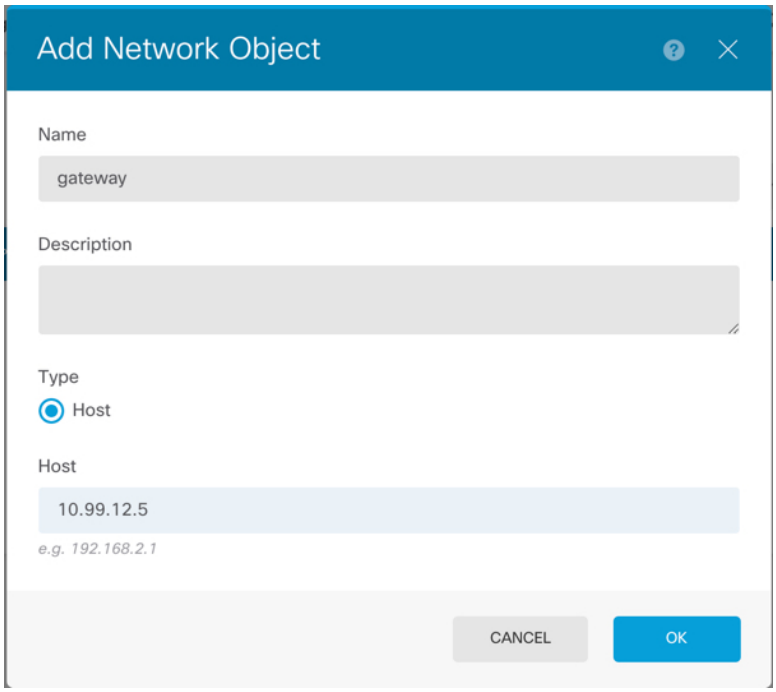
ステップ 3 デフォルトルートのプロパティを設定します。



a) [名前（Name）] を入力します。たとえば「default」とします。
b) [IPv4] または [IPv6] ラジオボタンをクリックします。

   IPv4 と IPv6 に対して個別のデフォルトルートを作成する必要があります。

c) [ゲートウェイ（Gateway）] をクリックしてから [新しいネットワークの作成（Create New Network）] をクリックして、ゲートウェイ IP アドレスをホストオブジェクトとして追加します。



d) ゲートウェイの [インターフェイス（Interface）] （たとえば [外部（outside）]）を選択します。

e) [ネットワーク（Network）] ＋アイコンをクリックし、IPv4 デフォルトルートの場合は [any-ipv4] 、IPv6 デフォルトルートの場合は [any-ipv6] を選択します。

ステップ 4 [OK] をクリックします。

NAT の設定

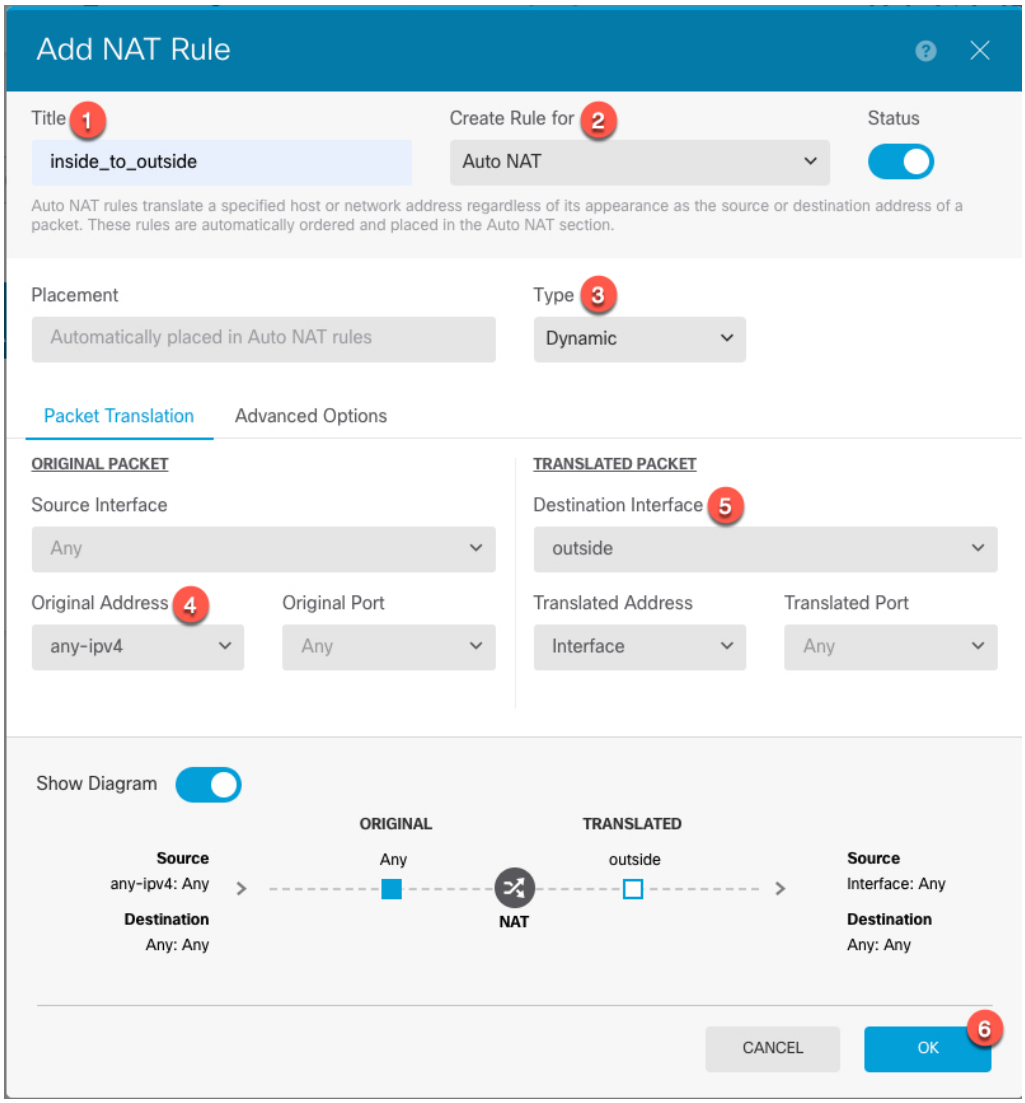
一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。IPv6 にインターフェイス PAT は使用できません。

手順

ステップ 1 [ポリシー（Policies）] をクリックしてから [NAT] をクリックします。

ステップ 2 ＋または [NATルールの作成（Create NAT Rule）] をクリックします。

ステップ 3 基本ルールのオプションを設定します。



a) [タイトル（Title）] を設定します。
b) **[ルールの作成対象（Create Rule For）] > [自動NAT（Auto NAT）]** を選択します。
c) **[タイプ（Type）] > [ダイナミック（Dynamic）]** を選択します。

ステップ 4 次のパケット変換オプションを設定します。

a) [元のパケット（Original Packet）] で、[元のアドレス（Original Address）] を [any-ipv4] に設定します。

このルールは、任意のインターフェイスから発信されるすべての IPv4 トラフィックを変換します。インターフェイスまたはアドレスを制限する場合は、特定の [送信元インターフェイス（Source Interface）] を選択し、[元のアドレス（Original Address）] に IP アドレスを指定できます。

b) [変換済みパケット（Translated Packet）] で、[接続先インターフェイス（Destination Interface）] を外部インターフェイスに設定します。

デフォルトでは、インターフェイス IP アドレスが変換済みアドレスに使用されます。

ステップ 5 （任意）[図の表示（Show Diagram）] をクリックして、ルールのビジュアル表現を表示します。

ステップ 6 [OK] をクリックします。

内部から外部へのトラフィックの許可

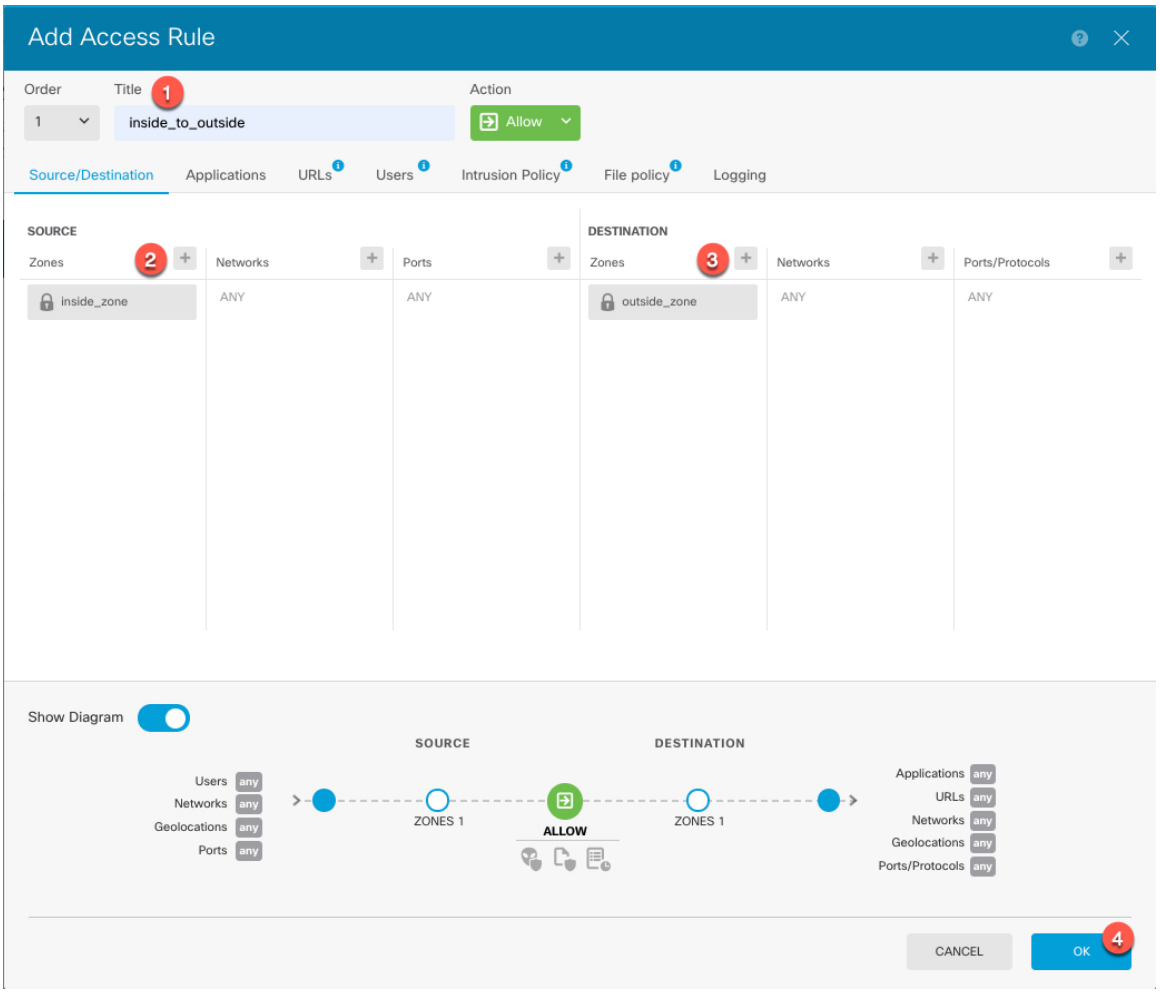
デフォルトでは、セキュリティゾーン間のトラフィックはブロックされます。この手順では、内部から外部へのトラフィックを許可する方法を示します。

手順

ステップ 1 **[ポリシー（Policies）]** > **[アクセス制御（Access Control）]** を選択します。

ステップ 2 + または [アクセスルールの作成（Create Access Rule）] をクリックします。

ステップ 3 基本ルールのオプションを設定します。



a) [タイトル（Title）] を設定します。

b) [ソース（Source）] で、[ゾーン（Zones）] + アイコンをクリックし、内部ゾーンを選択します。

c) [接続先（Destination）] で、[ゾーン（Zones）] + アイコンをクリックし、外部ゾーンを選択します。

d) （任意）[図の表示（Show Diagram）] をクリックして、ルールのビジュアル表現を表示します。

e) [OK] をクリックします。

（任意）DHCP サーバーの設定

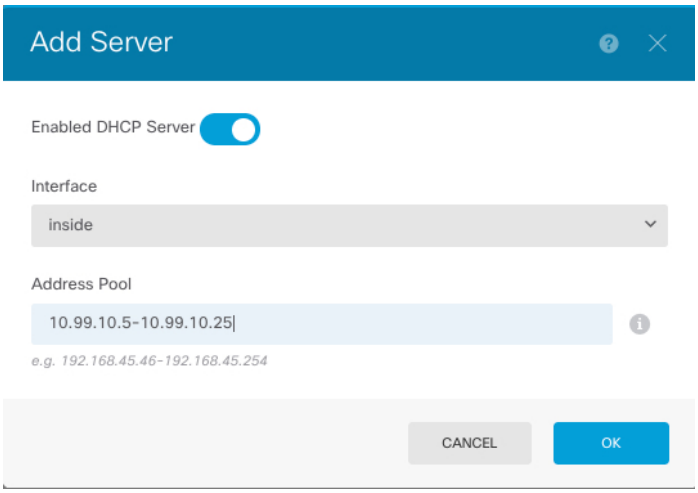
クライアントで DHCP を使用して 脅威に対する防御 から IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）] > [DHCPサーバー（DHCP Server）]** リンクをクリックします。

ステップ 2 + または [DHCPサーバーの作成（Create DHCP Server）] をクリックします。

ステップ 3 サーバーのプロパティを設定します。



a) [DHCPサーバーを有効にする（Enable DHCP Server）] スライダをクリックして、有効と表示します（ ）。

b) DHCP サーバーを有効にする [インターフェイス（Interface）] を選択します。

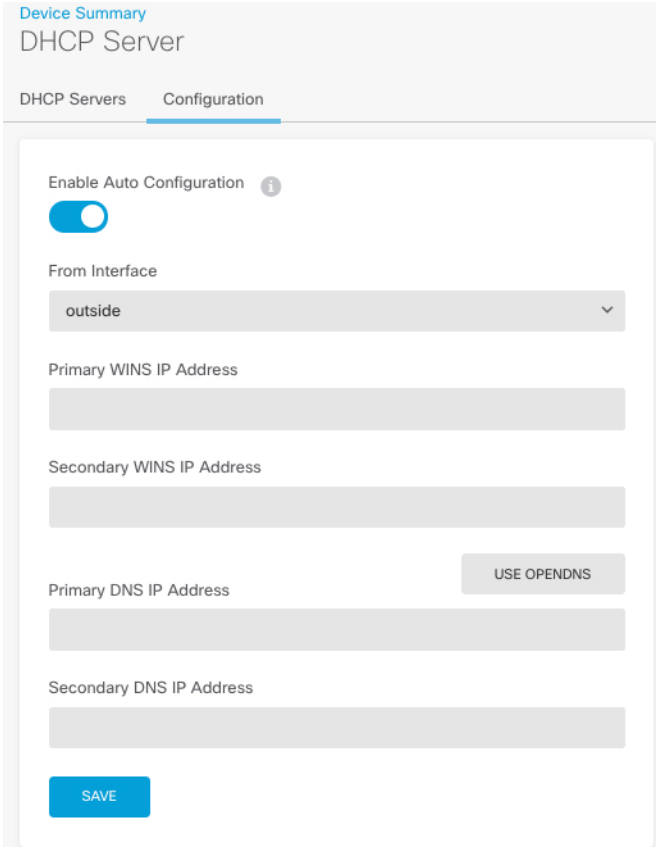
インターフェイスは静的 IP アドレスを持っている必要があります。インターフェイスで DHCP サーバーを実行する場合、インターフェイス アドレスの取得に DHCP を使用することはできません。

c) [アドレスプール（Address Pool）] を入力します

IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自体の IP アドレス、ブロードキャスト アドレス、またはサブネット ネットワーク アドレスを含めることはできません。

d) [OK] をクリックします。

ステップ 4 （任意） [設定（Configuration）] タブをクリックして、自動設定およびグローバル設定を設定します。



DHCP 自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。通常、外部インターフェイスで DHCP を使用してアドレスを取得する場合には自動設定を使用しますが、DHCP を介してアドレスを取得するインターフェイスを選択することもできます。自動設定を使用できない場合には、必要なオプションを手動で定義できます。

a) [自動設定を有効にする（Enable Auto Configuration）] スライダをクリックして、有効と表示します（ ）。
b) クライアントがサーバー設定を継承するインターフェイスを [継承元インターフェイス（From Interface）] ドロップダウンメニューで選択します。
c) 自動設定を有効にしない場合、または自動設定された設定を上書きするには、1 つ以上のグローバルオプションを設定します。これらの設定は、DHCP サーバーを実行するすべてのインターフェイスで DHCP クライアントに送信されます。
d) [保存（Save）] をクリックします。

（任意）管理ゲートウェイの設定とデータインターフェイスの管理の許可

Threat Defense を展開するときに、管理アドレスと外部ゲートウェイは設定済みです。次の手順では、管理インターフェイスではなくデータインターフェイスを介してバックプレーン経由で管理トラフィックを送信するように Threat Defense を設定できます。この場合、直接接続された管理ネットワーク上にいる場合は Threat Defense を管理できますが、他のネットワーク宛ての管理トラフィックは、管理インターフェイスではなくデータインターフェイスにルーティングされます。

また、デフォルトでは、管理インターフェイス（Device Manager または CLI アクセス）を介してのみ Threat Defense を管理できます。次の手順では、1 つ以上のデータインターフェイスで管理を有効にすることもできます。管理インターフェイス ゲートウェイは、データインターフェイスの Device Manager 管理トラフィックには影響を及ぼしません。この場合、Threat Defense では通常のルーティングテーブルが使用されます。

始める前に

インターフェイスの設定 （79 ページ）に従ってデータインターフェイスを設定します。

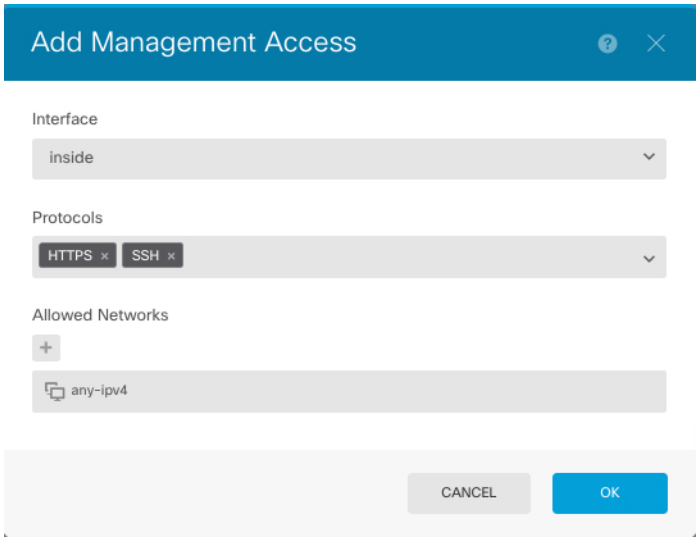
手順

ステップ 1 データインターフェイスからの管理を許可します。

a) [デバイス（Device）] をクリックしてから、**[システム設定（System Settings）] > [管理アクセス（Management Access）]** リンクの順にクリックします。

b) [データインターフェイス（Data Interface）] をクリックします。

c) + または [データインターフェイスの作成（Create Data Interface）] をクリックし、インターフェイスごとにルールを作成します。



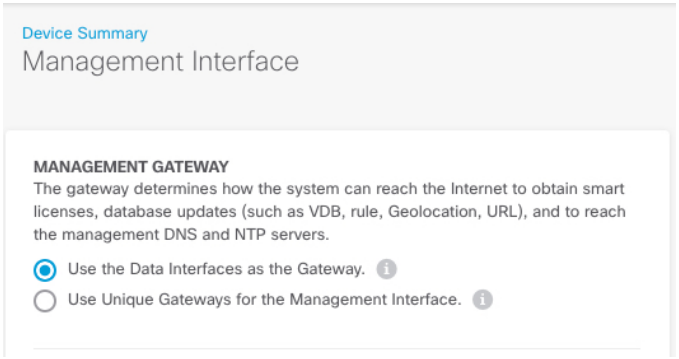
- [インターフェイス（Interface）]：管理アクセスを許可するインターフェイスを選択します。
- [プロトコル（Protocols）]：ルールが HTTPS（ポート 443）または SSH（ポート 22）、またはその両方用かを選択します。
- [許可されたネットワーク（Allowed Networks）]：システムにアクセスできる IPv4 ネットワーク、IPv6 ネットワーク、またはホストを定義するネットワークオブジェクトを選択します。「任意」のアドレスを指定するには、[any-ipv4] (0.0.0.0/0) および [any-ipv6] (::/0) を選択します。

d) [OK] をクリックします。

ステップ 2 データインターフェイスを使用するように管理ゲートウェイを設定します。

a) [デバイス（Device）] をクリックし、次に **[システム設定（System Settings）]** > **[管理インターフェイス（Management Interface）]** リンクをクリックします。

b) [データインターフェイスをゲートウェイとして使用する（Use the Data Interfaces as the Gateway）] を選択します。



c) [保存（Save）] をクリックして警告を読み、[OK] をクリックします。

設定の展開

設定の変更を 脅威に対する防御 に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

手順

ステップ 1 Web ページの右上にある [変更の展開（Deploy Changes）] アイコンをクリックします。

このアイコンは、展開されていない変更がある場合にドット マークで強調表示されます。

[保留中の変更（Pending Changes）] ウィンドウには、設定の展開バージョンと保留中の変更との比較が表示されます。それらの変更は、削除された要素、追加された要素、または編集された要素を示すために色分けされています。色の説明については、ウィンドウの凡例を参照してください。

ステップ 2 変更内容に問題がない場合は、[今すぐ展開（Deploy Now）] をクリックして、ジョブをすぐに開始できます。

ウィンドウに展開が進行中であることが示されます。ウィンドウを閉じるか、または展開が完了するまで待機できます。展開が進行中の間にウィンドウを閉じても、ジョブは停止しません。結果は、タスクリストや監査ログで確認できます。ウィンドウを開いたままにした場合、[展開履歴（Deployment History）] リンクをクリックすると結果が表示されます。

Threat Defense CLI へのアクセス

脅威に対する防御 CLI を使用して、管理インターフェイスパラメータを変更したり、トラブルシューティングを行ったりできます。CLI にアクセスするには、管理インターフェイスへの SSH を使用するか、FXOS CLI から接続します。

手順

ステップ 1 （オプション 1）脅威に対する防御 管理インターフェイスの IP アドレスに直接 SSH 接続します。

管理 IP アドレスは、論理デバイスを展開したときに設定したものです。初期展開時に設定した「admin」アカウントとパスワードを使用して 脅威に対する防御 にログインします。

パスワードを忘れた場合は、シャーシマネージャ で論理デバイスを編集して変更できます。

ステップ 2 （オプション 2）コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

a) セキュリティ モジュール に接続します。

connect module *slot_number* {**console** | **telnet**}

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

b) 脅威に対する防御 コンソールに接続します。

connect ftd *name*

複数のアプリケーションインスタンスがある場合は、インスタンスの名前を指定する必要があります。インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect ftd FTD_Instance1

============================ ATTENTION ============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
===================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to
bootCLI
>
```

c) **exit** と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

（注） 6.3 より前のバージョンの場合は、**Ctrl-a, d** と入力します。

d) FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了するには、以下を実行します。

1. ~ と入力

   Telnet アプリケーションに切り替わります。

2. Telnet アプリケーションを終了するには、次を入力します。

   telnet>**quit**

Telnet セッションを終了するには、以下を実行します。

Ctrl-], . と入力

例

次に、セキュリティモジュール 1 の 脅威に対する防御 に接続してから、FXOS CLI のスーパバイザレベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

============================ ATTENTION ============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
===================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

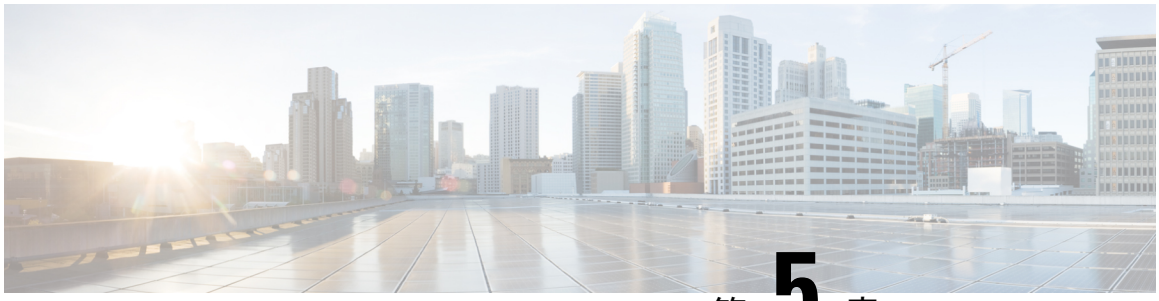
次のステップ

Threat Defense の設定を続行するには、「Cisco Firepower ドキュメント一覧」にあるお使いのソフトウェアバージョンのマニュアルを参照してください。

Device Manager の使用に関する情報については、「『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』」を参照してください。

Threat Defense と Device Manager の履歴

機能名	バージョン	機能情報
ネイティブインスタンスを使用した Device Manager のサポート	6.5.0	Device Manager を使用してネイティブインスタンスを展開できるようになりました。 新しい/変更された画面： **[論理デバイス（Logical Devices）] > [デバイスの追加（Add Device）]** （注） FXOS 2.7.1 が必要です。



第 5 章

CDO での Threat Defense の展開

この章の対象読者

使用可能なすべてのオペレーティングシステムとマネージャを確認するには、「最適なアプリケーションとマネージャを見つける方法 （1 ページ）」を参照してください。この章は、Cisco Defense Orchestrator（CDO）のクラウド提供型 Secure Firewall Management Center を使用する 脅威に対する防御 を対象としています。Device Manager の機能を使用して CDO を使用するには、CDO のマニュアルを参照してください。

（注） クラウド提供型 Management Center は、脅威に対する防御 7.2 以降をサポートします。以前のバージョンでは、CDO の Device Manager 機能を使用できます。ただし、デバイスマネージャモードは、このモードを使用して 脅威に対する防御 をすでに管理している既存の CDO ユーザーのみが使用できます。

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

ファイアウォールについて

ハードウェアでは、脅威に対する防御 ソフトウェアまたは ASA ソフトウェアを実行できます。脅威に対する防御 と ASA の間で切り替えを行う際には、デバイスの再イメージ化が必要になります。現在インストールされているものとは異なるソフトウェアバージョンが必要な場合も再イメージ化が必要です。「Cisco ASA および Firepower Threat Defense 再イメージ化ガイド」を参照してください。

ファイアウォールは、Secure Firewall eXtensible オペレーティングシステム（FXOS）と呼ばれる基盤となるオペレーティングシステムを実行します。ファイアウォールは FXOS Secure Firewall Chassis Manager をサポートしていません。トラブルシューティング用として限られた CLI のみがサポートされています。詳細については、Firepower 1000/2100 および Secure Firewall 3100 と Firepower Threat Defense の Cisco FXOS トラブルシューティング ガイドを参照してください。

プライバシー収集ステートメント：ファイアウォールには個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザー名などの設定では、個人識別情報を使用できま

す。この場合、設定作業時やSNMPの使用時に、管理者が個人識別情報を確認できる場合があります。

CDOによる Threat Defense 管理について

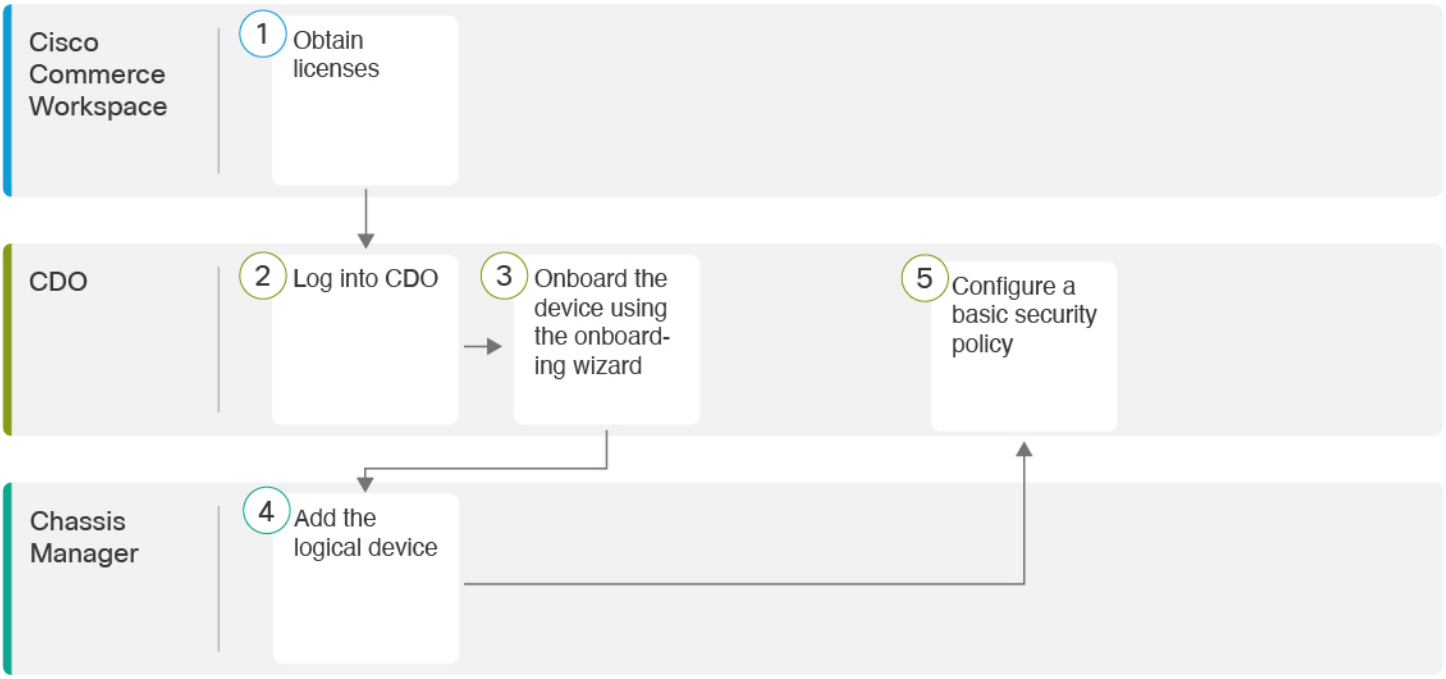
クラウド提供型 Management Center Management Center は、オンプレミスの Management Center と同じ機能の多くを提供し、同じルックアンドフィールを備えています。CDO をプライマリマネージャとして使用する場合、オンプレミスの Management Center は分析のみに使用できます。オンプレミスの Management Center は、ポリシーの構成やアップグレードをサポートしていません。

（注） CDO は、コンテナインスタンスやクラスタをサポートしていません。

エンドツーエンドの手順

オンボーディングウィザードを使用して Threat Defense を CDO にオンボードするには、次のタスクを参照してください。

図 *10* : エンドツーエンドの手順



1	Cisco Commerce Workspace	ライセンスを取得する （99 ページ）。
2	CDO	CDO へのログイン （101 ページ）。
3	CDO	オンボーディング ウィザードを使用したデバイスのオンボーディング （105 ページ）。
4	シャーシ マネージャ	Chassis Manager：Threat Defense 論理デバイスの追加 （107 ページ）。
5	CDO	基本的なセキュリティポリシーの設定 （48 ページ）。

ライセンスを取得する

すべてのライセンスは、CDO によって 脅威に対する防御 に提供されます。オプションで、次の機能ライセンスを購入できます。

- **IPS**：セキュリティインテリジェンスと次世代 IPS
- **マルウェア防御**：マルウェア防御
- **URL**：URL フィルタリング

- **Cisco Secure Client**：Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

始める前に

- Smart Software Manager にマスターアカウントを持ちます。

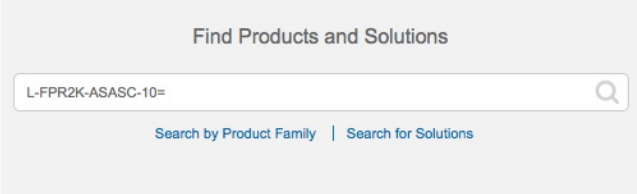
  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用のスマート ソフトウェア ライセンシング アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。

手順

ステップ 1 お使いのスマート ライセンシング アカウントに、必要なライセンスが含まれていることを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *11* : ライセンス検索



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

- IPS、マルウェア防御、および URL ライセンスの組み合わせ：
  - L-FPR9K-40T-TMC=
  - L-FPR9K-48T-TMC=
  - L-FPR9K-56T-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-FPR9K-40T-TMC-1Y

- L-FPR9K-40T-TMC-3Y
- L-FPR9K-40T-TMC-5Y
- L-FPR9K-48T-TMC-1Y
- L-FPR9K-48T-TMC-3Y
- L-FPR9K-48T-TMC-5Y
- L-FPR9K-56T-TMC-1Y
- L-FPR9K-56T-TMC-3Y
- L-FPR9K-56T-TMC-5Y

- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。
- キャリアライセンス：
  - L-FPR9K-FTD-CAR=

ステップ 2 Smart Software Manager に CDO を登録します（まだ登録していない場合）。

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、CDO のマニュアルを参照してください。

CDO へのログイン

CDOは、Cisco Secure Sign-On をアイデンティティプロバイダーとして使用し、Duo Security を多要素認証（MFA）に使用します。CDO には MFA が必要です。MFA は、ユーザーアイデンティティを保護するためのセキュリティを強化します。MFA の一種である二要素認証では、CDO にログインするユーザーの ID を確認するために、2 つのコンポーネントまたは要素が必要です。

最初の要素はユーザー名とパスワードで、2 番目の要素は Duo Security からオンデマンドで生成されるワンタイムパスワード（OTP）です。

Cisco Secure Sign-On クレデンシャルを確立したら、Cisco Secure Sign-On ダッシュボードから CDO にログインできます。Cisco Secure Sign-On ダッシュボードから、サポートされている他のシスコ製品にログインすることもできます。

- Cisco Secure Sign-On アカウントをお持ちの場合は、Cisco Secure Sign-On を使用した CDO へのログイン （104 ページ）に進みます。
- Cisco Secure Sign-On アカウントがない場合は、新しい Cisco Secure Sign-On アカウントの作成 （102 ページ）に進んでください。

新しい Cisco Secure Sign-On アカウントの作成

最初のサインオンワークフローは 4 段階のプロセスです。4 段階すべてを完了する必要があります。

始める前に

- **DUO Security のインストール**：Duo Security アプリケーションを携帯電話にインストールすることをお勧めします。Duo のインストールについてご質問がある場合は、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。
- **時刻の同期**：モバイルデバイスを使用してワンタイムパスワードを生成します。OTP は時間ベースであるため、デバイスのクロックがリアルタイムと同期していることが重要です。デバイスのクロックが正しい時刻に設定されていることを確認します。
- Firefox または Chrome の最新バージョンを使用します。

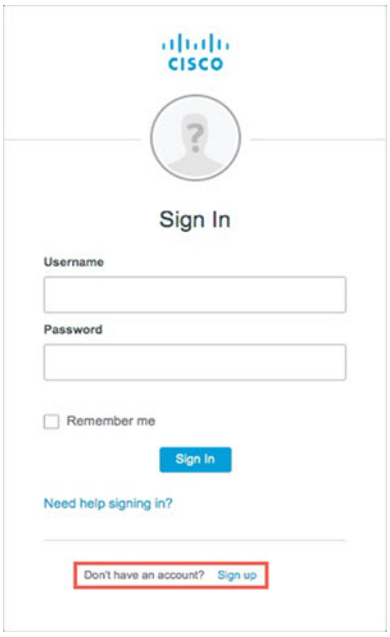
手順

ステップ 1 **新しい Cisco Secure Sign-On アカウントにサインアップします。**

a) https://sign-on.security.cisco.com にアクセスします。

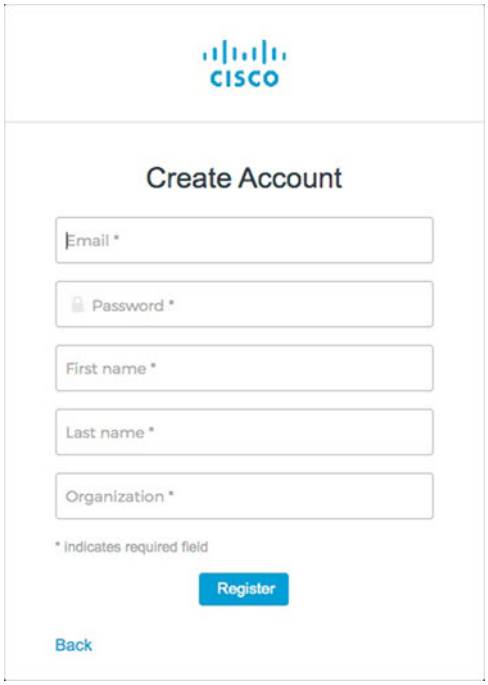
b) [サインイン（Sign In）] 画面の下部にある [サインアップ（Sign up）] をクリックします。

図 *12 : Cisco SSO* へのサインアップ



c) [アカウントの作成（Create Account）] ダイアログのフィールドに入力し、[登録（Register）] をクリックします。

図 *13* : アカウントの作成（*Create Account*）



ヒント　CDOへのログインに使用する予定の電子メールアドレスを入力し、会社を表す組織名を追加します。

d) [登録（Register）] をクリックすると、登録したアドレスに確認メールが送信されます。電子メールを開き、[アカウントの有効化（Activate Account）] をクリックします。

ステップ 2　Duo を使用して多要素認証をセットアップします。

a) [多要素認証の設定（Set up multi-factor authentication）] 画面で、[設定（Configure）] をクリックします。

b) [セットアップの開始（Start setup）] をクリックし、プロンプトに従ってデバイスを選択して、そのデバイスとアカウントのペアリングを確認します。

詳細については、『Duo Guide to Two Factor Authentication：Enrollment Guide』を参照してください。デバイスにDuoアプリケーションがすでにインストールされている場合は、このアカウントのアクティベーションコードが送信されます。Duo は 1 台のデバイスで複数のアカウントをサポートします。

c) ウィザードの最後で、[ログインを続行する（Continue to Login）] をクリックします。

d) 二要素認証を使用して Cisco Secure Sign-On にログインします。

ステップ 3　（任意）追加のオーセンティケータとして Google オーセンティケータを設定します。

a) Googleオーセンティケータとペアリングするモバイルデバイスを選択し、[次へ（Next）] をクリックします。

b) セットアップウィザードのプロンプトに従って、Google オーセンティケータをセットアップします。

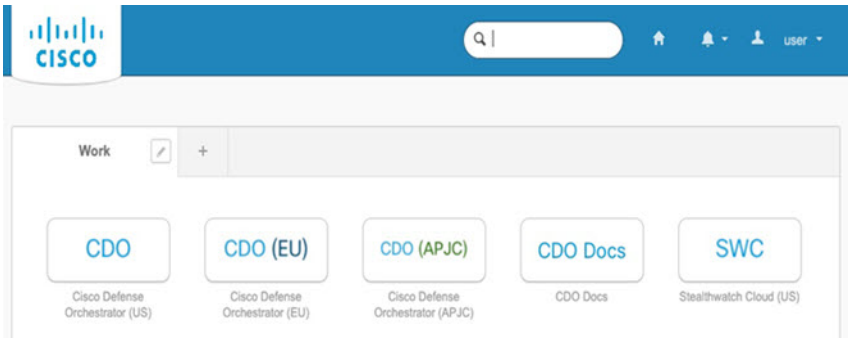
ステップ 4 **Cisco Secure Sign-On アカウントのアカウントリカバリのオプションを設定します。**

a) 「パスワードを忘れた場合（forgot password）」の質問と回答を選択します。
b) SMS を使用してアカウントをリセットするための予備の電話番号を選択します。
c) セキュリティイメージを選択します。
d) [マイアカウントの作成（Create My Account）] をクリックします。

これで、Cisco Security Sign-On ダッシュボードに CDO アプリケーションのタイルが表示されます。他のアプリケーションタイルも表示される場合があります。

ヒント ダッシュボード上でタイルをドラッグして並べ替えたり、タブを作成してタイルをグループ化したり、タブの名前を変更したりできます。

図 *14 : Cisco SSO* ダッシュボード



Cisco Secure Sign-On を使用した CDO へのログイン

CDO にログインし、デバイスのオンボードと管理を行います。

始める前に

Cisco Defense Orchestrator（CDO）は、Cisco Secure Sign-On をアイデンティティ プロバイダーとして使用し、多要素認証（MFA）に Duo Security を使用します。

- CDO にログインするには、まず Cisco Secure Sign-On でアカウントを作成し、Duo を使用して MFA を設定する必要があります。新しい Cisco Secure Sign-On アカウントの作成（102 ページ）を参照してください。
- Firefox または Chrome の最新バージョンを使用します。

手順

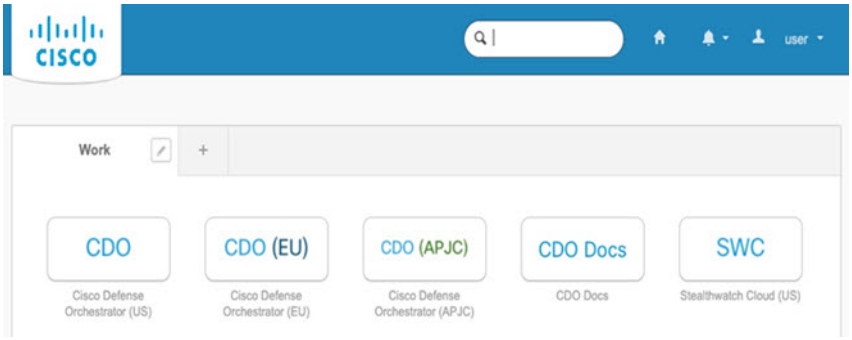
ステップ 1 Web ブラウザで、https://sign-on.security.cisco.com/を開きます。
ステップ 2 [ユーザー名（Username）] と [パスワード（Password）] に入力します。

ステップ 3 [ログイン（Log in）] をクリックします。

ステップ 4 Duo Security を使用して別の認証要素を受け取り、ログインを確認します。システムによってログインが確認され、Cisco Secure Sign-On ダッシュボードが表示されます。

ステップ 5 Cisco Secure Sign-on ダッシュボードで適切な CDO タイルをクリックします。**CDO** タイルをクリックすると https://defenseorchestrator.com に移動し、**CDO（EU）** タイルをクリックすると https://defenseorchestrator.eu に移動します。また、**CDO（APJC）** タイルをクリックすると https://www.apj.cdo.cisco.com に移動します。

図 *15 : Cisco SSO* ダッシュボード



ステップ 6 両方のオーセンティケータを設定している場合は、オーセンティケータのロゴをクリックして [Duo Security] か [Google Authenticator] を選択します。

- 既存のテナントにすでにユーザーレコードがある場合は、そのテナントにログインします。
- すでに複数のテナントにユーザーレコードがある場合は、接続先の CDO テナントを選択できます。
- 既存のテナントにユーザーレコードがない場合は、CDO の詳細を確認するか、またはトライアルアカウントを要求できます。

オンボーディングウィザードを使用したデバイスのオンボーディング

CLI 登録キーを使用し、CDO のオンボーディングウィザードを使用して Threat Defense をオンボードします。

手順

ステップ 1 CDO のナビゲーションウィンドウで [インベントリ（Inventory）] 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。

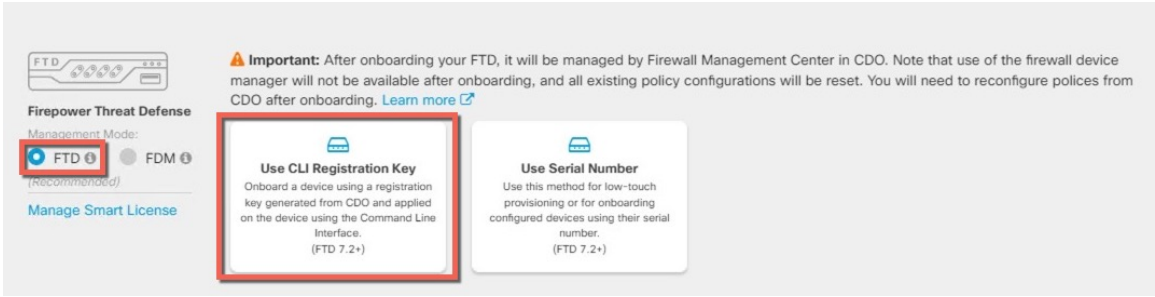
ステップ 2 [FTD] タイルを選択します。

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。

管理モードとして [FTD] を選択した後はいつでも、[スマートライセンスの管理（Manage Smart License）] をクリックして、デバイスで使用可能なスマートライセンスを登録したり、既存のスマートライセンスを変更したりできます。使用可能なライセンスについては、ライセンスを取得する （99 ページ）を参照してください。

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 *16 : 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。

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。

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）] オプションボタンをクリックして、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。

ステップ 8 [CLI登録キー（CLI Registration Key）] については、CDO 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。

configure manager add *cdo_hostname registration_key nat_id display_name*

Chassis Manager で論理デバイスを展開するときに（Chassis Manager：Threat Defense 論理デバイスの追加 （107 ページ） を参照）、*cdo_hostname*、*registration_key*、*nat_id* の部分を **[CDOオンボード（CDO Onboard）]** および **[CDOオンボードを確認（Confirm CDO Onboard）]** フィールドにコピーします。

例：

サンプルコマンド

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.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）[インベントリ（Inventory）] ページの並べ替えとフィルタ処理に役立つよう、デバイスにラベルを追加します。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、CDO への導入準備後にデバイスに適用されます。

次のタスク

[インベントリ] ページから、導入準備したばかりのデバイスを選択し、右側にある [管理] ペインに一覧表示されているオプションのいずれかを選択します。

Chassis Manager：Threat Defense 論理デバイスの追加

Threat Defense をスタンドアロンのネイティブインスタンスとして Firepower 9300 から展開できます。CDO は、コンテナインスタンスやクラスタをサポートしていません。

この手順では、アプリケーションで使用されるブートストラップ設定を含む、論理デバイスの特性を設定できます。

始める前に

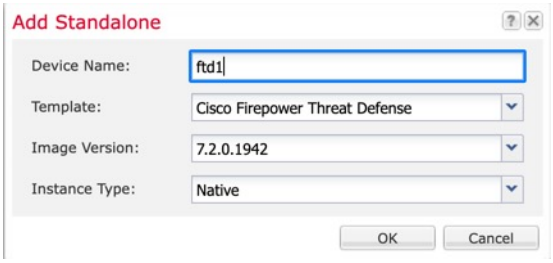
- Threat Defense と一緒に使用する管理インターフェイスを設定します。インターフェイスの設定 （24 ページ） を参照してください。管理インターフェイスが必要です。後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。この管理インターフェイスは、シャーシの管理のみに使用される（[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示される）シャーシ管理ポートと同じではありません。
- また、少なくとも 1 つのデータ インターフェイスを設定する必要があります。
- 次の情報を用意します。
  - このデバイスのインターフェイス Id
  - 管理インターフェイス IP アドレスとネットワークマスク
  - ゲートウェイ IP アドレス
  - CDO によって生成された CDO ホスト名、登録キー、および NAT ID。オンボーディング ウィザードを使用したデバイスのオンボーディング （105 ページ）を参照してください。
  - DNS サーバの IP アドレス

手順

ステップ 1 Chassis Manager で、[論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[追加（Add）]** > **[スタンドアロン（Standalone）]** をクリックし、次のパラメータを設定します。

図 *17*：スタンドアロンデバイスの追加



a) **デバイス名**を入力します。

この名前は、シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

b) [Template] では、[Cisco Firepower Threat Defense] を選択します。

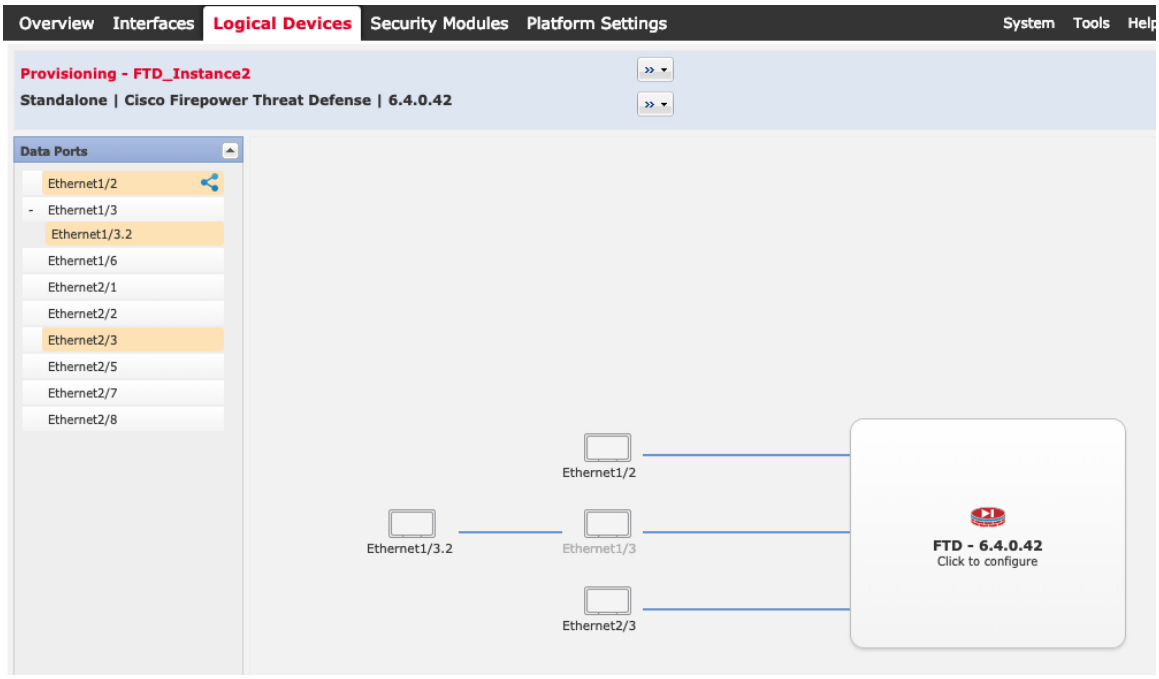
c) [Image Version] を選択します。

d) [Instance Type] で [Native] を選択します。

e) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。



以前に [Interfaces] ページで有効にしたデータ インターフェイスのみを割り当てることができます。後ほど CDO でこれらのインターフェイスを有効にして設定します。IP アドレスの設定も行います。

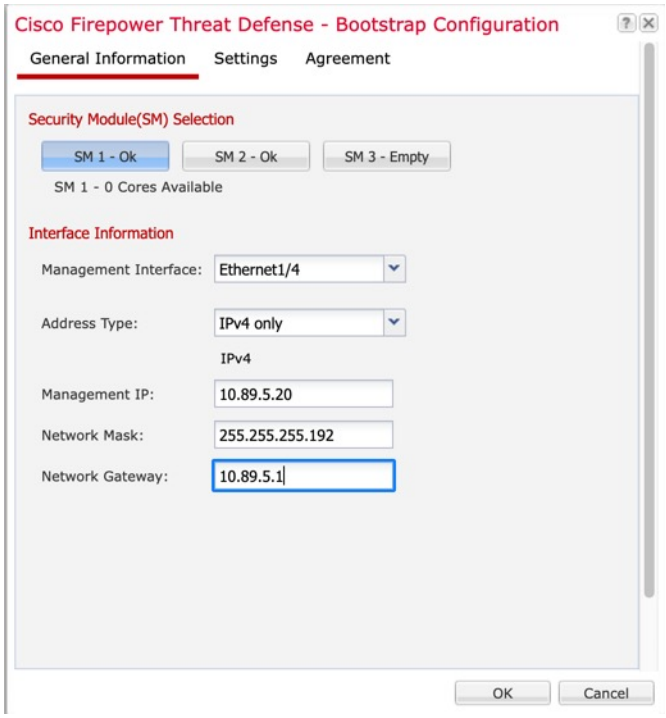
ハードウェア バイパス 対応のポートは次のアイコンで表示されます：。特定のインターフェイスモジュールでは、インライン セット インターフェイスに対してのみハードウェアバイパス機能を有効にできます。ハードウェア バイパスは、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。ハードウェア バイパス ペアの両方のインターフェイスとも割り当てられていない場合、割り当てが意図的であることを確認する警告メッセージが表示されます。ハードウェア バイパス 機能を使用する必要はないため、単一のインターフェイスを割り当てることができます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [一般情報（General Information）] ページで、次の手順を実行します。

図 *18 :* 全般情報



a) [セキュリティモジュールの選択（Security Module Selection）] の下で、この論理デバイスに使用するセキュリティ モジュールをクリックします。

b) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

c) 管理インターフェイスを選択します。[アドレスタイプ（Address Type）]：[IPv4のみ（IPv4 only）]、[IPv6のみ（IPv6 only）]、または [IPv4およびIPv6（IPv4 and IPv6）]。

d) [Management IP] アドレスを設定します。

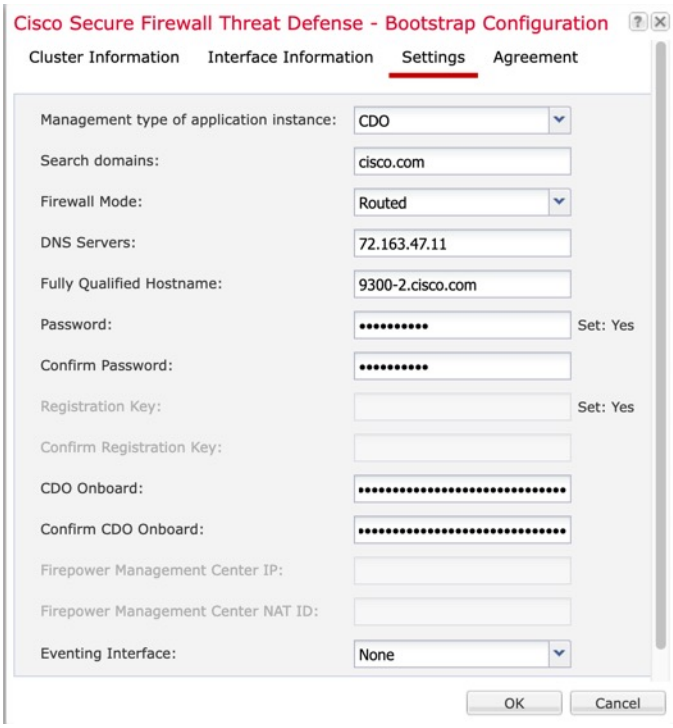
このインターフェイスに一意の IP アドレスを設定します。

e) [Network Mask] または [Prefix Length] に入力します。

f) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [設定（Settings）] タブで、次の項目を入力します。

図 *19 :* 設定



a) [アプリケーションインスタンスの管理タイプ（Management type of application instance）] ドロップダウンリストで、**[CDO]** を選択します。
b) カンマ区切りリストとして [検索ドメイン（Search Domains）] を入力します。
c) [Firewall Mode] を [Transparen] または [Routed] に選択します。

   ルーテッドモードでは、Threat Defenseはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

   ファイアウォールモードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

d) [DNS Servers] をカンマ区切りのリストとして入力します。

   たとえば、Management Centerのホスト名を指定する場合、Threat Defense は DNS を使用します。

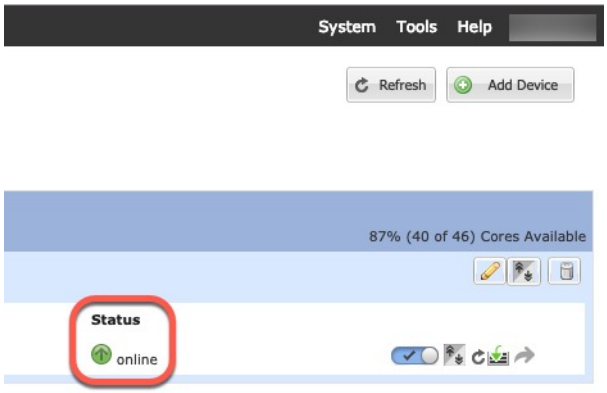
e) Threat Defense の [Fully Qualified Hostname] を入力します。
f) CLI アクセス用の Threat Defense 管理ユーザの [Password] を入力します。
g) CDO によって生成されたコマンドを [CDOオンボード（CDO Onboard）] および [CDOオンボードを確認（Confirm CDO Onboard）] フィールドにコピーします。
h) CDO では別の [イベントインターフェイス（Eventing Interface）] がサポートされていないため、この設定は無視されます。

ステップ 7 [利用規約（Agreement）] タブで、エンドユーザ ライセンス（EULA）を読んで、同意します。

ステップ 8 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 9 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



基本的なセキュリティポリシーの設定

ここでは、次の設定を使用して基本的なセキュリティポリシーを設定する方法について説明します。

- 内部インターフェイスと外部インターフェイス：内部インターフェイスにスタティック IP アドレスを割り当て、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。

基本的なセキュリティ ポリシーを設定するには、次のタスクを実行します。

1	インターフェイスの設定 （49 ページ）。
2	DHCP サーバーの設定 （53 ページ）。

3	デフォルトルートの追加 （54 ページ）。
4	NAT の設定 （55 ページ）。
5	内部から外部へのトラフィックの許可 （58 ページ）。
6	設定の展開 （59 ページ）。

インターフェイスの設定

脅威に対する防御 インターフェイスを有効にし、それらをセキュリティゾーンに割り当てて IP アドレスを設定します。通常は、システムで意味のあるトラフィックを通過させるように、少なくとも 2 つのインターフェイスを設定する必要があります。通常は、アップストリームルータまたはインターネットに面した外部インターフェイスと、組織のネットワークの 1 つ以上の内部インターフェイスを使用します。これらのインターフェイスの一部は、Web サーバーなどのパブリックアクセスが可能なアセットを配置する「緩衝地帯」（DMZ）となる場合があります。

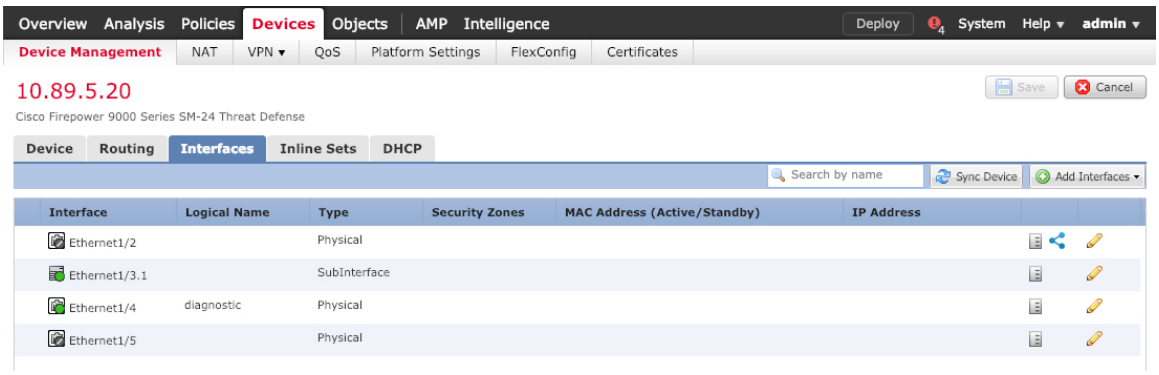
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

次の例では、DHCP によるスタティックアドレスとルーテッドモードの外部インターフェイスを使用して、ルーテッドモードの内部インターフェイスを設定します。

手順

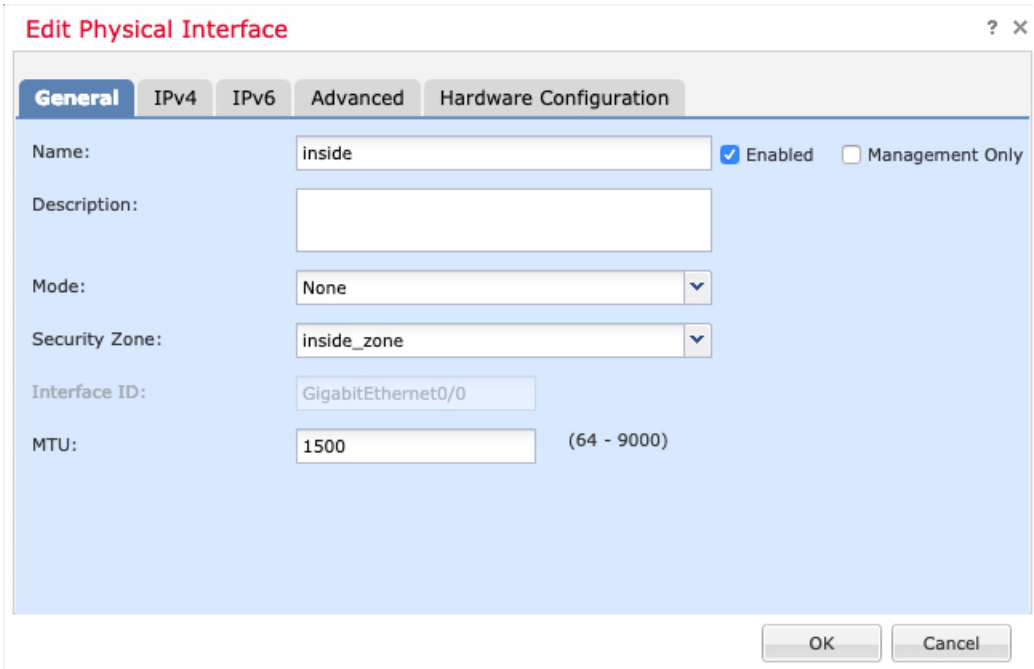
ステップ 1 [デバイス（Devices）]>[デバイス管理（Device Management）] の順に選択し、ファイアウォールの をクリックします。

ステップ 2 [インターフェイス（Interfaces）] をクリックします。



ステップ 3 内部に使用するインターフェイスの をクリックします。

[全般（General）] タブが表示されます。



a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに **inside** という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

c) [モード（Mode）] は [なし（None）] に設定したままにします。

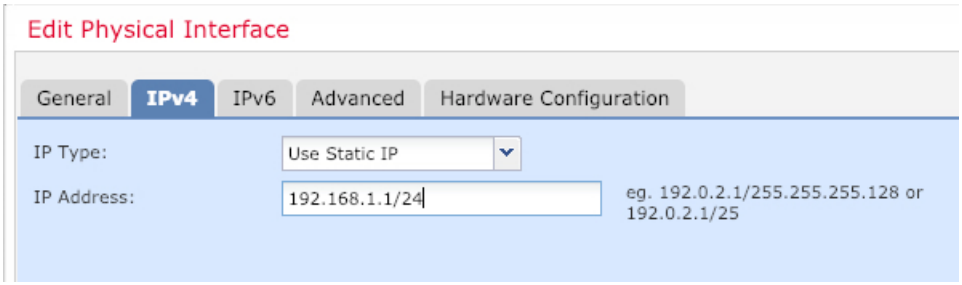
d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の内部セキュリティゾーンを選択するか、[新規（New）] をクリックして新しいセキュリティゾーンを追加します。

たとえば、**inside_zone** という名前のゾーンを追加します。各インターフェイスは、セキュリティゾーンおよびインターフェイスグループに割り当てる必要があります。インターフェイスは、1 つのセキュリティゾーンにのみ属することも、複数のインターフェイスグループに属することもできます。ゾーンまたはグループに基づいてセキュリティポリシーを適用します。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。この場合、トラフィックが内部から外部に移動できるようにアクセス コントロール ポリシーを設定することはできますが、外部から内部に向けては設定できません。ほとんどのポリシーはセキュリティゾーンのみサポートしています。NAT ポリシー、プレフィルタ ポリシー、および QoS ポリシーで、ゾーンまたはインターフェイスグループを使用できます。

e) [IPv4] タブ、[IPv6] タブ、または両方のタブをクリックします。

- [IPv4]：ドロップダウンリストから [スタティックIPを使用する（Use Static IP）] を選択し、IP アドレスとサブネットマスクをスラッシュ表記で入力します。

  たとえば、**192.168.1.1/24** などと入力します。

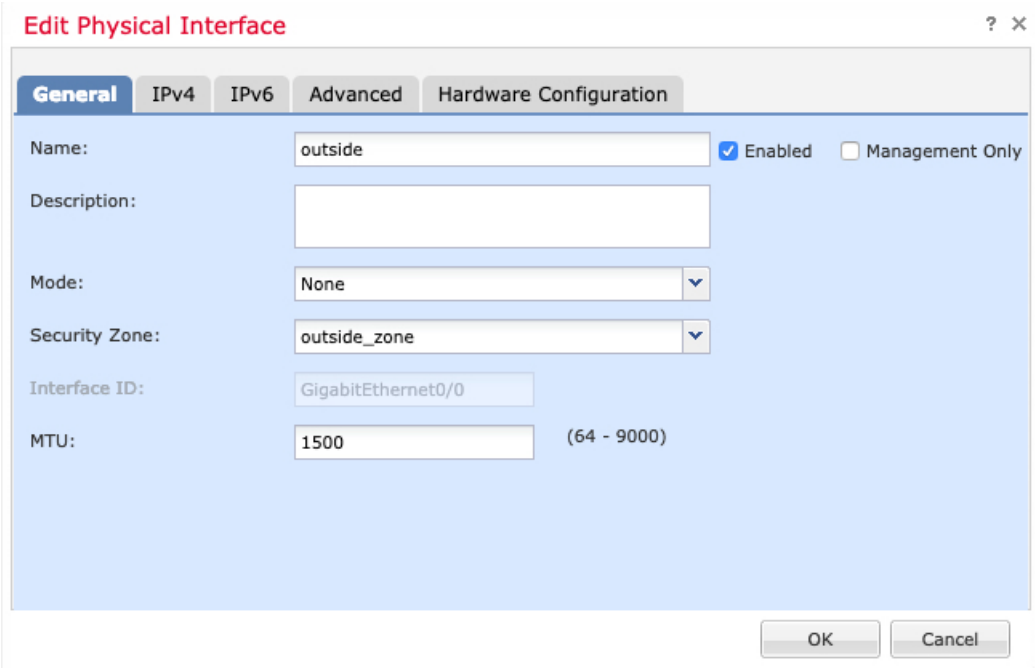


- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 4 「外部」に使用するインターフェイスをクリックします。

[全般（General）] タブが表示されます。



（注） 管理アクセス用にこのインターフェイスを事前に設定している場合、インターフェイスにはすでに名前が付けられており、有効化とアドレス指定が完了しています。これらの基本設定は変更しないでください。変更すると、Management Center の管理接続が中断されます。この画面でも、通過トラフィックポリシーのセキュリティゾーンを設定できます。

a) 48 文字までの [名前（Name）] を入力します。

たとえば、インターフェイスに「outside」という名前を付けます。

b) [有効（Enabled）] チェックボックスをオンにします。

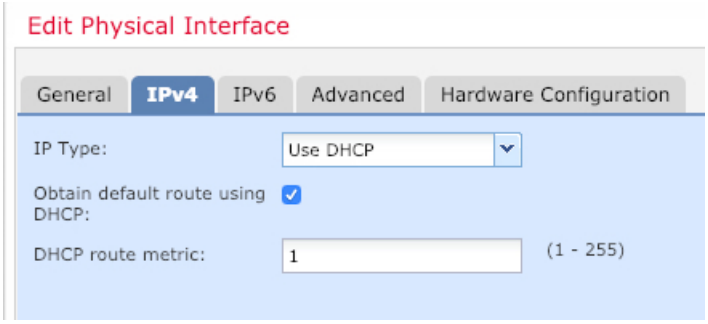
c) [モード（Mode）] は [なし（None）] に設定したままにします。

d) [セキュリティゾーン（Security Zone）] ドロップダウンリストから既存の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。

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。



- [IPv6]：ステートレス自動設定の場合は [自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

DHCP サーバーの設定

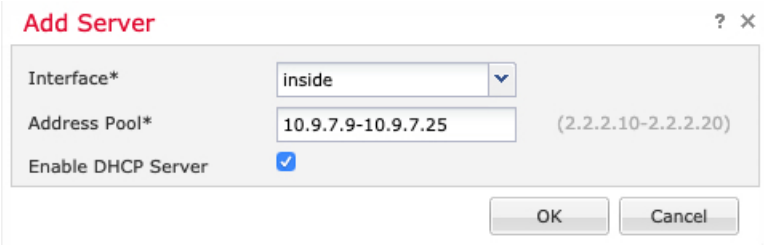
クライアントで DHCP を使用して 脅威に対する防御 から IP アドレスを取得するようにする場合は、DHCP サーバーを有効にします。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

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

ステップ 3 **[サーバー（Server）]** ページで、**[追加（Add）]** をクリックして、次のオプションを設定します。



- [インターフェイス（Interface）]：ドロップダウンリストからインターフェイスを選択します。
- [アドレスプール（Address Pool）]：DHCP サーバーが使用する IP アドレスの最下位から最上位の間の範囲を設定します。IP アドレスの範囲は、選択したインターフェイスと同じサブネット上に存在する必要があり、インターフェイス自身の IP アドレスを含めることはできません。
- [DHCPサーバーを有効にする（Enable DHCP Server）]：選択したインターフェイスの DHCP サーバーを有効にします。

ステップ 4 [OK] をクリックします。

ステップ 5 [保存（Save）] をクリックします。

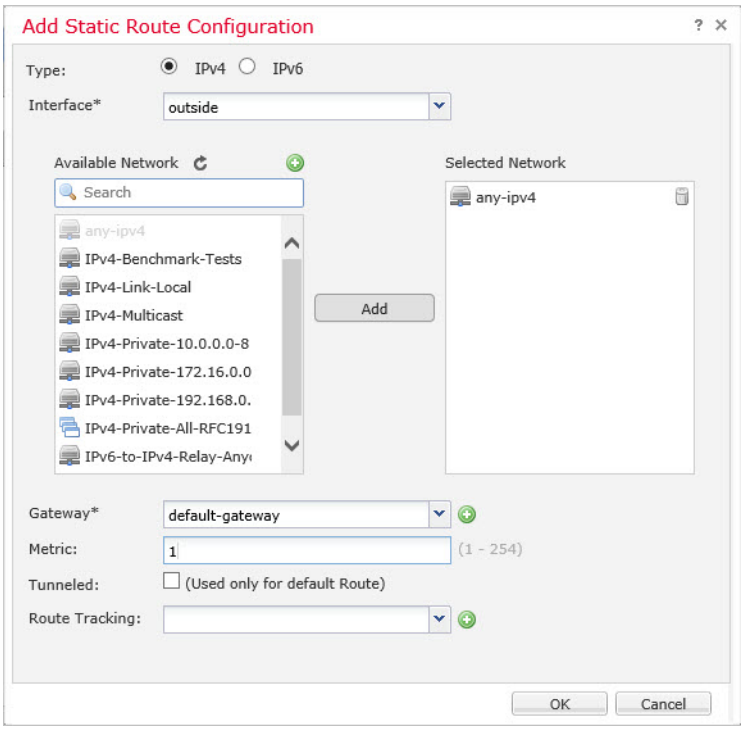
デフォルトルートの追加

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。外部インターフェイスに DHCP を使用する場合は、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。DHCP サーバーからデフォルトルートを受信した場合は、**[デバイス（Devices）]** > **[デバイス管理（Device Management）]** > **[ルーティング（Routing）]** > **[スタティックルート（Static Route）]** ページの [IPv4ルート（IPv4 Routes）] または [IPv6ルート（IPv6 Routes）] テーブルに表示されます。

手順

ステップ 1 **[デバイス（Devices）]** > **[デバイス管理（Device Management）]** を選択し、デバイスをクリックします。

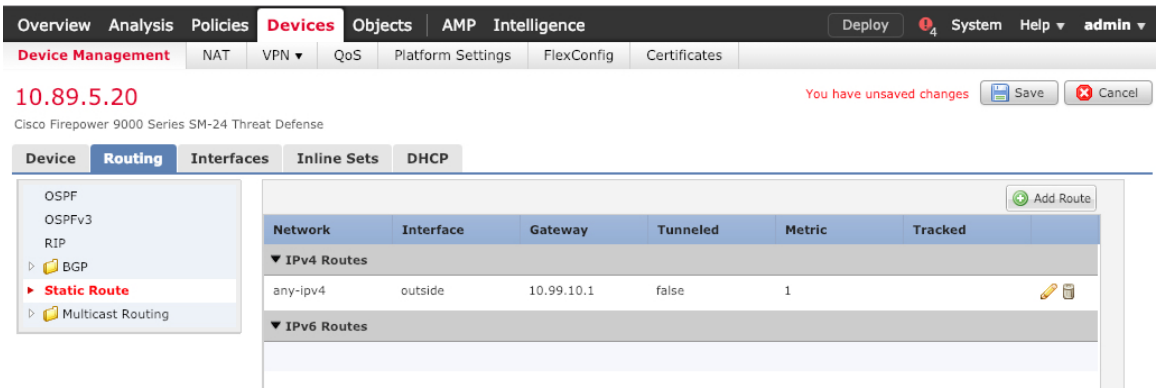
ステップ 2 **[ルーティング（Routing）]** > **[スタティックルート（Static route）]** を選択し、[ルートを追加（Add route）] をクリックして、次のように設定します。



- [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 [ipv4] を選択し、IPv6 デフォルト ルートの場合は [any] 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。
- [メトリック（Metric）]：宛先ネットワークへのホップの数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。

ステップ 3 [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 4 [保存（Save）] をクリックします。

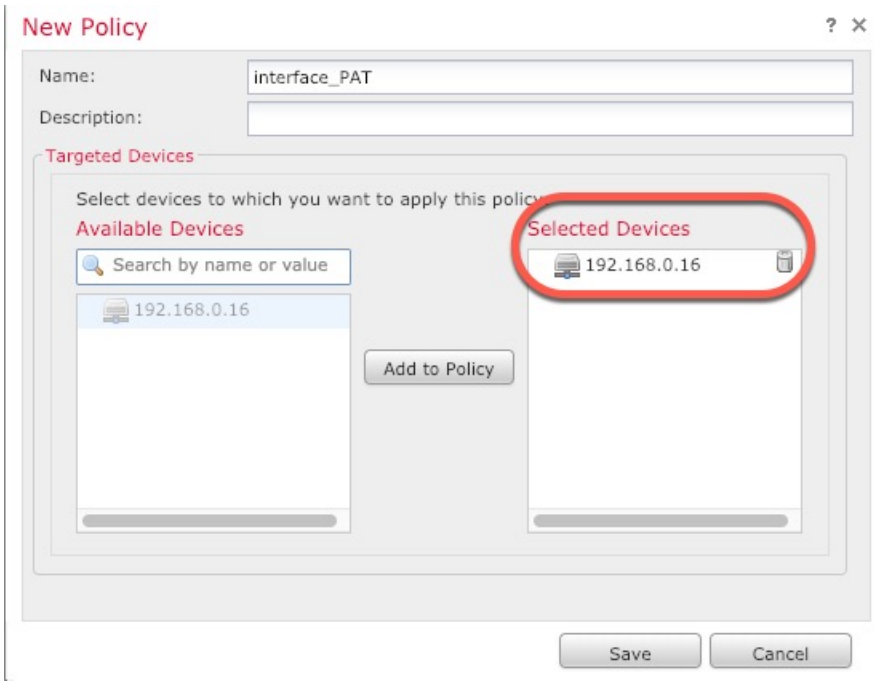
NAT の設定

一般的な NAT ルールでは、内部アドレスを外部インターフェイスの IP アドレスのポートに変換します。このタイプの NAT ルールのことをインターフェイス ポート アドレス変換（PAT）と呼びます。

手順

ステップ 1 **[デバイス（Devices）] > [NAT]** をクリックし、**[新しいポリシー（New Policy）] > [Threat Defense NAT]** をクリックします。

ステップ 2 ポリシーに名前を付け、ポリシーを使用するデバイスを選択し、[保存（Save）] をクリックします。



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

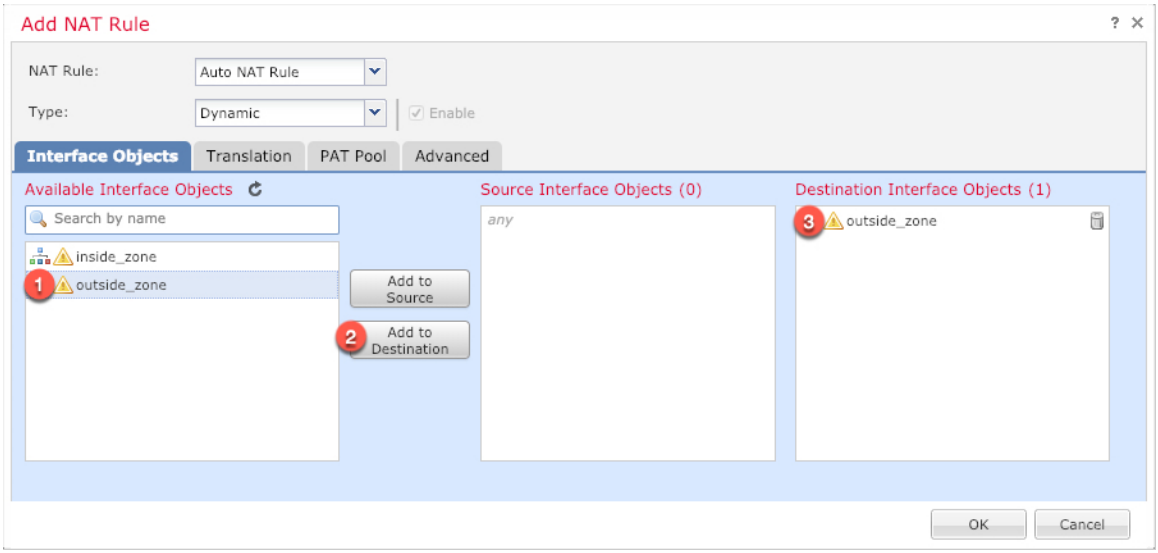
ステップ 3 [ルールの追加（Add Rule）] をクリックします。

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

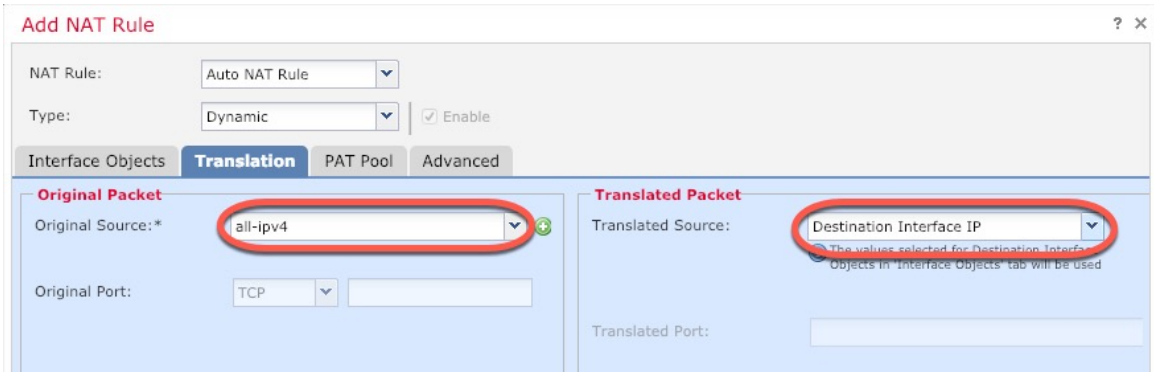
ステップ 4 基本ルールのオプションを設定します。

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

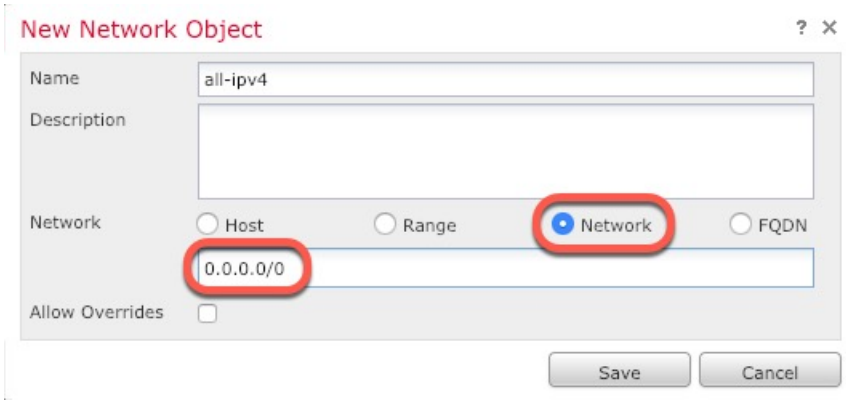
ステップ 5 [インターフェイスオブジェクト（Interface objects）] ページで、[使用可能なインターフェイスオブジェクト（Available Interface Objects）] 領域から [宛先インターフェイスオブジェクト（Destination Interface Objects）] 領域に外部ゾーンを追加します。



ステップ 6 [変換（Translation）] ページで、次のオプションを設定します。



- [元の送信元（Original Source）]：をクリックして、すべての IPv4 トラフィック（0.0.0.0/0）のネットワークオブジェクトを追加します。

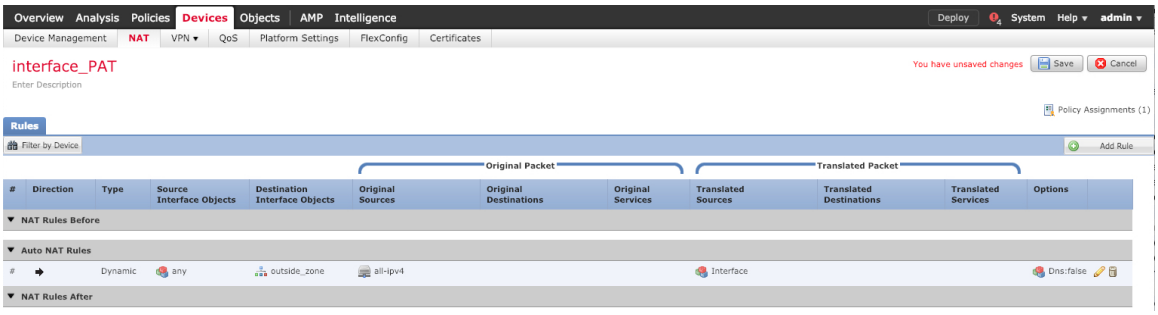


（注） 自動 NAT ルールはオブジェクト定義の一部として NAT を追加するため、システム定義の **any-ipv4** オブジェクトを使用することはできません。また、システム定義のオブジェクトを編集することはできません。

- [変換済みの送信元（Translated Source）]：[宛先インターフェイスIP（Destination Interface IP）] を選択します。

ステップ 7 [保存（Save）] をクリックしてルールを追加します。

ルールが [ルール（Rules）] テーブルに保存されます。



ステップ 8 NAT ページで [保存（Save）] をクリックして変更を保存します。

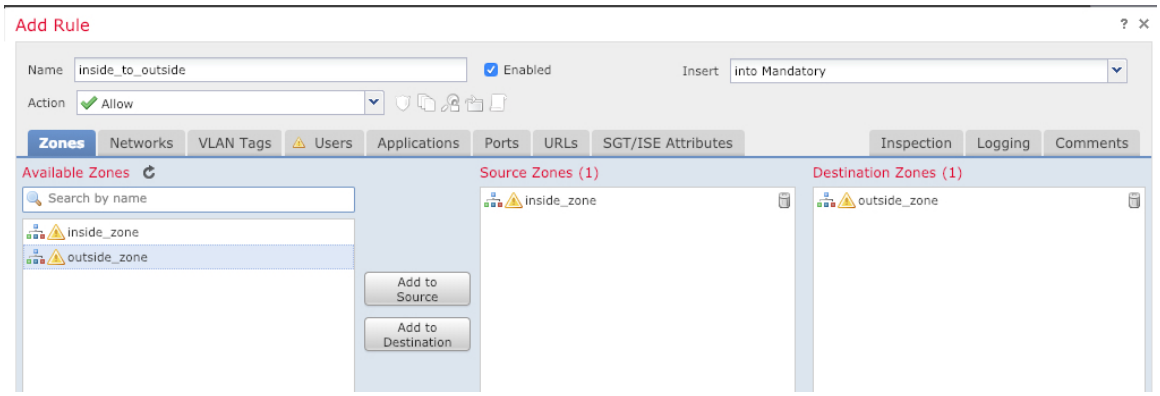
内部から外部へのトラフィックの許可

脅威に対する防御 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、デバイスを通過するトラフィックを許可するためにポリシーにルールを追加する必要があります。次の手順では、内部ゾーンから外部ゾーンへのトラフィックを許可するルールを追加します。他にゾーンがある場合は、適切なネットワークへのトラフィックを許可するルールを追加してください。

手順

ステップ 1 **[ポリシー（Policy）] > [アクセスポリシー（Access Policy）] > [アクセスポリシー（Access Policy）]**を選択し、脅威に対する防御 に割り当てられているアクセス コントロール ポリシーの をクリックします。

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

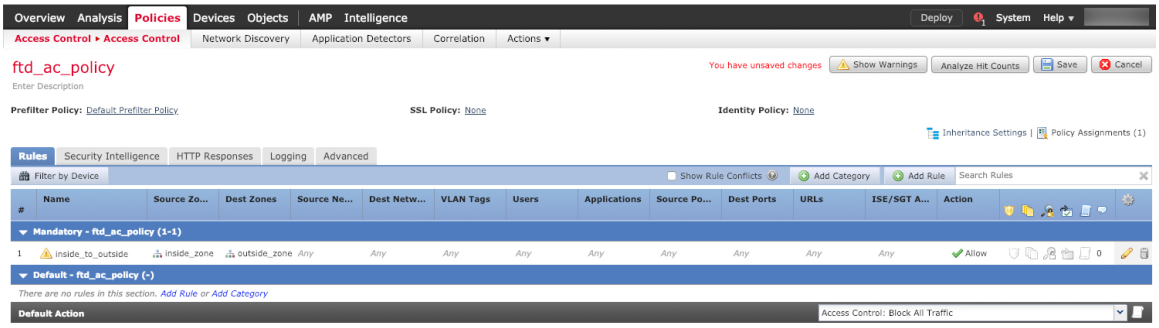


- [名前（Name）]：このルールに名前を付けます（たとえば、**inside_to_outside**）。
- [送信元ゾーン（Source Zones）]：[使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。
- [宛先ゾーン（Destination Zones）]：[使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

他の設定はそのままにしておきます。

ステップ 3 [追加（Add）] をクリックします。

ルールが [ルール（Rules）] テーブルに追加されます。



ステップ 4 [保存（Save）] をクリックします。

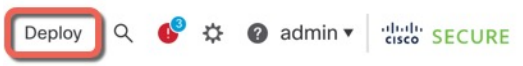
設定の展開

設定の変更を 脅威に対する防御 に展開します。変更を展開するまでは、デバイス上でどの変更もアクティブになりません。

手順

ステップ 1 右上の [展開（Deploy）] をクリックします。

図 *20 : [展開（Deploy）]*



ステップ 2 [すべて展開（Deploy All）] をクリックしてすべてのデバイスに展開するか、[高度な展開（Advanced Deploy）] をクリックして選択したデバイスに展開します。

図 *21* : すべて展開

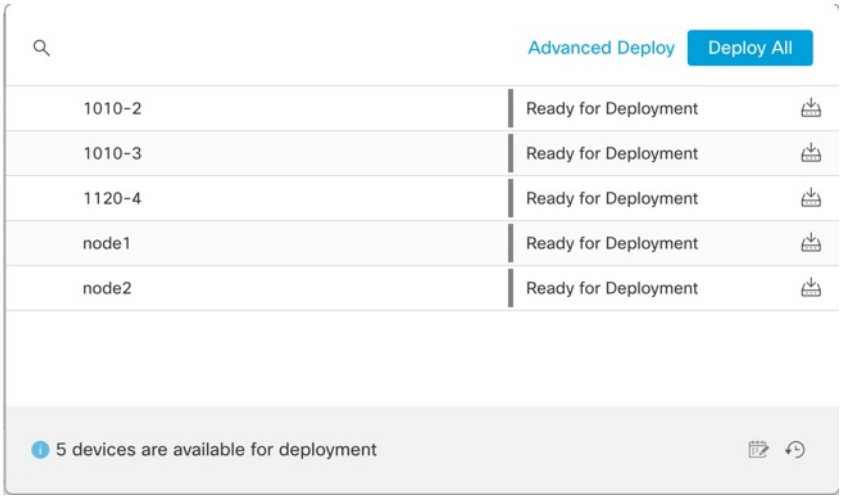
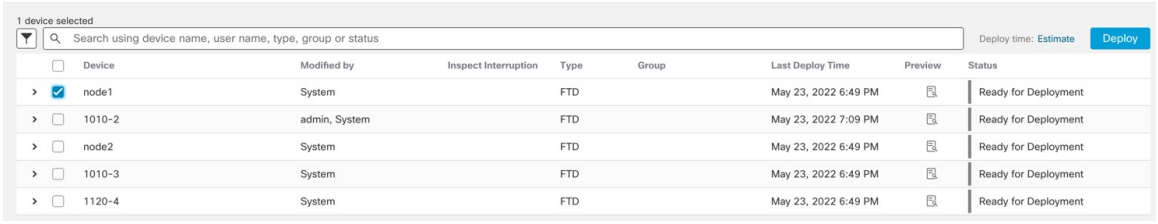
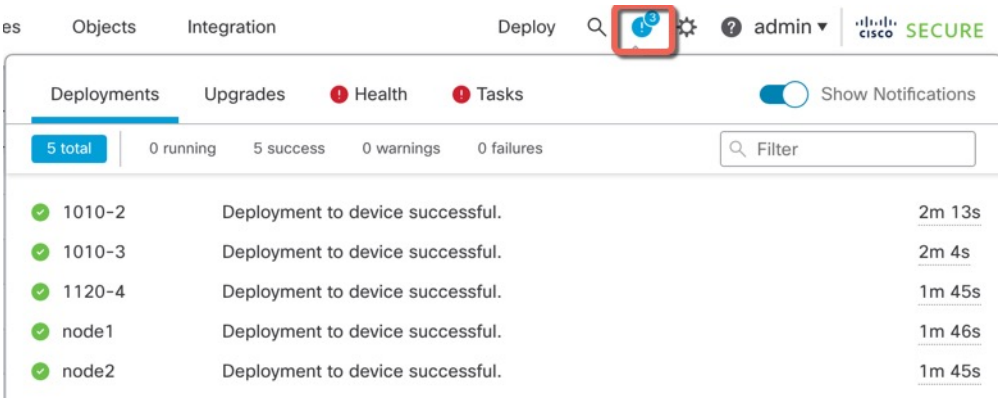


図 *22* : 高度な展開



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 *23* : 展開ステータス



Threat Defense および FXOS CLI へのアクセス

脅威に対する防御 CLI を使用して、管理インターフェイスパラメータを変更したり、トラブルシューティングを行ったりできます。CLI にアクセスするには、管理インターフェイスへの SSH を使用するか、FXOS CLI から接続します。

手順

ステップ 1 （オプション 1）脅威に対する防御 管理インターフェイスの IP アドレスに直接 SSH 接続します。

管理 IP アドレスは、論理デバイスを展開したときに設定したものです。初期展開時に設定した「admin」アカウントとパスワードを使用して 脅威に対する防御 にログインします。

パスワードを忘れた場合は、シャーシマネージャ で論理デバイスを編集して変更できます。

ステップ 2 （オプション 2）コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

a) セキュリティ モジュール に接続します。

connect module *slot_number* {**console** | **telnet**}

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) 脅威に対する防御 コンソールに接続します。

connect ftd *name*

複数のアプリケーションインスタンスがある場合は、インスタンスの名前を指定する必要があります。インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect ftd FTD_Instance1

============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
```

```
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.
==========================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to
bootCLI
>
```

c) **exit** と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

（注） 6.3 より前のバージョンの場合は、**Ctrl-a, d** と入力します。

d) FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了するには、以下を実行します。

1. **~** と入力

   Telnet アプリケーションに切り替わります。

2. Telnet アプリケーションを終了するには、次を入力します。

   telnet>**quit**

Telnet セッションを終了するには、以下を実行します。

Ctrl-], . と入力

例

次に、セキュリティモジュール 1 の 脅威に対する防御 に接続してから、FXOS CLI のスーパバイザレベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect ftd FTD_Instance1

============================ ATTENTION ==============================
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
```

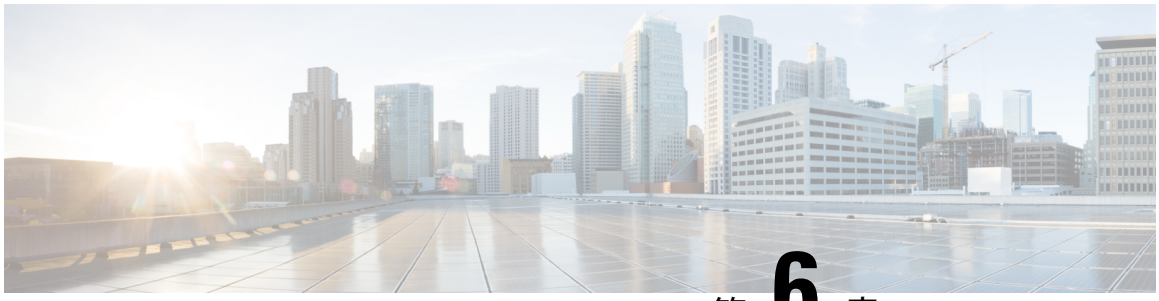
```
'connect module <slot> telnet' to connect to the security module.
==========================================================================

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

次のステップ

CDO を使用した Threat Defense の設定を続行するには、Cisco Defense Orchestrator ホームページを参照してください。

次のステップ



第 6 章

ASDM を使用した ASA の展開

この章の対象読者

この章では、スマート ライセンシングの設定方法など、スタンドアロンの ASA 論理デバイスを展開する方法について説明します。この章では以下の展開については取り上げていませんので、『ASA コンフィギュレーション ガイド』を参照してください。

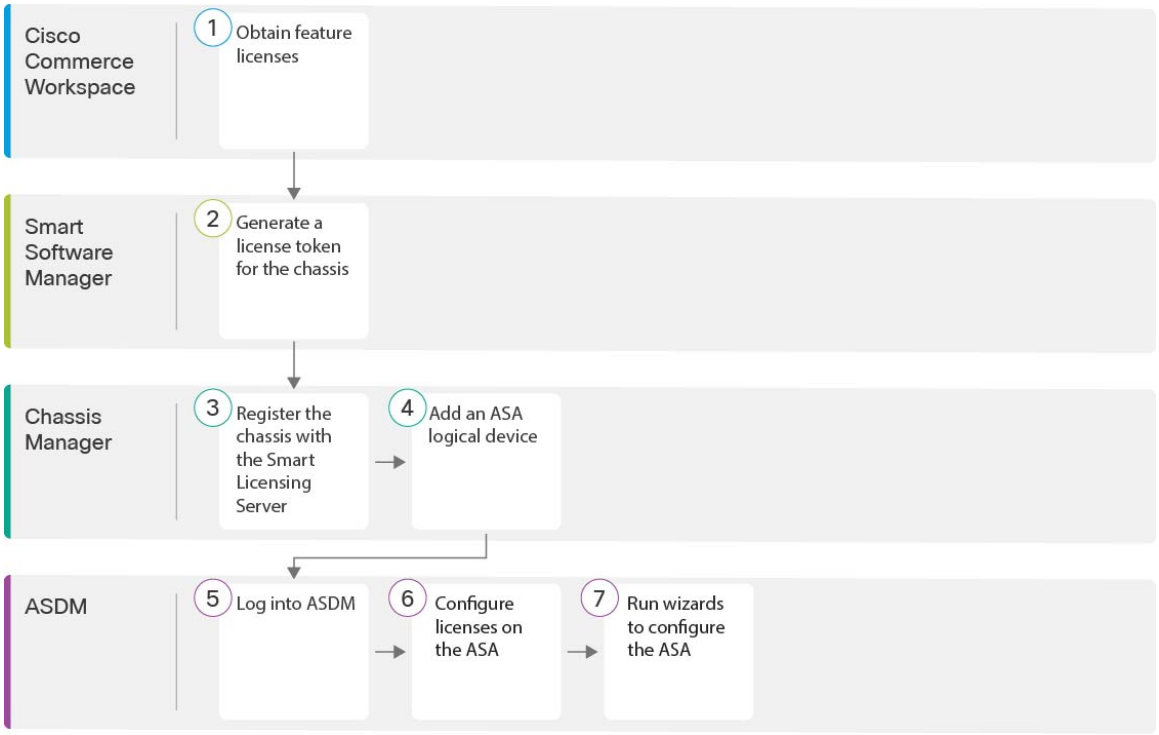
- クラスタリング
- フェールオーバー
- CLI 設定

この章では、基本的なセキュリティポリシーの設定手順についても説明します。より高度な要件がある場合は設定ガイドを参照してください。

プライバシー収集ステートメント：Firepower 9300 には個人識別情報は不要で、積極的に収集することもありません。ただし、ユーザー名などの設定では、個人識別情報を使用できます。この場合、設定作業時や SNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

エンドツーエンドの手順

シャーシで ASA を展開して設定するには、次のタスクを参照してください。



1	Cisco Commerce Workspace	Chassis Manager：ライセンス サーバーへのシャーシの登録 （131 ページ） ：機能ライセンスを取得します。
2	Smart Software Manager	Chassis Manager：ライセンス サーバーへのシャーシの登録 （131 ページ） ：シャーシのライセンス トークンを生成します。
3	Chassis Manager	Chassis Manager：ライセンス サーバーへのシャーシの登録 （131 ページ） ：スマート ライセンシング サーバーにシャーシを登録します。
4	Chassis Manager	Chassis Manager：ASA 論理デバイスの追加 （135 ページ）。
5	ASDM	ASDM へのログイン （139 ページ）。
6	ASDM	ASA でのライセンス権限付与の設定 （140 ページ）。
7	ASDM	ASA の設定 （141 ページ）。

Chassis Manager：ライセンス サーバーへのシャーシの登録

ASA はスマート ライセンスを使用します。通常のスマートライセンシング（インターネットアクセスが必要）を使用できます。または、オフライン管理の場合、永続ライセンス予約または Smart Software Manager On-Prem（以前のサテライトサーバ）を設定できます。これらのオフラインライセンス方式の詳細については、「Cisco ASA シリーズの機能ライセンス」を参照してください。このガイドは通常のスマートライセンシングに適用されます。

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

Firepower 9300 上の ASA では、スマート ソフトウェア ライセンシングの設定は、シャーシ上の FXOS と ASA に分割されています。

- Firepower 9300：ライセンス認証局との通信を行うためのパラメータを含めて、FXOS にすべてのスマート ソフトウェア ライセンス インフラストラクチャを設定します。Firepower 9300 自体には動作のためのライセンスは必要ありません。
- ASA：ASA のすべてのライセンスの権限付与を設定します。

シャーシを登録すると、Smart Software Manager はファイアウォールと Smart Software Manager 間の通信用の ID 証明書を発行します。また、該当するバーチャルアカウントにファイアウォールが割り当てられます。Smart Software Manager に登録するまでは、設定変更を行うことはできず、特殊なライセンスを必要とする機能へ、操作はその他の点では影響を受けません。ライセンス付与される機能は次のとおりです。

- Essentials
- セキュリティ コンテキスト
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）
- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。
- Cisco Secure Client：Secure Client Advantage、Secure Client Premier、または Secure Client VPN のみ

Smart Software Manager から ASA の登録トークンを要求する場合、[このトークンを使用して登録した製品でエクスポート制御機能を許可（Allow export-controlled functionality on the products registered with this token）] チェックボックスをオンにして、強力な暗号化の完全ライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。強力な暗号化ライセンスは、シャーシで登録トークンを適用すると、対象となるお客様の場合自動的に有効化されるため追加の操作は不要です。スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

ASDM アクセスには強力な暗号化が必要です。

始める前に

- Smart Software Manager にマスターアカウントを持ちます。

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

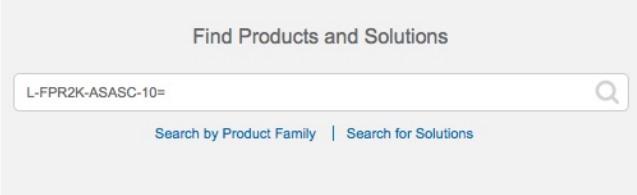
- （輸出コンプライアンスフラグを使用して有効化される）機能を使用するには、ご使用の Smart Software Manager アカウントで強力な暗号化（3DES/AES）ライセンスを使用できる必要があります。
- まだ実行していない場合は、NTP の設定 （20 ページ） を実行します。
- 初期設定時に DNS を設定しなかった場合は、**[プラットフォーム設定（Platform Settings）]** > **[DNS]** ページで DNS サーバーを追加します。

手順

ステップ 1 ご使用のスマート ライセンス アカウントに、必要なライセンスが含まれている（少なくとも Essentials ライセンスが含まれている）ことを確認してください。

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、Smart Software Manager アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス PID を検索します。

図 *24 :* ライセンス検索

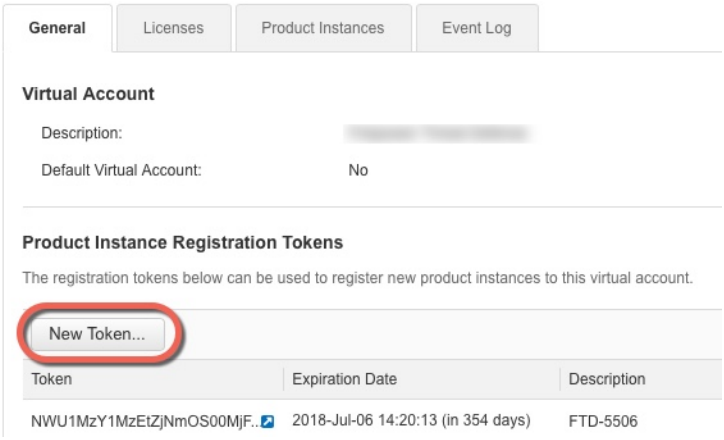


- Essentials ライセンス：L-F9K-ASA=。Essentials ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。
- 10 コンテキスト ライセンス：L-F9K-ASA-SC-10=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：L-F9K-ASA-CAR=
- 高度暗号化（3DES/AES）ライセンス：L-F9K-ASA-ENCR-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。
- Cisco Secure Client：『Cisco Secure Client 発注ガイド』を参照してください。ASA では、このライセンスを直接有効にしないでください。

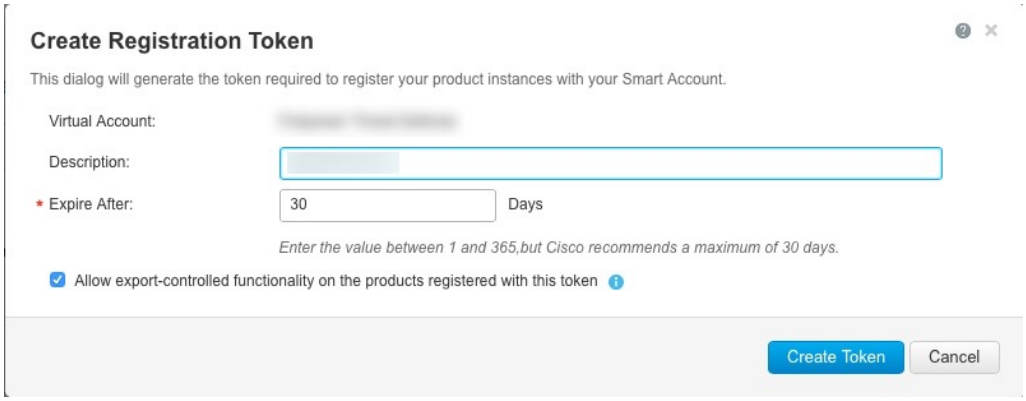
ステップ 2 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

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



c) [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（Description）]**
- [有効期限（Expire After）]：推奨値は 30 日です。
- [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）]：輸出コンプライアンス フラグを有効にします。

トークンはインベントリに追加されます。

d) 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。ASA 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 *25* : トークンの表示

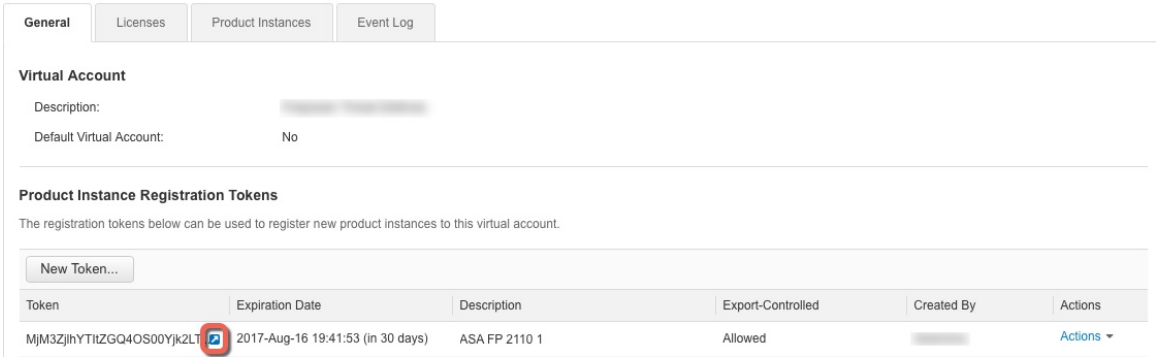
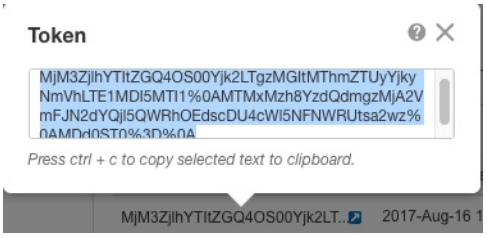
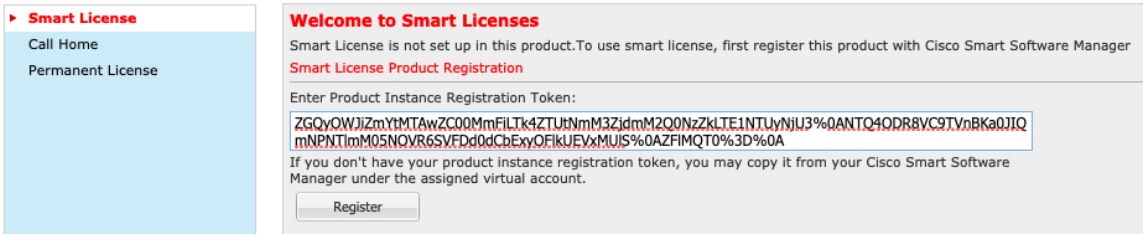


図 *26* : トークンのコピー



ステップ 3 Chassis Manager で、**[システム（System）]** > **[ライセンス（Licensing）]** > **[スマートライセンス（Smart License）]** の順に選択します。

ステップ 4 [Enter Product Instance Registration Token] フィールドに登録トークンを入力します。



ステップ 5 [Register] をクリックします。

Firepower 9300 がライセンス認証局に登録します。登録成功には数分かかることがあります。ページを更新してステータスを確認します。

図 *27*：登録が進行中

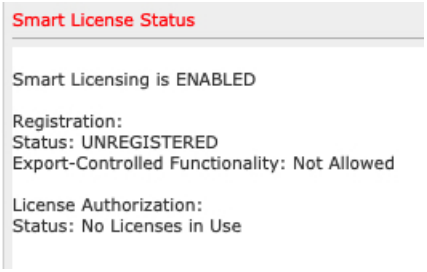
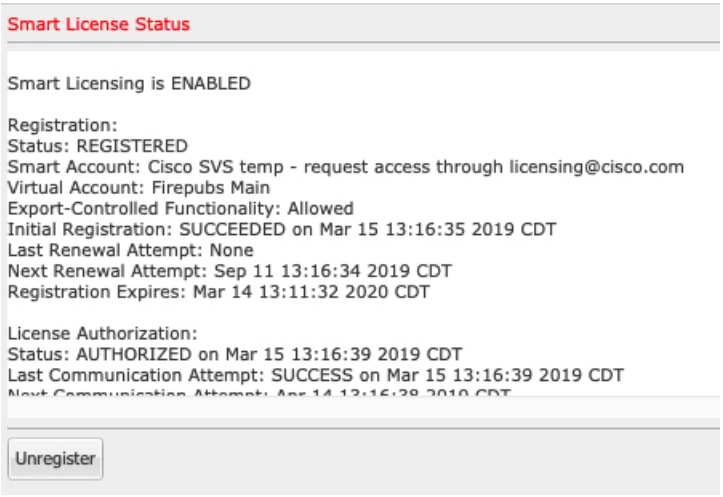


図 *28*：登録に成功しました



Chassis Manager：ASA 論理デバイスの追加

ASA をネイティブ インスタンスとして Firepower 9300 から展開できます。

フェールオーバー ペアまたはクラスタを追加するには、ASA の一般的な操作のコンフィギュレーション ガイドを参照してください。

この手順では、アプリケーションで使用されるブートストラップ設定を含む、論理デバイスの特性を設定できます。

始める前に

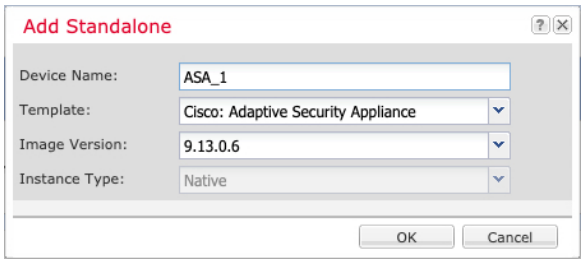
- ASA と一緒に使用する管理インターフェイスを設定します。インターフェイスの設定（24 ページ）を参照してください。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用される（[インターフェイス（Interfaces）] タブの上部に [MGMT] として表示される）シャーシ管理ポートと同じではありません。
- 次の情報を用意します。

- このデバイスのインターフェイス Id
- 管理インターフェイス IP アドレスとネットワークマスク
- ゲートウェイ IP アドレス
- 新規管理者パスワード/イネーブル パスワード

手順

ステップ 1 Chassis Manager で、[論理デバイス（Logical Devices）] を選択します。

ステップ 2 **[追加（Add）]** > **[スタンドアロン（Standalone）]** をクリックし、次のパラメータを設定します。



a) **デバイス名**を入力します。

この名前は、シャーシスーパーバイザが管理設定を行ってインターフェイスを割り当てるために使用します。これはアプリケーション設定で使用されるデバイス名ではありません。

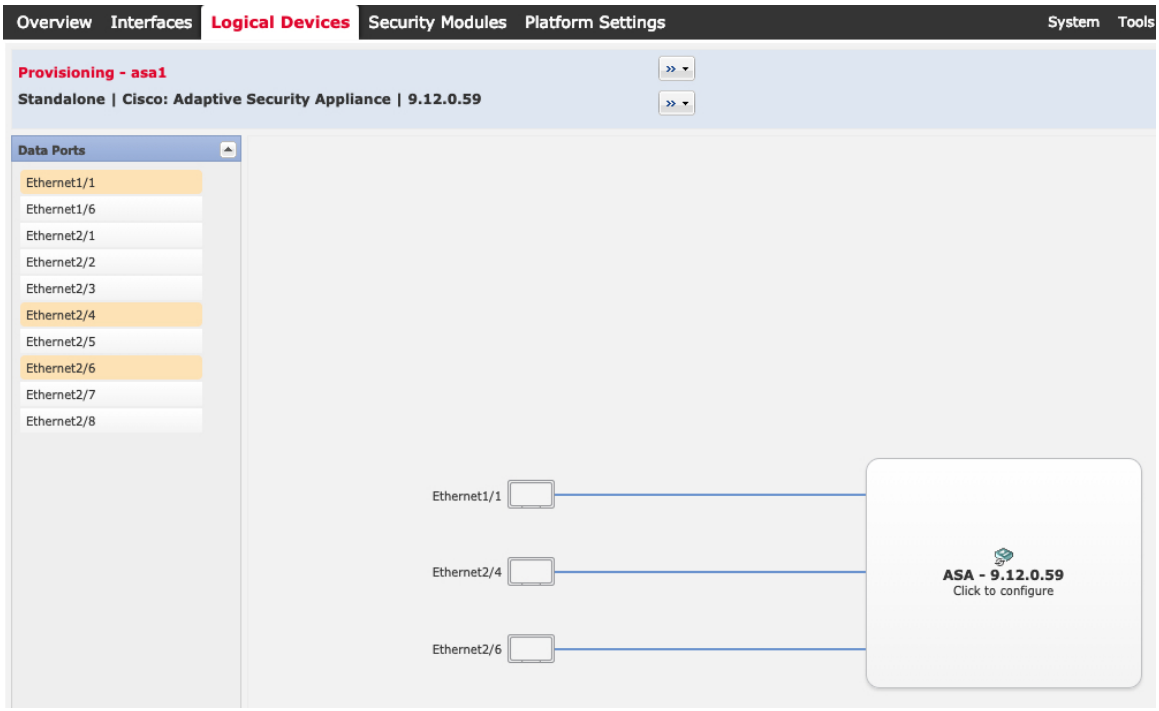
b) [Template] では、[Cisco Adaptive Security Appliance] を選択します。

c) [Image Version] を選択します。

d) [OK] をクリックします。

[Provisioning - *device name*] ウィンドウが表示されます。

ステップ 3 [Data Ports] 領域を展開し、デバイスに割り当てるインターフェイスをそれぞれクリックします。

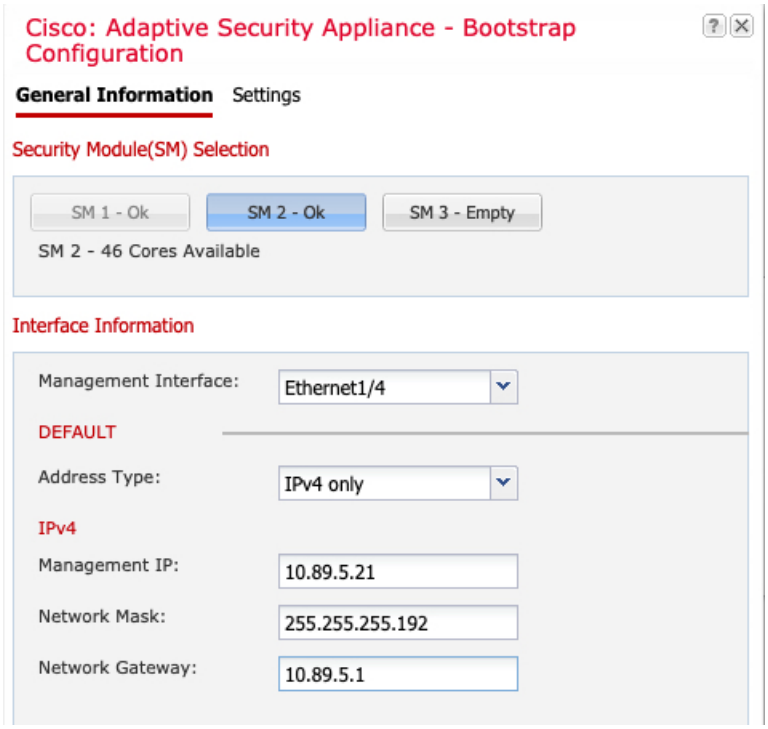


以前に [Interfaces] ページで有効にしたデータ インターフェイスのみを割り当てることができます。後ほど ASDM でこれらのインターフェイスを有効にして設定します。これには、IP アドレスの設定も含まれます。

ステップ 4 画面中央のデバイス アイコンをクリックします。

ダイアログボックスが表示され、初期のブートストラップ設定を行うことができます。これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

ステップ 5 [一般情報（General Information）] ページで、次の手順を実行します。



a) [セキュリティモジュールの選択（Security Module Selection）] の下で、この論理デバイスに使用するセキュリティ モジュールをクリックします。

b) [Management Interface] を選択します。

このインターフェイスは、論理デバイスを管理するために使用されます。このインターフェイスは、シャーシ管理ポートとは別のものです。

c) 管理インターフェイスを選択します。[アドレスタイプ（Address Type）]：[IPv4のみ（IPv4 only）]、[IPv6のみ（IPv6 only）]、または [IPv4およびIPv6（IPv4 and IPv6）]。

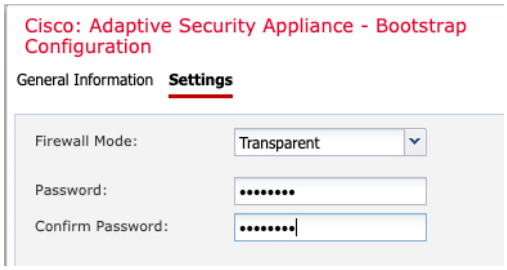
d) [Management IP] アドレスを設定します。

このインターフェイスに一意の IP アドレスを設定します。

e) [Network Mask] または [Prefix Length] に入力します。

f) **ネットワーク ゲートウェイ** アドレスを入力します。

ステップ 6 [設定（Settings）] をクリックします。



a) [Firewall Mode] を [Routed] または [Transparent] に指定します。

ルーテッドモードでは、ASA は、ネットワークのルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォール モードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

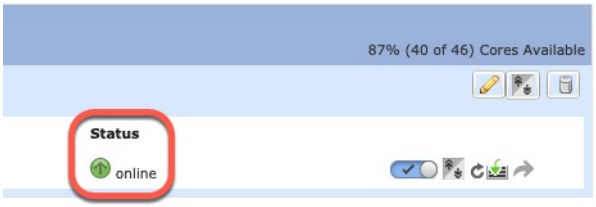
b) 管理者ユーザーの [パスワード（Password）] を入力して確認し、パスワードを有効にします。

事前設定されている ASA 管理者ユーザー/パスワードおよびイネーブル パスワードはパスワードの回復時に役立ちます。FXOS アクセスが可能な場合、パスワードを忘れたときに管理者ユーザー パスワードやイネーブル パスワードをリセットできます。

ステップ 7 [OK] をクリックして、設定ダイアログボックスを閉じます。

ステップ 8 [保存（Save）] をクリックします。

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。[**論理デバイス（Logical Devices）**] ページで、新しい論理デバイスのステータスを確認します。論理デバイスの [Status] が [online] と表示されたら、アプリケーションでセキュリティ ポリシーの設定を開始できます。



ASDM へのログイン

ASDM を起動して、ASA を設定できるようにします。

始める前に

- ASDM を実行するための要件については、Cisco.com の『ASDM リリース ノート』を参照してください。

- シャーシマネージャ の [論理デバイス（Logical Devices）] ページで、ASA の論理デバイスの [ステータス（Status）] が [オンライン（online）] になっていることを確認します。

手順

ステップ 1 ブラウザに次の URL を入力します。

- **https://***management_ip*：ブートストラップ設定に入力した管理インターフェイスの IP アドレス。

（注） **http://** や IP アドレス（デフォルトは HTTP）ではなく、必ず **https://** を指定してください。ASA は、HTTP リクエストを HTTPS に自動的に転送しません。

[Cisco ASDM] Web ページが表示されます。ASA に証明書がインストールされていないために、ブラウザのセキュリティ警告が表示されることがありますが、これらの警告は無視して、Web ページにアクセスできます。

ステップ 2 使用可能なオプション [Install ASDM Launcher] または [Run ASDM] のいずれかをクリックします。

ステップ 3 画面の指示に従ってオプションを選択し、ASDM を起動します。

[Cisco ASDM-IDM ランチャー（Cisco ASDM-IDM Launcher）] が表示されます。

ステップ 4 ユーザー名を空のままにして、ASA を展開したときに設定したイネーブルパスワードを入力し、[OK] をクリックします。

メイン ASDM ウィンドウが表示されます。

ASA でのライセンス権限付与の設定

ASA にライセンスを割り当てます。少なくとも標準ライセンスを割り当てる必要があります。

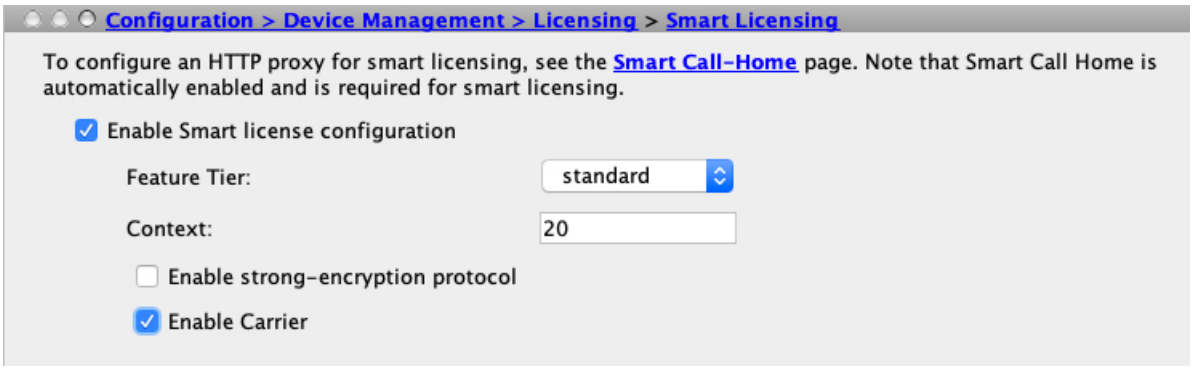
始める前に

- Chassis Manager：ライセンス サーバーへのシャーシの登録 （131 ページ）。

手順

ステップ 1 ASDM で、**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart Licensing]** の順に選択します。

ステップ 2 次のパラメータを設定します。



a) [Enable Smart license configuration] をオンにします。

b) [機能層（Feature Tier）] ドロップダウンリストから **[Essentials]** を選択します。

使用できるのは Essentials 層だけです。

c) （任意） [Context] ライセンスの場合、コンテキストの数を入力します。

10 コンテキストはライセンスなしで使用できます。コンテキストの最大数は 250 です。たとえば、最大数のコンテキストを使用するには、コンテキストの数として 240 を入力します。この値は、デフォルトの 10 に追加されます。

d) （任意） [キャリア（Carrier）] を確認します。

ステップ 3 [Apply] をクリックします。

アカウントに適切なライセンスがない場合は、ライセンスの変更を適用できません。

ステップ 4 ツールバーの [Save] アイコンをクリックします。

ステップ 5 ASDM を終了し、再起動します。

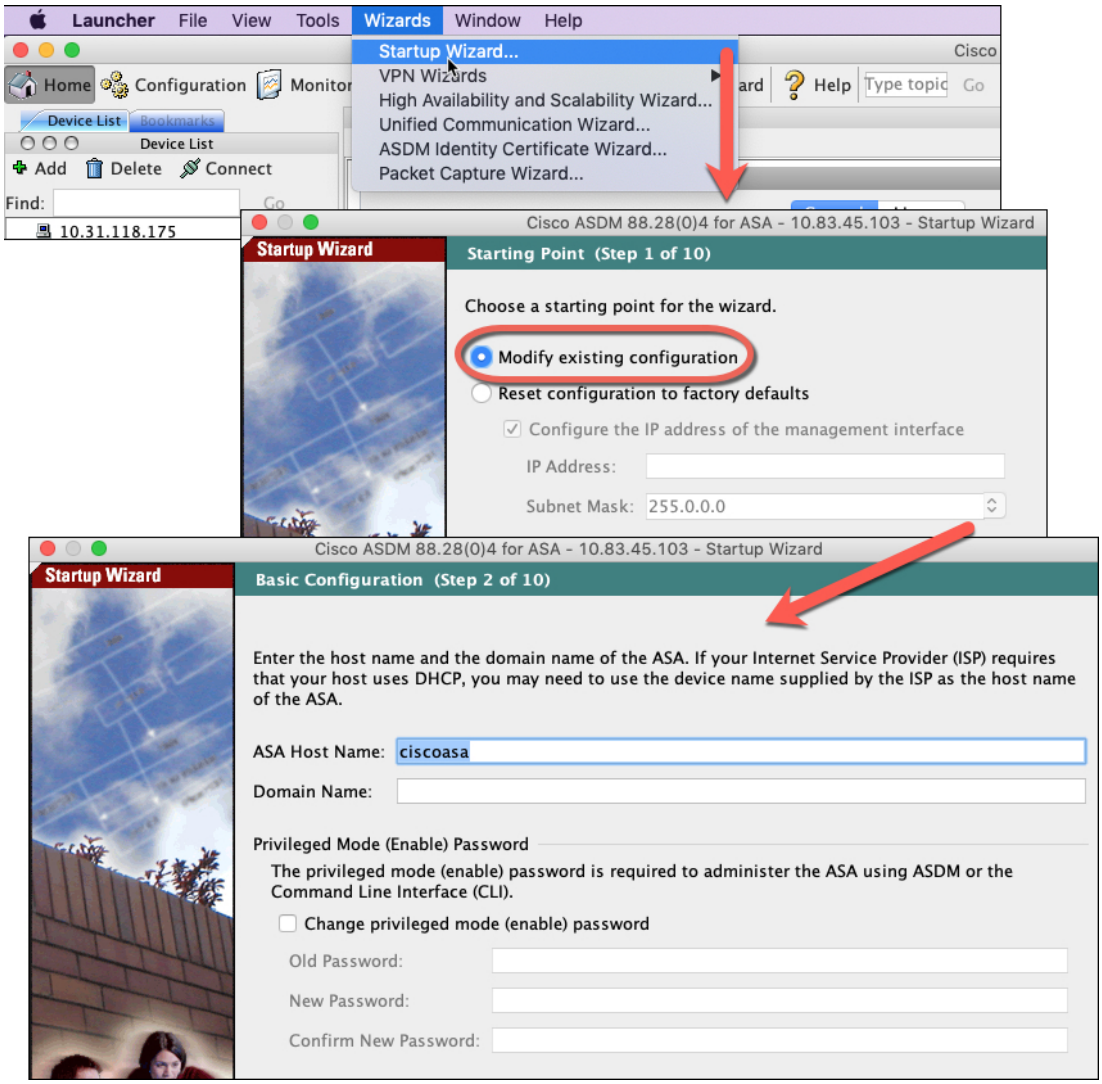
ライセンスを変更する場合、更新された画面を表示するには ASDM を再起動する必要があります。

ASA の設定

ASDM を使用する際、基本機能および拡張機能の設定にウィザードを使用できます。ウィザードに含まれていない機能を手動で設定することもできます。

手順

ステップ 1 [Wizards] > [Startup Wizard] の順に選択し、[Modify existing configuration] オプション ボタンをクリックします。



ステップ 2 [Startup Wizard] では、手順を追って以下を設定できます。

- イネーブル パスワード
- インターフェイス（内部および外部のインターフェイス IP アドレスの設定やインターフェイスの有効化など）
- スタティック ルート
- DHCP サーバー
- その他...

ステップ 3 （任意） [Wizards] メニューから、その他のウィザードを実行します。

ステップ 4 ASA の設定を続行するには、『Navigating the Cisco ASA Series Documentation』でソフトウェアバージョンに応じたマニュアルを参照してください。

ASA CLI へのアクセス

ASA CLI を使用して、ASDM を使用する代わりに ASA のトラブルシューティングや設定を行うことができます。CLI にアクセスするには、FXOS CLI から接続します。後で任意のインターフェイスからの SSH アクセスを設定できます。詳細については、ASA の一般的な操作の設定ガイドを参照してください。

手順

ステップ 1 コンソール接続または Telnet 接続を使用して、FXOS からモジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

ステップ 2 ASA コンソールに接続します。

connect asa

例：

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

ステップ 3 **Ctrl-a, d** と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

例

次に、セキュリティ モジュール 1 の ASA に接続してから、FXOS CLI のスーパバイザ レベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

次のステップ

- ASA の設定を続行するには、Cisco ASA シリーズの操作マニュアルの中から、お使いのソフトウェアバージョンに応じたマニュアルを参照してください。

ASA の履歴

機能	バージョン	詳細
ASA および 脅威に対する防御 を同じ Firepower 9300 の別のモジュールでサポート	9.12(1)	ASA および 脅威に対する防御 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 （注） FXOS 2.6.1 が必要です。

機能	バージョン	詳細
ASA 論理デバイスのトランスペアレントモード展開のサポート	9.10(1)	ASA を展開するときに、トランスペアレントまたはルーテッド モードを指定できるようになりました。 （注）　FXOS 2.4.1 が必要です。 新規/変更された Chassis Manager 画面： **[Logical Devices]** > **[Add Device]** > **[Settings]** > [Firewall Mode] ドロップダウン リスト
スマートエージェントの v1.6 へのアップグレード	9.6(2)	スマート エージェントはバージョン 1.1 からバージョン 1.6 へアップグレードされました。このアップグレードは永続ライセンス予約をサポートするほか、ライセンス アカウントに設定された権限に従って、高度暗号化（3DES/AES）ライセンス権限の設定もサポートします。
新しいキャリア ライセンス	9.5(2)	新しいキャリア ライセンスは既存の GTP/GPRS ライセンスを置き換え、SCTP と Diameter インスペクションもサポートします。Firepower 9300 上の ASA の場合、**feature mobile-sp** コマンドは **feature carrier** コマンドに自動的に移行します。 次の画面が変更されました。**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Smart License]**

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。