



Secure Firewall 3100/4200 のマルチインスタンスモードの使用

Secure Firewall 3100/4200 は、単一のデバイスとして（アプライアンスモード）、または複数のコンテナインスタンスとして（マルチインスタンスモード）展開できます。この章では、マルチインスタンスモードでデバイスを展開する方法について説明します。

- [マルチインスタンスモードについて](#)（1 ページ）
- [インスタンスのライセンス](#)（15 ページ）
- [インスタンスの要件と前提条件](#)（16 ページ）
- [ライセンスのガイドラインと制限事項](#)（17 ページ）
- [インスタンスの設定](#)（20 ページ）
- [マルチインスタンスモードのモニタリング](#)（70 ページ）
- [マルチインスタンスモードの履歴](#)（74 ページ）

マルチインスタンスモードについて

マルチインスタンスモードでは、完全に独立したデバイスとして機能する複数のコンテナインスタンスを1つのシャーシに展開できます。

マルチインスタンスモードとアプライアンスモード

デバイスは、マルチインスタンスモードまたはアプライアンスモードのいずれかで実行できます。

アプライアンスモード

アプライアンスモードがデフォルトです。デバイスはネイティブ Firewall Threat Defense イメージを実行し、単一のデバイスとして機能します。([シャーシマネージャ (Chassis Manager)] ページで) 使用可能な唯一のシャーシレベルの設定は、ネットワークモジュール管理（ブレイクアウトポートまたはネットワークモジュールの有効化/無効化）用です。

マルチインスタンスモード

マルチインスタンスモードに変更すると、デバイスはシャーシで Secure Firewall eXtensible Operating System (FXOS) を実行しますが、各インスタンスは個別の Firewall Threat Defense イメージを実行します。FXOS CLI を使用してモードを設定できます。

複数のインスタンスが同じシャーシで実行されるため、以下のシャーシレベルの管理を実行する必要があります。

- リソースプロファイルを使用した CPU およびメモリリソース。
- インターフェイスの設定と割り当て。
- インスタンスの展開とモニタリング。

マルチインスタンスデバイスの場合、Firewall Management Center に シャーシ を追加し、[シャーシマネージャ (Chassis Manager)] ページでシャーシレベルの設定を構成します。

シャーシ管理インターフェイス

シャーシ管理

シャーシは、デバイス上の専用の管理インターフェイスを使用します。マルチインスタンスモードでは、シャーシ管理用のデータインターフェイスまたは管理インターフェイスの DHCP アドレッシングの使用はサポートされていません。

シャーシ管理インターフェイスは、Firewall Threat Defense CLI (初期セットアップ時) または FXOS CLI (マルチインスタンスモードに変換後) でのみ設定できます。マルチインスタンスモードで管理インターフェイスの設定を変更するには、[FXOS CLI のシャーシ管理設定の変更 \(68 ページ\)](#) を参照してください。



- (注) デフォルトでは、SSH サーバーと SSH アクセスリストを有効にしない限り、マルチインスタンスモードのこのインターフェイスへの SSH アクセスは許可されません。この違いは、SSH を使用してアプリケーションモードの Threat Defense の管理インターフェイスに接続できるものの、マルチインスタンスモードに変換すると、デフォルトでは SSH を使用して接続できなくなることを意味します。[SSH および SSH アクセスリストの設定 \(50 ページ\)](#) を参照してください。

インスタンス管理

すべてのインスタンスがシャーシ管理インターフェイスを共有し、各インスタンスは管理ネットワーク上に独自の IP アドレスを持ちます。インスタンスを追加して IP アドレスを指定した後、Firewall Threat Defense CLI でネットワーク設定を変更できます。

インスタンスの管理 IP アドレスでは、デフォルトで SSH が許可されます。

インスタンス イベント インターフェイス

Cisco Secure Firewall 4200 には、イベントに使用できる 2 番目の専用インターフェイスである Management 1/2 が含まれています。このインターフェイスは、各インスタンスの Firewall Threat Defense CLI で設定できます。各インスタンスに同じネットワーク上の IP アドレスを割り当ててください。 [イベントインターフェイスの設定](#) を参照してください。

インスタンス インターフェイス

インターフェイスでの柔軟な物理インターフェイスの使用を可能にするため、シャーシで VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイス（VLAN または物理）を共有することができます。 [共有インターフェイスの拡張性（6 ページ）](#) および [サブインターフェイスの設定（33 ページ）](#) を参照してください。



- (注) この章では、シャーシ VLAN サブインターフェイスについてのみ説明します。Firewall Threat Defense インスタンス内でサブインターフェイスを個別に作成できます。詳細については、[シャーシインターフェイスとインスタンス インターフェイス（3 ページ）](#) を参照してください。

インターフェイス タイプ

物理インターフェイス、VLAN サブインターフェイス、EtherChannel インターフェイスは、次のいずれかのタイプになります。

- **データ**：通常のデータまたはフェールオーバーリンクに使用します。データインターフェイスはインスタンス間で共有できず、インスタンスはバックプレーンを介して他のインスタンスと通信できません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別のインスタンスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。データインターフェイスに VLAN サブインターフェイスを追加して、高可用性ペアごとに個別のフェールオーバーリンクを提供できます。
- **Data-sharing**：通常のデータに使用します。これらのデータインターフェイスは、1 つ以上のインスタンスで共有できます。各インスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バックプレーン経由で通信できます。共有インターフェイスは、展開可能なインスタンスの数に影響することがあります。共有インターフェイスは、ブリッジグループメンバーインターフェイス（トランスペアレントモードまたはルーテッドモード）、インラインセット、パッシブインターフェイス、またはフェールオーバーリンクではサポートされません。

シャーシインターフェイスとインスタンス インターフェイス

シャーシレベルで、物理インターフェイス、インスタンスの VLAN サブインターフェイス、EtherChannel インターフェイスの基本的なイーサネット設定を管理します。インスタンス内で、

より高いレベルの設定を行います。たとえば、シャード内では Etherchannel のみを作成できません。ただし、インスタンス内の EtherChannel には IP アドレスを割り当てることができます。

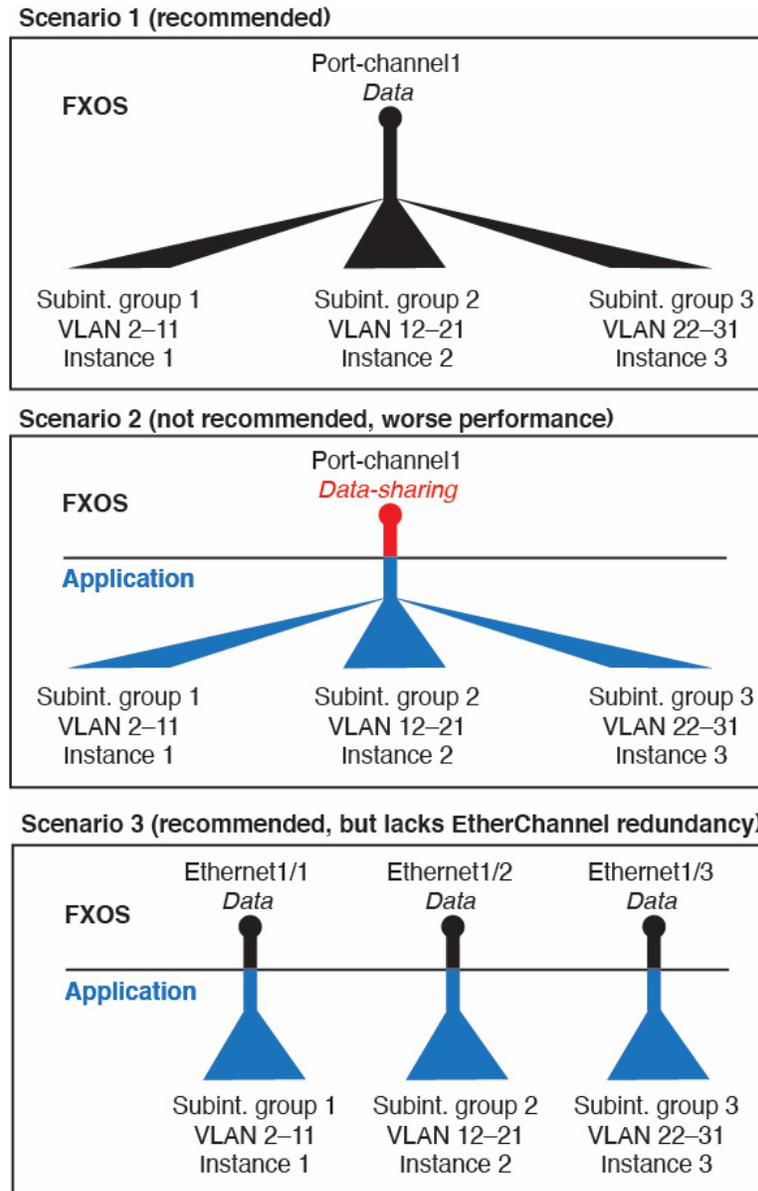
以下のセクションでは、インターフェイスのシャードとインスタンス間の連携について説明します。

VLAN サブインターフェイス

他のデバイスの場合と同様に、インスタンス内に VLAN サブインターフェイスを作成できます。

シャードに VLAN サブインターフェイスを作成することもできます。インスタンス定義のサブインターフェイスは、シャード制限の対象にはなりません。サブインターフェイスを作成する場所の選択は、ネットワーク導入および個人設定によって異なります。たとえば、サブインターフェイスを共有するには、シャードでサブインターフェイスを作成する必要があります。シャードのサブインターフェイスを優先するもう 1 つのシナリオでは、1 つのインターフェイス上の別のサブインターフェイスグループを複数のインスタンスに割り当てます。たとえば、インスタンス A で VLAN 2-11 を、インスタンス B で VLAN 12-21 を、インスタンス C で VLAN 22-31 を使用して Port-Channel を使うとします。インスタンス内でこれらのサブインターフェイスを作成する場合、シャード内で親インターフェイスを共有しますが、これはお勧めしません。このシナリオを実現する 3 つの方法については、次の図を参照してください。

図 1: シャード内の VLAN とインスタンス内の VLAN



シャードとインスタンスの独立したインターフェイスの状態

管理上、シャードとインスタンスの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方の場所で、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャードとインスタンスの間の不一致が生じることがあります。

インスタンス内のインターフェイスのデフォルトの状態は、インターフェイスのタイプによって異なります。たとえば、物理インターフェイスまたは EtherChannel は、インスタンス内では

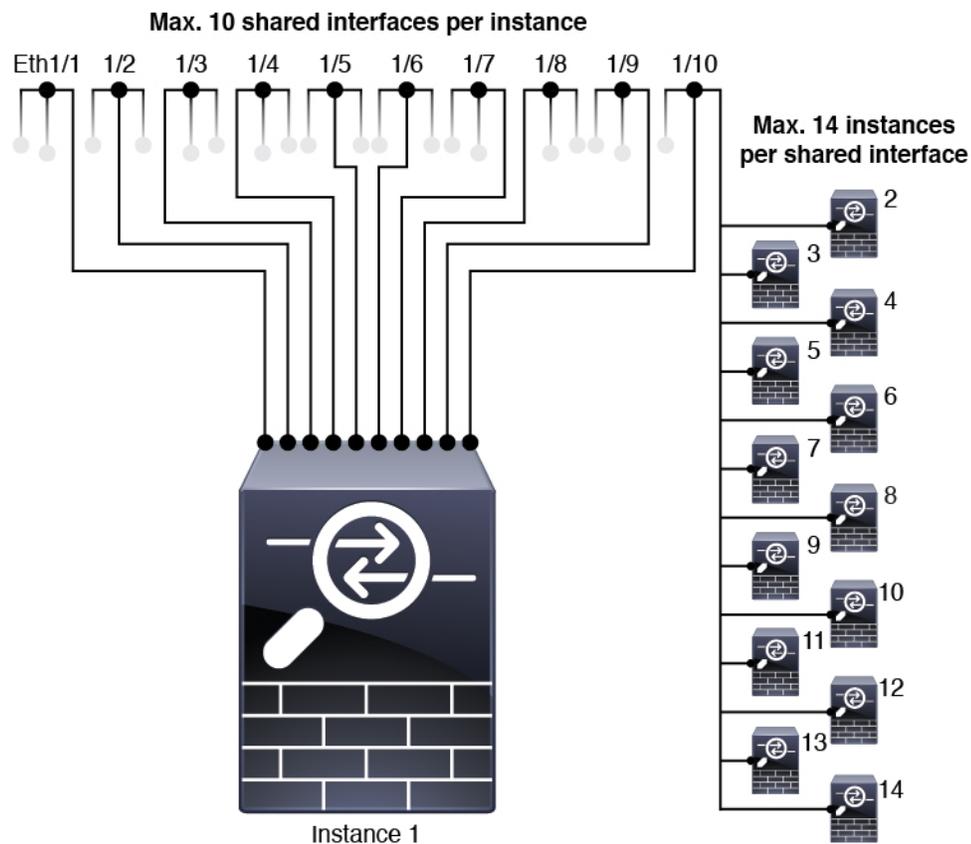
デフォルトで無効になっていますが、サブインターフェイスはデフォルトで有効になっています。

共有インターフェイスの拡張性

Instances can share data-sharing type interfaces. This capability lets you conserve physical interface usage as well as support flexible networking deployments. When you share an interface, the chassis uses unique MAC addresses to forward traffic to the correct instance. However, shared interfaces can cause the forwarding table to grow large due to the need for a full mesh topology within the chassis (every instance must be able to communicate with every other instance that is sharing the same interface). Therefore, there are limits to how many interfaces you can share.

In addition to the forwarding table, the chassis maintains a VLAN group table for VLAN subinterface forwarding. You can create up to 500 VLAN subinterfaces.

See the following limits for shared interface allocation:



共有インターフェイスのベスト プラクティス

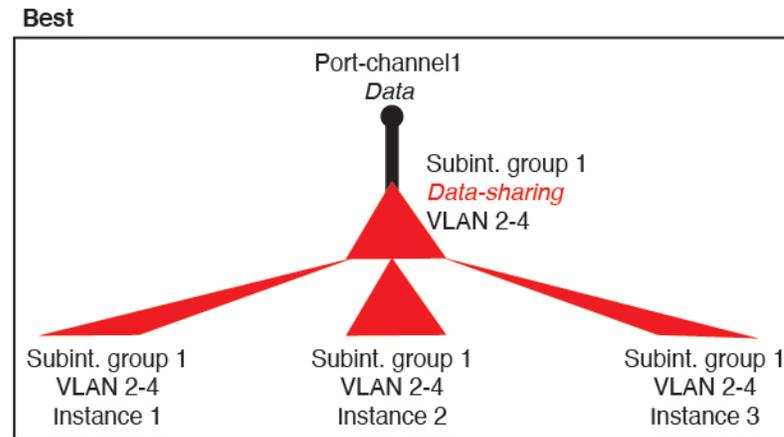
For optimal scalability of the forwarding table, share as few interfaces as possible. Instead, you can create up to 500 VLAN subinterfaces on one or more physical interfaces and then divide the VLANs among the container instances.

When sharing interfaces, follow these practices in the order of most scalable to least scalable:

1. Best—Share subinterfaces under a single parent, and use the same set of subinterfaces with the same group of instances.

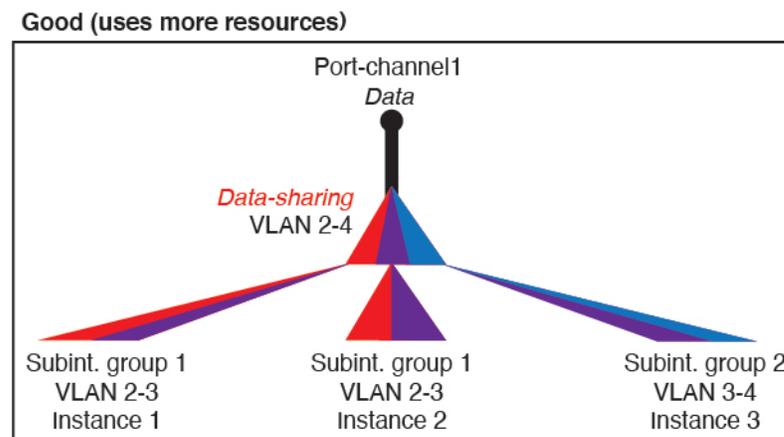
For example, create a large EtherChannel to bundle all of your like-kind interfaces together, and then share subinterfaces of that EtherChannel: Port-Channel1.2, 3, and 4 instead of Port-Channel2, Port-Channel3, and Port-Channel4. When you share subinterfaces from a single parent, the VLAN group table provides better scaling of the forwarding table than when sharing physical/EtherChannel interfaces or subinterfaces across parents.

図 2 : Best: Shared Subinterface Group on One Parent



If you do not share the same set of subinterfaces with a group of instances, your configuration can cause more resource usage (more VLAN groups). For example, share Port-Channel1.2, 3, and 4 with instances 1, 2, and 3 (one VLAN group) instead of sharing Port-Channel1.2 and 3 with instances 1 and 2, while sharing Port-Channel1.3 and 4 with instance 3 (two VLAN groups).

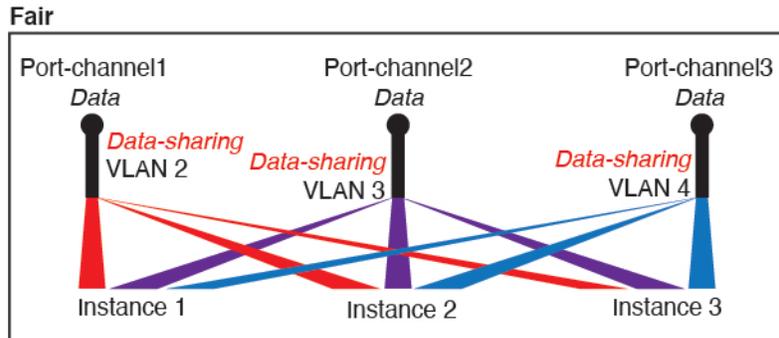
図 3 : Good: Sharing Multiple Subinterface Groups on One Parent



2. Fair—Share subinterfaces across parents.

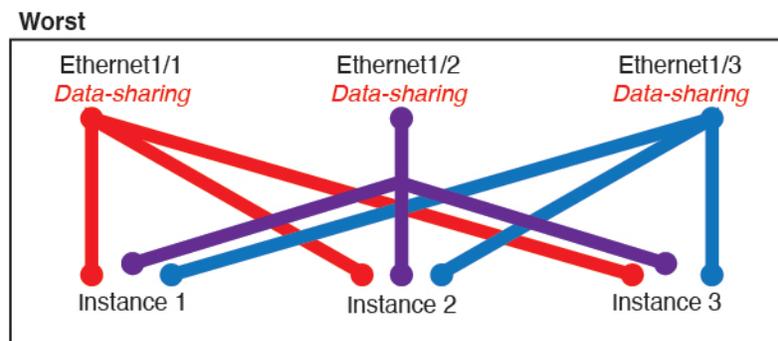
For example, share Port-Channel1.2, Port-Channel2.3, and Port-Channel3.4 instead of Port-Channel2, Port-Channel4, and Port-Channel4. Although this usage is not as efficient as only sharing subinterfaces on the same parent, it still takes advantage of VLAN groups.

図 4 : Fair: Shared Subinterfaces on Separate Parents



3. Worst—Share individual parent interfaces (physical or EtherChannel).
This method uses the most forwarding table entries.

図 5 : Worst: Shared Parent Interfaces



シャーシがパケットを分類する方法

Each packet that enters the chassis must be classified, so that the chassis can determine to which instance to send a packet.

- Unique Interfaces—If only one instance is associated with the ingress interface, the chassis classifies the packet into that instance. For bridge group member interfaces (in transparent mode or routed mode), inline sets, or passive interfaces, this method is used to classify packets at all times.
- Unique MAC Addresses—The chassis automatically generates unique MAC addresses for all interfaces, including shared interfaces. If multiple instances share an interface, then the classifier uses unique MAC addresses assigned to the interface in each instance. An upstream router cannot route directly to an instance without unique MAC addresses. You can also set the MAC addresses manually when you configure each interface within the application.



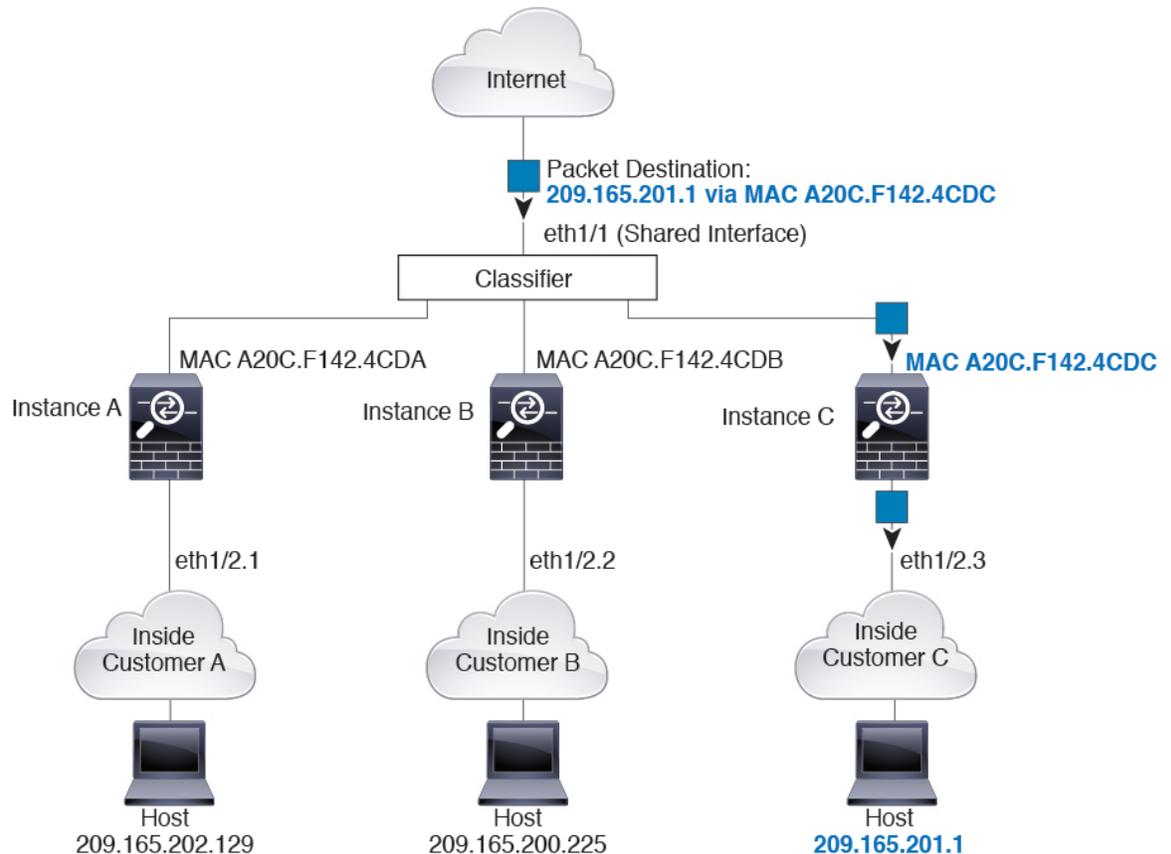
(注) If the destination MAC address is a multicast or broadcast MAC address, the packet is duplicated and delivered to each instance.

分類例

Packet Classification with a Shared Interface Using MAC Addresses

The following figure shows multiple instances sharing an outside interface. The classifier assigns the packet to Instance C because Instance C includes the MAC address to which the router sends the packet.

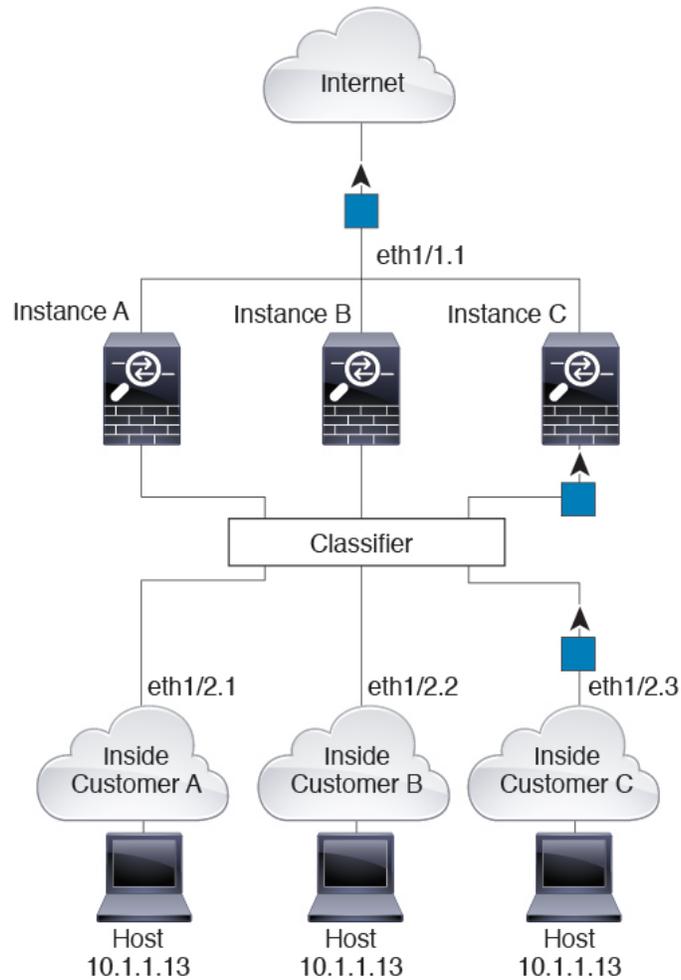
図 6 : Packet Classification with a Shared Interface Using MAC Addresses



Incoming Traffic from Inside Networks

Note that all new incoming traffic must be classified, even from inside networks. The following figure shows a host on the Instance C inside network accessing the internet. The classifier assigns the packet to Instance C because the ingress interface is Ethernet 1/2.3, which is assigned to Instance C.

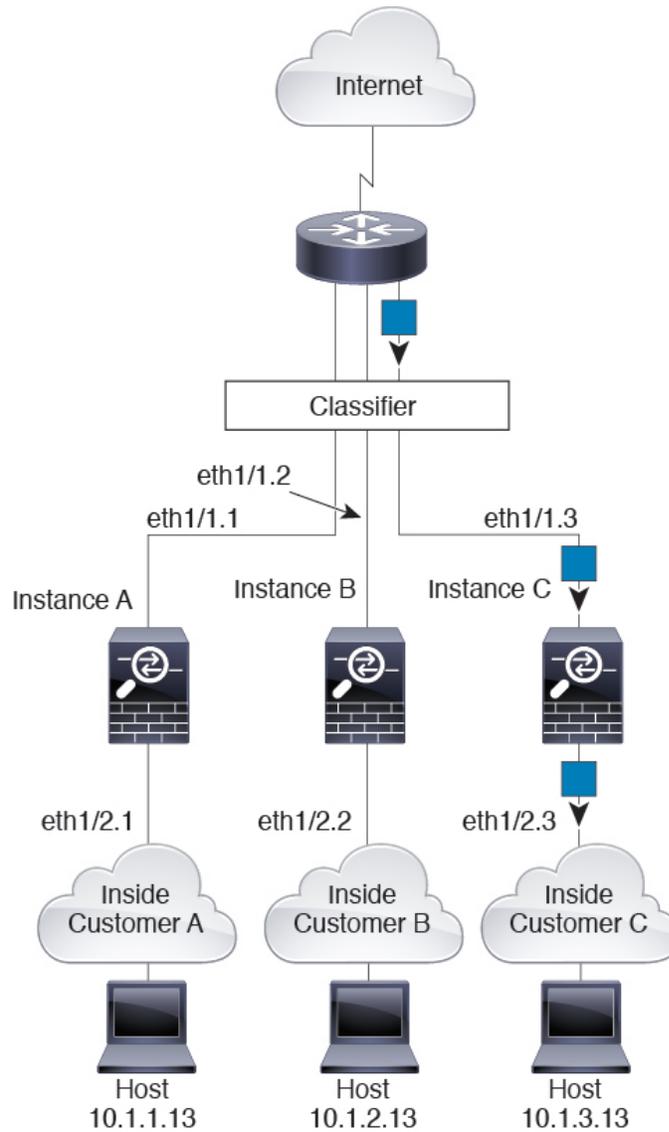
図 7: Incoming Traffic from Inside Networks



Transparent Firewall Instances

For transparent firewalls, you must use unique interfaces. The following figure shows a packet destined to a host on the Instance C inside network from the internet. The classifier assigns the packet to Instance C because the ingress interface is Ethernet 1/2.3, which is assigned to Instance C.

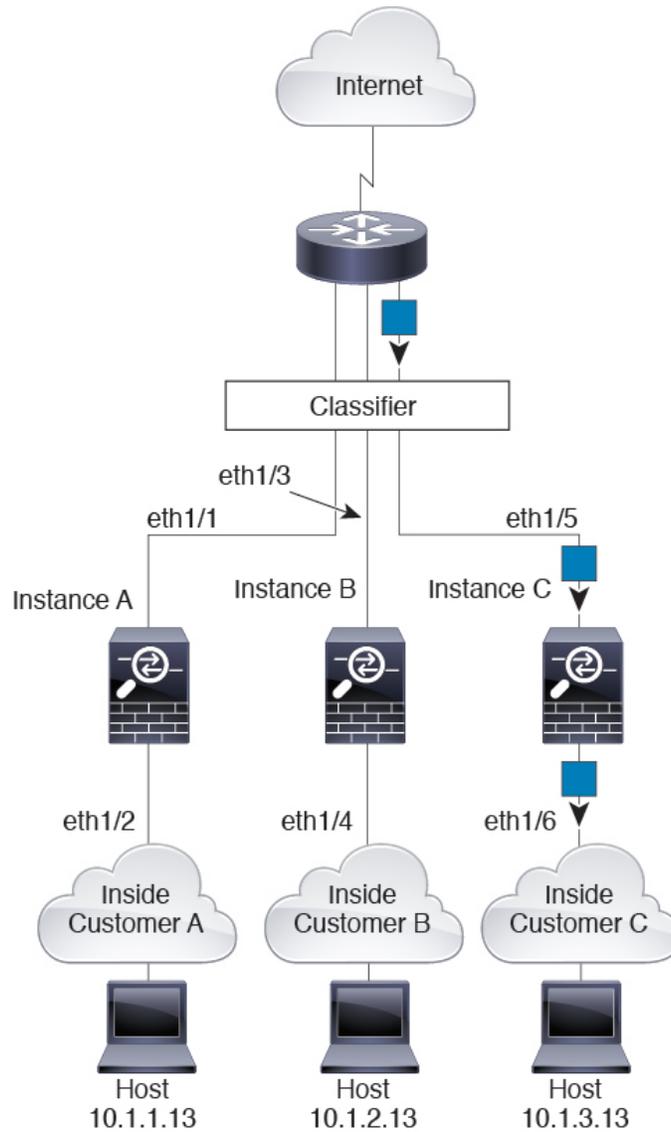
図 8 : Transparent Firewall Instances



Inline Sets

For inline sets, you must use unique interfaces and they must be physical interfaces or EtherChannels. The following figure shows a packet destined to a host on the Instance C inside network from the internet. The classifier assigns the packet to Instance C because the ingress interface is Ethernet 1/5, which is assigned to Instance C.

図 9: Inline Sets

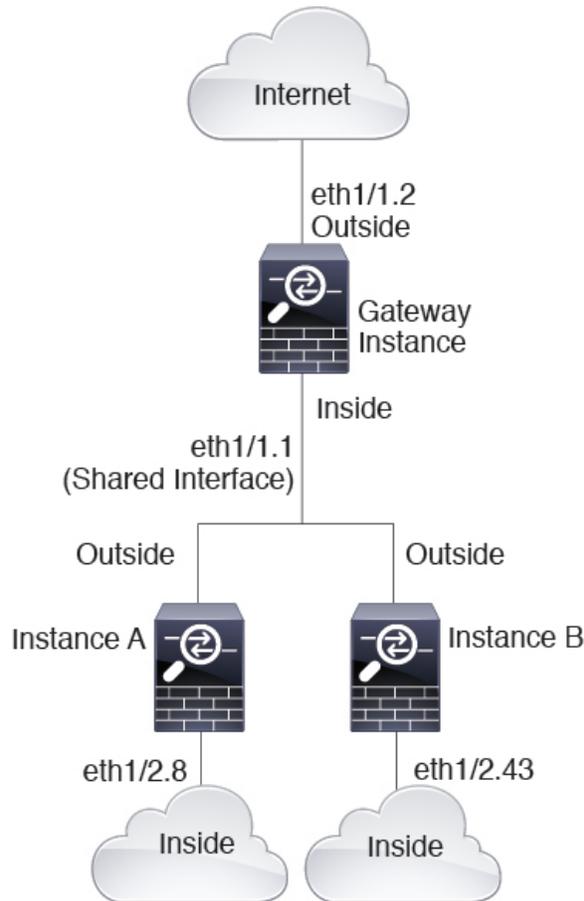


インスタンスのカスケード

Placing an instance directly in front of another instance is called *cascading instances*; the outside interface of one instance is the same interface as the inside interface of another instance. You might want to cascade instances if you want to simplify the configuration of some instances by configuring shared parameters in the top instance.

The following figure shows a gateway instance with two instances behind the gateway.

図 10: Cascading Instances



(注) Do not use cascading instances (using a shared interface) with High Availability. After a failover occurs and the standby unit rejoins, MAC addresses can overlap temporarily and cause an outage. You should instead use unique interfaces for the gateway instance and inside instance using an external switch to pass traffic between the instances.

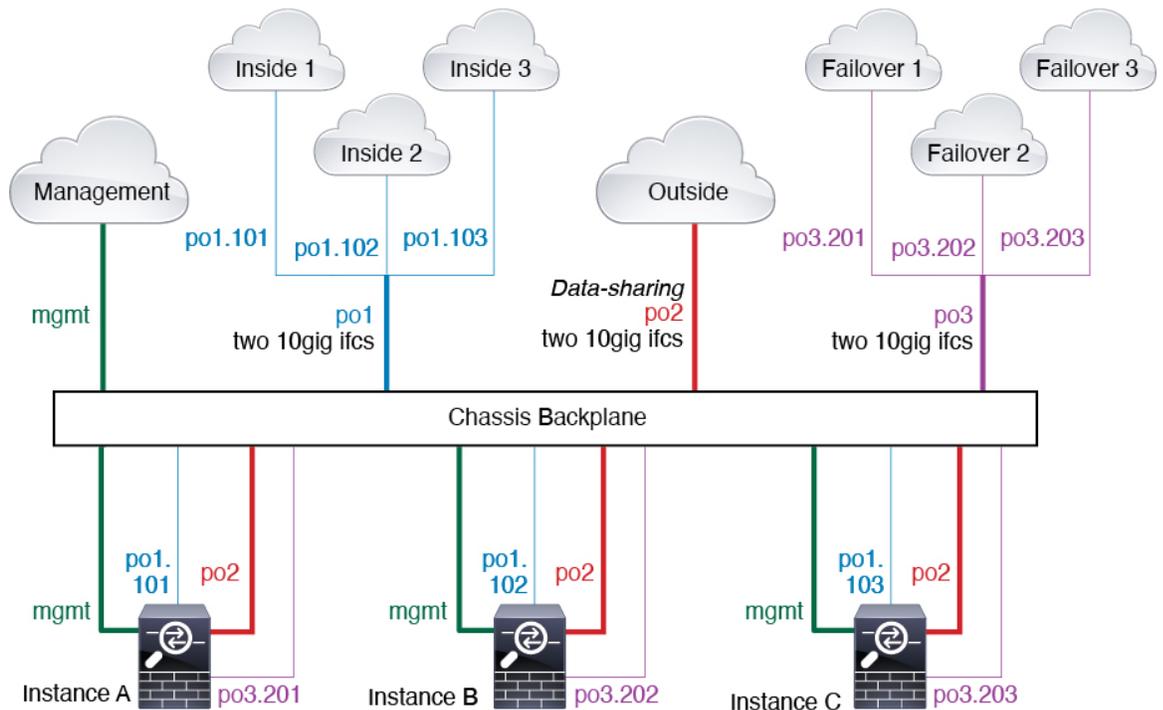
一般的な複数インスタンス展開

次の例には、ルーテッドファイアウォールモードのコンテナインスタンスが3つ含まれます。これらには次のインターフェイスが含まれます。

- 管理：すべてのインスタンスとシャーシが専用の管理インターフェイスを使用します。各インスタンス（およびシャーシ）内で、インターフェイスは同じ管理ネットワークで一意の IP アドレスを使用します。
- 内部：各インスタンスがポートチャンネル1（データタイプ）のサブインターフェイスを使用します。この EtherChannel には2つの 10 ギガビットイーサネットインターフェイスが含まれます。各サブインターフェイスは別々のネットワーク上に存在します。

- 外部：すべてのインスタンスがポートチャネル2インターフェイス（データ共有タイプ）を使用します。この EtherChannel には2つの 10 ギガビットイーサネットインターフェイスが含まれます。各アプリケーション内で、インターフェイスは同じ外部ネットワークで一意的 IP アドレスを使用します。
- フェールオーバー：各インスタンスがポートチャネル3（データタイプ）のサブインターフェイスを使用します。この EtherChannel には2つの 10 ギガビットイーサネットインターフェイスが含まれます。各サブインターフェイスは別々のネットワーク上に存在します。

図 11: 一般的な複数インスタンス展開



インスタンス インターフェイスの自動 MAC アドレス

The chassis automatically generates MAC addresses for instance interfaces, and guarantees that a shared interface in each instance uses a unique MAC address.

If you manually assign a MAC address to a shared interface within the instance, then the manually-assigned MAC address is used. If you later remove the manual MAC address, the autogenerated address is used. In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, we suggest that you manually set the MAC address for the interface within the instance.

Because autogenerated addresses start with A2, you should not start manual MAC addresses with A2 due to the risk of overlapping addresses.

The chassis generates the MAC address using the following format:

A2xx.yyyz.zzzz

Where *xx.yy* is a user-defined prefix or a system-defined prefix, and *zz.zzzz* is an internal counter generated by the chassis. The system-defined prefix matches the lower 2 bytes of the first MAC address in the burned-in MAC address pool that is programmed into the IDPROM. Use **connect fxos**, then **show module** to view the MAC address pool. For example, if the range of MAC addresses shown for module 1 is b0aa.772f.f0b0 to b0aa.772f.f0bf, then the system prefix will be f0b0.

The user-defined prefix is an integer that is converted into hexadecimal. For an example of how the user-defined prefix is used, if you set a prefix of 77, then the chassis converts 77 into the hexadecimal value 004D (*yyxx*). When used in the MAC address, the prefix is reversed (*xyyy*) to match the chassis native form:

A24D.00zz.zzzz

For a prefix of 1009 (03F1), the MAC address is:

A2F1.03zz.zzzz

マルチインスタンスモードのパフォーマンススケーリング係数

プラットフォームの最大スループット（接続数、VPNセッション数）は、アプライアンスモードのデバイスがメモリと CPU を使用するために計算されます（この値は **show resource usage** に示されます）。複数のインスタンスを使用する場合は、インスタンスに割り当てる CPU コアの割合に基づいてスループットを計算する必要があります。たとえば、コアの 50% でインスタンスを使用する場合は、最初にスループットの 50% を計算する必要があります。さらに、インスタンスで使用可能なスループットは、アプライアンスで使用可能なスループットよりも低い場合があります。

インスタンスのスループットを計算する方法の詳細については、<https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html> を参照してください。

インスタンスと高可用性

2つの個別のシャーシでインスタンスを使用して高可用性を使用することができます。たとえば、10個のインスタンスを持つシャーシを2つ使用する場合は、10個の高可用性ペアを作成できます。また、高可用性インスタンスと同じシャーシにスタンドアロンインスタンスを設定することもできます。詳細な要件については、[インスタンスの要件と前提条件（16ページ）](#)を参照してください。



(注) クラスタリングはサポートされません。

インスタンスのライセンス

すべてのライセンスは、インスタンスごとではなくシャーシごとに使用されます。次の詳細情報を参照してください。

- Essentials ライセンスはシャーシ全体に割り当てられ、シャーシごとに1つずつ割り当てられます。
- 機能ライセンスは各インスタンスに割り当てますが、シャーシにつき機能ごとに1つのライセンスのみを使用します。

インスタンスの要件と前提条件

モデルのサポート

- Secure Firewall 3110
- Secure Firewall 3120
- Secure Firewall 3130
- Secure Firewall 3140
- Cisco Secure Firewall 4215
- Cisco Secure Firewall 4225
- Cisco Secure Firewall 4245



(注) Secure Firewall 3105 はサポートされていません。

最大コンテナ インスタンスとモデルあたりのリソース

各コンテナインスタンスに対して、インスタンスに割り当てる CPU コア（より具体的にはスレッド）の数を指定できます。「コア」という用語は、さまざまなハードウェアアーキテクチャを説明するために汎用的に使用されます。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスあたり 40 GB に設定されます。

表 1: モデルごとの最大コンテナ インスタンス数とリソース

モデル	最大コンテナインスタンス数	使用可能な CPU コア（スレッド）
Secure Firewall 3110	3	22
Secure Firewall 3120	5	30
Secure Firewall 3130	7	46
Secure Firewall 3140	10	62
Cisco Secure Firewall 4215	10	62

モデル	最大コンテナインスタンス数	使用可能な CPU コア (スレッド)
Cisco Secure Firewall 4225	15	126
Cisco Secure Firewall 4245	34	254

ソフトウェア要件

- シャーシで実行されている FXOS のバージョンと互換性がある限り、各インスタンスで異なるバージョンの Firewall Threat Defense ソフトウェアを実行できます。
- Firewall Threat Defense ソフトウェアのパッチバージョンは完全なバンドルではないため、これを使用してインスタンスを展開することはできません。最初にメジャーバージョンまたはメンテナンスバージョンを展開してから、パッチを適用する必要があります。

ハイ アベイラビリティ要件

- 高可用性構成の 2 つのインスタンスは、以下の条件を満たす必要があります。
 - 別のシャーシ上にあること。
 - 同じモデルであること。
 - 同じインターフェイスが割り当てられていること。高可用性を有効にする前に、すべてのインターフェイスをシャーシで事前に同じ設定にすること。
 - 同じリソースプロファイル属性を使用すること。プロファイル名は異なってもかまいませんが、定義は一致している必要があります。

Firewall Management Center の要件

シャーシ管理とシャーシ上のすべてのインスタンスについては、ライセンスの実装のために、同じ Firewall Management Center を使用する必要があります。

ライセンスのガイドラインと制限事項

一般的なガイドライン

- 単一の Firewall Management Center は、シャーシ上のすべてのインスタンスを管理し、シャーシ自体も管理する必要があります。
- インスタンスの場合、次の機能はサポートされていません。
 - TLS 暗号化アクセラレーション
 - クラスタリング

- Firewall Management Center UCAPL/CC モード
- ハードウェアへのフローオフロード
- Security Cloud Control クラウド提供 Firewall Management Center によるシャーシのプライマリ管理と、オンプレミス Firewall Management Center によるシャーシの個別分析専用管理はサポートされていません。ただし、Security Cloud Control 管理対象インスタンスを分析専用のオンプレミス Firewall Management Center に追加することは可能です。

管理インターフェイス

- シャーシ管理用のデータインターフェイスはサポートされていません。専用の管理インターフェイスのみを使用できます
- 管理インターフェイスの DHCP アドレッシングがない

VLAN サブインターフェイス

- 本書では、シャーシ VLAN サブインターフェイスについてのみ説明します。インスタンス内でサブインターフェイスを個別に作成できます。
- インスタンスに親インターフェイスを割り当てる場合、タグなし（非VLAN）トラフィックのみを渡します。タグなしトラフィックを渡す必要がない限り、親インターフェイスを割り当てないでください。
- サブインターフェイスはデータまたはデータ共有タイプのインターフェイスでサポートされます。
- 最大 500 個の VLAN ID を作成できます。
- インラインセットに、またはパッシブインターフェイスとしてサブインターフェイスを使用することはできません。
- フェールオーバーリンクにサブインターフェイスを使用すると、その親のすべてのサブインターフェイスおよび親自体の、フェールオーバーリンクとしての使用が制限されます。一部のサブインターフェイスをフェールオーバーリンクとして、一部を通常のデータインターフェイスとして使用することはできません。

EtherChannel

- 最大 48 の EtherChannel を設定できますが、物理インターフェイスの数によって制限されます。
- EtherChannel には、最大 8 つのアクティブ インターフェイスを設定できます。
- EtherChannel 内のすべてのインターフェイスは、同じメディアタイプと速度容量である必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GB と 10GB のインターフェイスなど）を混在

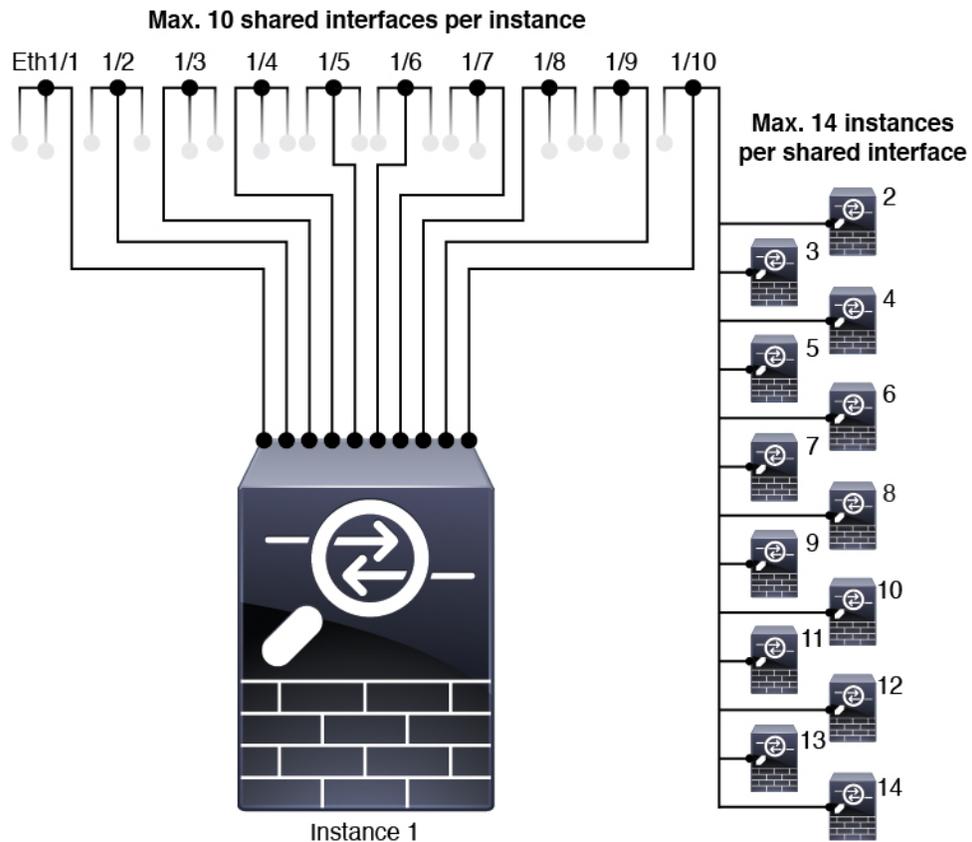
させることはできませんが、速度が [SFPを検出 (Detect SFP)] に設定されている場合は例外です。この場合は異なるインターフェイス容量を使用でき、共通の最低速度が使用されます。

- シャーシは、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS **vlan dot1Q tag native** コマンドを使用して、隣接スイッチのネイティブ VLAN タギングをイネーブルにすると、シャーシはタグ付きの LACPDU をドロップします。隣接スイッチのネイティブ VLAN タギングは、必ず無効化してください。
- 15.1(1)S2 以前の Cisco IOS ソフトウェアバージョンを実行するシャーシでは、スイッチスタックへの EtherChannel の接続がサポートされていませんでした。デフォルトのスイッチ設定では、シャーシの EtherChannel がクロススタックに接続されている場合、プライマリスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0 (無制限) などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。

データ共有インターフェイス

- 共有インターフェイスごとの最大インスタンス数：14。たとえば、Instance14 を介して Instance1 に Ethernet1/1 を割り当てることができます。

共有インターフェイスごとの最大インスタンス数は 10 です。たとえば、Ethernet1/1.10 を介して Instance1 に Ethernet1/1.1 を割り当てることができます。



- トランスペアレント ファイアウォール モードインスタンスでデータ共有インターフェイスを使用することはできません。
- インラインセットで、またはパッシブインターフェイスとしてデータ共有インターフェイスを使用することはできません。
- フェールオーバーリンクにデータ共有インターフェイスを使用することはできません。

デフォルトの MAC アドレス

- すべてのインターフェイスのMACアドレスは、MACアドレスプールから取得されます。サブインターフェイスの場合、手動でMACアドレスを設定する場合は、同じ親インターフェイス上のすべてのサブインターフェイスに一意的なMACアドレスを使用して、正しく分類されるようにしてください。「[インスタンスインターフェイスの自動MACアドレス \(14 ページ\)](#)」を参照してください。

インスタンスの設定

インスタンスを設定する前に、マルチインスタンスモードを有効にし、Firewall Management Center にシャージを追加し、シャージインターフェイスを設定する必要があります。シャージ設定をカスタマイズすることもできます。

デバイスのマルチインスタンスモードへの変換

Firewall Management Center 内のデバイスをマルチインスタンスモードに変換するには、この手順を使用します。この変換には約 15 分かかります。システムが再起動し、モード変更の一環として、管理ネットワーク設定と管理者パスワードを除いて設定が消去されます。シャーシのホスト名は「firepower-model」に設定されます。管理 IP アドレスが、Firewall Management Center との管理接続用にシャーシに割り当てられます。インスタンスを追加すると、それらのインスタンスは、管理インターフェイスで個別の IP アドレスを使用し、独自の管理接続を維持します。

マルチインスタンスモードに変換すると、Firewall Management Center を使用して、インスタンスだけでなくすべてのシャーシ設定を指定できます。Secure Firewall Chassis Manager または FXOS CLI での設定はサポートされていません。



- (注) デバイスを Firewall Management Center に追加する前に CLI を使用してマルチインスタンスモードに変換する場合は、[CLI のマルチインスタンスモードの有効化 \(62 ページ\)](#) を参照してください。

始める前に

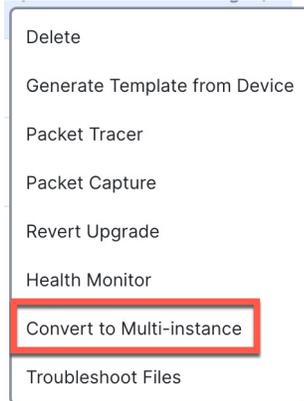
アプライアンスモードのデバイスをスタンドアロンデバイスとして Firewall Management Center に追加します。このデバイスでは以下を使用できません。

- マネージャアクセス用のデータインターフェイス
- 管理インターフェイスの DHCP
- Zero-Touch Provisioning

手順

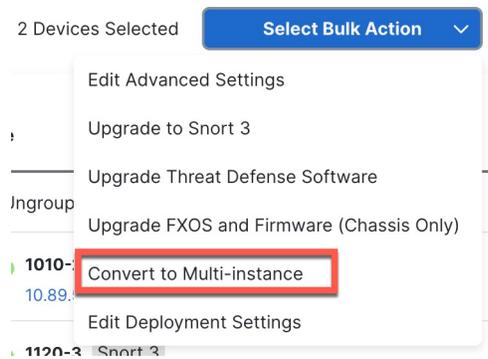
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] で、マルチインスタンスモードに変換するデバイスの横にある **More** (⋮) を選択し、[マルチインスタンスへの変換 (Convert to Multi-Instance)] を選択します。

図 12: マルチインスタンスへの変換



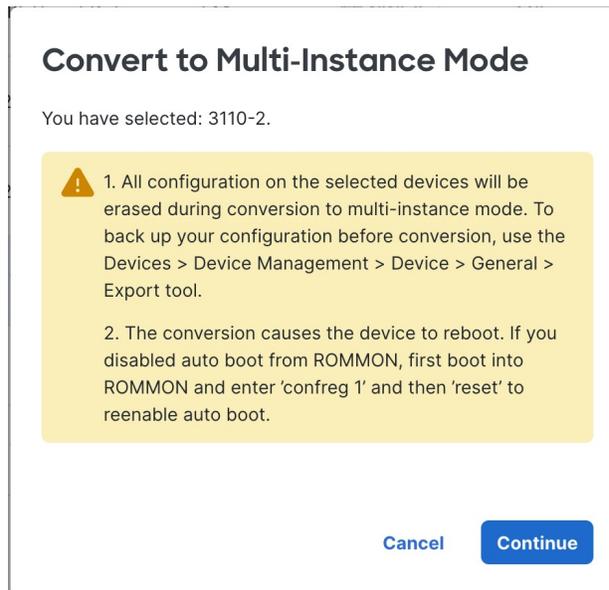
または、変換する複数のデバイスの横にあるチェックボックスをオンにして、[一括アクションの選択 (Select Bulk Action)] > [マルチインスタンスへの変換 (Convert to Multi-Instance)] を選択することもできます。

図 13: 一括変換



ステップ 2 変換の実行を確認し、[続行 (Continue)] をクリックします。

図 14: 変換の確認



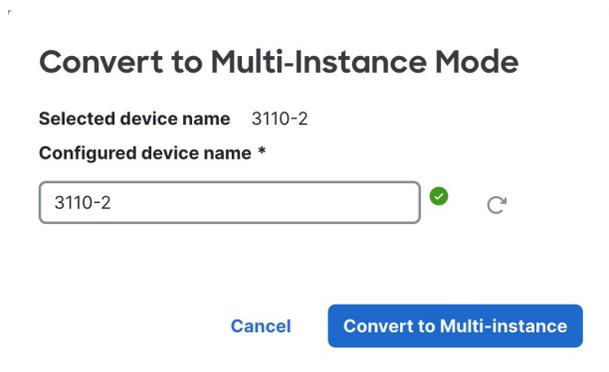
準備状況チェックが実行されます。たとえば、展開が進行中の場合、チェックに合格しない可能性があります。

ステップ 3 必要に応じて、シャーシの名前を変更し、[マルチインスタンスへの変換 (Convert to Multi-Instance)] をクリックします。デフォルトでは、デバイス名が使用されますが、マルチインスタンスシャーシに別の命名規則を使用したい場合があります。

(注)

展開が進行中であるといった理由で準備状況チェックに合格しなかった場合は、そのプロセスが完了するまで待つてから、 をクリックして準備状況チェックを再実行し、続行することができます。

図 15: シャーシ名の変更

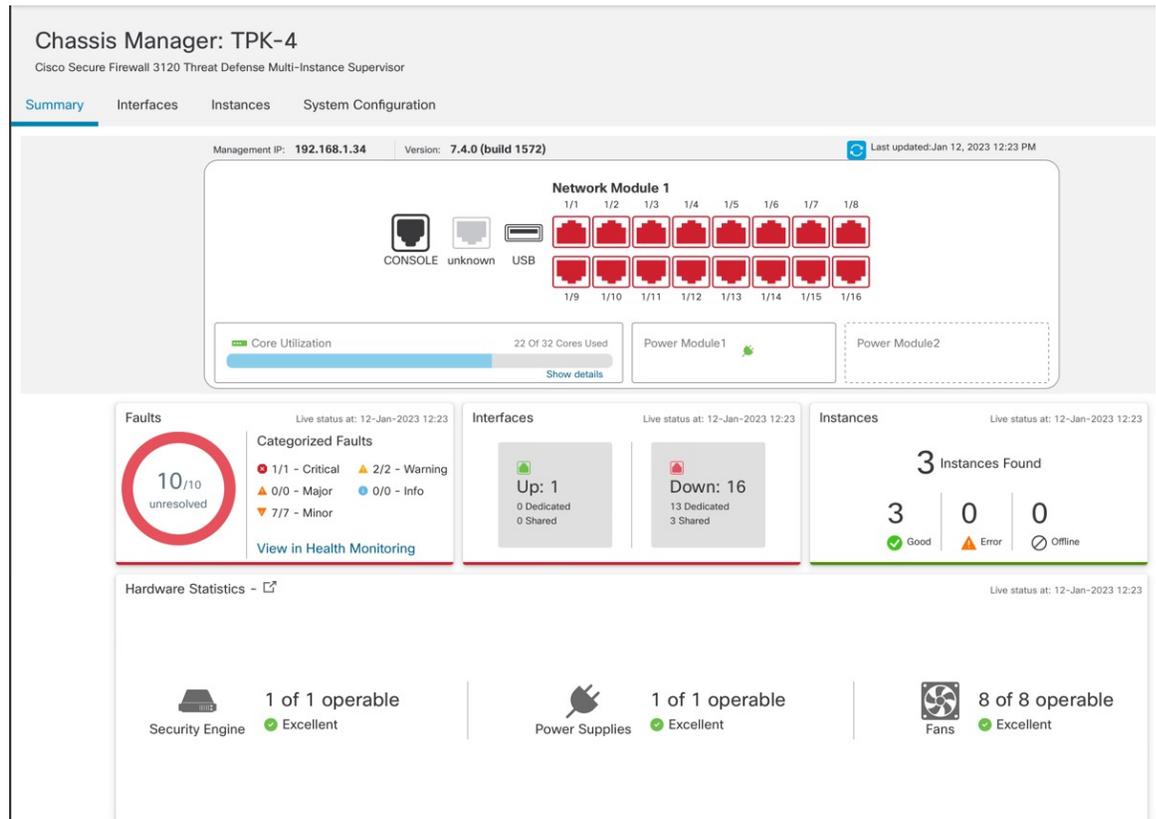


デバイスがデバイスリストから削除されるまで約 15 分待つと、変換後にシャーシとして再度追加されます。

ステップ 4 シャーシを表示および設定するには、[シャーシ (Chassis)] 列の [管理 (Manage)] をクリックするか、**Edit** (✎) をクリックします。

シャーシの [シャーシマネージャ (Chassis Manager)] ページが開き、[要約 (Summary)] ページが表示されます。

図 16: シャーシ要約



シャーシインターフェイスの設定

シャーシレベルで、物理インターフェイス、インスタンスの VLAN サブインターフェイス、EtherChannel インターフェイスの基本的なイーサネット設定を構成します。デフォルトでは、物理インターフェイスは無効になっています。



(注) ブレークアウトポートを設定し、他のネットワークモジュール操作を実行するには、[Cisco Secure Firewall 3100/4200 向けネットワークモジュールを管理する](#) を参照してください。



- (注) [デバイスの同期 (Sync Device)] ボタンの詳細については、[Firewall Management Center とのインターフェイスの変更の同期](#) を参照してください。

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすることや、インターフェイスの速度とデュプレックスを設定するなどのハードウェア設定が可能です。インターフェイスを使用するには、インターフェイスをシャーシに対して物理的に有効にし、インスタンスで論理的に有効にする必要があります。デフォルトでは、物理インターフェイスは無効になっています。VLAN サブインターフェイスの場合、管理状態は親インターフェイスから継承されます。

手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] で、[シャーシ (Chassis)] 列の [管理 (Manage)] をクリックするか **Edit** (🔗) をクリックします。

図 17: シャーシの管理

<input type="checkbox"/>	TPK-4 192.168.1.34	Firewall 3120 Threat Defense Multi- Instance Supervisor	7.4.0	Manage	N/A
--------------------------	------------------------------	---	-------	---------------	-----

シャーシの [シャーシマネージャ (Chassis Manager)] ページが開き、[要約 (Summary)] ページが表示されます。

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

図 18: インターフェイス

Chassis Manager: TPK-4
Cisco Secure Firewall 3120 Threat Defense Multi-Instance Supervisor

Summary **Interfaces** Instances System Configuration

CONSOLE unknown USB

Network Module 1

1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8
1/9 1/10 1/11 1/12 1/13 1/14 1/15 1/16

Search Interfaces Sync Device Add

Interface Name	Port Type	Instances	VLAN ID	Admin Speed	Admin Duplex	Admin State	Auto Negotiation	Admin FEC	
Ethernet1/1	Data	instance2		1Gbps	Full	Enabled	No	Auto	
Ethernet1/2	Data	instance1		100Mbps	Half	Disabled	No	Auto	
Ethernet1/3	Data	instance1		100Mbps	Half	Disabled	No	Auto	
Ethernet1/4	Data			1Gbps	Full	Enabled	Yes	Auto	
Ethernet1/5	Data	instance2		1Gbps	Full	Disabled	No	Auto	
Ethernet1/6	Data Sharing	instance2		1Gbps	Full	Enabled	No	Auto	
Ethernet1/7	Data Sharing	instance2		1Gbps	Full	Enabled	No	Auto	
Ethernet1/8	Data Sharing			1Gbps	Full	Disabled	Yes	Auto	
Ethernet1/9	Data			Detect SFP	Full	Disabled	Yes	Auto	
Ethernet1/10	Data	instance3		10Gbps	Full	Enabled	Yes	Auto	
Ethernet1/11	Data	instance3		10Gbps	Full	Disabled	Yes	Auto	
Ethernet1/12	Data	instance3		10Gbps	Full	Disabled	Yes	Auto	
Ethernet1/13	Data	instance3		Detect SFP	Full	Disabled	Yes	Auto	
Ethernet1/14	Data			10Gbps	Full	Enabled	Yes	Auto	
Ethernet1/15	Data			10Gbps	Full	Disabled	Yes	cl108-rs	

ステップ 3 編集するインターフェイス **Edit** () をクリックします。

図 19: 物理インターフェイスの編集

ステップ 4 [有効 (Enabled)] チェック ボックスをオンにして、インターフェイスを有効化します。

ステップ 5 [ポートタイプ (Port Type)] で、[データ (Data)] または [データ共有 (Data Sharing)] を選択します。

図 20: ポートタイプ (Port Type)

ステップ 6 [管理デュプレックス (Admin Duplex)] を設定します。

1Gbps 以上の速度は、フルデュプレックスのみをサポートします。SFP インターフェイスは [全二重 (Full)] のみをサポートします。

ステップ 7 [管理速度 (Admin Speed)] を設定します。

SFP の場合は [SFPを検出 (Detect SFP)] を選択してインストールされている SFP モジュールの速度を検出し、適切な速度を使用します。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。

ステップ 8 (任意) Link Layer Discovery Protocol (LLDP) パケットを有効にするには、[LLDP送信 (LLDP Transmit)] または [LLDP受信 (LLDP Receive)] をオンにします。

ステップ 9 (任意) フロー制御のポーズ (XOFF) フレームを有効にするには、[フロー制御送信 (Flow Control Send)] をオンにします。

フロー制御により、接続しているイーサネットポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止できるようにすることによって、輻輳時のトラフィックレートを制御できます。脅威防御ポートで輻輳が生じ (内部スイッチでキューイングリソースが枯渇)、それ以上はトラフィックを受信できなくなった場合、ポーズフレームを送信することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通知します。ポーズフレームを受信すると、送信側デバイスはデータパケットの送信を中止するので、輻輳時のデータパケット損失が防止されます。

(注)

Firewall Threat Defense は、リモートピアがトラフィックをレート制御できるように、ポーズフレームの送信をサポートしています。

ただし、ポーズフレームの受信はサポートされていません。

内部スイッチには、それぞれ 250 バイトの 8000 バッファのグローバルプールがあり、スイッチはバッファを各ポートに動的に割り当てます。バッファ使用量がグローバルハイウォーターマーク (2 MB (8000 バッファ)) を超えると、フロー制御が有効になっているすべてのインターフェイスからポーズフレームが送信されます。また、バッファがポートのハイウォーターマーク (3125 MB (1250 バッファ)) を超えると、特定のインターフェイスからポーズフレームが送信されます。ポーズの送信後、バッファ使用量が低ウォーターマークよりも下回ると、XON フレームを送信できます (グローバルでは 1.25MB (5000 バッファ)、ポートごとに 25 MB (1000 バッファ)) リンク パートナーは、XON フレームを受信するとトラフィックを再開できます。

802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

ステップ 10 (任意) [自動ネゴシエーション (Auto Negotiation)] をオンにして、速度、リンクステータス、およびフロー制御をネゴシエートするようにインターフェイスを設定します。1Gbps 未満の速度では、この設定を編集できません。SFP インターフェイスの場合、速度が 1Gbps に設定されている場合のみ、自動ネゴシエーションを無効にできます。

ステップ 11 [保存 (Save)] をクリックし、[インターフェイス (Interfaces)] ページの右上にある [保存 (Save)] をクリックします。

これで、ポリシーをシャーンに展開できます。変更はポリシーを展開するまで有効になりません。

EtherChannel の設定

EtherChannel (ポートチャンネルとも呼ばれる) は、同じメディアタイプと容量の最大 8 個のメンバーインターフェイスを含むことができ、同じ速度とデブプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ (銅と光ファイバ) の SFP を混在させることができます。大容量のインターフェイスで速度を低く設定することでインターフェイス容量 (1GB と 10GB のインターフェイスなど) を混在させることはできません。

んが、速度が [SFPを検出 (Detect SFP)] に設定されている場合は例外です。この場合は異なるインターフェイス容量を使用でき、共通の最低速度が使用されます。

リンク集約制御プロトコル (LACP) では、2つのネットワーク デバイス間でリンク集約制御プロトコルデータユニット (LACPDU) を交換することによって、インターフェイスが集約されます。LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャンネルグループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャンネルグループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

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

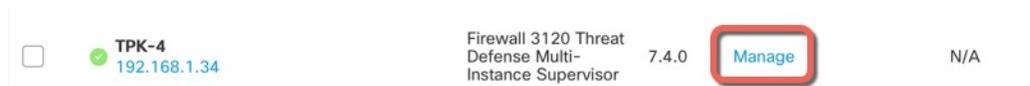
始める前に

物理インターフェイスを有効にし、ハードウェアパラメータを設定します。[物理インターフェイスの設定 \(25 ページ\)](#) を参照してください。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] で、[シャーシ (Chassis)] 列の [管理 (Manage)] をクリックするか **Edit** (🔗) をクリックします。

図 21: シャーシの管理



シャーシの [シャーシマネージャ (Chassis Manager)] ページが開き、[要約 (Summary)] ページが表示されます。

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

図 22: インターフェイス

Chassis Manager: TPK-4
Cisco Secure Firewall 3120 Threat Defense Multi-Instance Supervisor

Summary **Interfaces** Instances System Configuration

CONSOLE unknown USB

Network Module 1

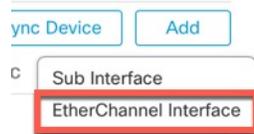
1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8
1/9 1/10 1/11 1/12 1/13 1/14 1/15 1/16

Search Interfaces Sync Device Add

Interface Name	Port Type	Instances	VLAN ID	Admin Speed	Admin Duplex	Admin State	Auto Negotiation	Admin FEC
Ethernet1/1	Data	instance2		1Gbps	Full	Enabled	No	Auto
Ethernet1/2	Data	instance1		100Mbps	Half	Disabled	No	Auto
Ethernet1/3	Data	instance1		100Mbps	Half	Disabled	No	Auto
Ethernet1/4	Data			1Gbps	Full	Enabled	Yes	Auto
Ethernet1/5	Data	instance2		1Gbps	Full	Disabled	No	Auto
Ethernet1/6	Data Sharing	instance2		1Gbps	Full	Enabled	No	Auto
Ethernet1/7	Data Sharing	instance2		1Gbps	Full	Enabled	No	Auto
Ethernet1/8	Data Sharing			1Gbps	Full	Disabled	Yes	Auto
Ethernet1/9	Data			Detect SFP	Full	Disabled	Yes	Auto
Ethernet1/10	Data	instance3		10Gbps	Full	Enabled	Yes	Auto
Ethernet1/11	Data	instance3		10Gbps	Full	Disabled	Yes	Auto
Ethernet1/12	Data	instance3		10Gbps	Full	Disabled	Yes	Auto
Ethernet1/13	Data	instance3		Detect SFP	Full	Disabled	Yes	Auto
Ethernet1/14	Data			10Gbps	Full	Enabled	Yes	Auto
Ethernet1/15	Data			10Gbps	Full	Disabled	Yes	cl108-rs

ステップ 3 [追加 (Add)] > [EtherChannel インターフェイス (EtherChannel Interface)] をクリックします。 >

図 23: EtherChannel の追加



ステップ 4 以下の [インターフェイス (Interfaces)] パラメータを設定します。

図 24: インターフェイスの設定

- a) [EtherChannel ID] には、1 ～ 48 の ID を指定します。
- b) [Enabled] をオンにします。
- c) [ポートタイプ (Port Type)] で、[データ (Data)] または [データ共有 (DataShared)] を選択します。
 ポートタイプの詳細については、[インターフェイスタイプ \(3 ページ\)](#) を参照してください。
- d) 物理インターフェイスをポートチャネルに追加するには、[使用可能なインターフェイス (Available Interface)] リストで **Add (+)** を選択し、[選択したインターフェイス (Selected Interfaces)] リストに移動します。
 すべてのインターフェイスを追加または削除するには、二重矢印ボタンをクリックします。
 (注)
 すでにインスタンスに割り当てられているインターフェイスは追加できません。

ステップ 5 (任意) 以下の [設定 (Configuration)] パラメータを設定します。

これらの設定の多く (LACP 設定を除く) は、EtherChannel に含めるインターフェイスの要件を設定します。メンバーインターフェイスの設定は上書きされません。たとえば、[LLDP送信

(LLDP Transmit)]をオンにする場合は、その設定を持つインターフェイスのみが追加されます。[管理速度 (Admin Speed)]を 1Gbps に設定すると、1Gbps のインターフェイスのみを含めることができます。

図 25: コンフィギュレーションの設定項目

The screenshot shows a configuration window titled "Add EtherChannel Interface". It has two tabs: "Interfaces" and "Configuration". The "Configuration" tab is selected. The settings are as follows:

- Admin Duplex: Full (dropdown menu)
- Admin Speed: 1Gbps (dropdown menu)
- LACP Mode: Active (dropdown menu)
- LACP Rate: Default (dropdown menu)
- Auto Negotiation:
- LLDP Transmit:
- LLDP Receive:
- Flow Control Send:

At the bottom right, there are "Cancel" and "Save" buttons.

- メンバーインターフェイスに適した [管理デュプレックス (Admin Duplex)] を選択します ([全二重 (Full Duplex)] または [半二重 (Half Duplex)]) 。
指定したデュプレックスのメンバーインターフェイスを追加すると、ポートチャネルに正常に参加されます。
- ドロップダウンリストでメンバーインターフェイスに適した [管理速度 (Admin Speed)] を選択します。
指定した速度ではないメンバーインターフェイスを追加すると、ポートチャネルに正常に参加できません。
- [LACPモード (LACP Mode)] ([アクティブ (Active)] または [On]) を選択します。
 - [アクティブ (Active)] : LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
 - [オン (On)] : EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

(注)

モードを [On] から [Active] に変更するか、[Active] から [On] に変更すると、EtherChannel が動作状態になるまで最大 3 分かかることがあります。

- d) [LACP速度 (LACP Rate)] ([デフォルト (Default)]、[高速 (Fast)]、または [標準 (Normal)]) を選択します。
デフォルトは [高速 (Fast)] です。
- e) [LLDP送信 (LLDP Transmit)] または [LLDP受信 (LLDP Receive)] をオンにして、メンバーインターフェイスに必要な Link Layer Discovery Protocol (LLDP) 設定を選択します。
- f) メンバーインターフェイスに必要な [フロー制御送信 (Flow Control Send)] 設定をオンにします。

ステップ 6 [保存 (Save)] をクリックし、[インターフェイス (Interfaces)] ページの右上にある [保存 (Save)] をクリックします。

これで、ポリシーをシャーシに展開できます。変更はポリシーを展開するまで有効になりません。

サブインターフェイスの設定

シャーシには最大 500 個のサブインターフェイスを追加できます。

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

このセクションでは、FXOS VLAN サブインターフェイスについてのみ説明します。インスタンス内でサブインターフェイスを個別に作成できます。[シャーシインターフェイスとインスタンスインターフェイス \(3 ページ\)](#) を参照してください。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] で、[シャーシ (Chassis)] 列の [管理 (Manage)] をクリックするか **Edit** (🔗) をクリックします。

図 26: シャーシの管理



シャーシの [シャーシマネージャ (Chassis Manager)] ページが開き、[要約 (Summary)] ページが表示されます。

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

図 27: インターフェイス

Chassis Manager: TPK-4
Cisco Secure Firewall 3120 Threat Defense Multi-Instance Supervisor

Summary **Interfaces** Instances System Configuration

Network Module 1

CONSOLE unknown USB

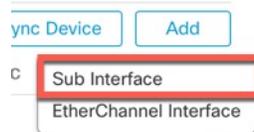
1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8
1/9 1/10 1/11 1/12 1/13 1/14 1/15 1/16

Search Interfaces Sync Device Add

Interface Name	Port Type	Instances	VLAN ID	Admin Speed	Admin Duplex	Admin State	Auto Negotiation	Admin FEC
Ethernet1/1	Data	instance2		1Gbps	Full	Enabled	No	Auto
Ethernet1/2	Data	instance1		100Mbps	Half	Disabled	No	Auto
Ethernet1/3	Data	instance1		100Mbps	Half	Disabled	No	Auto
Ethernet1/4	Data			1Gbps	Full	Enabled	Yes	Auto
Ethernet1/5	Data	instance2		1Gbps	Full	Disabled	No	Auto
Ethernet1/6	Data Sharing	instance2		1Gbps	Full	Enabled	No	Auto
Ethernet1/7	Data Sharing	instance2		1Gbps	Full	Enabled	No	Auto
Ethernet1/8	Data Sharing			1Gbps	Full	Disabled	Yes	Auto
Ethernet1/9	Data			Detect SFP	Full	Disabled	Yes	Auto
Ethernet1/10	Data	instance3		10Gbps	Full	Enabled	Yes	Auto
Ethernet1/11	Data	instance3		10Gbps	Full	Disabled	Yes	Auto
Ethernet1/12	Data	instance3		10Gbps	Full	Disabled	Yes	Auto
Ethernet1/13	Data	instance3		Detect SFP	Full	Disabled	Yes	Auto
Ethernet1/14	Data			10Gbps	Full	Enabled	Yes	Auto
Ethernet1/15	Data			10Gbps	Full	Disabled	Yes	cl108-rs

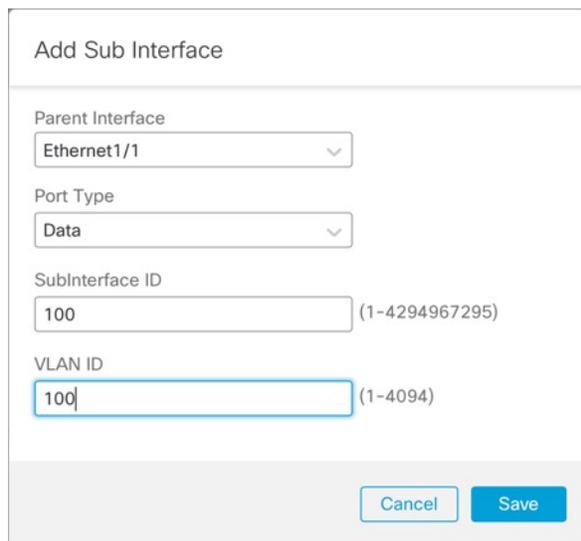
ステップ 3 [追加 (Add)] > [サブインターフェイス (Subinterface)] をクリックします。

図 28: サブインターフェイスの追加



ステップ 4 次のパラメータを設定します。

図 29: サブインターフェイス設定



a)

ステップ 5 [保存 (Save)] をクリックし、[インターフェイス (Interfaces)] ページの右上にある [保存 (Save)] をクリックします。

これで、ポリシーをシャーシに展開できます。変更はポリシーを展開するまで有効になりません。

インスタンスの追加

マルチインスタンスモードでは、1つ以上のインスタンスをシャーシに追加できます。サポートされるインスタンスの数は、モデルによって異なります。[インスタンスの要件と前提条件 \(16 ページ\)](#) を参照してください。

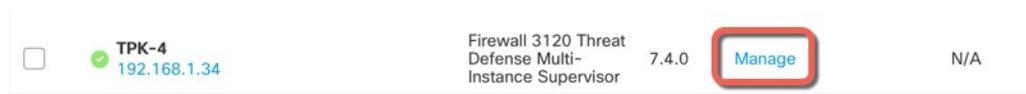
始める前に

[デバイスのマルチインスタンスモードへの変換 \(21 ページ\)](#)。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] で、[シャーシ (Chassis)] 列の [管理 (Manage)] をクリックするか **Edit** (🔗) をクリックします。

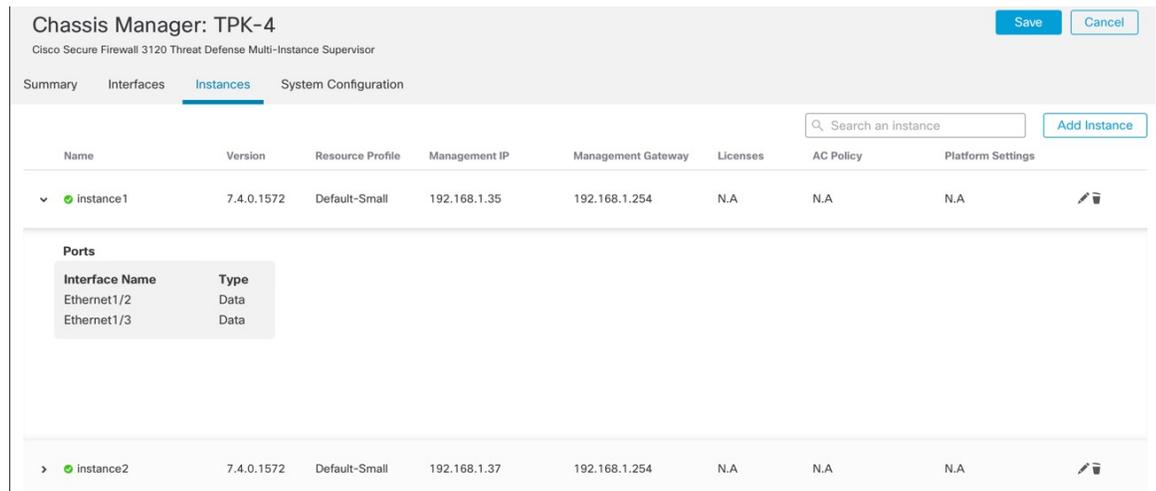
図 30: シャーシの管理



シャーシの [シャーシマネージャ (Chassis Manager)] ページが開き、[要約 (Summary)] ページが表示されます。

ステップ 2 [インスタンス (Instances)] をクリックし、[インスタンスの追加 (Add Instance)] をクリックします。

図 31: Instances



ステップ 3 [契約 (Agreement)] で、[契約の内容について理解し、同意します (I understand and accept the agreement)] をオンにし、[次へ (Next)] をクリックします。

図 32: 契約

Add Instance

1 Agreement — 2 Instance Configuration — 3 Interface Assignment — 4 Device Management — 5 Summary

End User License Agreement
Effective: May 10, 2022
Secure Firewall Terms and Conditions
By clicking 'Accept' below or using this Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and applicable Product Specific Terms available at:
<https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html>
You also acknowledge that you have read the Cisco Privacy Statement at:
<https://www.cisco.com/c/en/us/about/legal/privacy-full.html>
If you are a Cisco partner accepting on behalf of an end customer, you must inform the end customer that the EULA applies to such end customer's use of the Cisco Technology and provide the end customer with access to all relevant terms. If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'Accept' and do not use the Cisco Technology.
 I understand and accept the agreement.

Cancel Next

ステップ 4 [インスタンス設定 (Instance Configuration)] でインスタンスパラメータを設定し、[次へ (Next)] をクリックします。

図 33: インスタンス設定

Add Instance
✕

① Agreement
② Instance Configuration
③ Interface Assignment
④ Device Management
⑤ Summary

Display Name*

Device Version*

IPv4

Management IP*

Network Mask*

Network Gateway*

FQDN

Firewall Mode*

DNS Servers

Permit Expert mode for CLI

Resource Profile*
 +

Device SSH Password*

Confirm Password*

Show Password

Cancel
Back
Next

• Display Name

- [デバイスバージョン (Device Version)]: リストされているバージョンは、現在シャーシにダウンロードされているパッケージです。パッチバージョンは、バンドル全体が含まれていないため、表示されず、使用できません。新しいパッケージにアップグレードするには、を参照してください。アップグレードすると、古い Firewall Threat Defense バージョンと新しい Firewall Threat Defense バージョンの両方がメニューに表示されます。古いパッケージをダウンロードするには、FXOSCLIを使用する必要があります。注: FXOS イメージと Firewall Threat Defense イメージの両方が同じパッケージに含まれています。詳細については、『[トラブルシューティング ガイド](#)』を参照してください。

次に例を示します。

```
firepower-3110# scope firmware
firepower-3110# download image
https://10.10.7.89/Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-1.sh.DEV.tar
Please use the command 'show download-task' or 'show download-task detail' to check
download progress.
```

```
※ Download-task Cisco_FTD_SSP_FP3K_Upgrade-7.4.1-1.sh.DEV.tar : completed successfully.
```

- [IPv4]、[IPv6]、または [両方 (Both)] : シャーシの管理インターフェイスと同じネットワーク上の管理 IP アドレスを設定します。ネットワークマスクとゲートウェイを設定します (シャーシと同じゲートウェイである可能性があります)。シャーシの管理インターフェイスは各インスタンスと共有され、各インスタンスはネットワーク上で独自の IP アドレスを持ちます。デフォルトで、この IP アドレスに SSH で接続して Firewall Threat Defense CLI にアクセスできます。
- (任意) **FQDN**
- [ファイアウォールモード (Firewall Mode)] : [ルーテッド (Routed)] または [透過的 (Transparent)]。ファイアウォールモードの詳細については、[トランスペアレントファイアウォールモード](#)または[ルーテッドファイアウォールモード](#)を参照してください。
- [DNSサーバー (DNS Servers)] : 管理トラフィック専用の DNS サーバーのコンマ区切りリストを入力します。
- (任意) [CLIのエキスパートモードの許可 (Permit Expert Mode for CLI)] : エキスパートモードでは、高度なトラブルシューティングに Firewall Threat Defense シェルからアクセスできます。

このオプションを有効にすると、SSH セッションからインスタンスに直接アクセスするユーザーがエキスパートモードを開始できます。このオプションを無効にすると、FXOS CLI からインスタンスにアクセスするユーザーのみがエキスパートモードを開始できます。インスタンス間の分離を増やすには、このオプションを無効にすることをお勧めします。

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

- [リソースプロファイル (Resource Profile)] : リソースプロファイルは CPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。シャーシには、Default-Small、Default-Medium、Default-Large のデフォルトリソースプロファイルが含まれています。Add (+) をクリックすると、このシャーシのプロファイルを追加できます。後でリソースプロファイルを編集することはできません。

図 34: リソースプロファイルの追加

Add resource profile

Name*

silver

(Set the name of the profile between 1 and 64 characters.)

Description

Number of Cores*

24

Assign an even number of cores, 6 to 100.

Cancel Add

- コアの最小数は 6 です。

(注)

コア数が少ないインスタンスは、コア数が多いインスタンスよりも、CPU 使用率が比較的高くなる場合があります。コア数が少ないインスタンスは、トラフィック負荷の変化の影響を受けやすくなります。トラフィックのドロップが発生した場合には、より多くのコアを割り当ててください。

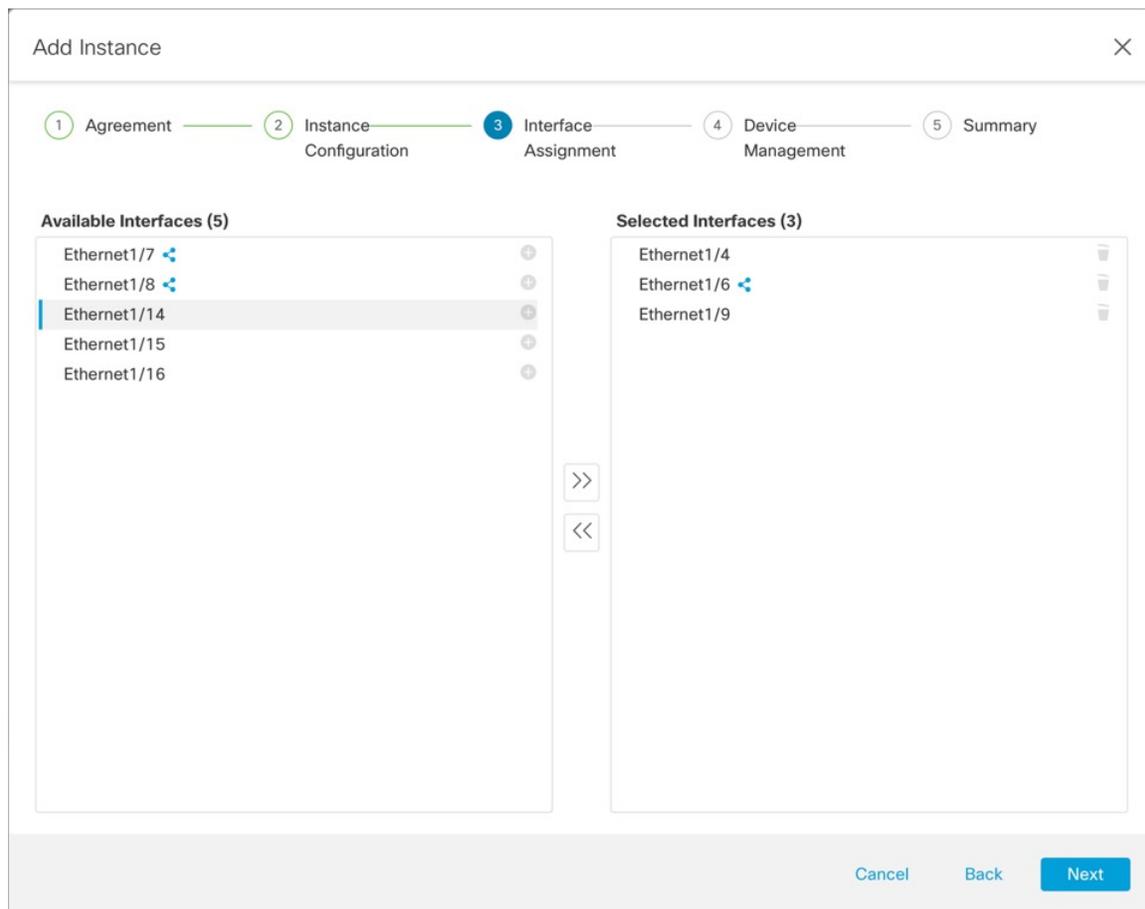
- コアは偶数（6、8、10、12、14 など）で最大値まで割り当てることができます。
- 利用可能な最大コア数は、モデルによって異なります。[インスタンスの要件と前提条件（16 ページ）](#)を参照してください。

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

- [デバイス SSH パスワード (Device SSH Password)] : CLI アクセス用の Firewall Threat Defense 管理者ユーザーパスワード (SSH またはコンソール) を設定します。[パスワードの確認 (Confirm Password)] フィールドにパスワードをもう一度入力します。

ステップ 5 [インターフェイスの割り当て (Interface Assignment)] で、シャードインターフェイスをインスタンスに割り当て、[次へ (Next)] をクリックします。

図 35: インターフェイスの割り当て



共有インターフェイスには、共有アイコン（）が表示されます。

ステップ 6 [デバイス管理 (Device Management)] で、デバイス固有の設定を行い、[次へ (Next)] をクリックします。

図 36: デバイス管理

- **Device Group**

- [アクセス制御ポリシー (Access Control Policy)] : 既存のアクセス制御ポリシーを選択するか、新しいポリシーを作成します。

- [プラットフォーム設定 (Platform Settings)] : 既存のプラットフォーム設定ポリシーを選択するか、新しいポリシーを作成します。

- **スマートライセンス**

ステップ7 [要約 (Summary)] で設定を確認し、[保存 (Save)] をクリックします。

図 37: サマリー

Add Instance

1 Agreement — 2 Instance Configuration — 3 Interface Assignment — 4 Device Management — 5 Summary

Instance Configuration		Device Management - This info is required only during instance creation.	
Name:	instance4	Auto registration:	true
Version:	7.4.0.1572	Access Policy:	inside-outside
Resource Profile:	Default-Small	Device Group:	
IP:	192.168.1.38	Platform Policy:	instance-settings
Mask:	255.255.255.0	Licenses:	MALWARE,THREAT,URLFilter
Gateway:	192.168.1.254		
Mode:	routed		
Password:	*****		
FQDN:	cisco-fw-4.cisco.com		
Expert Mode:	enabled		

Interface Assignment - 2 dedicated and 1 shared interfaces attached [Show All](#)

Cancel Back Save

インスタンスを保存する前に、この画面で設定を編集できます。保存すると、[インスタンス (Instances)] 画面にインスタンスが追加されます。

ステップ 8 [インスタンス (Instances)] 画面で、[保存 (Save)] をクリックします。

ステップ 9 シャーシ構成を展開します。

展開後、インスタンスは [デバイス管理 (Device Management)] ページにデバイスとして追加されます。

システム設定のカスタマイズ

SNMP などのシャーシレベルの設定を行うことができます。また、シャーシ FXOS 設定をインポートまたはエクスポートすることもできます。

SNMP の構成

シャーシレベルの MIB には、いずれかのインスタンスのデータインターフェイスを介してアクセスできます。これは、シャーシのシステム構成で指定します。このインスタンスは、シャーシ SNMP 情報にのみ使用できます。シャーシの管理インターフェイスを介して SNMP にアクセスすることはできません。

始める前に

インスタンスの 1 つに SNMP を設定します。SNMP を参照してください。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] で、[シャーシ (Chassis)] 列の [管理 (Manage)] をクリックするか **Edit** (🔗) をクリックします。

図 38: シャーシの管理

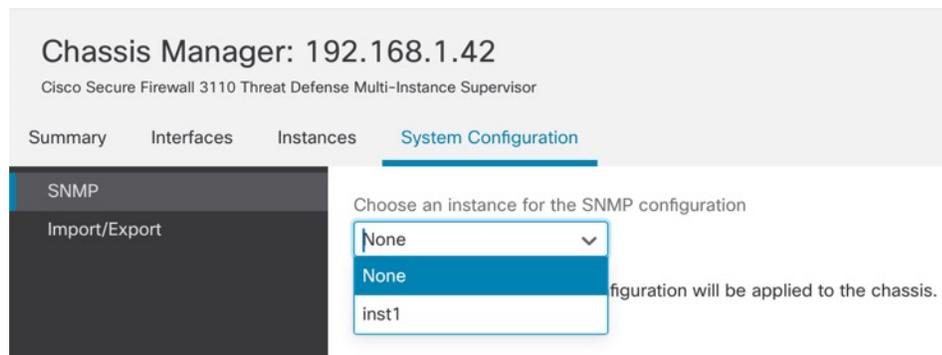


シャーシの [シャーシマネージャ (Chassis Manager)] ページが開き、[要約 (Summary)] ページが表示されます。

ステップ 2 [システム構成 (System Configuration)] をクリックします。

ステップ 3 [SNMP] をクリックして、ドロップダウンリストからインスタンスを選択します。

図 39: SNMP



選択したインスタンスからシャーシの SNMP にアクセスできます。

ステップ 4 [Save (保存)] をクリックします。

ステップ 5 シャーシ構成を展開します。

シャーシ設定のインポートまたはエクスポート

設定のエクスポート機能を使用して、シャーシのコンフィグレーション設定を含む XML ファイルをローカルコンピュータにエクスポートできます。そのコンフィギュレーションファイルの後でインポートしてシャーシに迅速にコンフィギュレーション設定を適用し、よくわかっている構成に戻したり、システム障害から回復させたりすることができます。また、前提条件が満たされていれば、RMA などの新しいシャーシにシャーシ設定をインポートすることもできます。

エクスポートする場合、シャーシ設定のみがエクスポートされます。インスタンスのコンフィギュレーション設定はエクスポートされません。インスタンスは、デバイスのバックアップ/復元機能を使用して個別にバックアップする必要があります。

インポートすると、シャーシの既存のすべての設定がインポートファイルの設定に置き換えられます。

始める前に

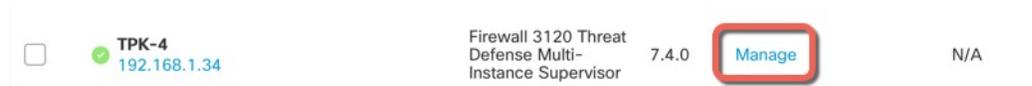
設定をインポートするシャーシでは、以下の特性が一致している必要があります。

- 同じシャーシ ソフトウェア バージョン
- 同じ Firewall Threat Defense インスタンスイメージ
- 同じネットワークモジュール

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] で、[シャーシ (Chassis)] 列の [管理 (Manage)] をクリックするか **Edit** (🔗) をクリックします。

図 40: シャーシの管理



シャーシの [シャーシマネージャ (Chassis Manager)] ページが開き、[要約 (Summary)] ページが表示されます。

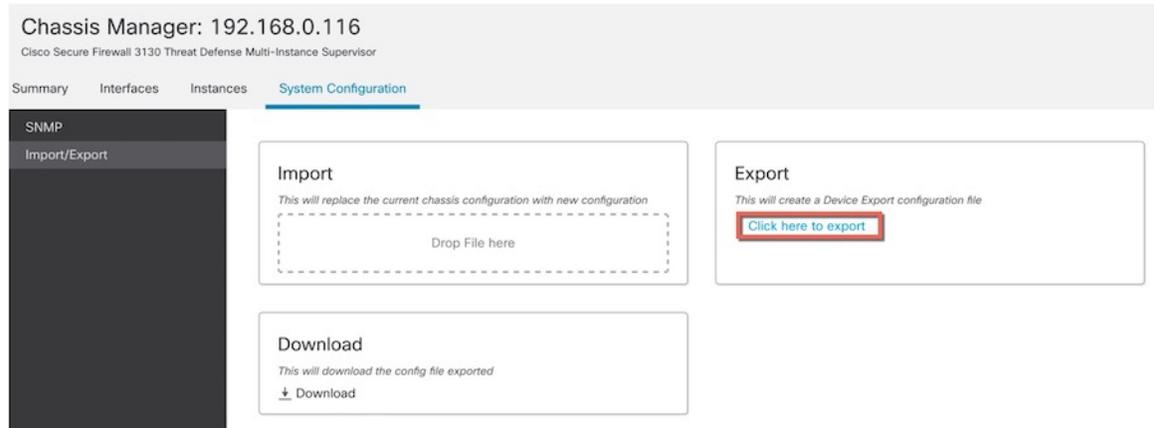
ステップ 2 [システム設定 (System Configuration)] をクリックします。

ステップ 3 [インポート/エクスポート (Import/Export)] をクリックします。

ステップ 4 設定をエクスポートするには、以下の手順を実行します。

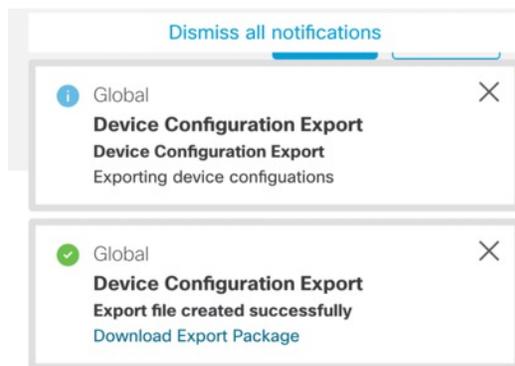
- [エクスポート (Export)] エリアで、[エクスポートするにはここをクリック (Click here to export)] をクリックします。

図 41: エクスポートファイルの作成



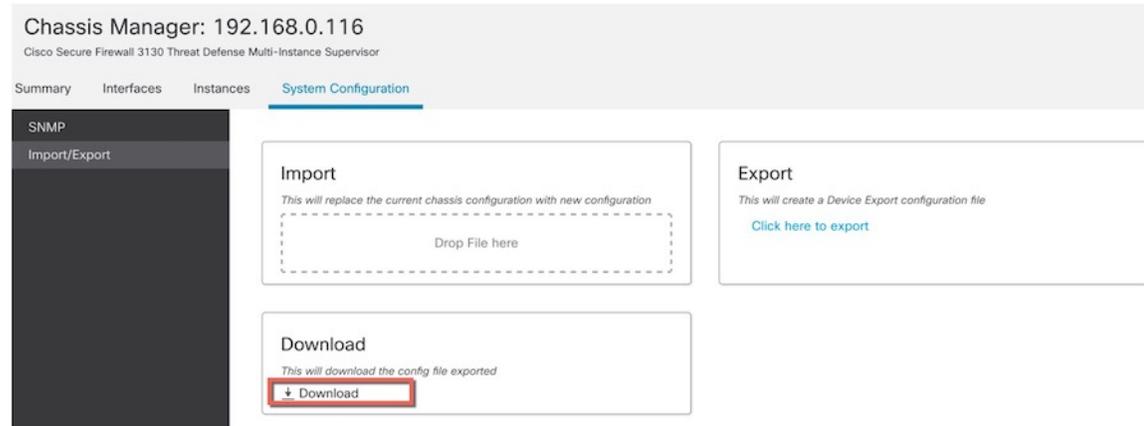
- b) [エクスポートファイルが正常に作成されました (Export file created successfully)] という通知をモニタリングします。

図 42: エクスポートファイルが正常に作成されました



- c) 通知メッセージ ([エクスポートパッケージのダウンロード (Download Export Package)]) をクリックするか、[ダウンロード (Download)] をクリックして、エクスポートファイルをダウンロードします。

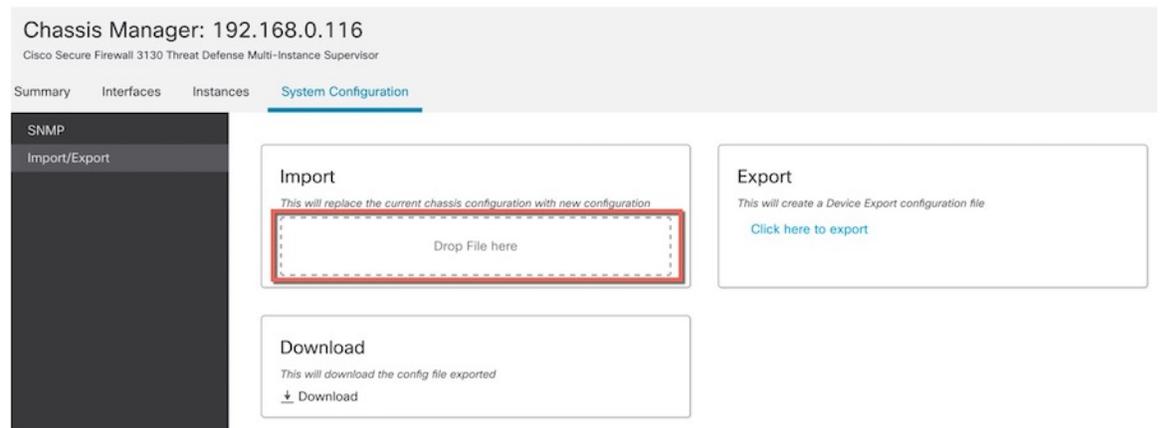
図 43: ダウンロード



ファイルは **.sfo** 拡張子で保存されます。

ステップ 5 設定をインポートするには、[インポート (**Import**)] > [ここにファイルをドロップ (**Drop File here**)] エリアに **.sfo** ファイルをドラッグします。

図 44: インポート



シャーシプラットフォームの設定

シャーシプラットフォーム設定では、シャーシを管理するためのさまざまな機能を設定します。複数のシャーシ間でポリシーを共有できます。シャーシごとに異なる設定が必要な場合は、複数のポリシーを作成する必要があります。

シャーシプラットフォーム設定ポリシーの作成

[プラットフォームの設定 (Platform Settings)] ページ (**Devices > Platform Settings**) を使用して、プラットフォーム設定ポリシーを管理します。このページには、各ポリシーのデバイスの

タイプが示されます。[ステータス (Status)]列で、ポリシーのデバイスターゲットが示されます。

手順

ステップ 1 **Devices > Platform Settings** を選択します。

ステップ 2 既存のポリシーの場合は、ポリシーを **Copy** (📄)、**Edit** (✎)、または **Delete** (🗑️) できます。

注意

どのターゲットデバイスでも、最後に展開したポリシーは期限切れであっても削除しないでください。ポリシーを完全に削除する前に、それらのターゲットに別のポリシーを展開するようにしてください。

ステップ 3 新しいポリシーを作成するには、[新しいポリシー (New Policy)] をクリックします。

- ドロップダウンリストから [シャーシプラットフォームの設定 (Chassis Platform Settings)] を選択します。
- 新しいポリシーの [名前 (Name)]、および必要に応じて [説明 (Description)] を入力します。
- 必要に応じて、ポリシーを適用する [使用可能なシャーシ (Available Chassis)] を選択し、[追加 (Add)] をクリック (またはドラッグ & ドロップ) して、選択したデバイスを追加します。[検索 (Search)] フィールドに検索文字列を入力して、シャーシのリストを絞り込むことができます。
- [保存 (Save)] をクリックします。

システムにより、ポリシーが作成され、編集のために開かれます。

ステップ 4 ポリシーのターゲットシャーシを変更するには、編集するプラットフォーム設定ポリシーの横にある **Edit** (✎) をクリックします。

- [ポリシーの割り当て (Policy Assignment)] をクリックします。
- ポリシーにシャーシを割り当てるには、[使用可能なシャーシ (Available Chassis)] リストでシャーシを選択し、[追加 (Add)] をクリックします。ドラッグアンドドロップを使用することもできます。
- シャーシの割り当てを削除するには、[選択したシャーシ (Selected Chassis)] リストでシャーシの横にある **Delete** (🗑️) をクリックします。
- [OK] をクリックします。

DNS の設定

シャーシでホスト名の IP アドレスへの解決が必要な場合は、DNS サーバーを指定する必要があります。これらのシャーシ DNS 設定は、デバイスプラットフォーム設定で設定されるインスタンスごとの DNS 設定とは異なります。

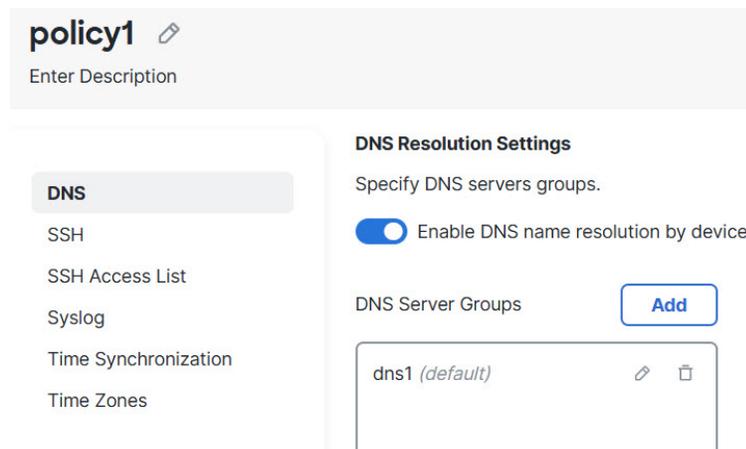
複数の DNS サーバーを設定する場合、シャーンによるサーバーの使用順はランダムになります。4 つの DNS サーバーグループにまたがって最大 4 つのサーバーを設定できます。たとえば、4 台のサーバーで 1 つのサーバーグループを設定したり、それぞれ 1 台のサーバーで 4 つのサーバーグループを設定したりできます。

手順

ステップ 1 [Devices > Platform Settings] を選択して、シャーンポリシーを作成するか編集します。

ステップ 2 [DNS] を選択します。

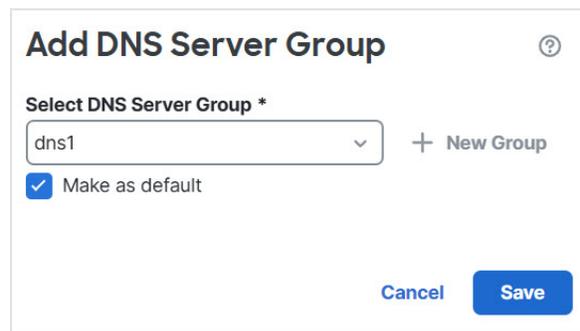
図 45: DNS



ステップ 3 [デバイスによるDNS名解決を有効にする (Enable DNS name resolution by device)] スライダを有効にします。

ステップ 4 [追加 (Add)] をクリックし、DNS サーバーグループを追加します。

図 46: DNS サーバーグループの追加



ステップ 5 既存の DNS サーバーグループを選択するか ([DNS サーバーグループオブジェクトの作成](#) を参照)、 (+) をクリックして [新しいグループ (New Group)] をクリックします。

新しいグループを追加すると、以下のダイアログボックスが表示されます。名前と、最大4つの DNS サーバー IP アドレスをカンマ区切り値として指定し、[追加 (Add)] をクリックします。

図 47: 新しい DNS サーバー グループ オブジェクト

ステップ 6 [保存 (Save)] をクリックすると、DNS サーバーがリストに追加されます。

ステップ 7 さらにサーバーグループを追加するには、こちらの手順を繰り返します。

指定できる DNS サーバーは、すべてのグループを合わせて最大 4 つです。

ステップ 8 [保存 (Save)] をクリックし、すべてのポリシー変更を保存します。

SSH および SSH アクセスリストの設定

管理インターフェイスで管理ユーザーからシャーマシへの SSH セッションを許可するには、SSH サーバーを有効にし、許可されたネットワークを設定します。

手順

ステップ 1 [Devices > Platform Settings] を選択して、シャーマシポリシーを作成するか編集します。

ステップ 2 [SSH] を選択します。

ステップ 3 シャーマシへの SSH アクセスを有効にするには、[SSHサーバーの有効化 (Enable SSH Server)] スライダを有効にします。

図 48 : SSH

policy1 [Edit](#) You have unsaved changes [Cancel](#) [Save](#)

Enter Description Policy Assignments (0)

DNS

SSH

SSH Access List

Syslog

Time Synchronization

Time Zones

SSH Server

Enable SSH Server

Algorithms [Edit](#)

Encryption

- aes128-cbc
- aes128-ctr
- aes128-gcm_openssh_com
- aes192-cbc
- aes192-ctr
- aes256-cbc
- aes256-ctr

Host Key*

Volume Rekey Limit KB

Time Rekey Limit Minutes

SSH Client

Strict Host Keycheck

Algorithms [Edit](#)

Encryption

- aes128-cbc
- aes128-ctr
- aes128-gcm_openssh_com
- aes192-cbc
- aes192-ctr
- aes256-cbc
- aes256-ctr

Volume Rekey Limit KB

Time Rekey Limit Minutes

ステップ 4 許可される [アルゴリズム (Algorithms)] を設定するには、**Edit** (🔗) をクリックします。

図 49 : アルゴリズムの追加

Add Algorithms ?

Available Algorithms (17)

- aes256-cbc +
- aes256-ctr +
- chacha20-poly1305_openssh_com +
- Key Exchange
- curve25519-sha256 +
- curve25519-sha256_libssh_org +
- diffie-hellman-group14-sha1 +
- diffie-hellman-group14-sha256 +
- ecdh-sha2-nistp256 +
- ecdh-sha2-nistp384 +
- Mac
- hmac-sha-1 +

Selected Algorithms (3)

- Encryption
 - aes256-gcm_openssh_com 🗑️
- Key Exchange
 - ecdh-sha2-nistp521 🗑️
- Mac
 - hmac-sha2-512 🗑️

[Cancel](#) [Add](#)

- a) [暗号化 (Encryption)] アルゴリズムを選択します。
- b) [キー交換 (Key Exchange)] アルゴリズムを選択します。

キー交換では、いずれの当事者も単独では決定できない共有秘密を使用します。キー交換を署名およびホストキーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。

- c) [Mac] 整合性アルゴリズムを選択します。

ステップ 5 [ホストキー (Host Key)] では、RSA キーペアのモジュラスサイズを入力します。

モジュラス値 (ビット単位) は、1024 ~ 2048 の範囲内の 8 の倍数です。指定するキー係数のサイズが大きいほど、RSA キーペアの生成にかかる時間は長くなります。値は 2048 にすることを勧めます。

ステップ 6 サーバの [キー再生成のボリューム制限 (Volume Rekey Limit)] に、FXOS がセッションを切断するまでにその接続で許可されるトラフィックの量を KB 単位で設定します。

ステップ 7 サーバの [キー再生成の時間制限 (Time Rekey Limit)] では、FXOS がセッションを切断する前に SSH セッションがアイドル状態を続けられる長さを分単位で設定します。

ステップ 8 [SSHクライアント (SSH Client)] では、次の設定を行います。

図 50: SSH

The screenshot shows the configuration page for 'policy1'. On the left is a navigation menu with 'SSH' selected. The main area is divided into two panels: 'SSH Server' and 'SSH Client'.
 In the 'SSH Server' panel:
 - 'Enable SSH Server' is a checked toggle.
 - 'Algorithms' is a list box containing: aes128-cbc, aes128-ctr, aes128-gcm_openssh_com, aes192-cbc, aes192-ctr, aes256-cbc, aes256-ctr.
 - 'Host Key*' is a text input field with '2048'.
 - 'Volume Rekey Limit' is a dropdown menu with 'none' selected, followed by 'KB'.
 - 'Time Rekey Limit' is a dropdown menu with 'none' selected, followed by 'Minutes'.
 In the 'SSH Client' panel:
 - 'Strict Host Keycheck' is a dropdown menu with 'disable' selected.
 - 'Algorithms' is a list box containing the same encryption methods as the server.
 - 'Volume Rekey Limit' is a dropdown menu with 'none' selected, followed by 'KB'.
 - 'Time Rekey Limit' is a dropdown menu with 'none' selected, followed by 'Minutes'.
 At the top right, there is a red notification 'You have unsaved changes' and 'Cancel' and 'Save' buttons.

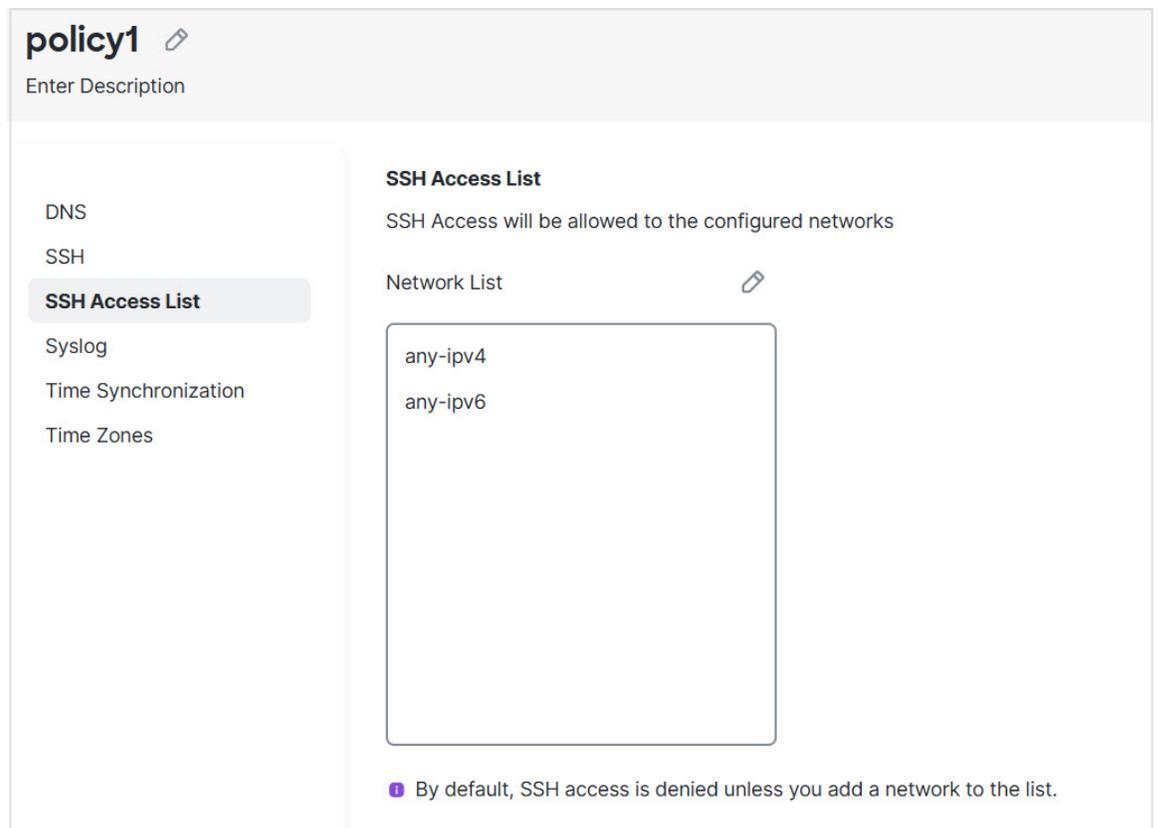
- [厳格なホストキーチェック (Strict Host Keycheck)]: [有効 (enable)], [無効 (disable)], または [プロンプト (prompt)] を選択して、SSH ホストキーチェックを制御します。
 - enable: FXOS が認識するホスト ファイルにそのホスト キーがまだ存在しない場合、接続は拒否されます。FXOS CLI でシステム スコープまたはサービス スコープの **enter ssh-host** コマンドを使用して、手動でホストを追加する必要があります。
 - prompt: シャーシにまだ格納されていないホストキーを許可または拒否するように求められます。

- **disable** : (デフォルト) シャーシは過去に保存されたことがないホストキーを自動的に許可します。
- [アルゴリズム (Algorithms)] : **Edit** (🔗) をクリックします。[暗号化 (Encryption)]、[キー交換 (Key Exchange)]、および [Mac] アルゴリズムを選択します。
- [キー再生成のボリューム制限 (Volume Rekey Limit)] : その接続で許可されるトラフィックの量の上限を KB 単位で設定します。この値を超えると FXOS はセッションを切断します。
- [キー再生成の時間制限 (Time Rekey Limit)] : FXOS がセッションを切断する前に SSH セッションがアイドルであることができる時間を分単位で設定します。

ステップ 9 [SSHアクセスリスト (SSH Access List)] を選択します。SSH を使用するには、IP アドレスまたはネットワークへのアクセスを許可する必要があります。

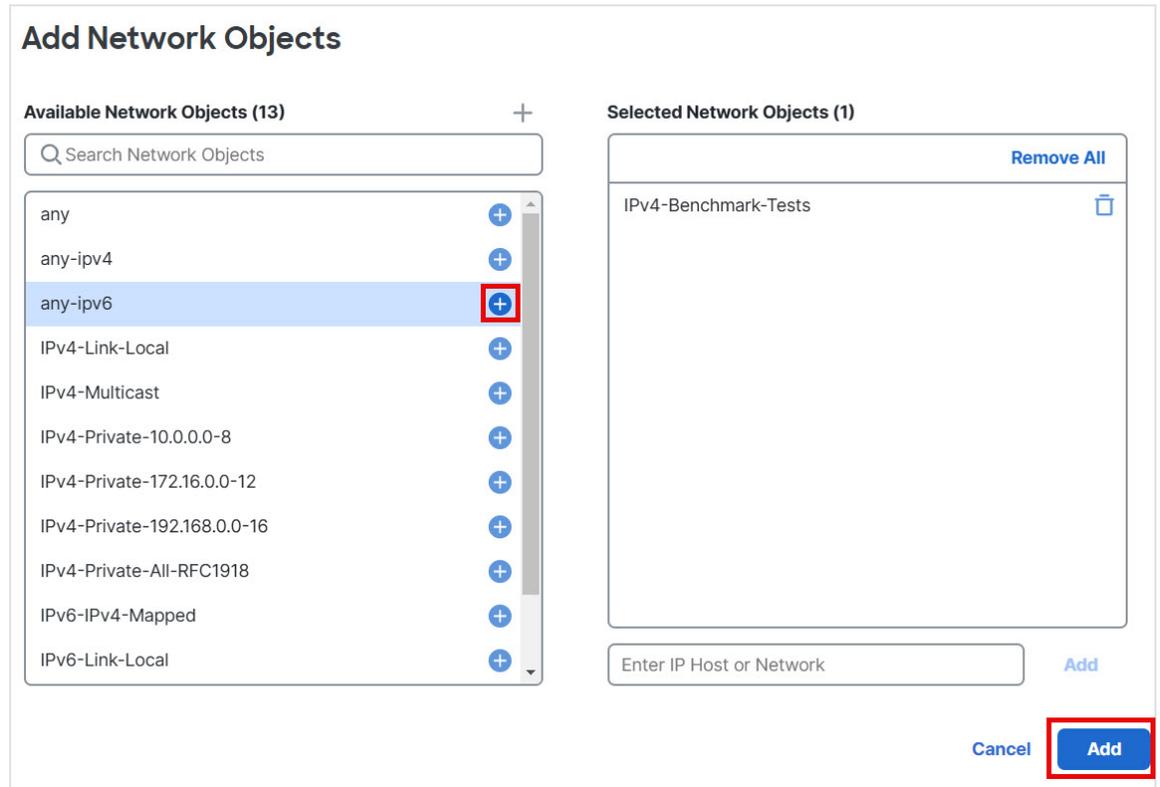
最大 25 のアクセスリストを追加できます。

図 51 : SSH アクセスリスト



ステップ 10 **Edit** (🔗) をクリックしてネットワークオブジェクトを追加し、[保存 (Save)] をクリックします。IP アドレスを手動で入力することもできます。

図 52: ネットワーク オブジェクト



ステップ 11 [保存 (Save)] をクリックし、すべてのポリシー変更を保存します。

Syslog の設定

シャーシから Syslog を有効化できます。これらの Syslog は、シャーシの FXOS オペレーティングシステムから取得されます。

手順

- ステップ 1 [Devices > Platform Settings] を選択して、シャーシポリシーを作成するか編集します。
- ステップ 2 [Syslog] を選択します。
- ステップ 3 [ローカル宛先 (Local Destinations)] をクリックし、以下のフィールドに入力します。

図 53 : Syslog のローカル接続先

名前	説明
[コンソール (Console)] セクション	
[管理状態 (Administrative State)] フィールド	<p>シャージがコンソールに syslog メッセージを表示するかどうかを指定します。</p> <p>ログに追加するとともに、コンソールに syslog メッセージを表示する場合は、[有効化 (Enable)] チェックボックスをオンにします。[有効 (Enable)] チェックボックスをオフにすると、syslog メッセージはログに追加されますが、コンソールに表示されません。</p>
[Level] フィールド	<p>[コンソール (Console)] > [管理状態 (Admin State)] で [有効化 (Enable)] チェックボックスをオンにした場合は、コンソールに表示する最低のメッセージ レベルを選択します。シャージのコンソールにはそのレベル以上のメッセージが表示されます。次のいずれかになります。</p> <ul style="list-style-type: none"> • 緊急 (Emergencies) • アラート (Alerts) • クリティカル (Critical)

名前	説明
[モニタ (Monitor)] セクション	
[管理状態 (Administrative State)] フィールド	<p>シャーンがモニタに syslog メッセージを表示するかどうかを指定します。</p> <p>syslog メッセージをログに追加するとともに、モニタに表示する場合は、[有効化 (Enable)] チェックボックスをオンにします。[有効 (Enable)] チェックボックスをオフにすると、syslog メッセージはログに追加されますが、モニタに表示されません。</p>
[レベル (Level)] ドロップダウン リスト	<p>[モニタ (Monitor)] > [管理状態 (Admin State)] で [有効 (Enable)] チェックボックスをオンにした場合は、モニタに表示する最低のメッセージレベルを選択します。モニタにはそのレベル以上のメッセージが表示されます。次のいずれかになります。</p> <ul style="list-style-type: none"> • 緊急 (Emergencies) • アラート (Alerts) • クリティカル (Critical) • [Errors] • [Warnings] • [Notifications] • [Information] • [Debugging]

ステップ 4 [リモート接続先 (Remote Destinations)] 領域で、シャーンによって生成されたメッセージを保存できる最大 3 個の外部ログの次のフィールドに入力します。

図 54 : Syslog のリモート接続先

The screenshot shows the configuration page for 'policy1' in the Syslog section. The 'Remote Destinations' tab is active, displaying three server configurations:

- Server1:** Enabled (checked), Level: Critical, Hostname: 10.89.4.2, Facility: Local7.
- Server2:** Disabled (unchecked), Level: Critical, Hostname: (empty), Facility: Local7.
- Server3:** Disabled (unchecked), Level: Critical, Hostname: (empty), Facility: Local7.

On the left sidebar, the 'Syslog' option is selected under the 'policy1' header. Other options include DNS, SSH, SSH Access List, Time Synchronization, and Time Zones.

syslog メッセージをリモート宛先に送信することで、外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、保存後にロギングデータを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたり、ログからデータが抽出されてレポート用の別のファイルにその記録が保存されたり、あるいはサイト固有のスクリプトを使用して統計情報が追跡されたりした場合に、特別なアクションが実行されるように指定できます。

名前	説明
[管理状態 (Admin State)] フィールド	リモート ログ ファイルに syslog メッセージを保存する場合は、[有効 (Enable)] チェックボックスをオンにします。
[レベル (Level)] ドロップダウン リスト	システムに保存するメッセージの最低レベルを選択します。リモート ファイルにそのレベル以上のメッセージが保存されます。次のいずれかになります。 <ul style="list-style-type: none"> • 緊急 (Emergencies) • アラート (Alerts) • クリティカル (Critical) • [Errors] • [Warnings] • [Notifications] • [Information] • [Debugging]
[ホスト名/IPアドレス (Hostname/IP Address)] フィールド	リモート ログ ファイルが存在するホスト名または IP アドレス。 (注) IP アドレスではなく、ホスト名を使用する場合は、DNS サーバを設定する必要があります。
[ファシリティ (Facility)] ドロップダウン リスト	ファイル メッセージのベースとして使用する syslog サーバのシステム ログ機能を選択します。次のいずれかになります。 <ul style="list-style-type: none"> • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7

ステップ 5 [ローカル送信元 (Local Sources)] をクリックし、以下のフィールドに入力します。

図 55: Syslog のローカル送信元

名前	説明
障害 > 管理状態の有効化	システム障害ロギングを有効にします。
監査 > 管理状態の有効化	監査ログを有効にします。
イベント > 管理状態の有効化	システムイベントロギングを有効にします。

ステップ 6 [保存 (Save)] をクリックし、すべてのポリシー変更を保存します。

時刻同期の設定

NTP を使用して階層的なサーバシステムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。最大 4 台の NTP サーバを設定できます。



- (注)
- FXOS では、NTP バージョン 3 を使用します。
 - 外部 NTP サーバのストラタム値が 13 以上の場合、アプリケーションインスタンスは FXOS シャーシ上の NTP サーバと同期できません。NTP クライアントが NTP サーバと同期するたびに、ストラタム値が 1 ずつ増加します。
- 独自の NTP サーバをセットアップしている場合は、サーバ上の `/etc/ntp.conf` ファイルでそのストラタム値を確認できます。NTP サーバのストラタム値が 13 以上の場合は、`ntp.conf` ファイルのストラタム値を変更してサーバを再起動するか、別の NTP サーバ（たとえば、`pool.ntp.org`）を使用することができます。

始める前に

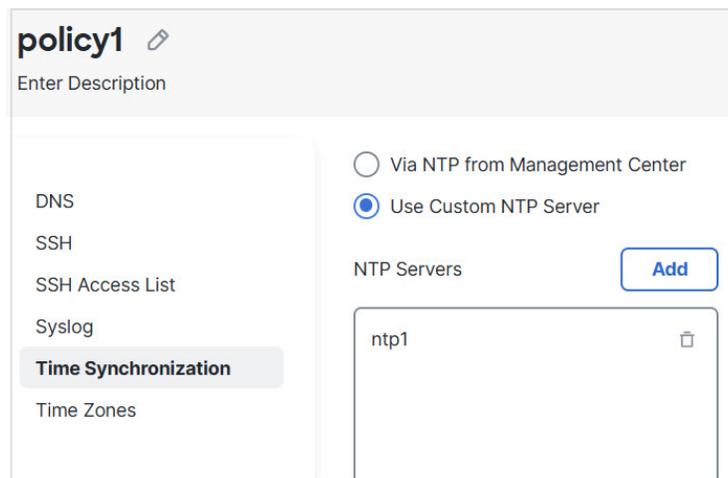
NTP サーバのホスト名を使用する場合は、DNS サーバを設定する必要があります。[DNS の設定 \(48 ページ\)](#) を参照してください。

手順

ステップ 1 [Devices > Platform Settings] を選択して、シャーシポリシーを作成するか編集します。

ステップ 2 [時刻の同期 (Time Synchronization)] を選択します。

図 56: 時刻の同期



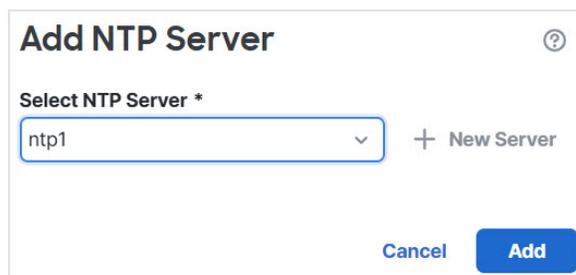
ステップ 3 Firewall Management Center から時刻を取得する場合は、[Management CenterのNTP経由 (Via NTP from Management Center)] をクリックします。

このオプションにより、シャーシと Firewall Management Center の両方が同じ時刻になります。

ステップ 4 外部 NTP サーバーを使用するには、[カスタムNTPサーバーを使用 (Use Custom NTP Server)] をクリックします。

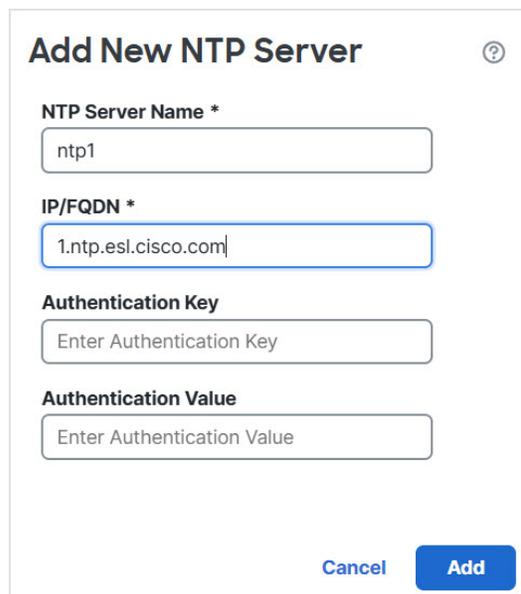
a) [追加 (Add)] をクリックしてサーバーを追加します。

図 57: NTP サーバーの追加



- b) ドロップダウンメニューから定義済みのサーバーを選択して [追加 (Add)] をクリックするか、[追加 (Add)] アイコン > [新規サーバー (New Server)] をクリックして新しいサーバーを追加します。+

図 58: 新しい NTP サーバーの追加



Add New NTP Server ⓘ

NTP Server Name *
ntp1

IP/FQDN *
1.ntp.esl.cisco.com

Authentication Key
Enter Authentication Key

Authentication Value
Enter Authentication Value

Cancel Add

- c) 新しいサーバーの場合は、次のフィールドに入力し、[追加 (Add)] をクリックします。
- [NTPサーバー名 (NTP Server Name)] : このサーバーを識別するための名前。
 - [IP/FQDN] : サーバーの IP アドレスまたはホスト名。
 - [認証キー (Authentication key)] および [認証値 (authentication VALUE)] : NTP サーバーからキー ID と値を取得します。たとえば、OpenSSL がインストールされた NTP サーババージョン 4.2.8 p8 以降で SHA1 キーを生成するには、**ntp-keygen -M** コマンドを入力して ntp.keys ファイルでキー ID と値を確認します。このキーは、クライアントとサーバの両方に対して、メッセージダイジェストの計算時に使用するキー値を通知するために使用します。
- NTP サーバ認証では SHA1 のみがサポートされます。

ステップ 5 [保存 (Save)] をクリックし、すべてのポリシー変更を保存します。

タイムゾーンの設定

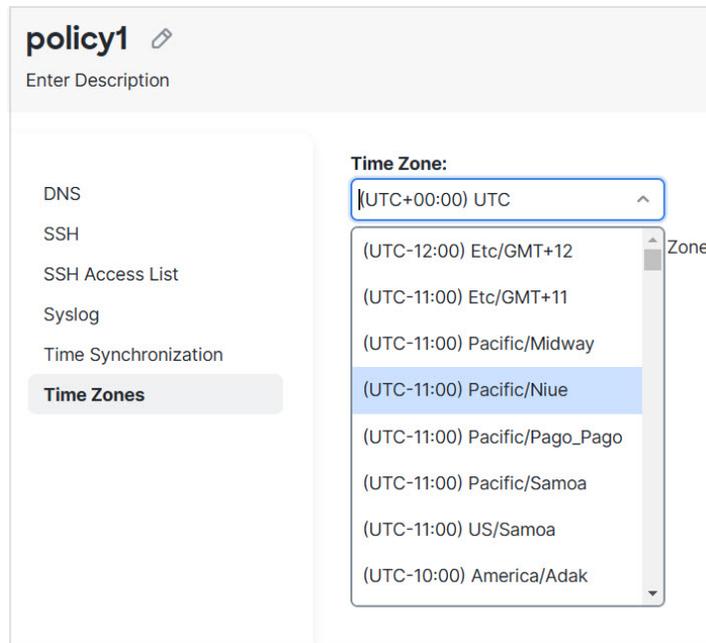
シャーシのタイムゾーンを設定します。

手順

ステップ 1 [Devices > Platform Settings] を選択して、シャードポリシーを作成するか編集します。

ステップ 2 [タイムゾーン (Time Zones)] を選択します。

図 59: タイムゾーン



ステップ 3 ドロップダウンメニューから適切な [タイムゾーン (Time Zones)] を選択します。

ステップ 4 [保存 (Save)] をクリックし、すべてのポリシー変更を保存します。

マルチインスタンスモードの管理

このセクションでは、FXOS CLI での設定変更やシャードに割り当てられたインターフェイスの変更など、あまり一般的ではないタスクについて説明します。

CLI のマルチインスタンスモードの有効化

デバイスを Firewall Management Center に追加する前にマルチインスタンスモード用に事前設定する場合は、以下の手順を実行します。Firewall Management Center を使用してマルチインスタンスモードに変換するには、[デバイスのマルチインスタンスモードへの変換 \(21 ページ\)](#) を参照してください。

マルチインスタンスモードを有効にするには、コンソールポートで Firewall Threat Defense CLI に接続する必要があります。モードを設定したら、Firewall Management Center に追加できます。



- (注) 管理ポートで SSH に接続できますが、複数回の切断を避けるために、コンソールポートを使用することをお勧めします。この手順は、コンソールポートを対象としています。

手順

ステップ 1 シャーシコンソールポートに接続します。

コンソールポートは FXOS CLI に接続します。

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。

初めて FXOS にログインしたときは、パスワードを変更するよう求められます。

(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。[再イメージ化の手順](#)については、[FXOS のトラブルシューティングガイド](#)を参照してください。

例：

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: *****
Confirm new password: *****
Your password was updated successfully.

[...]

firepower#
```

ステップ 3 現在のモード（ネイティブまたはコンテナ）を確認します。モードがネイティブの場合は、この手順を続行してマルチインスタンス（コンテナ）モードに変換できます。

show system detail

例：

```
firepower # show system detail

Systems:
```

```
Name: firepower
Mode: Stand Alone
System IP Address: 172.16.0.50
System IPv6 Address: ::
System Owner:
System Site:
Deploy Mode: Native
Description for System:
firepower #
```

ステップ 4 Firewall Threat Defense CLI に接続します。

connect ftd

例 :

```
firepower# connect ftd
>
```

ステップ 5 Firewall Threat Defense に初めてログインすると、一般利用規約に同意するよう求められます。その後、CLI セットアップスクリプトが表示されます。

セットアップスクリプトを使用すると、管理インターフェイスの IP アドレスなどを設定できます。ただし、マルチインスタンスモードに変換すると、次の設定のみが保持されます。

- 管理者パスワード (初回ログイン時に設定)
- DNS サーバ
- Search domains

マルチインスタンス モード コマンドの一環として、管理 IP アドレスとゲートウェイをリセットします。マルチインスタンスモードに変換した後、FXOS CLI で管理設定を変更できます。[FXOS CLI のシャーン管理設定の変更 \(68 ページ\)](#) を参照してください。

ステップ 6 マルチインスタンスモードを有効にし、シャーン管理インターフェイスを設定し、Firewall Management Center を特定します。IPv4 および/または IPv6 の静的アドレス指定を使用できます。DHCP はサポートされていません。コマンドを入力すると、設定を消去してリポートするように求められます。**ERASE** (すべて大文字) を入力します。システムがリポートし、モード変更の一環として、コマンドで設定した管理ネットワーク設定と管理者パスワードを除いて設定が消去されます。シャーンのホスト名は「*firepower-model*」に設定されます。

IPv4 :

```
configure multi-instance network ipv4 ip_address network_mask gateway_ip_address manager  
manager_name {hostname | ipv4_address | DONTRESOLVE} registration_key nat_id
```

IPv6

```
configure multi-instance network ipv6 ipv6_address prefix_length gateway_ip_address manager  
manager_name {hostname | ipv6_address | DONTRESOLVE} registration_key nat_id
```

次の **manager** コンポーネントを参照してください。

- `{hostname | ipv4_address | DONTRESOLVE}` : Firewall Management Center の FQDN または IP アドレスのいずれかを指定します。双方向の SSL 暗号化通信チャネルを 2 台のデバイス間に確立するには、少なくとも 1 台のデバイス (Firewall Management Center または シャーシ) に到達可能な IP アドレスが必要です。このコマンドでマネージャのホスト名または IP アドレスを指定しない場合は、**DONTRESOLVE** を入力してください。この場合、シャーシに到達可能な IP アドレスまたはホスト名が必要となり、`nat-id` を指定する必要があります。
- `registration_key` : シャーシを登録するときに Firewall Management Center でも指定する任意のワンタイム登録キーを入力します。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、シャーシを登録するときに Firewall Management Center でも指定する任意の一意のワンタイム文字列を指定します。これはマネージャのアドレスまたはホスト名を指定しない場合に必須となりますが、ホスト名または IP アドレスを指定する場合でも、常に NAT ID を設定することを推奨します。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、Firewall Management Center に登録する他のデバイスには使用できません。

モードをアプライアンスモードに戻すには、FXOS CLI を使用し、**scope system**、**set deploymode native** の順に入力する必要があります。FXOS CLI の [シャーシ管理設定の変更 \(68 ページ\)](#) を参照してください。

例 :

```
> configure multi-instance network ipv4 172.16.0.104 255.255.255.0 172.16.0.1 manager
fmc1 172.16.0.103 impala67 winchester1
WARNING: This command will discard any FTD configuration (except admin's credentials).
Make sure you backup your content. All previous content will be lost. System is going
to be re-initialized.
Type ERASE to confirm:ERASE
Exit...
>
```

ステップ 7 Firewall Management Center にシャーシを追加します。 [シャーシの追加](#) を参照してください。

インスタンスに割り当てられたインターフェイスの変更

インスタンスのインターフェイスは割り当てたり、割り当て解除したりできます。新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、インスタンスの設定に与える影響は最小限です。インスタンスに影響を与えずに、割り当てられた EtherChannel のメンバーシップを編集することもできます。ただし、セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。

インターフェイスは、アクセスルール、NAT、SSL、アイデンティティルール、VPN、DHCP サーバーなど、インスタンスの設定における多くの場所で直接参照されている可能性があります。インターフェイスを削除すると、そのインターフェイスに関連付けられている設定がすべて削除されます。

セキュリティゾーンを参照するポリシーは影響を受けません。



(注) 高可用性を実現するには、他のユニットに対して同じインターフェイスの変更を行う必要があります。そうしなければ、高可用性が正しく機能しない可能性があります。

始める前に

- [インスタンスの設定 \(20 ページ\)](#) に従ってインターフェイスを設定します。
- すでに割り当てられているインターフェイスを EtherChannel に追加するには、まずインスタンスからインターフェイスの割り当てを解除し、次に EtherChannel にインターフェイスを追加する必要があります。新しい EtherChannel の場合、その後でインスタンスに EtherChannel を割り当てることができます。

手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] で、[シャーシ (Chassis)] 列の [管理 (Manage)] をクリックするか **Edit** (🔗) をクリックします。

図 60: シャーシの管理

<input type="checkbox"/>	● TPK-4 192.168.1.34	Firewall 3120 Threat Defense Multi- Instance Supervisor	7.4.0	Manage	N/A
--------------------------	---	---	-------	---------------	-----

シャーシの [シャーシマネージャ (Chassis Manager)] ページが開き、[要約 (Summary)] ページが表示されます。

ステップ 2 [インスタンス (Instances)] をクリックし、インターフェイスを変更するインスタンスの横にある **Edit** (🔗) をクリックします。

図 61: Instances

Chassis Manager: TPK-4 Save Cancel

Cisco Secure Firewall 3120 Threat Defense Multi-Instance Supervisor

Summary Interfaces **Instances** System Configuration

Search an instance Add Instance

Name	Version	Resource Profile	Management IP	Management Gateway	Licenses	AC Policy	Platform Settings
instance1	7.4.0.1572	Default-Small	192.168.1.35	192.168.1.254	N.A	N.A	N.A
instance2	7.4.0.1572	Default-Small	192.168.1.37	192.168.1.254	N.A	N.A	N.A

Ports

Interface Name	Type
Ethernet1/2	Data
Ethernet1/3	Data

ステップ 3 [インターフェイスの割り当て (Interface Assignment)] 画面が表示されるまで、[次へ (Next)] をクリックします。

図 62: インターフェイスの割り当て

Edit Instance ×

1 Instance Configuration — 2 **Interface Assignment** — 3 Summary

Available Interfaces (13)

- Ethernet1/1
- Ethernet1/3
- Ethernet1/5.11
- Ethernet1/5.12
- Ethernet1/9
- Ethernet1/10
- Ethernet1/11
- Ethernet1/12
- Ethernet1/13
- Ethernet1/14
- Ethernet1/15
- Ethernet1/16
- Port-channel1

Selected Interfaces (3)

- Ethernet1/2
- Ethernet1/4
- Ethernet1/5

>> <<

Cancel Back **Next**

共有インターフェイスには、共有アイコン () が表示されます。

- ステップ 4 インターフェイスを変更し、[次へ (Next)] をクリックします。
- ステップ 5 [要約 (Summary)] 画面で [保存 (Save)] をクリックします。
- ステップ 6 高可用性を実現するには、他のユニットに対して同じインターフェイスの変更を行う必要があります。そうしなければ、高可用性が正しく機能しない可能性があります。

FXOS CLI のシャーシ管理設定の変更

シャーシ管理インターフェイスの IP アドレスとゲートウェイを変更する場合、Firewall Management Center を新しいマネージャに変更する場合、管理者パスワードを変更する場合、またはマルチインスタンスモードを無効にする場合は、FXOS CLI から実行できます。

手順

- ステップ 1 シャーシコンソールポートに接続します。

コンソールポートは FXOS CLI に接続します。

(注)

コンソールポートを使用することを推奨します。Firewall Management Center のシャーシプラットフォーム設定で構成されている場合は、SSH を使用して管理インターフェイスに接続することもできます。ただし、管理 IP アドレスを変更すると切断されます。

- ステップ 2 ユーザ名 **admin** と、初期セットアップ時に設定したパスワードを使用してログインします。
- ステップ 3 管理 IP アドレスの変更静的 IPv4 アドレスと IPv6 アドレス (どちらか一方も可) を使用できます。

IPv4 :

scope fabric-interconnect

set out-of-band static ip *ip_address netmask network_mask gw gateway_ip_address*

IPv6 :

scope fabric-interconnect

scope ipv6-config

set out-of-band static ipv6 *ipv6_address ipv6-prefix prefix_length ipv6-gw gateway_address*

例 :

IPv4 :

```
firepower-3110# scope fabric-interconnect
firepower-3110 /fabric-interconnect # set out-of-band static ip 10.5.23.8 netmask
255.255.255.0
gw 10.5.23.1
```

IPv6

```
firepower-3110# scope fabric-interconnect
firepower-3110 / fabric-interconnect # scope ipv6-config
firepower-3110 / fabric-interconnect /ipv6-config # set out-of-band static ipv6
2001:DB8::34
ipv6-prefix 64 ipv6-gw 2001:DB8::1
```

ステップ 4 Firewall Management Center を変更します。

最初に、現在の Firewall Management Center からシャーシを登録解除する必要があります。

```
enter device-manager manager_name [hostname {hostname | ipv4_address | ipv6_address}] [nat-id
nat_id]
```

登録キーの入力を求められます。

このコマンドは、どのスコープからでも入力できます。

- **hostname** {*hostname* | *ipv4_address* | *ipv6_address*} : Firewall Management Center の FQDN または IP アドレスを指定します。双方向の TLS-1.3 暗号化通信チャネルを 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 (Firewall Management Center またはシャーシ) に到達可能な IP アドレスが必要です。 **hostname** を指定しない場合は、シャーシに到達可能な IP アドレスまたはホスト名が必要となり、 **nat-id** を指定する必要があります。
- **nat-id** *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、シャーシを登録するときに Firewall Management Center でも指定する任意の一意のワントタイム文字列を指定します。これは **hostname** を指定しない場合に必須となりますが、ホスト名または IP アドレスを指定する場合でも、常に NAT ID を設定することを推奨します。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、Firewall Management Center に登録する他のデバイスには使用できません。
- **Registration Key:** *reg_key* : シャーシを登録するときに Firewall Management Center でも指定する任意のワントタイム登録キーを要求するプロンプトが表示されます。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。

例 :

```
firepower-3110# enter device-manager boulder_fmc hostname 10.89.5.35 nat-id 93002
(Valid registration key characters: [a-z],[A-Z],[0-9],[ -]. Length: [2-36])
Registration Key: Impala67
```

ステップ 5 admin パスワードを変更します。

```
scope security
```

```
set password
```

パスワードを入力します。 *password*

パスワードを確認します。 *password*

例 :

```
firepower-3110# scope security
firepower-3110 /security # set password
Enter new password: Sw@nsong67
Confirm new password: Sw@nsong67
firepower-3110 /security #
```

ステップ 6 マルチインスタンスモードを無効にして、システムをアプライアンスモードに戻します。

scope system

set deploymode native

再起動するように求められます。

例 :

```
firepower-3110# scope system
firepower-3110 /system # set deploymode native
All configuration and bootable images will be lost and system will reboot.
If there was out of band upgrade, it might reboot with the base version and
need to re-image to get the expected running version.
Do you still want to change deploy mode? (yes/no):yes
firepower-3110 /system #
```

モードをマルチインスタンスモードに戻すには、「**set deploymode container**」と入力します。
show system detail コマンドを使用して、現在のモードを確認できます。

マルチインスタンスモードのモニタリング

このセクションは、マルチインスタンスモードのシャーシとインスタンスのトラブルシューティングおよび診断に役立ちます。

マルチインスタンス設定のモニタリング

show system detail

このFXOS コマンドは、現在のモード（ネイティブまたはコンテナ）を表示します。モードがネイティブ（アプライアンスモードとも呼ばれる）の場合は、マルチインスタンス（コンテナ）モードに変換できます。マルチインスタンスモードのプロンプト/名前は一般的な「firepower-<モデル>」で、アプライアンスモードのプロンプトは、Firewall Threat Defense に設定したホスト名です（デフォルトでは「firepower」）。

```
firepower # show system detail
```

```
Systems:
  Name: firepower
  Mode: Stand Alone
  System IP Address: 172.16.0.50
  System IPv6 Address: ::
  System Owner:
  System Site:
  Deploy Mode: Native
  Description for System:
firepower #
```

scope system > show

このFXOS コマンドは、現在のモードを表形式で表示します。マルチインスタンスモードのプロンプト/名前は一般的な「firepower-<モデル>」で、アプライアンスモードのプロンプトは、Firewall Threat Defense に設定したホスト名です。

```
firepower-3110# scope system
firepower-3110 /system # show
```

```
Systems:
  Name           Mode           Deploy Mode   System IP Address System IPv6 Address
  -----
firepower-3110
  Stand Alone Container  10.89.5.42      ::
```

```
3110-1# scope system
3110-1 /system # show
```

```
Systems:
  Name           Mode           Deploy Mode   System IP Address System IPv6 Address
  -----
3110-1
  Stand Alone Native    10.89.5.41      ::
3110-1 /system #
```

インスタンス インターフェイスのモニタリング

show portmanager switch forward-rules hardware mac-filter

このコマンドは、各インスタンスに専用の物理インターフェイスが割り当てられた2つのインスタンスの内部スイッチ転送ルールを表示します。イーサネット 1/2 は ftd1 に割り当てられ、イーサネット 1/1 は ftd2 に割り当てられます。

ECMP グループ 1540 は ftd1 に割り当てられ、ECMP グループ 1541 は ftd2 に割り当てられません。

```
secfw-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN  SRC_PORT  PC_ID  SRC_ID  DST_PORT  PKT_CNT  DMAC
1         0         17      0       17         19    29164  0:0:0:0:0:0
2         0         19      0       19         17    67588  0:0:0:0:0:0
3         0          1      0      101        1541      0  a2:5b:83:0:0:15
4         0          1      0      101        1541    8181  ff:ff:ff:ff:ff:ff
5         0          2      0      102        1540      0  a2:5b:83:0:0:18
6         0          2      0      102        1540     431  ff:ff:ff:ff:ff:ff
```

```

7      0      17      0      0      0      11133  0:0:0:0:0:0
8      0      17      0      0      0          0  0:0:0:0:0:0

```

このコマンドは、共有物理インターフェイスが両方に割り当てられた2つのインスタンスの内部スイッチ転送ルールを表示します。イーサネット 1/1 は ftd1 と ftd2 の間で共有されます。

ECMP グループ 1540 は ftd1 に割り当てられ、ECMP グループ 1541 は ftd2 に割り当てられます。

MCAST グループ 4096 は、ftd1 と ftd2 の間でブロードキャストトラフィックを複製するために使用されます。

```

firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN  SRC_PORT  PC_ID  SRC_ID  DST_PORT  PKT_CNT  DMAC
1         0         17      0       17       19      2268  0:0:0:0:0:0
2         0         19      0       19       17      4844  0:0:0:0:0:0
3         0          1      0      101     1541       0  a2:5b:83:0:0:9
4         0          1      0      101     4096      546  ff:ff:ff:ff:ff:ff
5         0          1      0      101     1540       0  a2:5b:83:0:0:c
6         0         17      0        0        0     1263  0:0:0:0:0:0
7         0         17      0        0        0       0  0:0:0:0:0:0

```

このコマンドは、共有サブインターフェイスが両方に割り当てられた2つのインスタンスの内部スイッチ転送ルールを表示します。イーサネット 1/1.2452 は ftd1 と ftd2 の間で共有されます。

ECMP グループ 1540 は ftd1 に割り当てられ、ECMP グループ 1541 は ftd2 に割り当てられます。

MCAST グループ 4097 は、ftd1 と ftd2 の間でブロードキャストトラフィックを複製するために使用されます。

```

firepower-3140(local-mgmt)# show portmanager switch forward-rules hardware mac-filter
      VLAN  SRC_PORT  PC_ID  SRC_ID  DST_PORT  PKT_CNT  DMAC
1         0         17      0       17       19     21305  0:0:0:0:0:0
2         0         19      0       19       17     50976  0:0:0:0:0:0
3     2452          1      0      101     1541      430  a2:5b:83:0:0:f
4     2452          1      0      101     4097       0  ff:ff:ff:ff:ff:ff
5     2452          1      0      101     1540       0  a2:5b:83:0:0:12
6         0         17      0        0        0     11038  0:0:0:0:0:0
7         0         17      0        0        0       0  0:0:0:0:0:0

```

show portmanager switch ecmp-groups detail

このコマンドを使用して、各インスタンスの Ecmp-Vport-Physical ポートマッピングの詳細を一覧表示します。



(注) 物理ポート 18 は、内部スイッチとインスタンス間のバックプレーンアップリンク インターフェイスです。

```

firepower-3140(local-mgmt)# show portmanager switch ecmp-groups detail
      ECMP-GROUP  VPORT  PHYSICAL-PORT
1         1536      256         18
2         1537      257         18
3         1538      258         18

```

4	1539	259	18
5	1540	260	18
6	1541	261	18
7	1542	262	18
8	1543	263	18
9	1544	264	18
10	1545	265	18

show portmanager switch mcast-groups detail

このコマンドを使用して、MCAST グループメンバーシップの詳細を一覧表示します。

```
firepower-3140(local-mgmt)# show portmanager switch mcast-groups detail
MCAST-GROUP
1      4096
      Member-ports
      Ethernet 1/1
      ECMP-ID 1541
      ECMP-ID 1540
```

show portmanager counters mcast-group

このコマンドを使用して、MCAST グループパケットカウンタを確認します。

```
firepower-3140(local-mgmt)# show portmanager counters mcast-group 4096
PKT_CNT: 8106
```

show portmanager counters ecmp

このコマンドを使用して、ECMP グループパケットカウンタを確認します。

```
firepower-3140(local-mgmt)# show portmanager counters ecmp 1541
PKT_CNT: 430
```

マルチインスタンスモードの履歴

表 2:

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Firewall Management Center でのマルチインスタンスモード変換	7.6.0	7.6.0	<p>アプリケーションモードのデバイスを Firewall Management Center に登録し、CLI を使用せずにマルチインスタンスモードに変換できるようになりました。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> • [デバイス (Devices)] > [デバイス管理 (Device Management)] [その他 (More)] [マルチインスタンスに変換 (Convert to Multi-Instance)] • [デバイス (Devices)] > [デバイス管理 (Device Management)] > [一括アクションの選択 (Select Bulk Action)] > [マルチインスタンスに変換 (Convert to Multi-Instance)]
Secure Firewall 4200 のマルチインスタンスモード	7.6.0	7.6.0	Secure Firewall 4200 でマルチインスタンスモードがサポートされるようになりました。
Multi-instance mode for the Secure Firewall 3100.	7.4.1	7.4.1	<p>You can deploy the Secure Firewall 3100 as a single device (<i>appliance mode</i>) or as multiple container instances (<i>multi-instance mode</i>). In multi-instance mode, you can deploy multiple container instances on a single chassis that act as completely independent devices. Note that in multi-instance mode, you upgrade the operating system and the firmware (<i>chassis upgrade</i>) separately from the container instances (<i>Firewall Threat Defense upgrade</i>).</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Devices > Device Management > Add > Chassis • Devices > Device Management > Device > Chassis Manager • Devices > Platform Settings > New Policy > Chassis Platform Settings • Devices > Chassis Upgrade <p>New/modified Firewall Threat Defense CLI commands: configure multi-instance network ipv4, configure multi-instance network ipv6</p> <p>New/modified FXOS CLI commands: create device-manager, set deploymode</p> <p>Platform restrictions: Not supported on the Secure Firewall 3105.</p>

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。