



Cisco ISA 3000 スタートアップガイド

初版：2019年9月25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

最適なオペレーティングシステム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つのオペレーティングシステムのいずれかを実行できます。オペレーティングシステムごとに、マネージャを選択できます。この章では、オペレーティングシステムとマネージャの選択肢について説明します。

- [オペレーティングシステム \(1 ページ\)](#)
- [マネージャ \(2 ページ\)](#)

オペレーティングシステム

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) オペレーティングシステムを使用できます。

- **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。

ASA と Threat Defense 間での再イメージ化の方法については、『[Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド](#)』を参照してください。

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)	<p>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。</p> <p>6.7以降、Management Center では、標準の管理インターフェイスではなく、外部（またはその他のデータ）インターフェイスから Threat Defense を管理できます。この機能は、リモート支社の展開に役立ちます。</p> <p>(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。</p> <p>Management Center を開始するには、「Management Center での Threat Defense の展開 (39 ページ)」を参照してください。</p>
Secure Firewall Device Manager (旧 Firepower Device Manager)	<p>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。</p> <p>(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。</p> <p>Device Manager を開始するには、「Device Manager での Threat Defense の展開 (5 ページ)」を参照してください。</p>

マネージャ	説明
Cisco Defense Orchestrator (CDO)	<p>CDOには2つの管理モードがあります。</p> <ul style="list-style-type: none"> • (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。 <p>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。</p> <p>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。</p>
Cisco Secure Firewall Threat Defense REST API	<p>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。</p> <p>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。</p>
Secure Firewall Management Center REST API	<p>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。</p> <p>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。</p>

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)	<p>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。</p> <p>ASDM を使用する前に ASDM を使用した ASA の展開 (79 ページ) を参照してください。</p>
CLI	<p>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。</p> <p>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。</p>
CDO	<p>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。</p> <p>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。</p>
Cisco Security Manager (CSM)	<p>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。</p> <p>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。</p>
ASA REST API	<p>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。</p> <p>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。</p>



第 2 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 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、脅威に対する防御 デバイスの初期セットアップと設定を完了する方法について説明します。

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。

ISA 3000 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。「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。

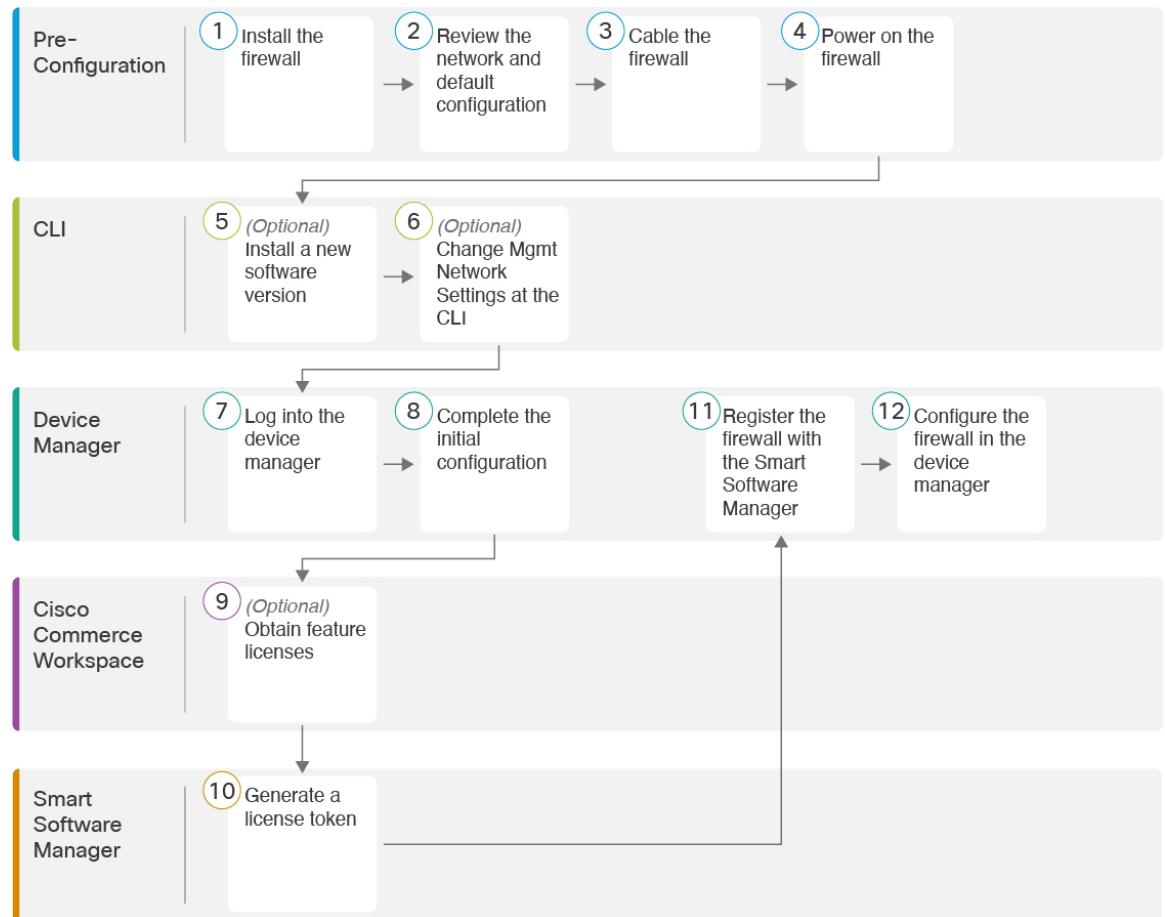
プライバシー収集ステートメント : Firepower 1100 シリーズには個人識別情報は不要で、積極的に収集することはありません。ただし、ユーザー名などの設定では、個人識別情報を使用できます。この場合、設定作業時や SNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

- [エンドツーエンドの手順 \(6 ページ\)](#)
- [ネットワーク配置とデフォルト設定の確認 \(7 ページ\)](#)
- [デバイスのケーブル接続 \(6.5 以降\) \(11 ページ\)](#)
- [デバイスの配線 \(6.4 以降\) \(12 ページ\)](#)
- [デバイスの電源投入 \(13 ページ\)](#)
- [\(任意\) CLI での管理ネットワーク設定の変更 \(14 ページ\)](#)
- [へのログイン Device Manager \(15 ページ\)](#)
- [初期設定の完了 \(6.5 以降\) \(16 ページ\)](#)
- [初期設定の完了 \(6.4 以前\) \(21 ページ\)](#)
- [ライセンスの設定 \(23 ページ\)](#)
- [Device Manager \(6.5 以降\) でのデバイスの設定 \(28 ページ\)](#)
- [Device Manager \(6.4 以前\) でのファイアウォールの設定 \(30 ページ\)](#)

- [Threat Defense CLI へのアクセス](#) (35 ページ)
- [ファイアウォールの電源の切断](#) (36 ページ)
- [次のステップ](#) (38 ページ)

エンドツーエンドの手順

シャーシで Device Manager を使用して脅威に対する防御を展開するには、次のタスクを参照してください。



①	事前設定	ネットワーク配置とデフォルト設定の確認 (7 ページ)。
②	事前設定	<ul style="list-style-type: none"> • デバイスのケーブル接続 (6.5 以降) (11 ページ)。 • デバイスの配線 (6.4 以降) (12 ページ)
③	事前設定	デバイスの電源投入 (13 ページ)。

4	Threat Defense CLI	(任意) CLI での管理ネットワーク設定の変更 (14 ページ)。
5	Device Manager	へのログイン Device Manager (15 ページ)。
6	Device Manager	<ul style="list-style-type: none"> 初期設定の完了 (6.5 以降) (16 ページ) 初期設定の完了 (6.4 以前) (21 ページ)。
7	Cisco Commerce Workspace	ライセンスの設定 (23 ページ) : ライセンス機能を取得します。
8	Smart Software Manager	ライセンスの設定 (23 ページ) : ライセンス トークンを生成します。
9	Device Manager	ライセンスの設定 (23 ページ) : スマート ライセンシング サーバーにデバイスを登録します。
10	Device Manager	<ul style="list-style-type: none"> Device Manager (6.5 以降) でのデバイスの設定 (28 ページ) Device Manager (6.4 以前) でのファイアウォールの設定 (30 ページ)。

ネットワーク配置とデフォルト設定の確認

次の図は、バージョン 6.5 以降およびバージョン 6.4 以前の ISA 3000 における推奨されるネットワーク配置を示しています。デフォルト設定はバージョン 6.5 で変更されました。



- (注) デフォルトの管理 IP アドレスを使用できない場合 (たとえば、デバイスを既存のネットワークに追加する場合)、コンソールポートに接続して、CLI で初期セットアップ (管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定など) を実行できます。 (任意) CLI での管理ネットワーク設定の変更 (14 ページ) を参照してください。

図 1: 6.5以降 : 推奨されるネットワーク展開

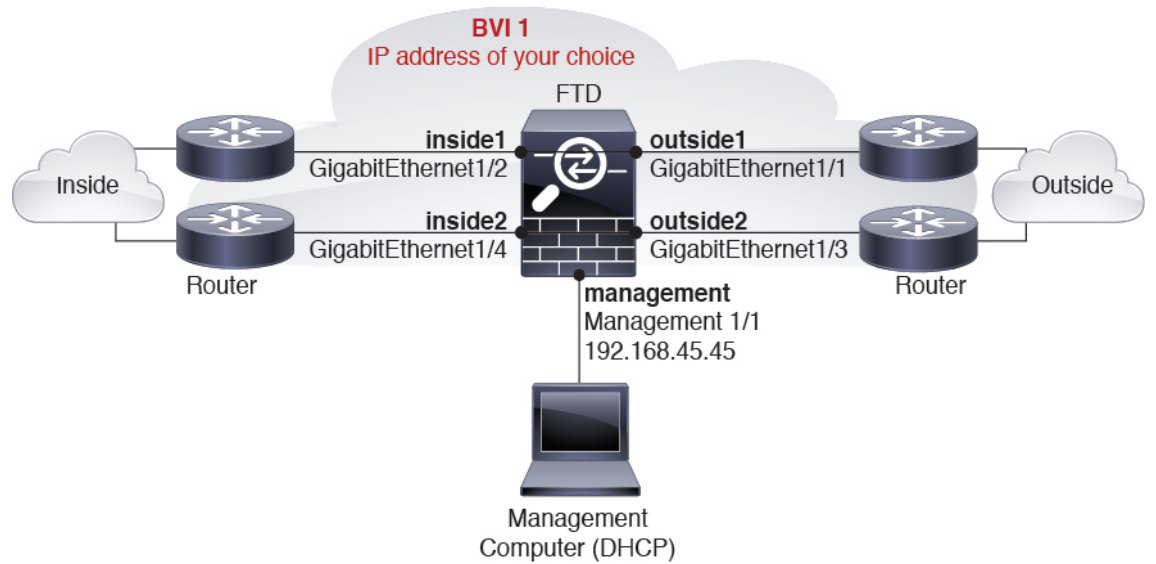
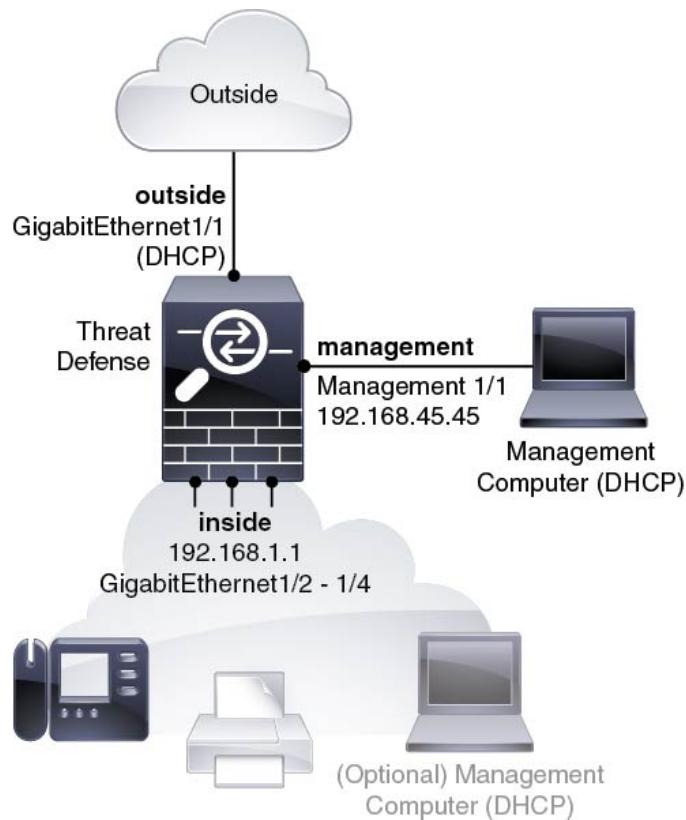


図 2: 6.4以前 : 推奨されるネットワーク展開



デフォルト設定 (6.5 以降)

出荷前に特別なデフォルト設定が適用されている ISA 3000 の設定には、以下が含まれます。

- BVI 1 : すべてのメンバーインターフェイスは同じネットワーク内に存在しています (IP アドレスは事前設定されていません。ネットワークと一致するように設定する必要があります) : GigabitEthernet 1/1 (outside1)、GigabitEthernet 1/2 (inside1)、GigabitEthernet 1/3 (outside2)、GigabitEthernet 1/4 (inside2)
- 内部→外部トラフィックフローすべてのインターフェイスは相互通信できます。
- 管理 : Management 1/1 (管理)、IP アドレス 192.168.45.45



(注) Management 1/1 インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有できます。『[FDM コンフィギュレーションガイド](#)』を参照してください。

- 管理用の DNS サーバー : OpenDNS: 208.67.222.222, 208.67.220.220
- NTP : Cisco NTP サーバー : 0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org
- デフォルトルート
 - 管理インターフェイス : 192.168.45.1 への管理インターフェイス経由。
 - データインターフェイス : なし。
- FDM アクセス : 管理ホストが許可されます。
- ハードウェアバイパス : 次のインターフェイスペアで有効になっています。GigabitEthernet 1/1 および 1/2。GigabitEthernet 1/3 および 1/4



(注) ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのは上記のインターフェイスペアのみになります。inside1 と inside2 および outside1 と outside2 は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。電源が再投入されると、脅威に対する防御 がフローを引き継ぐため、接続が短時間中断されます。

デフォルト設定 (6.4 以前)

初期セットアップ後の ISA 3000 の設定には、次のものが含まれます。

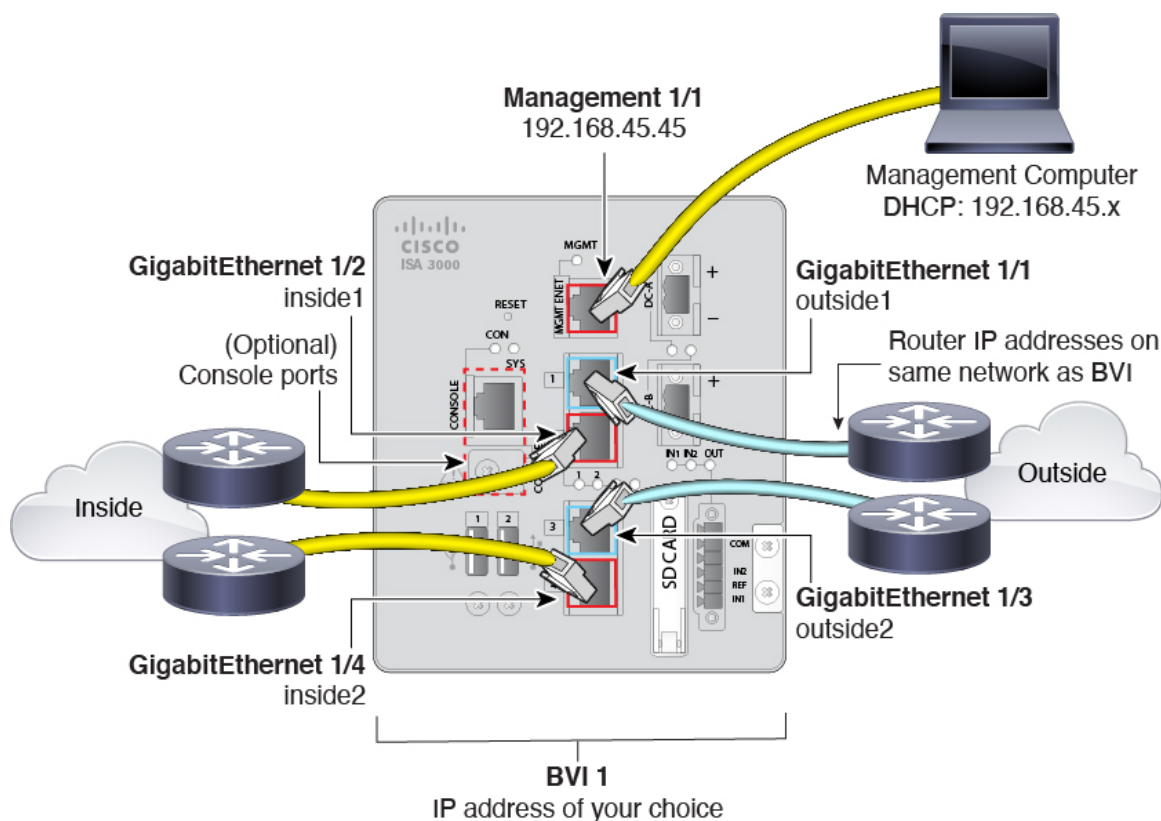
- 内部 : GigabitEthernet 1/2 ~ 1/4 は、□ブリッジグループ インターフェイス (BVI) 1、IP アドレス 192.168.1.1 に属します。
- 外部 : GigabitEthernet 1/1、DHCP からの IP アドレス、またはセットアップ時に指定したアドレス
- 内部→外部トラフィックフロー
- 管理 : Management 1/1 (管理)、IP アドレス 192.168.45.45



(注) Management 1/1 インターフェイスは、管理論理インターフェイスと診断論理インターフェイスの間で共有できます。『[FDM コンフィギュレーションガイド](#)』を参照してください。

- [管理用のDNSサーバー (DNS server for management)] : OpenDNS : 208.67.222.222、208.67.220.220、またはセットアップ時に指定したサーバー。
- NTP : Cisco NTP サーバー : 0.sourcefire.pool.ntp.org、1.sourcefire.pool.ntp.org、2.sourcefire.pool.ntp.org、またはセットアップ時に指定したサーバー
- デフォルトルート
 - データインターフェイス : 外部DHCPから取得したもの、またはセットアップ時に指定したゲートウェイ IP アドレス
 - 管理インターフェイス : バックプレーンを介しデータインターフェイスを経由脅威に対する防御 には、ライセンスおよびアップデート用のインターネットアクセスが必要です。
- 内部インターフェイスの **DHCP サーバー**、管理インターフェイス
- **FDM アクセス** : 管理ホストと内部ホストに許可されます
- **NAT** : 内部から外部へのすべてのトラフィック用のインターフェイス PAT

デバイスのケーブル接続 (6.5 以降)



Management 1/1 インターフェイスで ISA 3000 を管理します。

手順

ステップ 1 GigabitEthernet 1/1 を外部ルータに接続し、GigabitEthernet 1/2 を内部ルータに接続します。

これらのインターフェイスによってハードウェアバイパスペアが形成されます。

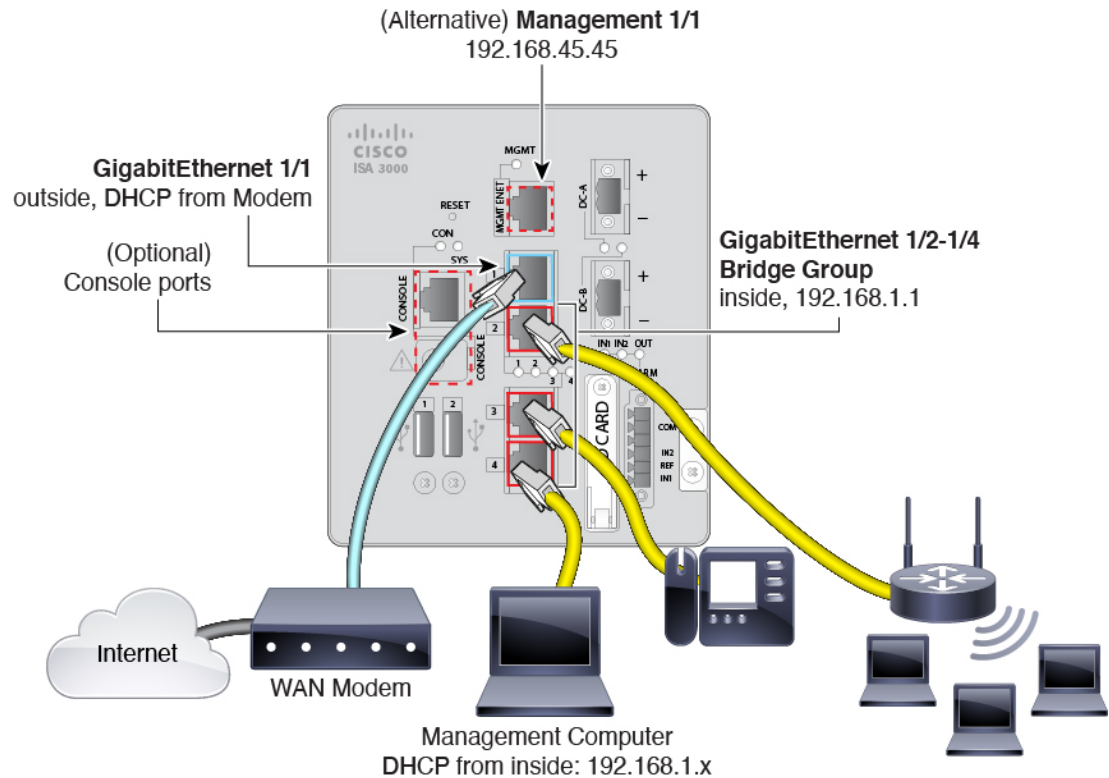
ステップ 2 GigabitEthernet 1/3 を冗長外部ルータに接続し、GigabitEthernet 1/4 を冗長内部ルータに接続します。

これらのインターフェイスによってハードウェアバイパスペアが形成されます。これらのインターフェイスは、他方のペアで障害が発生した場合に冗長ネットワークパスを提供します。これら 4 つのデータインターフェイスはすべて、選択した同じネットワーク上に存在します。BVI 1 の IP アドレスを、内部ルータおよび外部ルータと同じネットワーク上に配置するように設定する必要があります。

ステップ 3 Management 1/1 を管理 PC (またはネットワーク) に接続します。

Management 1/1 の IP アドレスをデフォルトから変更する必要がある場合は、管理 PC をコンソールポートにケーブル接続する必要もあります（ケーブル接続は表示されていません）。
 「(任意) CLI での管理ネットワーク設定の変更 (14 ページ)」を参照してください。

デバイスの配線 (6.4 以降)



Management 1/1 または GigabitEthernet 1/2 ~ 1/4 のいずれかで ISA 3000 を管理します。デフォルト設定でも、GigabitEthernet 1/1 は外部として設定されています。

手順

ステップ 1 管理コンピュータを次のいずれかのインターフェイスに接続します。

- GigabitEthernet 1/2 ~ 1/4 : 管理コンピュータをいずれかの内部ポート（イーサネット 1/2 ~ 1/4）に直接接続します。内部にはデフォルトの IP アドレス（192.168.1.1）があり、クライアントに IP アドレスを提供するために DHCP サーバーも実行されます（管理コンピュータを含む）。したがって、これらの設定が既存の内部ネットワーク設定と競合しないようにしてください（[デフォルト設定 \(6.4 以前\) \(9 ページ\)](#) を参照）。

- **Management 1/1** : 管理コンピュータを Management 1/1 に直接接続します。または、Management 1/1 を管理ネットワークに接続します。管理 1/1 にはデフォルトの IP アドレス (192.168.45.45) があり、クライアント (管理コンピュータを含む) に IP アドレスを提供するために DHCP サーバーも実行されるため、これらの設定が既存の管理ネットワークの設定と競合しないようにしてください ([デフォルト設定 \(6.4 以前\)](#) ([9 ページ](#)) を参照)。

Management 1/1 の IP アドレスをデフォルトから変更する必要がある場合は、管理 PC をコンソールポートにケーブル接続する必要もあります (ケーブル接続は表示されていません)。(任意) [CLI での管理ネットワーク設定の変更 \(14 ページ\)](#) を参照してください。

ステップ 2 外部ネットワークを GigabitEthernet 1/1 インターフェイスに接続します。

デフォルトでは、IP アドレスは DHCP を使用して取得しますが、初期設定時にスタティックアドレスを設定することもできます。

ステップ 3 内部デバイスを残りのポート (GigabitEthernet 1/2 ~ 1/8) に接続します。

デバイスの電源投入

システムの電源は DC 電源で制御されます。電源ボタンはありません。

始める前に

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

手順

ステップ 1 電源プラグは DC 電源に配線した後に ISA 3000 に接続します。

電源プラグの正しい配線手順については、『[ハードウェア設定ガイド](#)』の「[DC 電源への接続](#)」を参照してください。

ステップ 2 ISA 3000 デバイスの前面にあるシステム LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。緑色に点滅している場合、デバイスはブートアップフェーズおよび POST (電源投入時自己診断テスト) の状態です。

すべてのデバイスが ISA 3000 に正しく接続されているか確認するには、『[ハードウェア設置ガイド](#)』の「[接続の確認](#)」を参照してください。

(任意) CLI での管理ネットワーク設定の変更

デフォルトの IP アドレスを使用できない場合（たとえば、デバイスを既存のネットワークに追加する場合）、コンソールポートに接続して、CLI で初期セットアップ（管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定など）を実行できます。管理インターフェイスのみを設定できます。内部インターフェイスや外部インターフェイスは設定できません。これらは後で GUI を使用して設定できます。



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

手順

- ステップ 1** 脅威に対する防御 コンソールポートに接続します。詳細については、[Threat Defense CLI へのアクセス \(35 ページ\)](#) を参照してください。

admin ユーザーとデフォルトパスワードの **Admin123** を使用してログインします。

- (注) パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。手順については、『[Cisco ASA and Firepower Threat Defense Device Reimage Guide](#)』を参照してください。

- ステップ 2** Threat Defense に初めてログインすると、エンドユーザーライセンス契約 (EULA) に同意して管理者パスワードを変更するように求められます。その後、CLI セットアップスクリプトが表示されます。

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

次のガイドラインを参照してください。

- [管理インターフェイスの IPv4 デフォルトゲートウェイを入力します (Enter the IPv4 default gateway for the management interface)] : 手動 IP アドレスを設定した場合は、「**data-interfaces**」またはゲートウェイルータの IP アドレスのいずれかを入力します。**data-interfaces** を設定すると、アウトバウンド管理トラフィックがバックプレーン経由で送信され、データインターフェイスが終了します。この設定は、インターネットにアクセスできる個別の管理ネットワークがない場合に役立ちます。管理インターフェイスから発信されるトラフィックには、インターネットアクセスを必要とするライセンス登録とデータベースの更新が含まれます。**data-interfaces** を使用する場合、管理ネットワークに直接接続していれば管理インターフェイスで Device Manager（または SSH）を引き続き使用できますが、特定のネットワークまたはホストのリモート管理の場合は、**configure network**

static-routes コマンドを使用して静的ルートを追加する必要があります。データインターフェイスでの Device Manager の管理は、この設定の影響を受けないことに注意してください。DHCPを使用する場合、システムはDHCPによって提供されるゲートウェイを使用します。DHCP がゲートウェイを提供しない場合は、フォールバックメソッドとして **data-interfaces** を使用します。

- [ネットワーク情報が変更された場合は再接続が必要になります (If your networking information has changed, you will need to reconnect)] : SSH でデフォルトの IP アドレスに接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか (Manage the device locally?)] : または Device Manager を使用するには [はい (yes)] を入力します。[いいえ (no)] と応えると、Management Center デバイスの管理にはオンプレミスまたはクラウド配信を使用することになります。

例 :

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: *****
Confirm new password: *****
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

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

>
```

ステップ 3 新しい管理 IP アドレスで Device Manager にログインしてください。

へのログインDevice Manager

Device Manager にログインして 脅威に対する防衛 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。

手順

ステップ 1 ブラウザに次の URL を入力します。

- 管理 : <https://192.168.45.45>。CLI セットアップで管理 IP アドレスを変更した場合は、そのアドレスを入力します。
- (6.4 以前のみ) 内部 : <https://192.168.1.1>。任意の内部 BVI インターフェイス (Ethernet1/2 から 1/4) の内部アドレスに接続できます。6.5 以降の場合、デフォルト設定ではデータインターフェイスの管理が事前設定されません。

ステップ 2 ユーザー名 **admin**、デフォルトパスワード **Admin123** を使用してログインします。

次のタスク

- 6.4 以前の場合 : Device Manager セットアップウィザードを実行します。 [初期設定の完了 \(6.4 以前\) \(21 ページ\)](#) を参照してください。 6.5 以降の場合 : ISA 3000 はセットアップウィザードをサポートしていません。出荷前に特別なデフォルト設定が適用されます。FTD を手動で設定するには、 [初期設定の完了 \(6.5 以降\) \(16 ページ\)](#) を参照してください。

初期設定の完了 (6.5 以降)

ここでは、次の重要設定を設定する方法について説明します。

- BVI 1 IP アドレス : ブリッジグループ メンバー インターフェイス間でトラフィックが流れるには、BVI 1 IP アドレスを設定する必要があります。
- デバイスで発信されるトラフィックのデフォルトルート : すべてのインターフェイスはブリッジグループの一部であり、トラフィック転送に MAC アドレスルックアップを使用します。ただし、デバイスで発信されるトラフィックの場合は、デフォルトルートが必要です。管理ゲートウェイをデータインターフェイスに変更すると、このルートは管理インターフェイストラフィックにも使用されます。

手順

ステップ 1 CLI セットアップスクリプト ([\(任意\) CLI での管理ネットワーク設定の変更 \(14 ページ\)](#)) を使用していない場合、この接続が最初の接続であれば、次のプロンプトが表示されます。

- エンドユーザーライセンス契約書を確認して、内容に同意します。
- admin パスワードを変更します。
- 90 日間の評価ライセンスに同意します

ステップ2 BVI1 IP アドレスを設定します。

ブリッジグループメンバー インターフェイス間でトラフィックが流れるには、BVI1 IP アドレスを設定する必要があります。

- a) [デバイス (Device)] ページで、[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、[ブリッジグループ (Bridge Groups)] をクリックします。
- b) BVI1 ブリッジグループの編集アイコン (🔗) をクリックします。
- c) [IPv4 アドレス (IPv4 Address)] タブをクリックして、IPv4 アドレスを設定します。
[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

- [スタティック (Static)] : 変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。ブリッジグループの IP アドレスとサブネットマスクを入力します。接続されているエンドポイントはすべて、このネットワーク上に存在することになります。このアドレスがネットワーク上ですでに使用されていないことを確認します。

高可用性を設定し、このインターフェイスの HA をモニターしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイアドレスは、スタンバイデバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。

- [DHCP] : ネットワーク上の DHCP サーバーからアドレスを取得する場合は、このオプションを選択します。これはブリッジグループの一般的なオプションではありませんが、必要に応じて設定できます。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。

- [DHCPを使用してデフォルトルートを取得 (Obtain Default Route Using DHCP)] : デフォルトルートを DHCP サーバーから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。

- d) [IPv6 アドレス (IPv6 Address)] タブをクリックして、IPv6 アドレスを設定します。
 - [状態 (State)] : グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、スライダをクリックして有効にします (🔗)。リンクローカルアドレスはインターフェイスの MAC アドレス (*Modified EUI-64* 形式) に基づいて生成されます。

- (注) IPv6 を無効にしても、明示的な IPv6 アドレスを指定して設定されているインターフェイス、または自動設定が有効になっているインターフェイスの IPv6 処理は無効になりません。

- [スタティックアドレスとプレフィックス (Static Address/Prefix)]: ステータス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワークプレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。
- [RAを抑制 (Suppress RA)]: ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、脅威に対する防御はルータアドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ (ICMPv6 Type 134) は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

ルータ アドバタイズメントもルータ要請メッセージ (ICMPv6 Type 133) に応答して送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定できます。

脅威に対する防御 デバイスで IPv6 プレフィックスを提供する必要がないインターフェイス (外部インターフェイスなど) では、これらのメッセージを抑制できます。

- [スタンバイIPアドレス (Standby IP Address)]: 高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイアドレスは、スタンバイデバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。


e) [OK] をクリックします。

ステップ 3 デバイスで発信されるトラフィックのデフォルトルートを設定します。

すべてのインターフェイスはブリッジグループの一部であり、トラフィック転送に MAC アドレスルックアップを使用します。ただし、デバイスで発信されるトラフィックの場合は、デフォルトルートが必要です。管理ゲートウェイをデータインターフェイス (デフォルト) のままにすると、このルートは管理インターフェイス トラフィックにも使用されます。


- a) [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。

- b)  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。
- c) デフォルトルートのプロパティを設定します。

The screenshot shows the 'Add Static Route' dialog box. The fields are filled as follows: Name: default; Description: (empty); Protocol: IPv4 (selected); Gateway: gateway; Interface: bvi1 (BV11); Metric: 1; Networks: any-ipv4; SLA Monitor: Please select an SLA Monitor.

1. [名前 (Name)]を入力します。たとえば「default」とします。
2. [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。
3. [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。[OK] をクリックしてオブジェクトを追加します。

4. [インターフェイス (Interface)] で [BVI1] を選択します。
5. [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。
- d) [OK] をクリックします。
- e) [OK] をクリックします。

ステップ 4 (任意) CLI での管理ネットワーク設定の変更 (14 ページ) を使用して新しい管理 IP アドレスとゲートウェイを設定していない場合は、[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] ページで IP アドレスとゲートウェイを変更できます。ブラウザを使用して新しいアドレスに再接続する必要があります。

ステップ 5 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 6 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、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。

次のタスク

- 評価ライセンスを引き続き使用することもできますが、デバイスを登録してライセンスを取得することをお勧めします。[ライセンスの設定 \(23 ページ\)](#) を参照してください。
- また、デバイスの設定を選択することもできます。[Device Manager \(6.5 以降\) でのデバイスの設定 \(28 ページ\)](#) を参照してください。

初期設定の完了 (6.4 以前)

初期設定を完了するには、最初に **Device Manager** にログインしたときにセットアップウィザードを使用します。セットアップウィザードの完了後、いくつかの基本ポリシーが適切に設定された機能しているデバイスが必要です。

- 外部 (GigabitEthernet1/1) および内部インターフェイス。GigabitEthernet1/2 ~ 1/4 は、ブリッジグループメンバー内にあります。
- 内部インターフェイスと外部インターフェイスのセキュリティゾーン。
- 内部から外部へのすべてのトラフィックを信頼するアクセスルール。
- 内部から外部へのすべてのトラフィックを外部インターフェイスの IP アドレスの固有のポートへ変換するインターフェイス NAT ルール。
- 内部インターフェイスで実行されている DHCP サーバー。



(注) [\(任意\) CLI での管理ネットワーク設定の変更 \(14 ページ\)](#) の手順を実行した場合は、これらのタスクの一部、具体的には管理者パスワードの変更、および外部インターフェイスと管理インターフェイスの設定がすでに完了しているはずです。

手順

ステップ 1 エンドユーザー ライセンス契約書を読んで同意し、管理者パスワードを変更するように求められます。

続行するには、これらの手順を完了する必要があります。

ステップ 2 外部インターフェイスおよび管理インターフェイスに対して次のオプションを設定し、[次へ (Next)]をクリックします。

(注) [次へ (Next)]をクリックすると、設定がデバイスに展開されます。インターフェイスの名前は「外部」となり、「outside_zone」セキュリティゾーンに追加されます。設定値が正しいことを確認します。

- a) [外部インターフェイス (Outside Interface)]: これは、ゲートウェイ ルータに接続するためのデータポートです。デバイスの初期設定時に別の外部インターフェイスを選択することはできません。最初のデータインターフェイスがデフォルトの外部インターフェイスです。

[IPv4の設定 (Configure IPv4)]: 外部インターフェイス用の IPv4 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、サブネットマスク、およびゲートウェイを入力できます。[オフ (Off)]を選択して、IPv4 アドレスを設定しないという選択肢もあります。セットアップウィザードを使用して PPPoE を設定することはできません。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。ウィザードの完了後に PPPoE を設定できます。

[IPv6の設定 (Configure IPv6)]: 外部インターフェイス用の IPv6 アドレスです。DHCP を使用するか、または手動でスタティック IP アドレス、プレフィックス、およびゲートウェイを入力できます。[オフ (Off)]を選択して、IPv6 アドレスを設定しないという選択肢もあります。

- b) [管理インターフェイス (Management Interface)]

[DNSサーバ (DNS Servers)]: システムの管理アドレス用の DNS サーバ。名前解決用に 1 つ以上の DNS サーバのアドレスを入力します。デフォルトは OpenDNS パブリック DNS サーバです。フィールドを編集し、デフォルトに戻りたい場合は、[OpenDNSを使用 (Use OpenDNS)]をクリックすると、フィールドに適切な IP アドレスがリロードされます。

[ファイアウォールホスト名 (Firewall Hostname)]: システムの管理アドレスのホスト名です。

ステップ 3 システム時刻を設定し、[次へ (Next)]をクリックします。

- a) [タイムゾーン (Time Zone)]: システムのタイムゾーンを選択します。
- b) [NTPタイムサーバ (NTP Time Server)]: デフォルトの NTP サーバを使用するか、使用している NTP サーバのアドレスを手動で入力するかを選択します。バックアップ用に複数のサーバを追加できます。

ステップ 4 (任意) システムのスマートライセンスを設定します。

Threat Defense デバイスを購入すると、自動的に基本ライセンスが付いてきます。すべての追加ライセンスはオプションです。

スマートライセンスのアカウントを取得し、システムが必要とするライセンスを適用する必要があります。最初は 90 日間の評価ライセンスを使用し、後でスマートライセンスを設定できます。

デバイスを今すぐ登録するには、リンクをクリックして Smart Software Manager のアカウントにログインします。[ライセンスの設定 \(23 ページ\)](#) を参照してください。

評価ライセンスを使用するには、[登録せずに90日間の評価期間を開始する (Start 90 day evaluation period without registration)] を選択します。

ステップ 5 [終了 (Finish)] をクリックします。

次のタスク

- 評価ライセンスを引き続き使用することもできますが、デバイスを登録し、ライセンスを取得することをお勧めします。を参照してください[ライセンスの設定 \(23 ページ\)](#)。
- Device Manager を使用してデバイスを設定することもできます。「[Device Manager \(6.4 以前\) でのファイアウォールの設定 \(30 ページ\)](#)」を参照してください。

ライセンスの設定

脅威に対する防御 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シスコ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、License Authority によって シャーシと License Authority 間の通信に使用される ID 証明書が発行されます。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。

基本ライセンスは自動的に含まれます。スマートライセンシングでは、まだ購入していない製品機能を使用することはできませんが、次のオプション機能ライセンスを購入して準拠する必要があります。

- **Cisco Secure Firewall Threat Defense の IPS** : セキュリティ インテリジェンスと Cisco Secure IPS
- **Cisco Secure Firewall Threat Defense のマルウェア防御** : マルウェア防御
- **Cisco Secure Firewall Threat Defense の URL フィルタリング** : URL フィルタリング
- **RA VPN** : AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN 専用。

上記のライセンスに加えて、1、3、または5年のアップデートにアクセスするため、該当するサブスクリプションを購入する必要があります。

システムのライセンシングの詳細については、『[FDM コンフィグレーション ガイド](#)』を参照してください。

始める前に

- [Cisco 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、ご使用のシスコ 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。

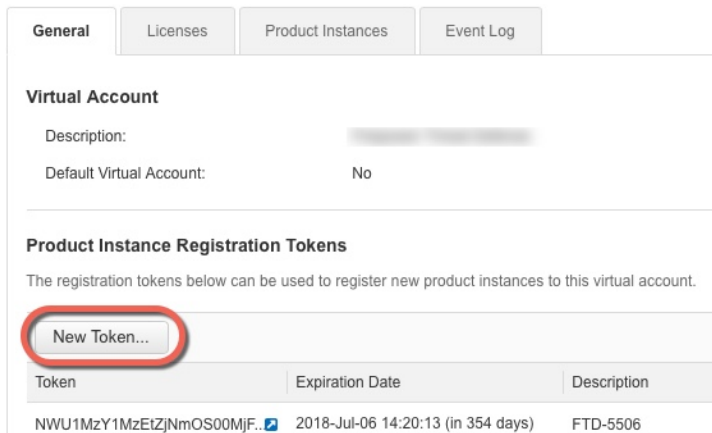
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマートソフトウェアライセンス アカウントにリンクされています。

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。

Create Registration Token

This dialog will generate the token required to register your product instances with your Smart Account.

Virtual Account: [Redacted]

Description: [Empty text box]

* Expire After: [30] Days

Enter the value between 1 and 365, but Cisco recommends a maximum of 30 days.

Allow export-controlled functionality on the products registered with this token

[Create Token] [Cancel]

• [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。

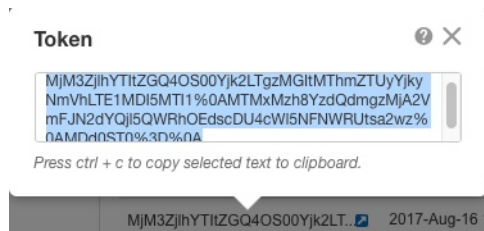
トークンはインベントリに追加されます。

- 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。脅威に対する防御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 3: トークンの表示

Token	Expiration Date	Description	Export-Controlled	Created By	Actions
MjM3ZjYhYTIzGQ4OS00Yjk2LT...	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed	[Redacted]	Actions

図 4: 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。

The screenshot shows the 'Smart License' summary page in Device Manager. At the top, it says 'Device Summary' and 'Smart License'. Below that, there is a warning icon and the text 'LICENSE ISSUE EVALUATION PERIOD You are in Evaluation mode now.' In the center, it displays '69/90 days left.' To the right of this, there is a blue button labeled 'REGISTER DEVICE'.

次に、 [スマートライセンス登録 (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。

The screenshot shows the 'Smart License Registration' dialog box. It contains five numbered steps:

- 1 Create or log in into your [Cisco Smart Software Manager](#) account.
- 2 On your assigned virtual account, under "General tab", click on "New Token" to create token.
- 3 Copy the token and paste it here:

```
MGY2Nz-MwOGItODJiZi00NzFiLWJiNitYWMwNzU0ODY2ZGVlTE1NIUz
Nzly%QAODq5Mzh8SUQ5Vm5XbzZiSmN5M3I6K3owZ3ovVmpmc3Vtal
JLQ2FFeGhFWmIW%0AWC9WTT0%3D%0A
```
- 4 Select Region
 When you register the device, you are also registered with Cisco Security Services Exchange (SSE). Please select the region in which your device is operating. You will be able to see your device in the device list of the regional SSE portal.
 Region
 SSE US Region
- 5 Cisco Success Network
 Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.
 Check out the [Sample Data](#) that will be sent to Cisco. [See more](#)

At the bottom, there are two buttons: 'CANCEL' and 'REGISTER DEVICE'.

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。

Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in Task List. Refresh this page to see the updated status.

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。

Device Summary
Smart License

✓ **CONNECTED**
SUFFICIENT LICENSE

Last sync: 10 Jul 2019 11:39 AM
Next sync: 10 Jul 2019 11:49 AM

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。

SUBSCRIPTION LICENSES INCLUDED

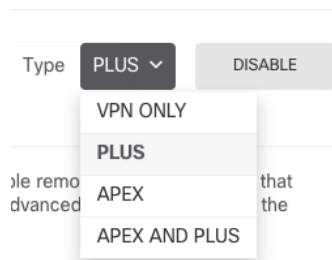
Threat ENABLE
Disabled by user
This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.
Includes: Intrusion Policy

Malware ENABLE
Disabled by user
This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.
Includes: File Policy

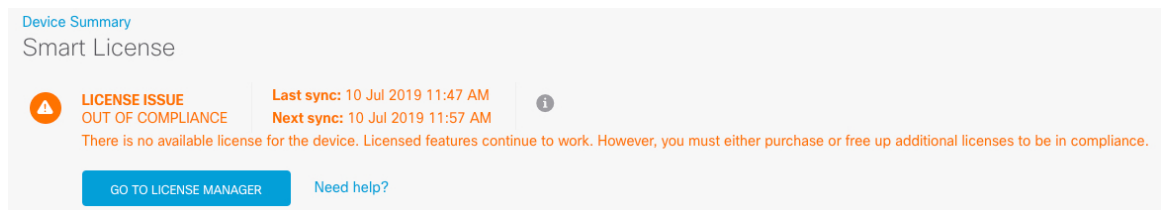
URL License ENABLE
Disabled by user
This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.
Includes: URL Reputation

RA VPN License Type PLUS ENABLE
Disabled by user
Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.
Includes: RA-VPN

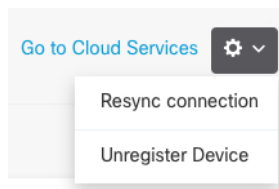
- [有効化 (Enable)] : Cisco Smart Software Manager アカウントにライセンスを登録し、制御された機能が有効になります。ライセンスによって制御されるポリシーを設定し、展開できます。
- [無効化 (Disable)] : Cisco Smart Software Manager アカウントのライセンスを登録解除し、制御された機能が無効になります。新しいポリシーの機能の設定も、その機能を使用するポリシーの展開もできません。
- **RA VPN** ライセンスを有効にした場合は、使用するライセンスのタイプ ([Plus]、[Apex]、[VPN 専用 (VPN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



Device Manager (6.5 以降) でのデバイスの設定

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン (?) をクリックしてください。

手順

ステップ 1 ブリッジグループインターフェイスを変換する場合は、[デバイス (Device)] を選択し、[インターフェイス (Interfaces)] の概要のリンクをクリックします。

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

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

図 5: インターフェイスの編集

The screenshot shows the 'Edit Physical Interface' configuration page. At the top, there is a blue header with the text 'Edit Physical Interface'. Below this, there are several sections:

- Interface Name:** A text input field containing 'dmz'.
- Status:** A toggle switch that is currently turned on (blue).
- Description:** A large empty text area.
- IP Address and Subnet Mask:** A section with three tabs: 'IPv4 Address' (selected), 'IPv6 Address', and 'Advanced Options'. Under the 'IPv4 Address' tab, there is a 'Type' dropdown menu set to 'Static'. Below that, there are two input fields for the IP address and subnet mask, containing '192.168.6.1' and '24' respectively. A small note below these fields reads 'e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0'.

ステップ 2 [ポリシー (Policies)] を選択してネットワークのセキュリティ ポリシーを構成します。

デフォルトでは、すべてのインターフェイス間ですべてのトラフィックが許可されます。他のセキュリティゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、アクセスルールを微調整できます。次のポリシーを設定できます。

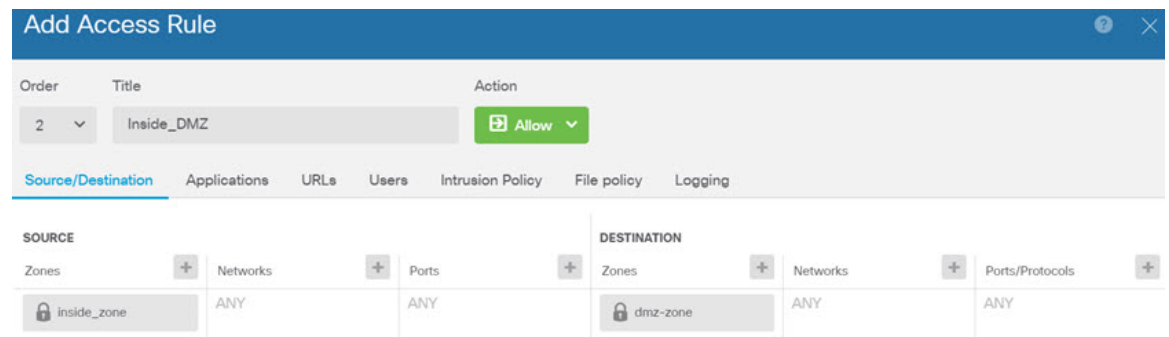
- [SSL復号 (SSL Decryption)] : 侵入、マルウェアなどについて暗号化された接続 (HTTPS など) を検査する場合は、接続を復号化する必要があります。どの接続を復号する必要があるかを判断するには SSL 復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。
- [アイデンティティ (Identity)] : 個々のユーザーにネットワークアクティビティを関連付ける、またはユーザーまたはユーザーグループのメンバーシップに基づいてネットワークアクセスを制御する場合は、特定のソース IP アドレスに関連付けられているユーザーを判定するためにアイデンティティ ポリシーを使用します。
- [セキュリティインテリジェンス (Security Intelligence)] : ブラックリスト登録済みの IP アドレスまたは URL の接続をただちにドロップするには、セキュリティインテリジェンスポリシーを使用します。既知の不正なサイトをブラックリストに登録すれば、アクセスコントロールポリシーでそれらを考慮する必要がなくなります。Cisco では、セキュリティインテリジェンスのブラックリストが動的に更新されるように、既知の不正なアドレスや URL の定期更新フィードを提供しています。フィードを使用すると、ブラックリストの項目を追加または削除するためにポリシーを編集する必要がありません。
- [NAT] (ネットワークアドレス変換) : 内部 IP アドレスを外部のルーティング可能なアドレスに変換するために NAT ポリシーを使用します。
- [アクセス制御 (Access Control)] : ネットワーク上で許可する接続の決定にアクセスコントロールポリシーを使用します。セキュリティゾーン、IP アドレス、プロトコル、ポー

ト、アプリケーション、URL、ユーザーまたはユーザーグループによってフィルタ処理できます。また、アクセス制御ルールを使用して侵入やファイル（マルウェア）ポリシーを適用します。このポリシーを使用して URL フィルタリングを実装します。

- [侵入 (Intrusion)]: 侵入ポリシーを使用して、既知の脅威を検査します。アクセス制御ルールを使用して侵入ポリシーを適用しますが、侵入ポリシーを編集して特定の侵入ルールを選択的に有効または無効にできます。

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーンの間でのトラフィックを許可する方法を示します。この例では、[接続の最後で (At End of Connection)] が選択されている場合、[ロギング (Logging)] を除いて他のいずれのタブでもオプションは設定されません。

図 6: アクセスコントロールポリシー



ステップ 3 [デバイス (Device)] を選択してから、[更新 (Updates)] グループで [設定の表示 (View Configuration)] をクリックし、システムデータベースの更新スケジュールを設定します。

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

ステップ 4 メニューの [導入 (Deploy)] ボタンをクリックし、[今すぐ導入する (Deploy Now)] ボタン



() をクリックして、変更内容をデバイスに展開します。

変更は、それらを展開するまでデバイスで有効になりません。

Device Manager (6.4 以前) でのファイアウォールの設定

次の手順では、追加機能の設定の概要を説明します。各手順について詳細な情報を表示するには、ページのヘルプ ボタン (?) をクリックしてください。

手順

- ステップ 1** □ブリッジグループ インターフェイスを変換する場合は、[デバイス (Device)] を選択して [インターフェイス (Interfaces)] の概要のリンクをクリックします。

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

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

図 7: インターフェイスの編集

Edit Physical Interface

Interface Name: dmz Status:

Description:

IPv4 Address | IPv6 Address | Advanced Options

Type: Static

IP Address and Subnet Mask: 192.168.6.1 / 24
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

- ステップ 2** 新しいインターフェイスを構成する場合は、[オブジェクト (Objects)] を選択し、目次から [セキュリティゾーン (Security Zones)] を選択します。

編集または必要に応じて新しいゾーンを作成します。インターフェイスではなく、セキュリティゾーンに基づいてポリシーを構成するため、各インターフェイスはゾーンに属している必要があります。インターフェイスを構成する場合、ゾーンにインターフェイスを置くことはできません。このため、新しいインターフェイスを作成した後、または既存のインターフェイスの目的を変更した後は常にゾーン オブジェクトを編集する必要があります。

次の例では、DMZ インターフェイスのために新しい DMZ ゾーンを作成する方法を示します。

図 8: セキュリティ ゾーンオブジェクト

ステップ 3 内部クライアントで DHCP を使用してデバイスから IP アドレスを取得する場合は、[デバイス (Device)] > [システム設定 (System Settings)] > [DHCPサーバー (DHCP Server)] を選択してから、[DHCPサーバー (DHCP Servers)] タブを選択します。

すでに内部インターフェイス用に構成されている DHCP サーバーがありますが、アドレスプールを編集したり、それを削除したりすることができます。他の内部インターフェイスを構成した場合は、それらのインターフェイス上に DHCP サーバーをセットアップするのがごく一般的です。[+] をクリックして各内部インターフェイスのサーバーとアドレスプールを構成します。

[構成 (Configuration)] タブでクライアントに提供される WINS および DNS のリストを微調整することもできます。次の例では、アドレスプールの 192.168.4.50 ~ 192.168.4.240 で inside2 インターフェイス上の DHCP サーバーを設定する方法を示しています。

図 9: DHCPサーバー

ステップ 4 [デバイス (Device)] を選択してから、[ルーティング (Routing)] グループで [設定の表示 (View Configuration)] (または [最初のスタティックルートを作成 (Create First Static Route)]) をクリックし、デフォルトルートを構成します。

デフォルトルートは通常、外部インターフェイス以外に存在するアップストリームまたは ISP ルータを指しています。デフォルトの IPv4 ルートは任意の ipv4 (0.0.0.0/0)、デフォルトの IPv6 ルートは任意の ipv6 (:::0/0) です。使用する IP バージョンごとにルートを作成します。

外部インターフェイスのアドレスの取得に DHCP を使用する場合、必要なデフォルト ルートをすでに持っていることがあります。

(注) このページで定義したルートは、データ インターフェイス用のみです。管理インターフェイスには影響しません。[デバイス (Device)] > [システム設定 (System Settings)] > [管理インターフェイス (Management Interface)] で管理ゲートウェイを設定します。

次の例に、IPv4 のデフォルト ルートを示します。この例では、isp ゲートウェイは ISP ゲートウェイの IP アドレスを識別するネットワーク オブジェクトです (アドレスは ISP から取得する必要があります)。[ゲートウェイ (Gateway)] の下部の [新しいネットワークを作成する (Create New Network)] ドロップダウン リストをクリックしてこのオブジェクトを作成することができます。

図 10: デフォルトルート

The screenshot shows the 'Add Static Route' configuration page. It includes the following fields and options:

- Protocol:** Radio buttons for IPv4 (selected) and IPv6.
- Gateway:** A text input field containing 'isp-gateway'.
- Interface:** A text input field containing 'outside'.
- Metric:** A text input field containing '1'.
- Networks:** A dropdown menu with a plus sign and a selected item 'amy-ipv4'.

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

デバイス セットアップ ウィザードは、内部ゾーンと外部ゾーンの間でのトラフィック フローを有効にします。また、外部インターフェイスを使用する場合に、全インターフェイスに対するインターフェイス NAT も有効にします。新しいインターフェイスを構成した場合でも、内部ゾーンオブジェクトに追加する場合はそれらにアクセス制御ルールが自動的に適用されます。

ただし、複数の内部インターフェイスがある場合は、内部ゾーンから内部ゾーンへのトラフィックフローを許可するアクセス制御ルールが必要です。他のセキュリティゾーンを追加する場合は、それらのゾーンとのトラフィックを許可するルールが必要です。これらは最低限の変更になります。

さらに、組織が必要とする結果を得るために、その他のポリシーを設定して、追加サービスの提供や、NAT およびアクセス ルールを微調整できます。次のポリシーを設定できます。

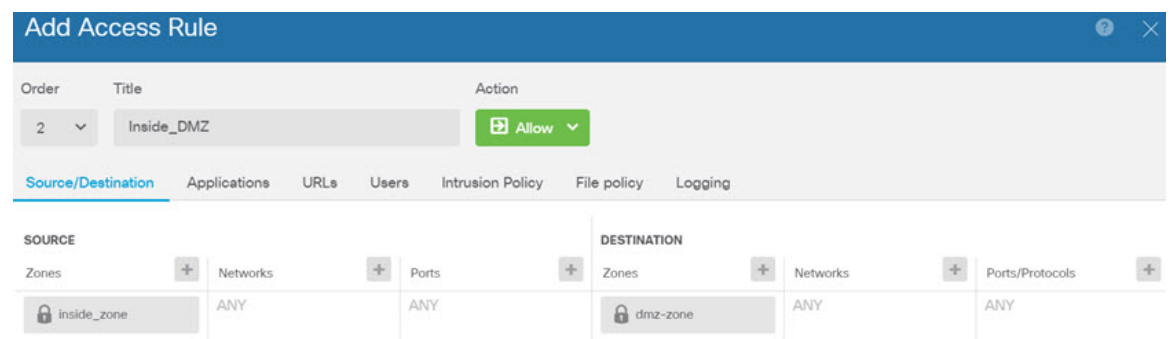
- [SSL 復号 (SSL Decryption)]: 侵入、マルウェアなどについて暗号化された接続 (HTTPS など) を検査する場合は、接続を復号化する必要があります。どの接続を復号化する必要があります。

あるかを判断するには SSL 復号ポリシーを使用します。システムは、検査後に接続を再暗号化します。

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

次の例では、アクセス制御ポリシーで内部ゾーンと DMZ ゾーンの間でのトラフィックを許可する方法を示します。この例では、[接続の最後で (At End of Connection)] が選択されている場合、[ロギング (Logging)] を除いて他のいずれのタブでもオプションは設定されません。

図 11: アクセスコントロールポリシー



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

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

ステップ 7 メニューの [導入 (Deploy)] ボタンをクリックし、[今すぐ導入する (Deploy Now)] ボタン



をクリックして、変更内容をデバイスに展開します。

変更は、それらを展開するまでデバイスで有効になりません。

Threat Defense CLI へのアクセス

コマンドラインインターフェイス (CLI) を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLI セッションからポリシーを設定することはできません。CLI には、コンソールポートに接続してアクセスできます。

脅威に対する防御 デバイスの管理インターフェイスに SSH で接続できます。SSH 接続用のインターフェイスを開いている場合、データインターフェイス上のアドレスにも接続できます。データ インターフェイスへの SSH アクセスはデフォルトで無効になっています。

手順

ステップ 1 CLI にログインして、管理コンピュータをコンソールポート、RJ-45 ポート、ミニ USB ポートのいずれかに接続します。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください。次のシリアル設定を使用します。

- 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 2 ユーザー名 **admin**、および初期セットアップ時に設定したパスワードを使用して脅威に対する防御 CLI にログインします (デフォルトは **Admin123**)。

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用法の詳細については、『[Cisco Firepower Threat Defense Command Reference](#)』を参照してください。

ファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されており、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールシステムをグレースフルシャットダウンできないことを覚えておいてください。

ISA 3000 シャーシには、外部電源スイッチはありません。Device Manager を使用してファイアウォールの電源を切断するか、CLI を使用できます。

Device Manager を使用したファイアウォールの電源の切断

Device Manager を使用してシステムを適切にシャットダウンできます。



(注) シャットダウンは 7.0.2+/7.2+ でサポートされています。

手順

ステップ 1 Device Manager を使用してファイアウォールをシャットダウンします。

- a) [デバイス (Device)] をクリックしてから、[システム設定 (System Settings)] > [再起動/シャットダウン (Reboot/Shutdown)] リンクをクリックします。
- b) [シャットダウン (Shut Down)] をクリックします。

ステップ 2 シャットダウンプロセスをモニターします。デバイスを監視できない場合は、約 3 分間待ってシステムがシャットダウンしたことを確認します。

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

```
System is stopped.
It is safe to power off now.

To restart the device, you must Power cycle to the device.
```

ステップ 3 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

CLI におけるファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数

のプロセスが実行されており、電源プラグを抜いたり、電源を切断したりすると、システムをグレースフルシャットダウンできないことを覚えておいてください。ISA 3000 シャーシには、外部電源スイッチはありません。



(注) シャットダウンは 7.0.2+/7.2+ でサポートされています。

手順

ステップ 1 コンソールポートに接続して脅威に対する防御 CLI にアクセスし、脅威に対する防御 をシャットダウンします。

shutdown

例：

```
> shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
Shutting down sfid... [ OK ]
Clearing static routes
Unconfiguring default route [ OK ]
Unconfiguring address on br1 [ OK ]
Unconfiguring IPv6 [ OK ]
Downing interface [ OK ]
Stopping xinetd:
Stopping nsd... [ OK ]
Stopping system log daemon... [ OK ]
Stopping Threat Defense ...
Stopping system message bus: dbus. [ OK ]
Un-mounting disk partitions ...
device-mapper: remove ioctl on root failed: Device or resource busy
[...]
mdadm: Cannot get exclusive access to /dev/md0:Perhaps a running process, mounted
filesystem or active volume group?
Stopping OpenBSD Secure Shell server: sshd
stopped /usr/sbin/sshd (pid 3520)
done.
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid
3525)
acpid.
Stopping system message bus: dbus.
Stopping internet superserver: xinetd.
no /etc/sysconfig/kdump.conf
Deconfiguring network interfaces... ifdown: interface br1 not configured
done.
SSP-Security-Module is shutting down ...
Sending ALL processes the TERM signal ...
acpid: exiting
Sending ALL processes the KILL signal ...
Deactivating swap...
Unmounting local filesystems...

Firepower Threat Defense stopped.
It is safe to power off now.
```

To restart the device, you must Power cycle to the device.

ステップ 2 脅威に対する防御 がシャットダウンし、コンソールに「今すぐに電源をオフにする」と表示された場合は、必要に応じて電源を抜いてシャーシから電源を物理的に取り外します。

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。



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、脅威に対する防御の初期設定の方法と Management Center へのデバイスの登録方法について説明します。大規模ネットワークにおける一般的な展開では、複数の管理対象デバイスをネットワークセグメントにインストールし、分析のためにトラフィックをモニターして、管理 Management Center にレポートします。これにより、管理、分析、およびレポートタスクの実行に使用できる Web インターフェイスがある集中管理コンソールを使用できます。

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。

Cisco ISA 3000 では、脅威に対する防御ソフトウェアか 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。「[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。

プライバシー収集ステートメント : ISA 3000 には個人識別情報は不要で、積極的に収集することはありません。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](#) (40 ページ)
- [エンドツーエンドの手順](#) (40 ページ)
- [ネットワーク展開の確認](#) (41 ページ)
- [デバイスの配線](#) (46 ページ)
- [デバイスの電源投入](#) (50 ページ)
- [CLI を使用した Threat Defense 初期設定の実行の完了](#) (51 ページ)
- [へのログイン Management Center](#) (57 ページ)
- [Management Center のライセンスの取得](#) (58 ページ)
- [Management Center への Threat Defense の登録](#) (59 ページ)
- [基本的なセキュリティポリシーの設定](#) (62 ページ)

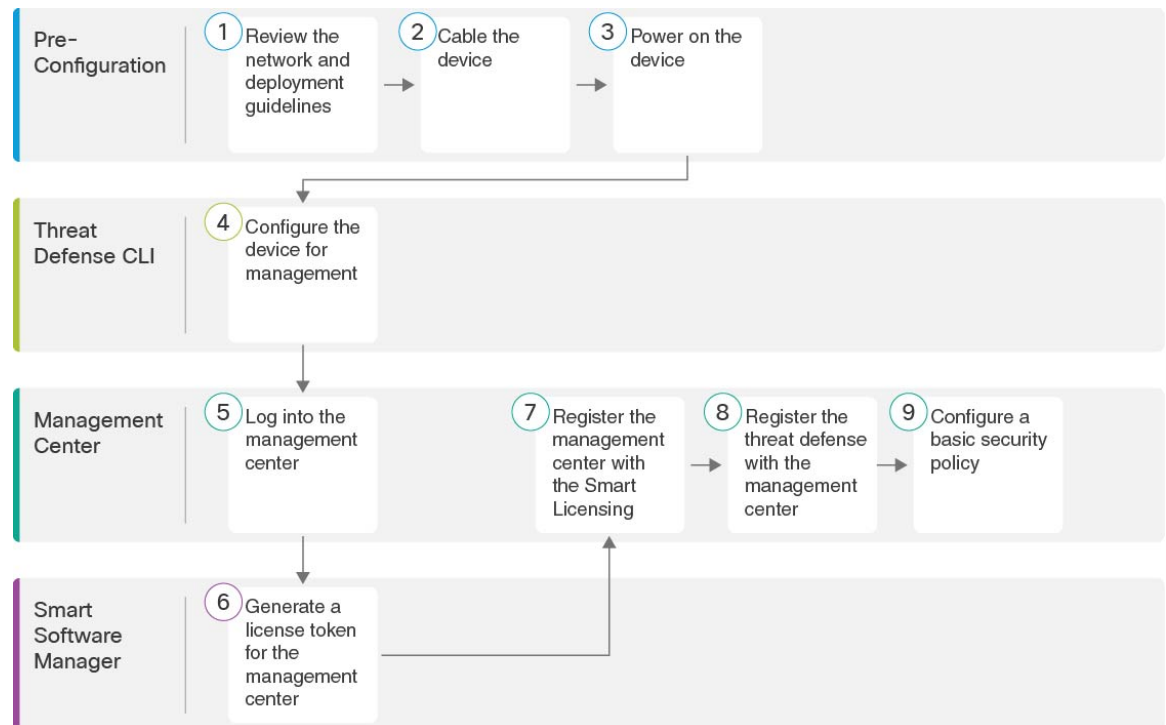
- [Threat Defense CLI へのアクセス](#) (75 ページ)
- [ファイアウォールの電源の切断](#) (75 ページ)
- [次のステップ](#) (78 ページ)

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 Management Center を使用して脅威に対する防御を展開するには、次のタスクを参照してください。



①	事前設定	ネットワーク展開の確認 (41 ページ)。
②	事前設定	デバイスの配線 (46 ページ)。
③	事前設定	デバイスの電源投入 (50 ページ)。

④	Threat Defense CLI	CLI を使用した Threat Defense 初期設定の実行の完了 (51 ページ)。
⑤	Management Center	へのログイン Management Center (57 ページ)。
⑥	Smart Software Manager	Management Center のライセンスの取得 (58 ページ) : Management Center のライセンストークンを生成します。
⑦	Management Center	Management Center のライセンスの取得 (58 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。
⑧	Management Center	Management Center への Threat Defense の登録 (59 ページ)。
⑨	Management Center	基本的なセキュリティポリシーの設定 (62 ページ)。

ネットワーク展開の確認

脅威に対する防御 は、管理1/1インターフェイスからか、または 6.7 以降ではデータインターフェイスから Management Center を使用して管理できます。デフォルトでは、Management 1/1 インターフェイスが有効になっており、IP アドレス (192.168.45.45) が設定されています。このインターフェイスは、最初に DHCP サーバーも実行します。初期設定時にマネージャとして Management Center を選択すると、DHCP サーバーは無効になります。コンソールポートでの初期セットアップ時に、管理インターフェイスと Management Center アクセス データ インターフェイスを設定できます。脅威に対する防御 を Management Center に接続した後は、他のインターフェイスを設定できます。



- (注) データインターフェイスからの Management Center アクセスには、次の制限があります。
- マネージャアクセスを有効にできるのは、1つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。
 - このインターフェイスは管理専用にはできません。
 - ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
 - PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを脅威に対する防御 と WAN モデム の間に配置する必要があります。
 - インターフェイスを配置する必要があるのはグローバル VRF のみです。
 - 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
 - SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。

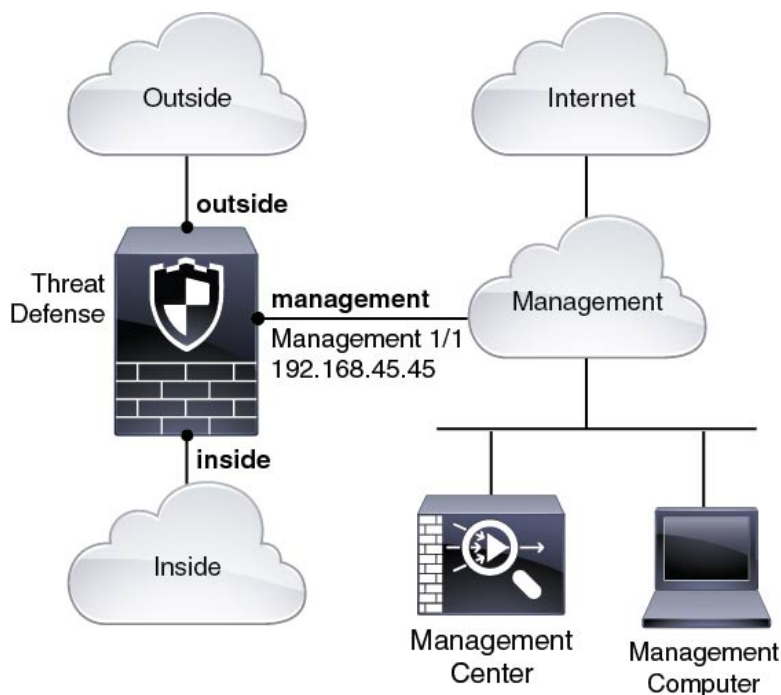
ネットワークに脅威に対する防御 デバイスを配置する方法については、次のネットワーク配置例を参照してください。

個別の管理ネットワーク

Management Center と脅威に対する防御 の両方で、ライセンスと更新を行うには管理からのインターネットアクセスが必要です。

次の図に、Management Center と管理コンピュータが管理ネットワークに接続している ISA 3000 について考えられるネットワーク展開を示します。管理ネットワークには、ライセンスと更新のためのインターネットへのパスがあります。

図 12: 個別の管理ネットワーク



6.7 以降のリモート管理展開

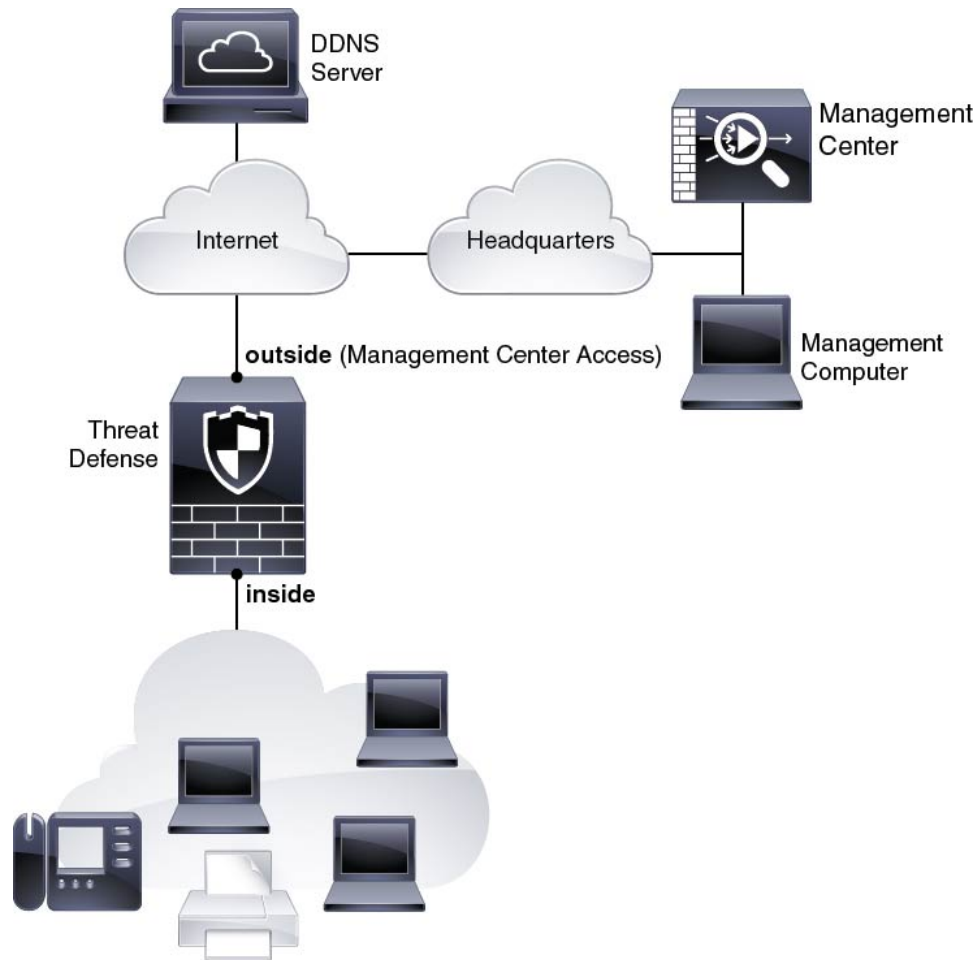


- (注) リモートブランチのセットアップでは、その展開に固有の[スタンドアロンドキュメント](#)を使用することを推奨します。

次の図に、外部インターフェイスを管理に使用した ISA 3000 向けに推奨されるネットワーク展開を示します。このシナリオは、本社から支社を管理する場合に最適です。脅威に対する防御の初期セットアップを本社で実行し、事前に設定されたデバイスを支社の場所へ送信できます。

脅威に対する防御 または Management Center のいずれかにパブリック IP アドレスまたはホスト名が必要です。DHCP を使用して脅威に対する防御でパブリック IP アドレスを受信する場合は、オプションで外部インターフェイスのダイナミック DNS (DDNS) を設定できます。DDNS は、脅威に対する防御の IP アドレスが変更された場合に Management Center が完全修飾ドメイン名 (FQDN) で脅威に対する防御に到達できるようにします。脅威に対する防御でプライベート IP アドレスを受信する場合は、Management Center にはパブリック IP アドレスまたはホスト名が必要です。

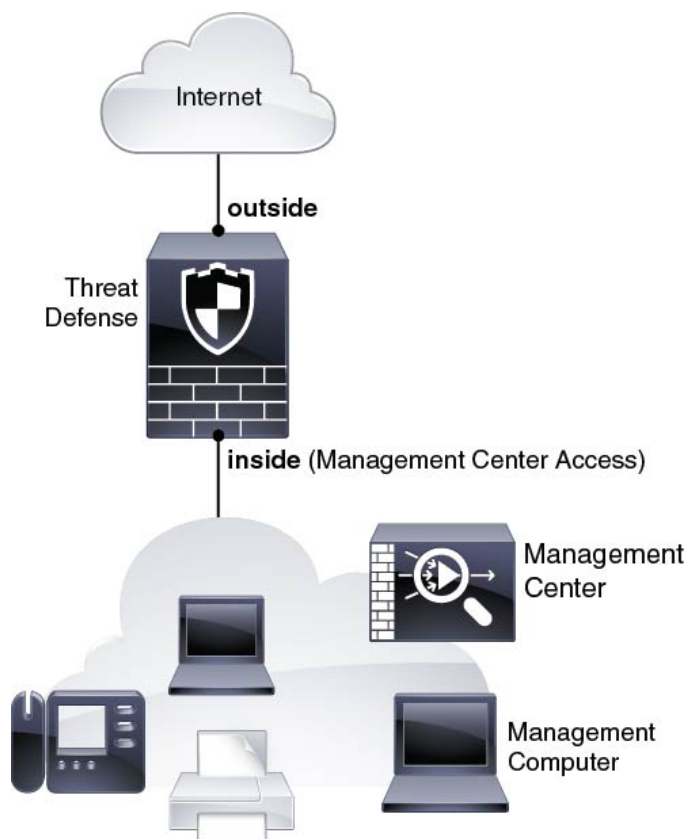
図 13: リモート管理の展開



6.7 以降の内部管理の展開

次の図に、内部インターフェイスを管理に使用した ISA 3000 向けに推奨されるネットワーク展開を示します。

図 14: 内部管理の展開



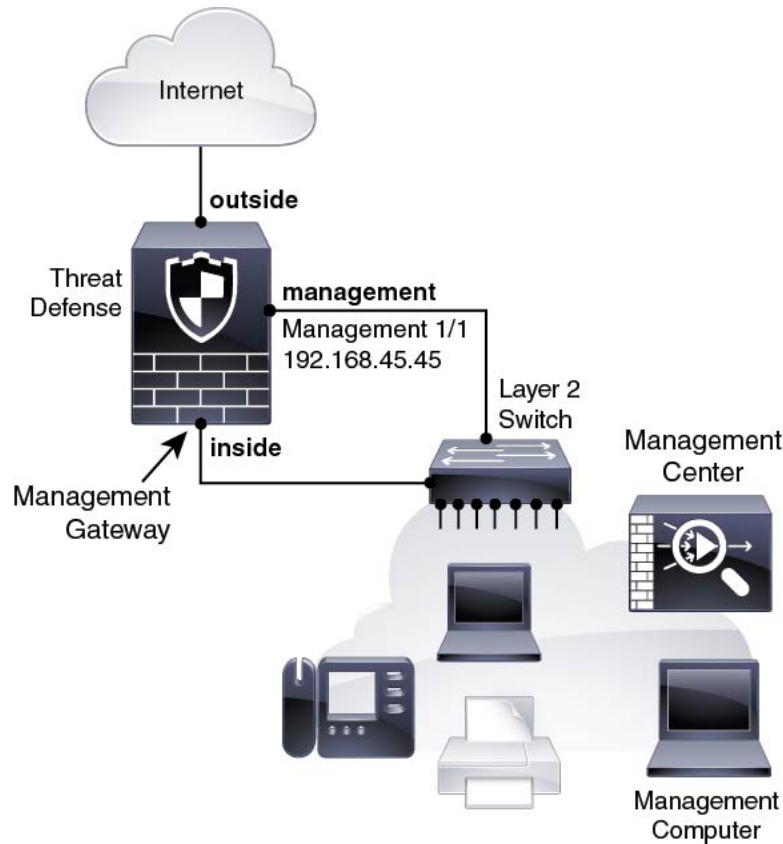
6.6 以前エッジネットワークの展開

6.6 以前では、Management Center は管理インターフェイス上の脅威に対する防御のみと通信できます。さらに、Management Center と脅威に対する防御の両方で、ライセンスと更新を行うには管理からのインターネットアクセスが必要です。

次の図は、Management Center および脅威に対する防御管理用のインターネットゲートウェイとして機能する場合の、ISA 3000 の可能なネットワーク展開を示しています。このシナリオは、たとえば 6.7 以降の高可用性展開にも使用できます。

次の図では、Management 1/1 をレイヤ 2 スイッチを介して内部のインターフェイスに接続するとともに、Management Center と管理コンピュータをスイッチに接続することにより、ISA 3000 が管理インターフェイスと Management Center のインターネットゲートウェイとして機能しています。（管理インターフェイスは脅威に対する防御上の他のインターフェイスとは別のものであるため、このような直接接続が許可されます）。

図 15: エッジネットワークの展開



デバイスの配線

ISA 3000 で推奨シナリオのいずれかに相当するケーブル接続を行うには、次の手順を参照してください。



- (注) ISA 3000 と Management Center の両方に同じデフォルトの管理 IP アドレス (192.168.45.45) が設定されています。このガイドでは、初期セットアップ時に異なる IP アドレスをデバイスに設定することを前提としています。6.5 以降の Management Center は、管理インターフェイス用の DHCP クライアントにデフォルト設定されていることに注意してください。ただし、DHCP サーバーが存在しない場合は、デフォルトで 192.168.45.45 になります。

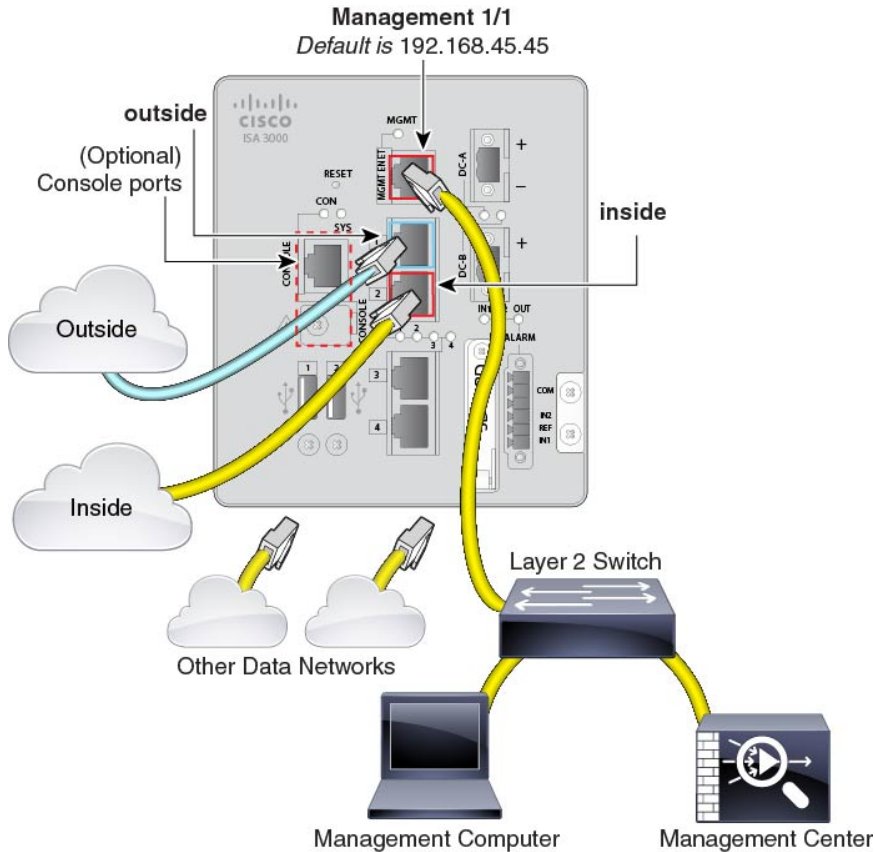


- (注) その他のトポロジも使用可能で、基本的な論理ネットワーク接続、ポート、アドレッシング、構成の要件によって導入方法が異なります。

手順

ステップ 1 別の管理ネットワーク用のケーブル配線

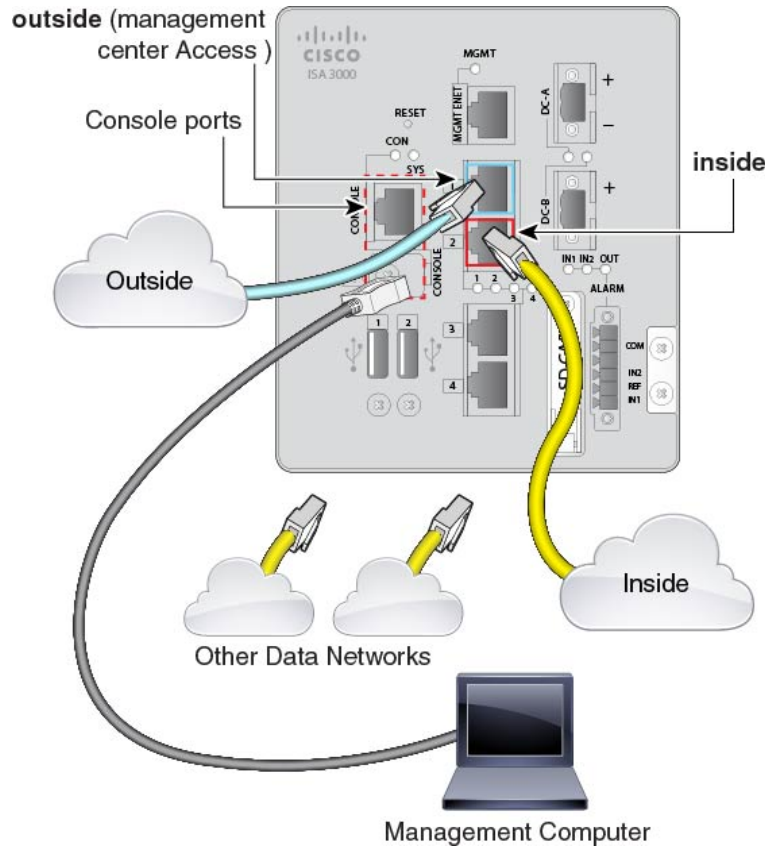
図 16: 個別の管理ネットワークのケーブル配線



- a) 次のように管理ネットワークにケーブルを配線します。
 - Management 1/1 インターフェイス
 - Management Center
 - 管理コンピュータ
- b) 管理コンピュータをコンソールポートに接続します。管理インターフェイスへの SSH を使用しない場合は、コンソールポートを使用して初期設定のために CLI にアクセスする必要があります。
- c) 内部インターフェイス (GigabitEthernet 1/2 など) を内部ルータに接続します。
- d) 外部インターフェイス (GigabitEthernet 1/1 など) を外部ルータに接続します。
- e) 残りのインターフェイスに他のネットワークを接続します。

ステップ 2 (6.7 以降) リモート管理展開のケーブル接続 :

図 17: リモート管理展開のケーブル接続



Management Center と管理コンピュータはリモートの本社にあり、脅威に対する防御にはインターネット経由で到達できます。

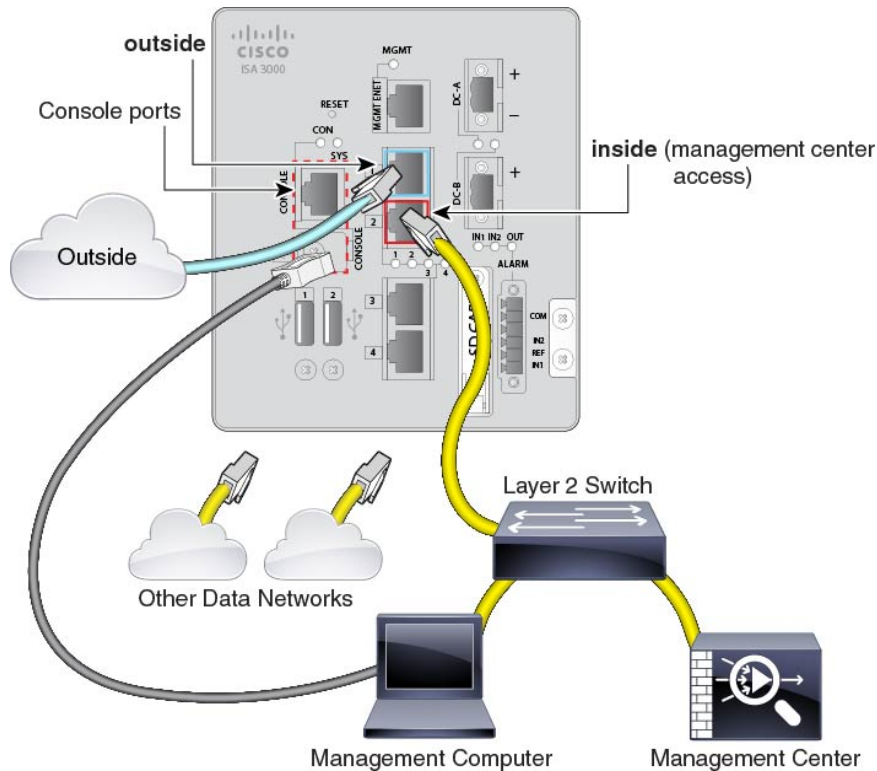
- a) 管理コンピュータをコンソールポートに接続します。コンソールポートを使用して CLI にアクセスし、初期セットアップを行う必要があります。

本社で CLI の初期セットアップを実行してから、脅威に対する防御をリモートの支社に送信できます。支社では、日常的に使用するためのコンソール接続は必要ありません。ただし、トラブルシューティングに必要な場合があります。

- b) 内部ネットワーク (GigabitEthernet 1/2 など) をケーブル接続します。
 c) 外部インターフェイス (GigabitEthernet 1/1 など) を外部ルータに接続します。
 d) 残りのインターフェイスに他のネットワークを接続します。

ステップ 3 (6.7以降) 内部管理展開のケーブル接続 :

図 18: 内部管理展開のケーブル接続

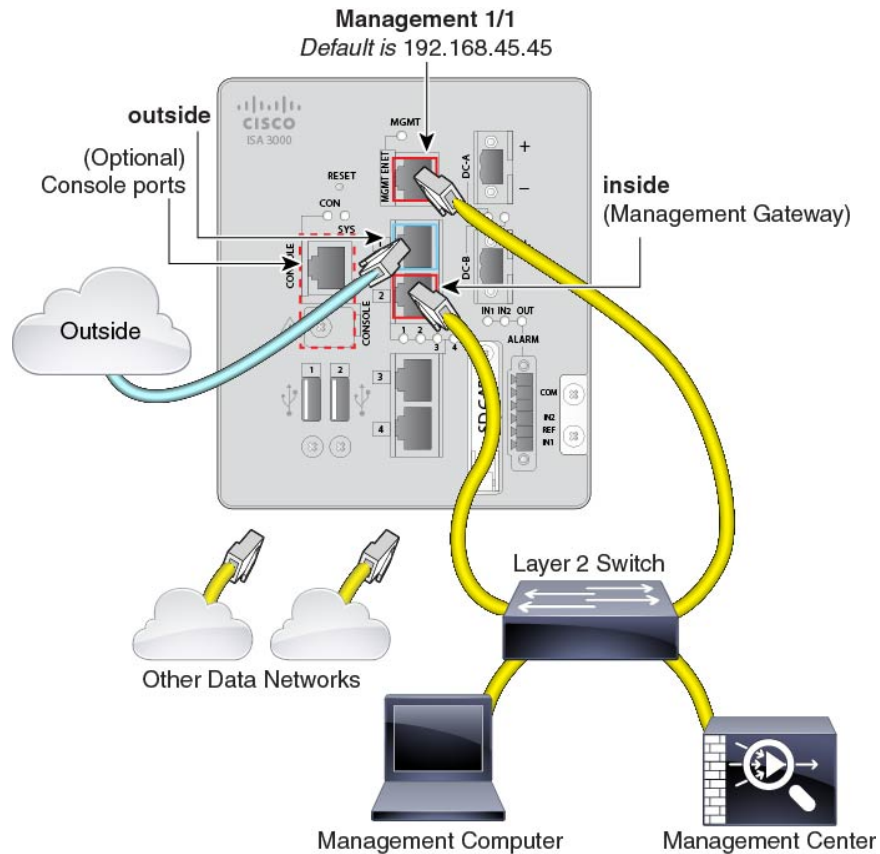


Management Center と管理コンピュータは、他の内部エンドポイントとともに内部ネットワーク上に存在します。

- a) 管理コンピュータをコンソールポートに接続します。コンソールポートを使用して CLI にアクセスし、初期セットアップを行う必要があります。
- b) 内部ネットワーク（GigabitEthernet 1/2 など）に次のケーブルを接続します。
 - Management Center
 - 管理コンピュータ
- c) 外部インターフェイス（GigabitEthernet 1/1 など）を外部ルータに接続します。
- d) 残りのインターフェイスに他のネットワークを接続します。

ステップ 4 （6.6 以降）エッジ展開用のケーブル接続。

図 19: エッジ展開のケーブル配線



- 以下の機器のケーブルをレイヤ2イーサネットスイッチに接続します。
 - 内部インターフェイス（GigabitEthernet 1/2など）
 - Management 1/1 インターフェイス
 - Management Center
 - 管理コンピュータ
- 管理コンピュータをコンソールポートに接続します。管理インターフェイスへのSSHを使用しない場合は、コンソールポートを使用して初期設定のためにCLIにアクセスする必要があります。
- 外部インターフェイス（GigabitEthernet 1/1 など）を外部ルータに接続します。
- 残りのインターフェイスに他のネットワークを接続します。

デバイスの電源投入

システムの電源は DC 電源で制御されます。電源ボタンはありません。

始める前に

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

手順

ステップ 1 電源プラグは DC 電源に配線した後に ISA 3000 に接続します。

電源プラグの正しい配線手順については、『[ハードウェア設定ガイド](#)』の「DC 電源への接続」を参照してください。

ステップ 2 ISA 3000 デバイスの前面にあるシステム LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。緑色に点滅している場合、デバイスはブートアップフェーズおよび POST（電源投入時自己診断テスト）の状態です。

すべてのデバイスが ISA 3000 に正しく接続されているか確認するには、『[ハードウェア設置ガイド](#)』の「接続の確認」を参照してください。

CLI を使用した Threat Defense 初期設定の実行の完了

脅威に対する防御 CLI に接続して初期設定を実行します。これには、セットアップウィザードを使用した管理 IP アドレス、ゲートウェイ、およびその他の基本ネットワーク設定の指定などが含まれます。専用の管理インターフェイスは、独自のネットワーク設定を持つ特別なインターフェイスです。6.7 以降：Management Center アクセスに管理インターフェイスを使用しない場合は、代わりに CLI を使用してデータインターフェイスを設定できます。また、Management Center 通信の設定を行います。

手順

ステップ 1 コンソールポートから、または管理インターフェイスへの SSH を使用して、脅威に対する防御 CLI に接続します。デフォルトで DHCP サーバーから IP アドレスが取得されます。ネットワーク設定を変更する場合は、切断されないようにコンソールポートを使用することを推奨します。

ステップ 2 ユーザー名 **admin** およびパスワード **Admin123** でログインします。

(注) パスワードがすでに変更されていて、パスワードがわからない場合は、デバイスを再イメージ化してパスワードをデフォルトにリセットする必要があります。手順については、[再イメージ化のガイド](#)を参照してください。

ステップ 3 脅威に対する防御 に初めてログインすると、エンドユーザーライセンス契約（EULA）に同意して管理者パスワードを変更するように求められます。その後、CLI セットアップスクリプトが表示されます。

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

デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

(注) 6.7以降：データインターフェイスで Management Center アクセスを有効にした場合でも、管理インターフェイスの設定が使用されます。たとえば、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ルーティングされる管理トラフィックは、データインターフェイス DNS サーバーではなく、管理インターフェイス DNS サーバーを使用して FQDN を解決します。

次のガイドラインを参照してください。

- [DHCP経由または手動でIPv4を設定しますか? (Configure IPv4 via DHCP or manually?)] : 6.7以降：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 Management Center アクセスに使用する場合は、[手動 (manual)] を選択します。管理インターフェイスを使用する予定がない場合でも、プライベートアドレスなどの IP アドレスを設定する必要があります。管理インターフェイスが DHCP に設定されている場合、管理用のデータインターフェイスを設定することはできません。これは、**data-interfaces** である必要があるデフォルトルートが DHCP サーバーから受信したルートで上書きされる可能性があるためです。
- [管理インターフェイスのIPv4デフォルトゲートウェイを入力 (Enter the IPv4 default gateway for the management interface)] : 6.7以降：管理インターフェイスの代わりに Management Center アクセスにデータインターフェイスを使用する場合は、ゲートウェイを [data-interfaces] に設定します。この設定は、Management Center アクセス データインターフェイスを通じてルーティングできるように、バックプレーンを介して管理トラフィックを転送します。Management Center アクセスに管理インターフェイスを使用する場合は、Management 1/1 ネットワークでゲートウェイ IP アドレスを設定する必要があります。
- ネットワーク情報が変更された場合は再接続が必要：SSH で接続しているのに、初期セットアップでその IP アドレスを変更すると、接続が切断されます。新しい IP アドレスとパスワードで再接続してください。コンソール接続は影響を受けません。
- [デバイスをローカルで管理しますか (Manage the device locally?)] : Management Center を使用するには「no」を入力します。yes と入力すると、代わりに Device Manager を使用することになります。
- [ファイアウォールモードを設定しますか (Configure firewall mode?)] : 初期設定でファイアウォールモードを設定することをお勧めします。初期設定後にファイアウォールモードを変更すると、実行コンフィギュレーションが消去されます。データインターフェイス Management Center アクセスは、ルーテッドファイアウォールモードでのみサポートされることに注意してください。

例 :

```

You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: *****
Confirm new password: *****
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>

```

ステップ 4 この脅威に対する防御 を管理する Management Center を特定します。

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

- {hostname | IPv4_address | IPv6_address | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the Management Center. Management Center を直接アドレス指定できない場合は、

DONTRESOLVE を使用します。また、*nat_id* も指定します。双方向の SSL 暗号化通信チャンネルを2台のデバイス間に確立するには、少なくとも1台以上のデバイス（Management Center または 脅威に対する防御）に到達可能な IP アドレスが必要です。このコマンドで **DONTRESOLVE** を指定するには、到達可能な IP アドレスまたはホスト名が 脅威に対する防御 に必要です。

- *reg_key* : 脅威に対する防御 を登録するときに Management Center でも指定する任意のワントタイム登録キーを指定します。登録キーは 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン (-) があります。
- *nat_id* : 一方の側で到達可能な IP アドレスまたはホスト名が指定されていない場合は、脅威に対する防御 を登録するときに Management Center にも指定する任意の一意的ワントタイム文字列を指定します。この文字列は、Management Center を **DONTRESOLVE** に設定した場合に必要です。NAT ID は 37 文字以下にする必要があります。有効な文字には、英数字（A～Z、a～z、0～9）、およびハイフン (-) があります。この ID は、Management Center に登録する他のデバイスには使用できません。

(注) 管理にデータインターフェイスを使用する場合は、登録用に脅威に対する防御と Management Center の両方で NAT ID を指定する必要があります。

例 :

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

Management Center が NAT デバイスの背後にある場合は、次の例に示すように、一意的 NAT ID とともに登録キーを入力し、ホスト名の代わりに **DONTRESOLVE** を指定します。

例 :

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

脅威に対する防御 が NAT デバイスの背後にある場合は、次の例に示すように、一意的 NAT ID とともに Management Center IP アドレスまたはホスト名を入力します。

例 :

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

ステップ 5 (任意) (6.7以降) Management Center アクセス用のデータインターフェイスを設定します。

configure network management-data-interface

その後、データインターフェイスの基本的なネットワーク設定を行うように求めるプロンプトが表示されます。

- (注) このコマンドを使用する場合は、コンソールポートを使用する必要があります。管理インターフェイスに SSH を使用すると、接続が切断され、コンソールポートに再接続する必要がある場合があります。SSH の詳細な使用方法については、次を参照してください。

このコマンドの使用については、次の詳細を参照してください。

- データインターフェイスを管理に使用する場合、元の管理インターフェイスは DHCP を使用できません。初期セットアップ時に IP アドレスを手動で設定しなかった場合は、**configure network {ipv4|ipv6} manual** コマンドを使用して設定できるようになりました。管理インターフェイスゲートウェイを **data-interfaces** に設定しなかった場合は、ここでこのコマンドで設定します。
- データインターフェイスからの Management Center アクセスには、次の制限があります。
 - マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスと EtherChannel は使用できません。
 - このインターフェイスは管理専用にできません。
 - ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
 - PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを脅威に対する防御 と WAN モデム の間に配置する必要があります。
 - インターフェイスを配置する必要があるのはグローバル VRF のみです。
 - 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
 - SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイスゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。
- 脅威に対する防御 を Management Center に追加すると、Management Center はインターフェイス設定（インターフェイス名と IP アドレス、ゲートウェイへの静的ルート、DNS サーバー、DDNS サーバーなど）を検出して維持します。DNS サーバー設定の詳細については、次を参照してください。Management Center では、後で Management Center アクセスインターフェイス設定を変更できますが、脅威に対する防御 または Management Center が管理接続による再確立を妨げるような変更を加えないようにしてください。管理接続が中断された場合、脅威に対する防御 には以前の展開を復元する **configure policy rollback** コマンドが含まれます。
- DDNS サーバー更新の URL を設定すると、脅威に対する防御 は Cisco Trusted Root CA バンドルからすべての主要 CA の証明書を自動的に追加するため、脅威に対する防御 は HTTPS 接続の DDNS サーバー証明書を検証できます。脅威に対する防御 は、DynDNS リモート API 仕様 (<https://help.dyn.com/remote-access-api/>) を使用するすべての DDNS サーバーをサポートします。
- このコマンドは、「データ」インターフェイス DNS サーバーを設定します。セットアップスクリプトで（または **configure network dns servers** コマンドを使用して）設定した管

理 DNS サーバーは、管理トラフィックに使用されます。データ DNS サーバーは、DDNS（設定されている場合）またはこのインターフェイスに適用されるセキュリティポリシーに使用されます。

Management Center では、この脅威に対する防御に割り当てるプラットフォーム設定ポリシーでデータインターフェイス DNS サーバーが設定されます。Management Center に脅威に対する防御を追加すると、ローカル設定が維持され、DNS サーバーはプラットフォーム設定ポリシーに追加されません。ただし、DNS 設定を含む脅威に対する防御に後でプラットフォーム設定ポリシーを割り当てると、その設定によってローカル設定が上書きされます。Management Center と脅威に対する防御を同期させるには、この設定に一致するように DNS プラットフォーム設定をアクティブに設定することをお勧めします。

また、ローカル DNS サーバーは、DNS サーバーが初期登録で検出された場合にのみ Management Center で保持されます。たとえば、管理インターフェイスを使用してデバイスを登録し、後で **configure network management-data-interface** コマンドを使用してデータインターフェイスを設定した場合、脅威に対する防御設定と一致するように、DNS サーバーを含むこれらの設定のすべてを Management Center で手動で設定する必要があります。

- 管理インターフェイスは、脅威に対する防御を Management Center に登録した後に、管理インターフェイスまたは別のデータインターフェイスのいずれかに変更できます。
- セットアップウィザードで設定した FQDN がこのインターフェイスに使用されます。
- コマンドの一部としてデバイス設定全体をクリアできます。このオプションはリカバリシナリオで使用できますが、初期セットアップや通常操作には使用しないでください。
- データ管理を無効にするには、**configure network management-data-interface disable** コマンドを入力します。

例：

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

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

Setting IPv4 network configuration.
Network settings changed.
```

>

例：

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
```

```
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

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

Setting IPv4 network configuration.
Network settings changed.

>
```

ステップ 6 (任意) (6.7 以降) 特定のネットワーク上の Management Center へのデータ インターフェイス アクセスを制限します。

configure network management-data-interface client ip_address netmask

デフォルトでは、すべてのネットワークが許可されます。

次のタスク

デバイスを Management Center に登録します。

へのログインManagement Center

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。

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

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

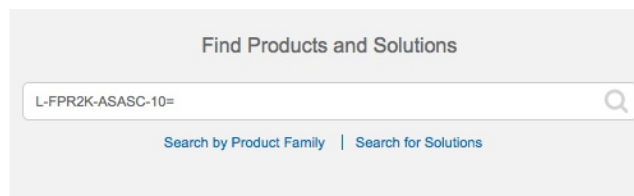
- **Smart Software Manager** にマスターアカウントを持ちます。
まだアカウントをお持ちでない場合は、リンクをクリックして**新しいアカウントを設定**してください。Smart Software Manager では、組織のマスターアカウントを作成できます。
- (輸出コンプライアンスフラグを使用して有効化される) 機能を使用するには、ご使用のスマートソフトウェアライセンシングアカウントで強力な暗号化 (3DES/AES) ライセンスを使用できる必要があります。

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 20: 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。

- 脅威、マルウェア、および URL ライセンスの組み合わせ：

- L-ISA3000T-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-ISA3000T-TMC-1Y
- L-ISA3000T-TMC-3Y
- L-ISA3000T-TMC-5Y

- RA VPN : 『[Cisco Secure Client 発注ガイド](#)』を参照してください。

ステップ 2 まだ設定していない場合は、スマートライセンスサーバーに 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

デバイスの IP アドレスかホスト名を使用して、手動で Threat Defense を Management Center に登録します。

始める前に

- Threat Defense の最初の設定で設定した次の情報を収集します。
 - 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

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。

Add Device ?

Host:†

Display Name:

Registration Key:†*

Group:

Access Control Policy:†*

Smart Licensing

Malware

Threat

URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

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 の最初の設定で指定したものと同一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 \(72 ページ\)](#)」を参照してください。

図 21 : New Policy

The screenshot shows the 'New Policy' configuration interface. It includes the following elements:

- Name:** A text input field containing 'ftd-ac-policy'.
- Description:** An empty text input field.
- Select Base Policy:** A dropdown menu currently set to 'None'.
- Default Action:** Three radio button options:
 - Block all traffic (highlighted with a red box)
 - Intrusion Prevention
 - Network Discovery
- Buttons:** 'Cancel' and 'Save' buttons located at the bottom right of the form area.

- [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 AnyConnect 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。

- 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 (63 ページ) 。
②	DHCP サーバーの設定 (66 ページ) 。

3	デフォルトルートの追加 (67 ページ)。
4	NAT の設定 (69 ページ)。
5	内部から外部へのトラフィックの許可 (72 ページ)。
6	設定の展開 (73 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。

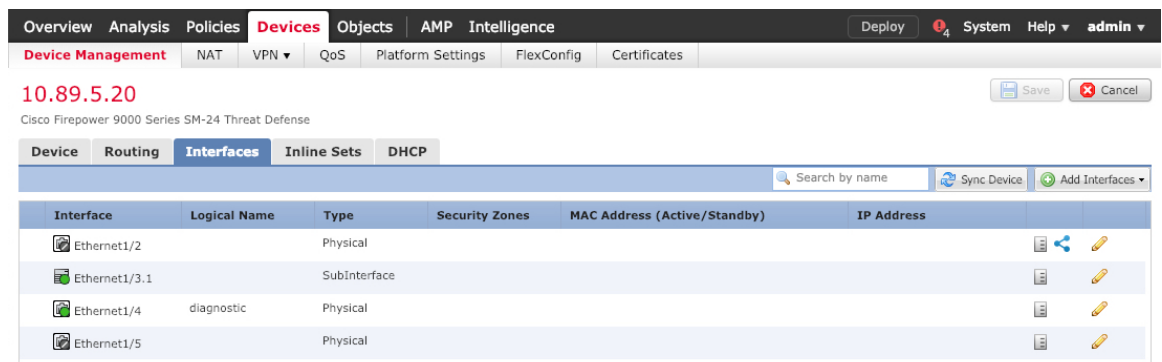
一般的なエッジルーティングの状況は、内部インターフェイスでスタティックアドレスを定義すると同時に、ISP から DHCP を介して外部インターフェイスアドレスを取得することです。

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。

The screenshot shows the 'Edit Physical Interface' dialog box with the following configuration:

- Name: inside
- Description: (empty)
- Mode: None
- Security Zone: inside_zone
- Interface ID: GigabitEthernet0/0
- MTU: 1500 (range 64 - 9000)
- Enabled: Management Only:

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

- [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。

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: Use Static IP

IP Address: 192.168.1.1/24 eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

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

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。

Edit Physical Interface ? x

General **IPv4** IPv6 Advanced Hardware Configuration

Name: outside Enabled Management Only

Description:

Mode: None

Security Zone: outside_zone

Interface ID: GigabitEthernet0/0

MTU: 1500 (64 - 9000)

OK Cancel

(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。

The screenshot shows the 'Edit Physical Interface' configuration window with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use DHCP'. Below it, the 'Obtain default route using DHCP' checkbox is checked. The 'DHCP route metric' is set to '1' in a text input field, with '(1 - 255)' indicating the valid range.

- [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。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy 4 System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

10.99.5.20 You have unsaved changes Save Cancel

Cisco Firepower 9000 Series SM-24 Threat Defense

Device Routing Interfaces Inline Sets DHCP

- OSPF
- OSPFv3
- RIP
- ▶ BGP
- ▶ **Static Route**
- ▶ Multicast Routing

Network	Interface	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes					
any-ipv4	outside	10.99.10.1	false	1	
▼ IPv6 Routes					

Add Route

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。

New Policy ? X

Name:

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

192.168.0.16

Selected Devices

192.168.0.16

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 (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。

Add NAT Rule

NAT Rule:

Type: Enable

- [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。

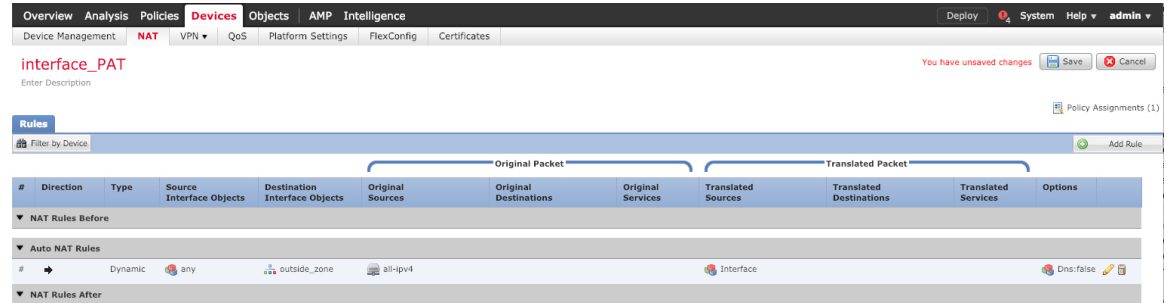
- [元の送信元 (Original Source)] : をクリックして、すべてのIPv4トラフィック (0.0.0.0/0) のネットワークオブジェクトを追加します。

- (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。

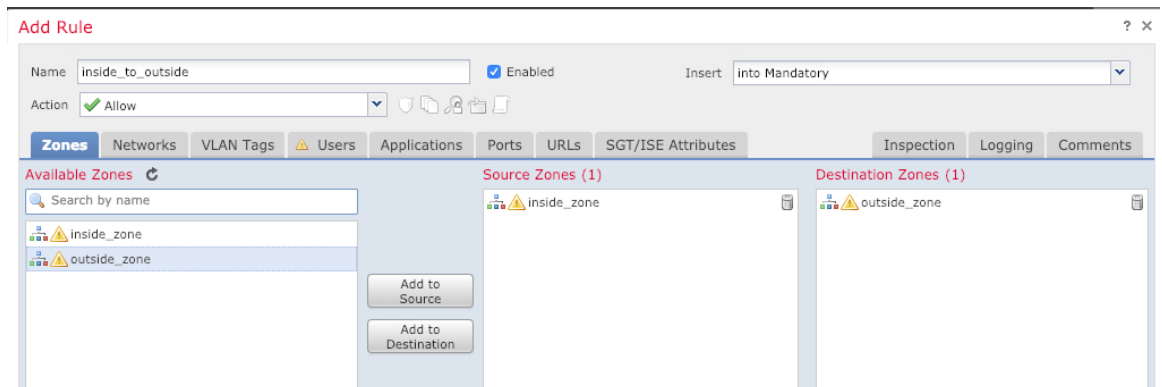
内部から外部へのトラフィックの許可

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。

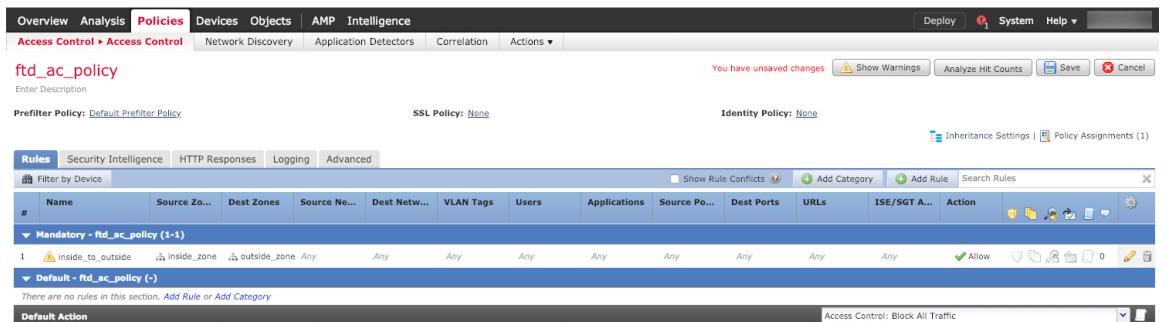


- [名前 (Name)] : このルールに名前を付けます (たとえば、**inside_to_outside**) 。
- [送信元ゾーン (Source Zones)] : [使用可能なゾーン (Available Zones)] から内部ゾーンを選択し、[送信元に追加 (Add to Source)] をクリックします。
- [宛先ゾーン (Destination Zones)] : [使用可能なゾーン (Available Zones)] から外部ゾーンを選択し、[宛先に追加 (Add to Destination)] をクリックします。

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。

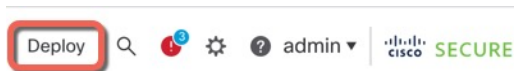
設定の展開

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 22: [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 23: すべて展開

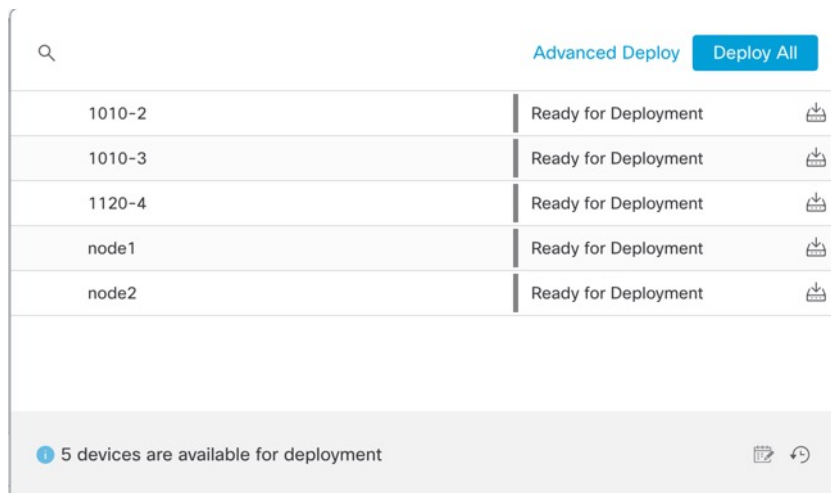


図 24: 高度な展開

1 device selected

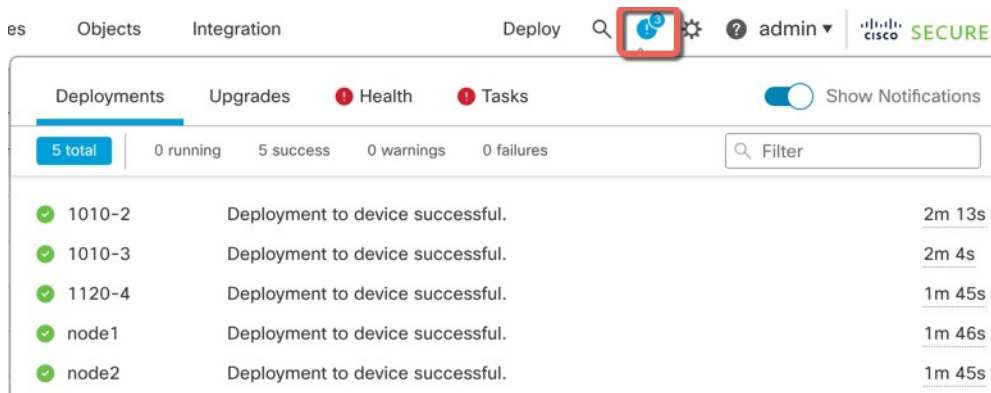
Search using device name, user name, type, group or status

Deploy time: Estimate Deploy

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
<input checked="" type="checkbox"/> node1	System		FTD		May 23, 2022 6:49 PM	📄	Ready for Deployment
<input type="checkbox"/> 1010-2	admin, System		FTD		May 23, 2022 7:09 PM	📄	Ready for Deployment
<input type="checkbox"/> node2	System		FTD		May 23, 2022 6:49 PM	📄	Ready for Deployment
<input type="checkbox"/> 1010-3	System		FTD		May 23, 2022 6:49 PM	📄	Ready for Deployment
<input type="checkbox"/> 1120-4	System		FTD		May 23, 2022 6:49 PM	📄	Ready for Deployment

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 25: 展開ステータス



Threat Defense CLI へのアクセス

コマンドラインインターフェイス (CLI) を使用してシステムのセットアップを行い、基本的なシステムのトラブルシューティングを行います。CLI セッションからポリシーを設定することはできません。CLI には、コンソールポートに接続してアクセスできます。

脅威に対する防御 デバイスの管理インターフェイスに SSH で接続できます。SSH 接続用のインターフェイスを開いている場合、データインターフェイス上のアドレスにも接続できます。データインターフェイスへの SSH アクセスはデフォルトで無効になっています。

手順

ステップ 1 CLI にログインして、管理コンピュータをコンソールポート、RJ-45 ポート、ミニ USB ポートのいずれかに接続します。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください。次のシリアル設定を使用します。

- 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 2 ユーザー名 **admin**、および初期セットアップ時に設定したパスワードを使用して脅威に対する防御 CLI にログインします (デフォルトは **Admin123**)。

ログイン後に、CLI で使用可能なコマンドの情報を確認するには、**help** または **?** を入力します。使用法の詳細については、『[Cisco Firepower Threat Defense Command Reference](#)』を参照してください。

ファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されており、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールシステムをグレースフルシャットダウンできないことを覚えておいてください。

ISA 3000 シャーシには、外部電源スイッチはありません。Management Center のデバイス管理ページを使用してデバイスの電源を切断するか、CLI を使用できます。

Management Center を使用したファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたり、電源スイッチを押したりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されていて、電源プラグを抜いたり、電源を切断したりすると、ファイアウォールをグレースフルシャットダウンできないことを覚えておいてください。



(注) シャットダウンは 7.0.2+/7.2+ でサポートされています。

Management Center を使用してシステムを適切にシャットダウンできます。

手順

ステップ 1 [Devices] > [Device Management] を選択します。

ステップ 2 再起動するデバイスの横にある編集アイコン (✎) をクリックします。

ステップ 3 [デバイス (Device)] タブをクリックします。

ステップ 4 [システム (System)] セクションでデバイスのシャットダウンアイコン (🔴) をクリックします。

ステップ 5 プロンプトが表示されたら、デバイスのシャットダウンを確認します。

ステップ 6 シャットダウンプロセスをモニターします。デバイスを監視できない場合は、約3分間待ってシステムがシャットダウンしたことを確認します。

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

```
Firepower Threat Defense is stopped.
It is safe to power off now.
```

```
To restart the device, you must Power cycle to the device.
```

ステップ 7 必要に応じて電源プラグを抜いてシャーシから物理的に電源を取り外すことができます。

CLI におけるファイアウォールの電源の切断

システムを適切にシャットダウンすることが重要です。単純に電源プラグを抜いたりすると、重大なファイルシステムの損傷を引き起こすことがあります。バックグラウンドでは常に多数のプロセスが実行されており、電源プラグを抜いたり、電源を切断したりすると、システムをグレースフルシャットダウンできないことを覚えておいてください。ISA 3000 シャーシには、外部電源スイッチはありません。



(注) シャットダウンは 7.0.2+/7.2+ でサポートされています。

手順

ステップ 1 コンソールポートに接続して脅威に対する防御 CLI にアクセスし、脅威に対する防御 をシャットダウンします。

shutdown

例 :

```
> shutdown
This command will shutdown the system. Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense.....ok
Shutting down sfid... [ OK ]
Clearing static routes
Unconfiguring default route [ OK ]
Unconfiguring address on br1 [ OK ]
Unconfiguring IPv6 [ OK ]
Downing interface [ OK ]
Stopping xinetd:
Stopping nsd... [ OK ]
Stopping system log daemon... [ OK ]
Stopping Threat Defense ...
Stopping system message bus: dbus. [ OK ]
Un-mounting disk partitions ...
device-mapper: remove ioctl on root failed: Device or resource busy
[...]
mdadm: Cannot get exclusive access to /dev/md0:Perhaps a running process, mounted
filesystem or active volume group?
Stopping OpenBSD Secure Shell server: sshd
stopped /usr/sbin/sshd (pid 3520)
done.
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid
3525)
acpid.
Stopping system message bus: dbus.
Stopping internet superserver: xinetd.
no /etc/sysconfig/kdump.conf
Deconfiguring network interfaces... ifdown: interface br1 not configured
done.
SSP-Security-Module is shutting down ...
Sending ALL processes the TERM signal ...
acpid: exiting
Sending ALL processes the KILL signal ...
Deactivating swap...
Unmounting local filesystems...

Firepower Threat Defense stopped.
It is safe to power off now.

To restart the device, you must Power cycle to the device.
```

ステップ2 脅威に対する防御 がシャットダウンし、コンソールに「今すぐに電源をオフにする」と表示された場合は、必要に応じて電源を抜いてシャーシから電源を物理的に取り外します。

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 Configuration Guide](#)」を参照してください。



第 4 章

ASDM を使用した ASA の展開

この章の対象読者

Cisco ISA 3000 は、強力なラックマウント型のファイアウォールです。この章では、ネットワークに ISA 3000 ASA を展開する方法と初期設定の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。

- フェールオーバー
- CLI 設定
- (9.16 以前) FirePOWER モジュール

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。

ISA 3000 ハードウェアでは、ASA ソフトウェアか脅威に対する防御 ソフトウェアを実行できます。ASA と脅威に対する防御 と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。「[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。

プライバシー収集ステートメント：ISA 3000 には個人識別情報は不要です。積極的に収集することはありません。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。

- [ASA について \(80 ページ\)](#)
- [エンドツーエンドの手順 \(80 ページ\)](#)
- [ネットワーク配置とデフォルト設定の確認 \(82 ページ\)](#)
- [ファイアウォールのケーブル接続 \(85 ページ\)](#)
- [デバイスの電源投入 \(86 ページ\)](#)
- [\(任意\) IP アドレスの変更 \(86 ページ\)](#)
- [ASDM へのログイン \(87 ページ\)](#)
- [\(任意\) ASA ライセンスの設定 \(88 ページ\)](#)
- [ASA の設定 \(90 ページ\)](#)
- [ASA CLI へのアクセス \(91 ページ\)](#)

- [次のステップ \(92 ページ\)](#)

ASA について

ASA は、1 つのデバイスで高度でステートフルなファイアウォール機能および VPN コンセントレーター機能を提供します。

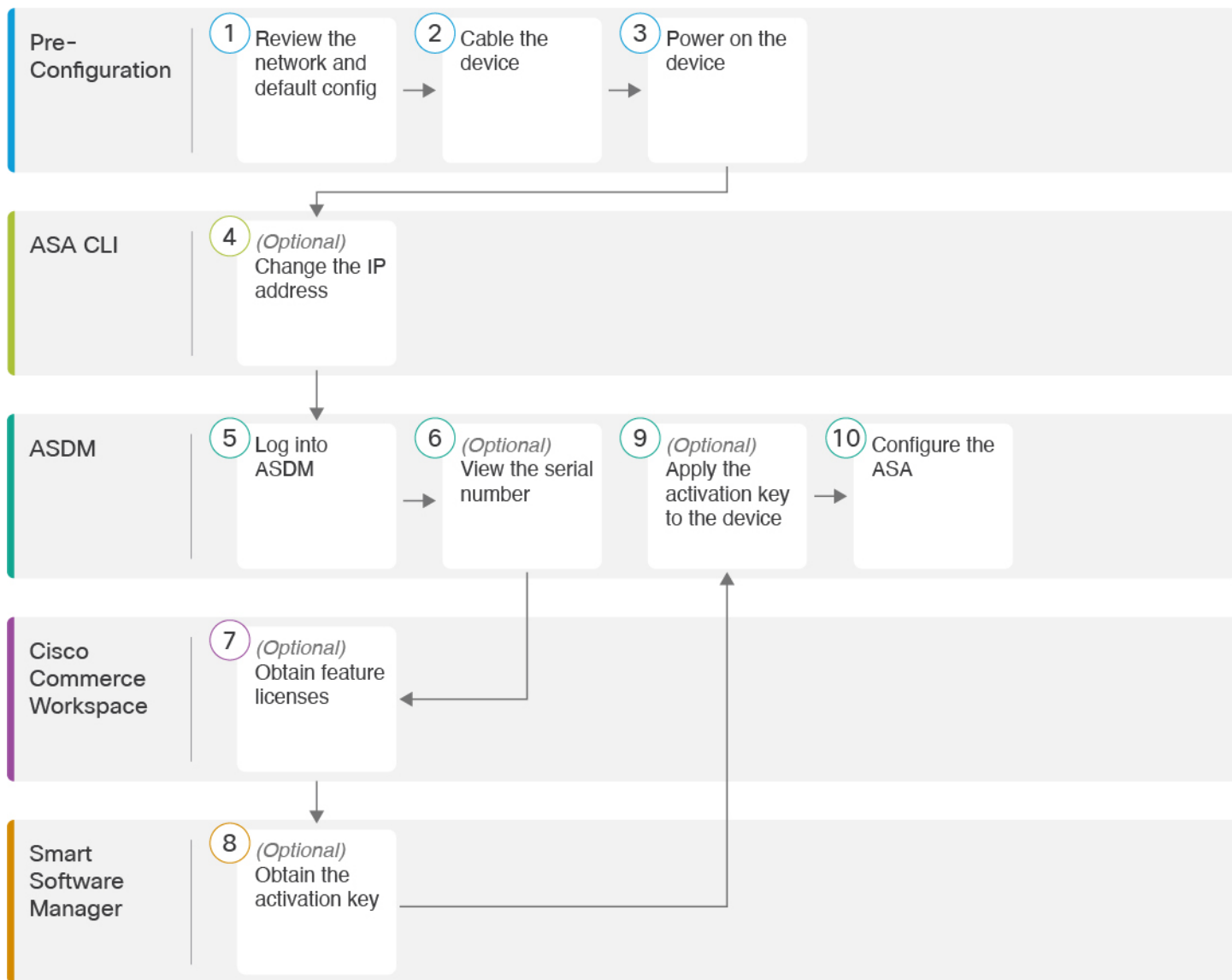
次のいずれかのマネージャを使用して ASA を管理できます。

- ASDM (このガイドで説明) : デバイスに含まれる単独のデバイスマネージャ。
- CLI
- CDO : 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。
- Cisco Security Manager : 別のサーバー上のマルチデバイス マネージャ。

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。

図 26: エンドツーエンドの手順



①	事前設定	ネットワーク配置とデフォルト設定の確認 (82 ページ)。
②	事前設定	ファイアウォールのケーブル接続 (85 ページ)。
③	事前設定	デバイスの電源投入 (86 ページ)。
④	ASA CLI	(任意) IP アドレスの変更 (86 ページ)。
⑤	ASDM	ASDM へのログイン (87 ページ)。

6	ASDM	(任意) ASA ライセンスの設定 (88 ページ) : シリアル番号を表示します。
7	Cisco Commerce Workspace	(任意) ASA ライセンスの設定 (88 ページ) : 機能ライセンスを取得します。
8	Smart Software Manager	(任意) ASA ライセンスの設定 (88 ページ) : アクティベーションキーを取得します。
9	ASDM	(任意) ASA ライセンスの設定 (88 ページ) : アクティベーションキーをデバイスへ適用します。
10	ASDM	ASA の設定 (90 ページ) 。

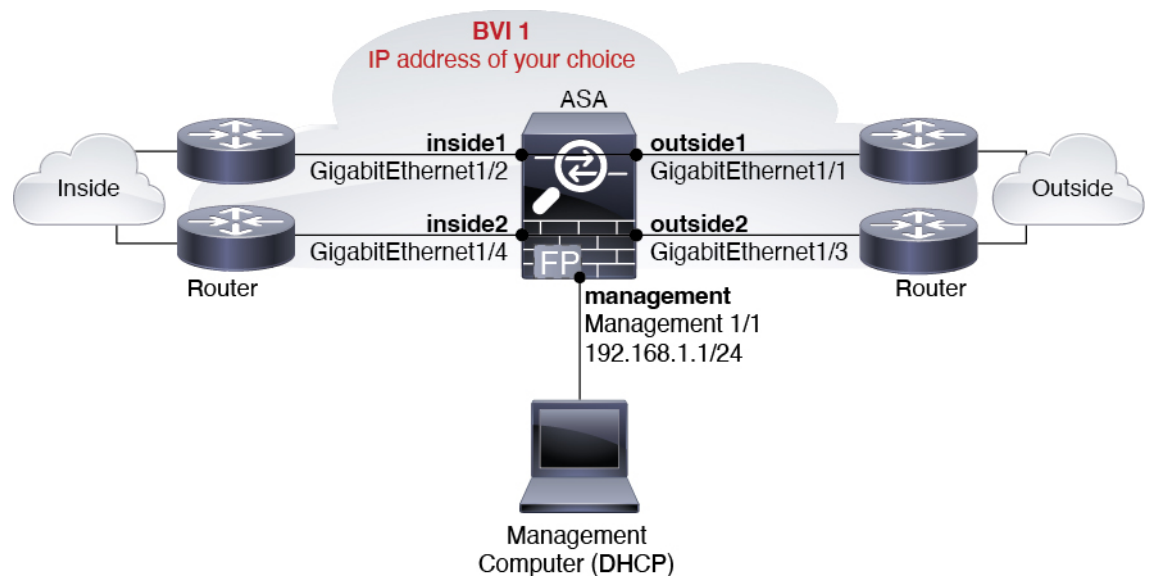
ネットワーク配置とデフォルト設定の確認

次の図に、ISA 3000 で推奨されるネットワーク展開を示します。



(注) ASDM アクセスにデフォルト管理 IP アドレスを使用できない場合は、ASA CLI で管理 IP アドレスを設定できます。「(任意) IP アドレスの変更 (86 ページ)」を参照してください。

図 27: ISA 3000 ネットワーク



ISA 3000 のデフォルト設定

ISA 3000 の工場出荷時のデフォルト設定は、次のとおりです。

- **トランスペアレントファイアウォールモード**：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」のように動作するレイヤ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。
- **1ブリッジ仮想インターフェイス**：すべてのメンバーインターフェイスは同じネットワーク内に存在しています（IPアドレスは事前設定されていません。ネットワークと一致するように設定する必要があります）：GigabitEthernet 1/1（outside1）、GigabitEthernet 1/2（inside1）、GigabitEthernet 1/3（outside2）、GigabitEthernet 1/4（inside2）
- すべての内部および外部インターフェイスは相互通信できます。
- **管理 1/1** インターフェイス：ASDM アクセスの 192.168.1.1/24。
- 管理上のクライアントに対する **DHCP**。
- **ASDM** アクセス：管理ホストに許可されます。
- **ハードウェアバイパス**は、次のインターフェイスペアで有効になっています。GigabitEthernet 1/1 および 1/2。GigabitEthernet 1/3 および 1/4



(注) ISA 3000 への電源が切断され、ハードウェアバイパスモードに移行すると、通信できるのは上記のインターフェイスペアのみになります。inside1 と inside2 および outside1 と outside2 は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。電源が再投入されると、ASAがフローを引き継ぐため、接続が短時間中断されます。

このコンフィギュレーションは次のコマンドで構成されています。

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
```

```
nameif inside2
security-level 100
no shutdown
interface Management1/1
management-only
no shutdown
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
interface BVI1
no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

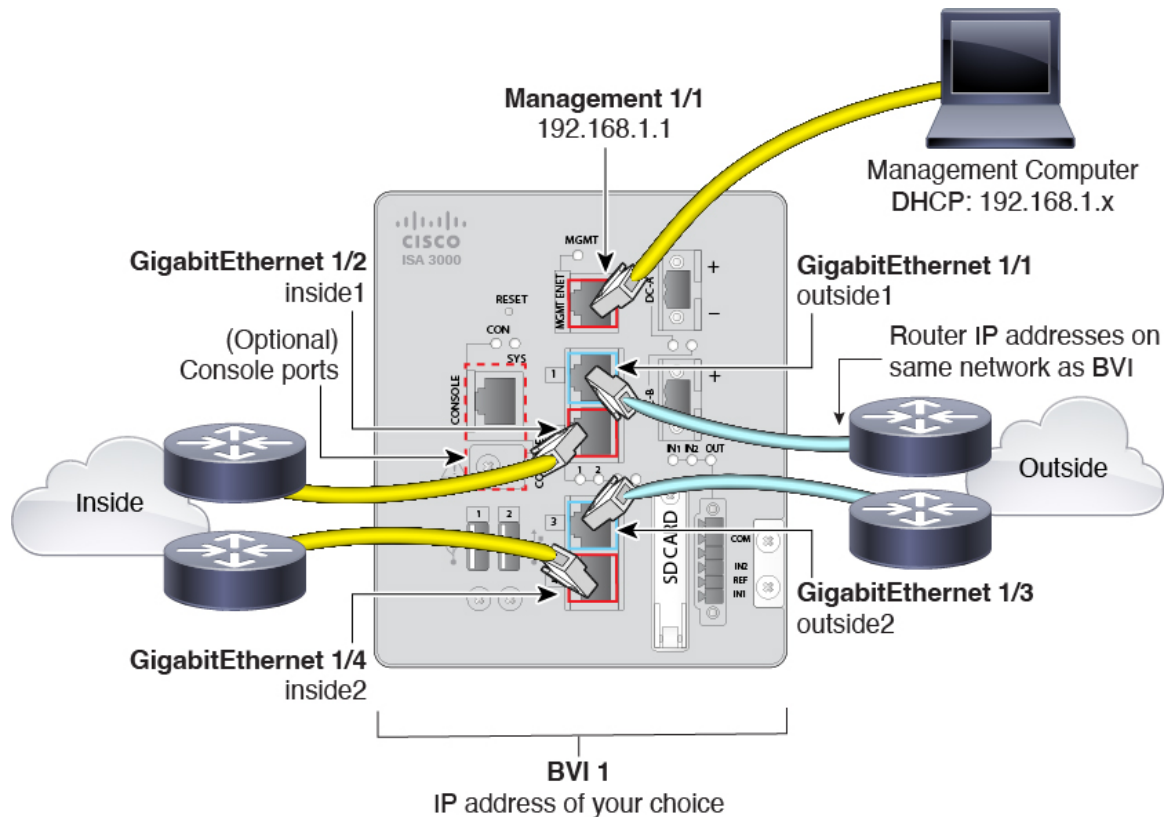
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management
```

ファイアウォールのケーブル接続

図 28: ファイアウォールのケーブル接続



Management 1/1 インターフェイスで ISA 3000 を管理します。

手順

ステップ 1 GigabitEthernet 1/1 を外部ルータに接続し、GigabitEthernet 1/2 を内部ルータに接続します。

これらのインターフェイスによってハードウェアバイパスペアが形成されます。

ステップ 2 GigabitEthernet 1/3 を冗長外部ルータに接続し、GigabitEthernet 1/4 を冗長内部ルータに接続します。

これらのインターフェイスによってハードウェアバイパスペアが形成されます。これらのインターフェイスは、他方のペアで障害が発生した場合に冗長ネットワークパスを提供します。これら 4 つのデータインターフェイスはすべて、選択した同じネットワーク上に存在します。BVI1 の IP アドレスを、内部ルータおよび外部ルータと同じネットワーク上に配置するように設定する必要があります。

ステップ 3 Management 1/1 を管理コンピュータ（またはネットワーク）に接続します。

ステップ 4 (任意) 管理コンピュータをコンソールポートに接続します。

管理 IP アドレスをデフォルトから変更する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「[\(任意\) IP アドレスの変更 \(86 ページ\)](#)」を参照してください。

デバイスの電源投入

システムの電源は DC 電源で制御されます。電源ボタンはありません。

手順

ステップ 1 電源プラグは DC 電源に配線した後に ISA 3000 に接続します。

電源プラグの正しい配線手順については、『[ハードウェア設定ガイド](#)』の「DC 電源への接続」を参照してください。

ステップ 2 ISA 3000 デバイスの前面にあるシステム LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。緑色に点滅している場合、デバイスはブートアップフェーズおよび POST (電源投入時自己診断テスト) の状態です。

すべてのデバイスが ISA 3000 に正しく接続されているか確認するには、『[ハードウェア設置ガイド](#)』の「接続の確認」を参照してください。

(任意) IP アドレスの変更

ASDM アクセスにデフォルトの IP アドレスを使用できない場合は、ASA CLI で管理インターフェイスの IP アドレスを設定できます。



(注) この手順では、デフォルト設定を復元し、選択した IP アドレスも設定します。このため、保持する ASA 設定に変更を加えた場合は、この手順を使用しないでください。

手順

ステップ 1 ASA コンソールポートに接続し、グローバル コンフィギュレーションモードに入ります。詳細については、「[ASA CLI へのアクセス \(91 ページ\)](#)」を参照してください。

ステップ 2 選択した IP アドレスを使用してデフォルト設定を復元します。

configure factory-default [*ip_address* [*mask*]]

例 :

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management1/1
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

ステップ3 デフォルト コンフィギュレーションをフラッシュメモリに保存します。

write memory

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。

手順

ステップ1 ブラウザに次の URL を入力します。

- **https://192.168.1.1** : 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 ユーザー名とパスワードのフィールドを空のままにして、[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。

(任意) ASA ライセンスの設定

ISA 3000 には、注文されたバージョンに応じて**基本ライセンス**または**Security Plus**ライセンスが含まれます。**Security Plus**ライセンスによって、複数のファイアウォール接続、VPN 接続、フェールオーバー機能と VLAN が提供されます。

ライセンスの使用に制限を付ける場合は、**Strong Encryption (3DES/AES)** ライセンスもプリインストールします。このライセンスは、アメリカ合衆国の輸出管理ポリシーによって、一部の国では使用可能できません。**Strong Encryption** ライセンスによって、VPN トラフィックなどの高度に暗号化されたトラフィックが許可されます。

この手順では、追加のライセンスを取得してアクティブ化する方法について説明します。新規ライセンスを取得しない場合は、この手順に従う必要がありません。

無料の **Strong Encryption** ライセンスを手動でリクエストする必要がある場合は、<https://www.cisco.com/go/license> を参照してください。

必要に応じて、**AnyConnect Plus** または **Apex** ライセンスを購入することができます。このライセンスによって、AnyConnect VPN クライアントの接続が許可されます。

追加の ASA ライセンスをインストールするには、次の手順を実行します。

手順

ステップ 1 [Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択して、ASDM で ASA のシリアル番号を取得します。

(注) ライセンスに使用されるシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカルサポートで使用され、ライセンスには使用されません。ライセンスのシリアル番号を表示するには、**show version | grep Serial** コマンドを入力するか、ASDM の [Configuration] > [Device Management] > [Licensing Activation Key] ページを参照してください。

ステップ 2 PID (**L-ASA-SC-5=**) を使用して 5 セキュリティ コンテキスト ライセンスを購入するには、<http://www.cisco.com/go/ccw> を参照してください。ASA は、PID (**L-ISA3000SEC+-K9=**) を使用して、基本ライセンスと Security Plus ライセンスを持った 2 つのコンテキストをサポートしています。

AnyConnect ライセンスの場合、『Cisco AnyConnect 発注ガイド』および『AnyConnect ライセンスによく寄せられる質問 (FAQ)』も参照してください。

ライセンスを購入すると、製品認証キー (PAK) が記載された電子メールを受け取り、ライセンス アクティベーションキーを取得できます。AnyConnect ライセンスの場合、ユーザー セッションの同じプールを使用する複数の ASA に適用できるマルチユース PAK を受け取ります。場合によっては、PAK が記載された電子メールを受け取るまで数日かかることがあります。

ステップ 3 以下のライセンス Web サイトからアクティベーションキーを取得します。 <https://www.cisco.com/go/license>

プロンプトが表示されたら、次の情報を入力します。

- 製品認証キー
- ASA のシリアル番号
- 電子メールアドレス

アクティベーションキーが自動的に生成され、指定した電子メールアドレスに送信されます。このキーには、永続ライセンス用にそれまでに登録した機能がすべて含まれています。

ステップ 4 ASDM の [Configuration] > [Device Management] > [Licensing] > [Activation Key] ペインで、新しいアクティベーションキーを入力します。

キーは、5 つの要素で構成される 16 進ストリングで、各要素は 1 つのスペースで区切られています。先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。次に例を示します。

```
ASA0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

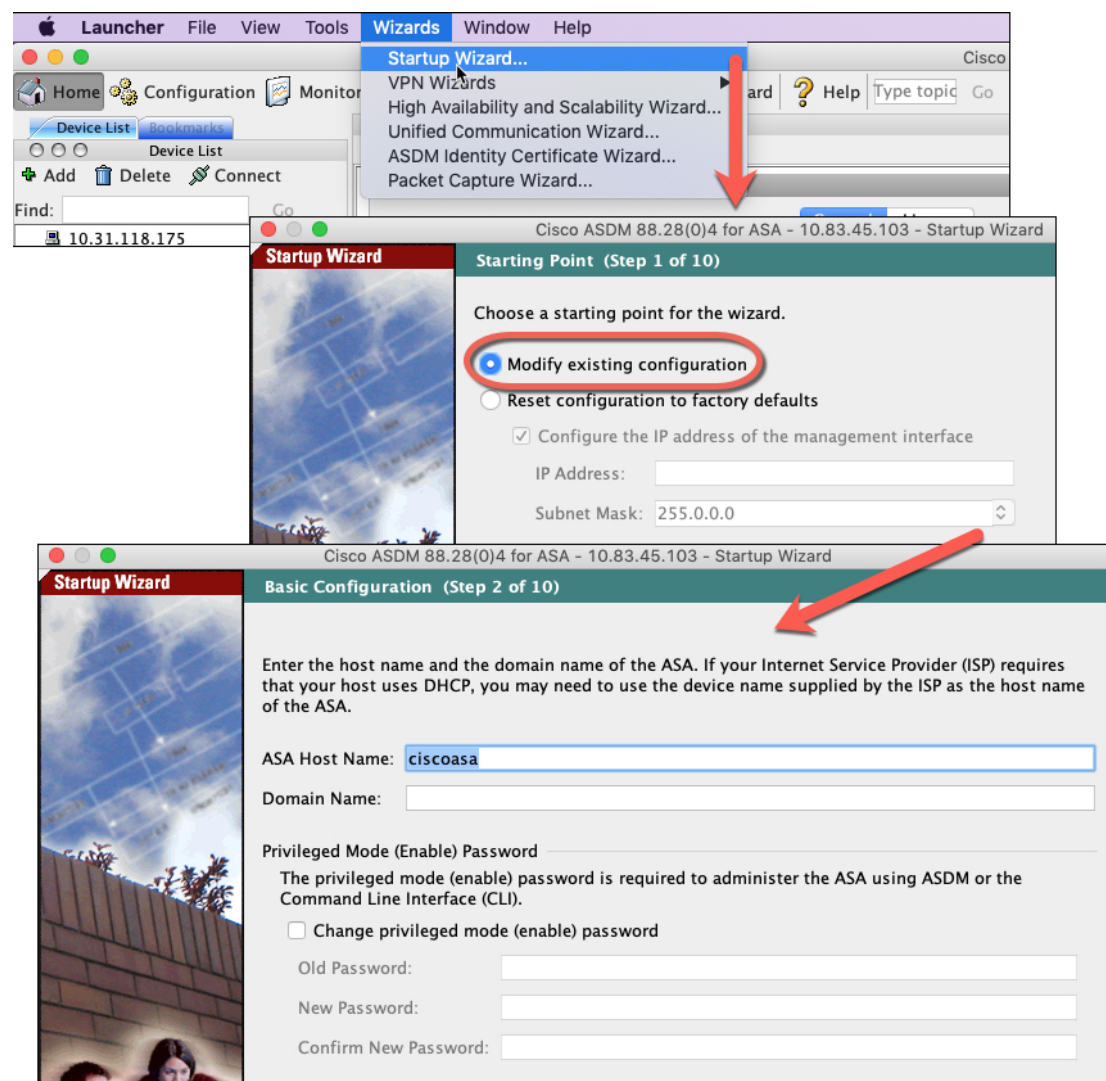
ステップ 5 [Update Activation Key] をクリックします。

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。ネットワークに合わせて BVI1 IP アドレスを設定する必要があります。

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 には、コンソールポートに接続してアクセスできます。後で任意のインターフェイスでの ASA への SSH アクセスを設定できます。SSH アクセスはデフォルトで無効になっています。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 管理コンピュータをコンソールポート、RJ-45 ポートまたはミニ USB ポートのいずれかに接続します。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください。次のシリアル設定を使用します。

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

ASA CLI に接続します。デフォルトでは、コンソールアクセスに必要なユーザークレデンシャルはありません。

ステップ 2 特権 EXEC モードにアクセスします。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
```

```
Enter Password: *****  
Repeat Password: *****  
ciscoasa#
```

設定以外のすべてのコマンドは、特権EXECモードで使用できます。特権EXECモードからコンフィギュレーションモードに入ることもできます。

特権 EXEC モードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例 :

```
ciscoasa# configure terminal  
ciscoasa (config)#
```

グローバルコンフィギュレーションモードから ASA の設定を開始できます。グローバルコンフィギュレーションモードを終了するには、**exit**、**quit**、または **end** コマンドを入力します。

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。

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。