Secure Firewall 3100 にマルチインスタンスモードを

Secure Firewall 3100 は、単一のデバイス（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（マルチインスタンスモード）として展開できます。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

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 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（ブレー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 オペレーティングシステム（FXOS）を実行しますが、各インスタンスは個別の 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は、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、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。初期設定については、マルチインスタンスモードの有効化 （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 （67 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 （52 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、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 （35 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。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、シャーシ内では Etherchannel のみを作成できます。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。

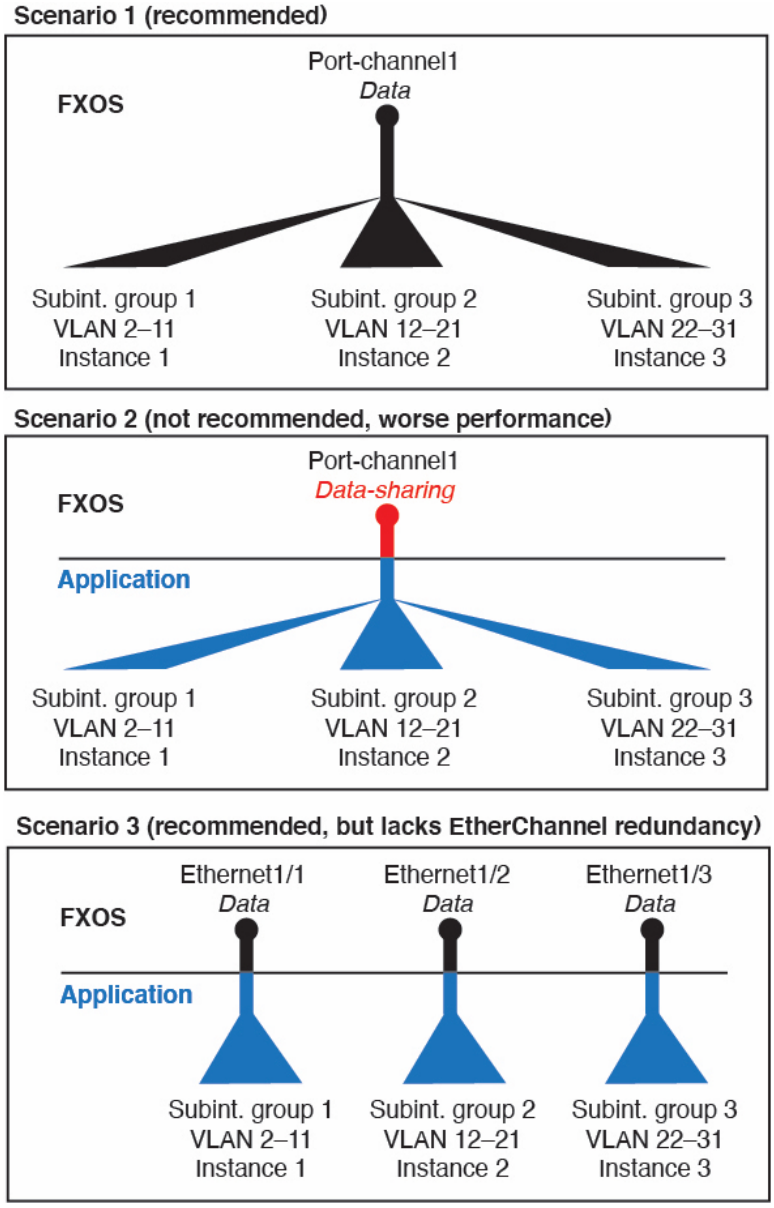
以下のセクションでは、インターフェイスのシャーシとインスタンス間の連携について説明します。

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。

シャーシに 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、シャーシ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、シャーシでサブインターフェイスを作成する必要があります。シャーシ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-Channel1 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、シャーシ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* : シャーシ内の *VLAN* とインスタンス内の *VLAN*



シャーシ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、シャーシ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、シャーシ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

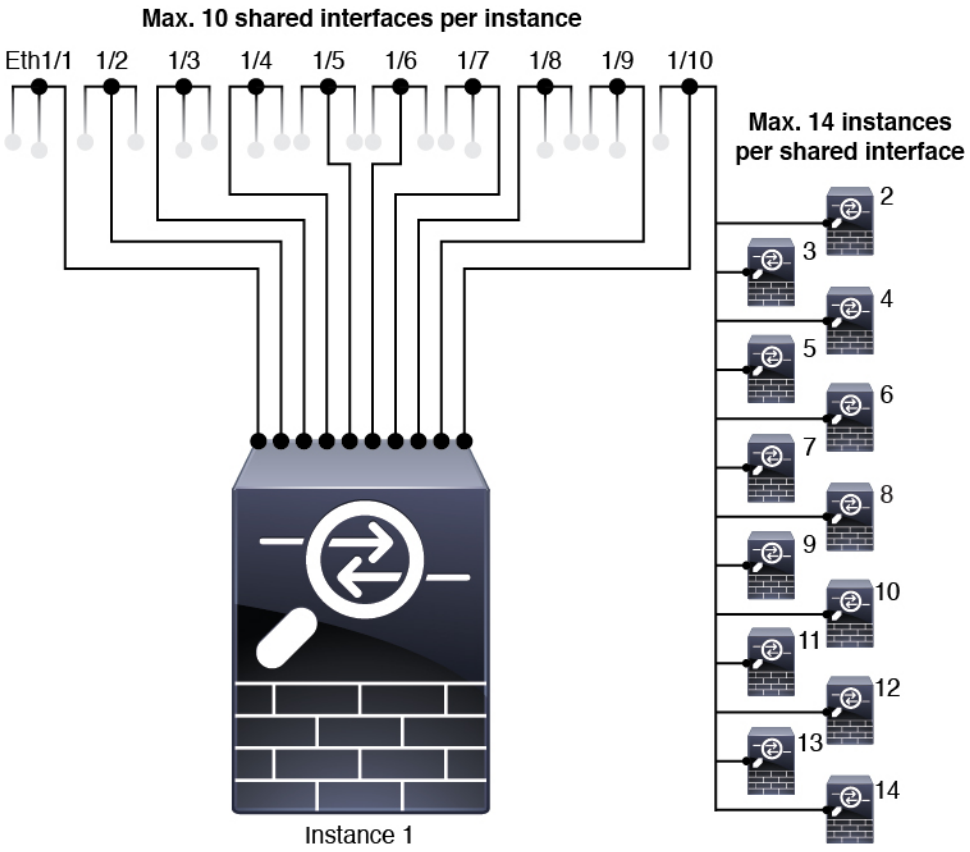
デフォルトで無効になっていますが、サブインターフェイスはデフォルトで有効になっています。

共有インターフェイスの拡張性

インスタンスは、データ共有タイプのインターフェイスを共有できます。この機能を使用して、物理インターフェイスの使用率を節約し、柔軟なネットワークの導入をサポートできます。インターフェイスを共有すると、シャーシは一意の MAC アドレスを使用して、正しいインスタンスにトラフィックを転送します。ただし、共有インターフェイスでは、シャーシ内にフルメッシュトポロジが必要になるため、転送テーブルが大きくなることがあります（すべてのインスタンスが、同じインターフェイスを共有するその他すべてのインスタンスと通信できる必要があります）。そのため、共有できるインターフェイスの数には制限があります。

転送テーブルに加えて、シャーシは VLAN サブインターフェイスの転送用に VLAN グループテーブルも保持します。 最大 500 個の VLAN サブインターフェイスを作成できます。

共有インターフェイスの割り当てに次の制限を参照してください。



共有インターフェイスのベスト プラクティス

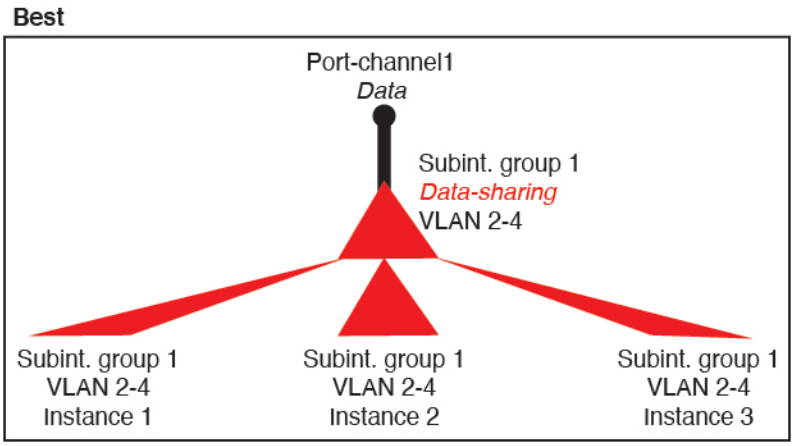
転送テーブルの拡張性を最適にするには、共有するインターフェイスの数をできる限り少なくします。代わりに、1 つまたは複数の物理インターフェイスに最大 500 個の VLAN サブインターフェイスを作成し、コンテナインスタンスで VLAN を分割できます。

インターフェイスを共有する場合は、拡張性の高いものから低いものの順に次の手順を実行します。

1. 最適：単一の親の下のサブインターフェイスを共有し、インスタンスグループと同じサブインターフェイスのセットを使用します。

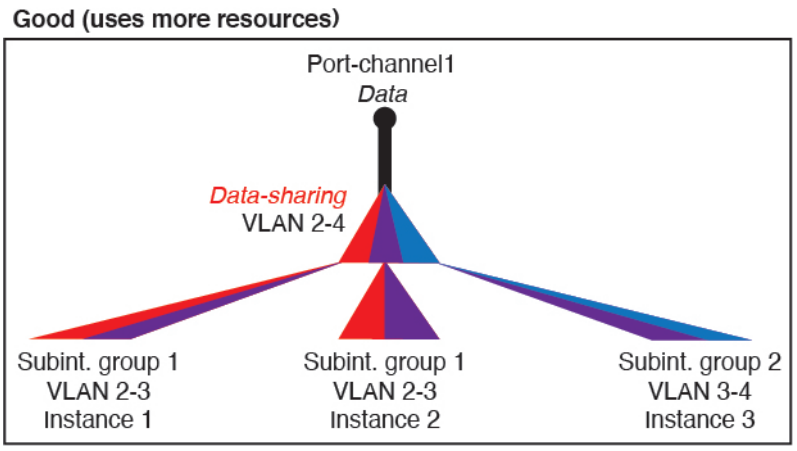
   たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模なEtherChannelを作成し、Port-Channel2、Port-Channel3、Port-Channel4 の代わりに、その EtherChannel のサブインターフェイス（Port-Channel1.2、3、4）を共有します。単一の親のサブインターフェイスを共有する場合、物理/EtherChannel インターフェイスまたは複数の親にわたるサブインターフェイスを共有するときの VLAN グループ テーブルの拡張性は転送テーブルよりも優れています。

   図 *2*：最適：単一の親のサブインターフェイスグループを共有



インスタンスグループと同じサブインターフェイスのセットを共有しない場合は、（VLAN グループよりも）より多くのリソースを設定で使用することになる可能性があります。たとえば、Port-Channel1.2 および 3 をインスタンス 1 および 2 と共有するとともに Port-Channel1.3 および 4 をインスタンス 3 と共有する（2 つの VLAN グループ）のではなく、Port-Channel1.2、3、および 4 をインスタンス 1、2、および 3 と共有（1 つの VLAN グループ）します。

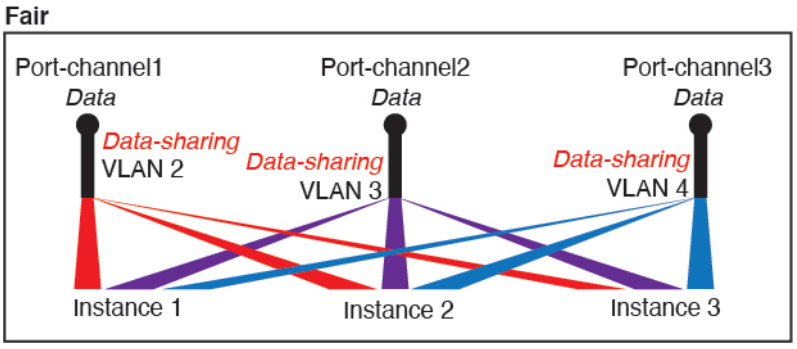
図 *3:* 良好：単一の親の複数のサブインターフェイスグループを共有



2. 普通：親の間でサブインターフェイスを共有します。

   たとえば、Port-Channel2、Port-Channel4、および Port-Channel4 ではなく、Port-Channel1.2、Port-Channel2.3、および Port-Channel3.4 を共有します。この使用方法は同じ親のサブインターフェイスのみを共有するよりも効率は劣りますが、VLAN グループを利用しています。

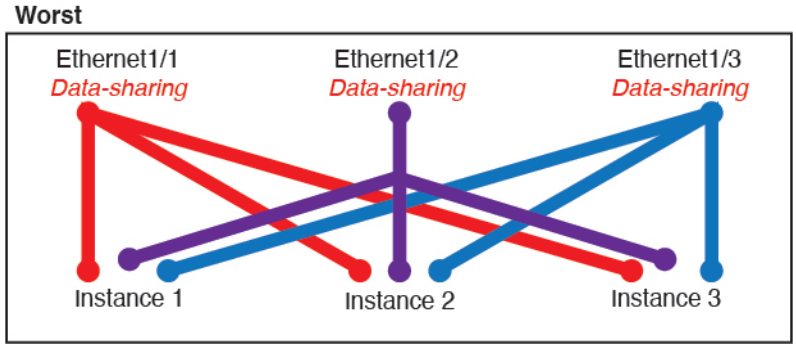
図 *4:* 普通：個別の親のサブインターフェイスを共有



3. 最悪：個々の親インターフェイス（物理または EtherChannel）を共有します。

   この方法は、最も多くの転送テーブル エントリを使用します。

図 *5:* 最悪：親インターフェイスを共有



シャーシがパケットを分類する方法

シャーシに入ってくるパケットはいずれも分類する必要があります。その結果、シャーシは、どのインスタンスにパケットを送信するかを決定できます。

- 一意のインターフェイス：1 つのインスタンスしか入力インターフェイスに関連付けられていない場合、シャーシはそのインスタンスにパケットを分類します。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、またはパッシブ インターフェイスの場合は、この方法を常にパケットの分類に使用します。
- 一意の MAC アドレス：シャーシは、共有インターフェイスを含むすべてのインターフェイスに一意の MAC アドレスを自動的に生成します。複数のインスタンスが同じインターフェイスを共有している場合、分類子には各インスタンスでそのインターフェイスに割り当てられた固有の MAC アドレスが使用されます。固有の MAC アドレスがないと、アップストリーム ルータはインスタンスに直接ルーティングできません。アプリケーション内で各インターフェイスを設定するときに、手動で MAC アドレスを設定することもできます。

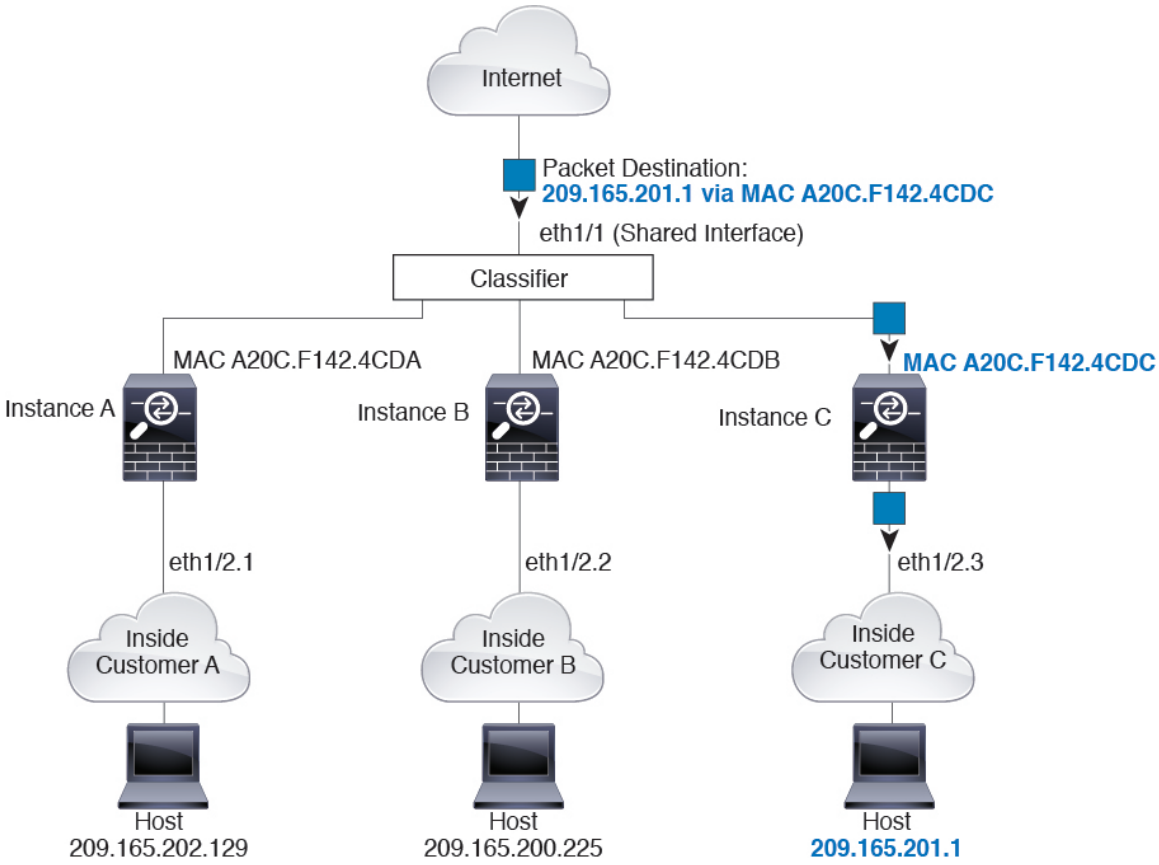
（注） 宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製されて各インスタンスに送信されます。

分類例

MAC アドレスを使用した共有インターフェイスのパケット分類

次の図に、外部インターフェイスを共有する複数のインスタンスを示します。インスタンス C にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをインスタンス C に割り当てます。

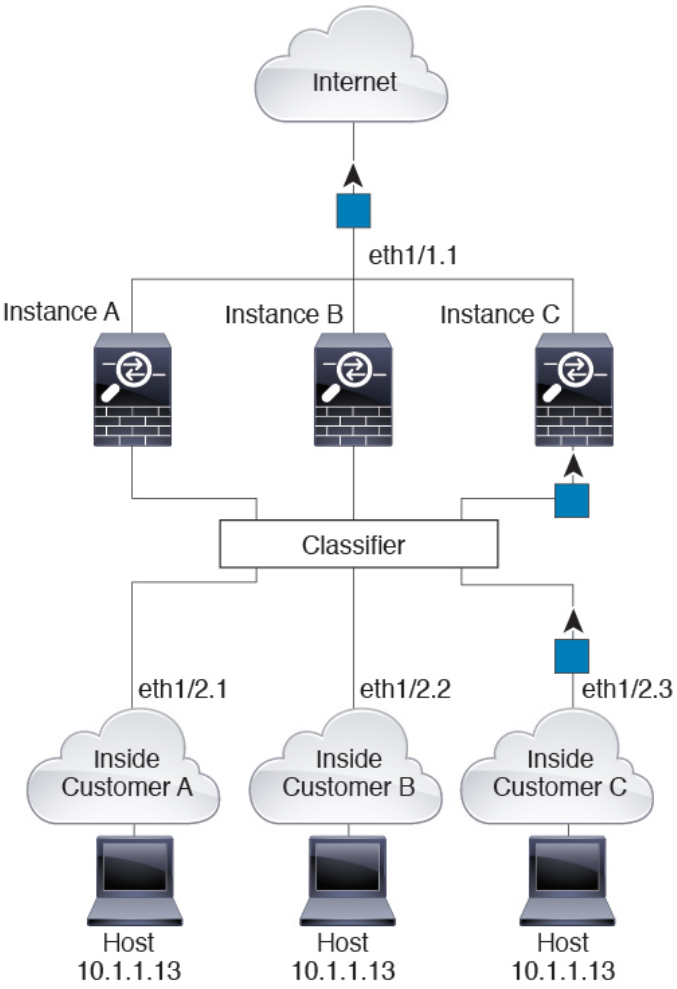
図 *6 : MAC* アドレスを使用した共有インターフェイスのパケット分類



内部ネットワークからの着信トラフィック

内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のインスタンスCのホストを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

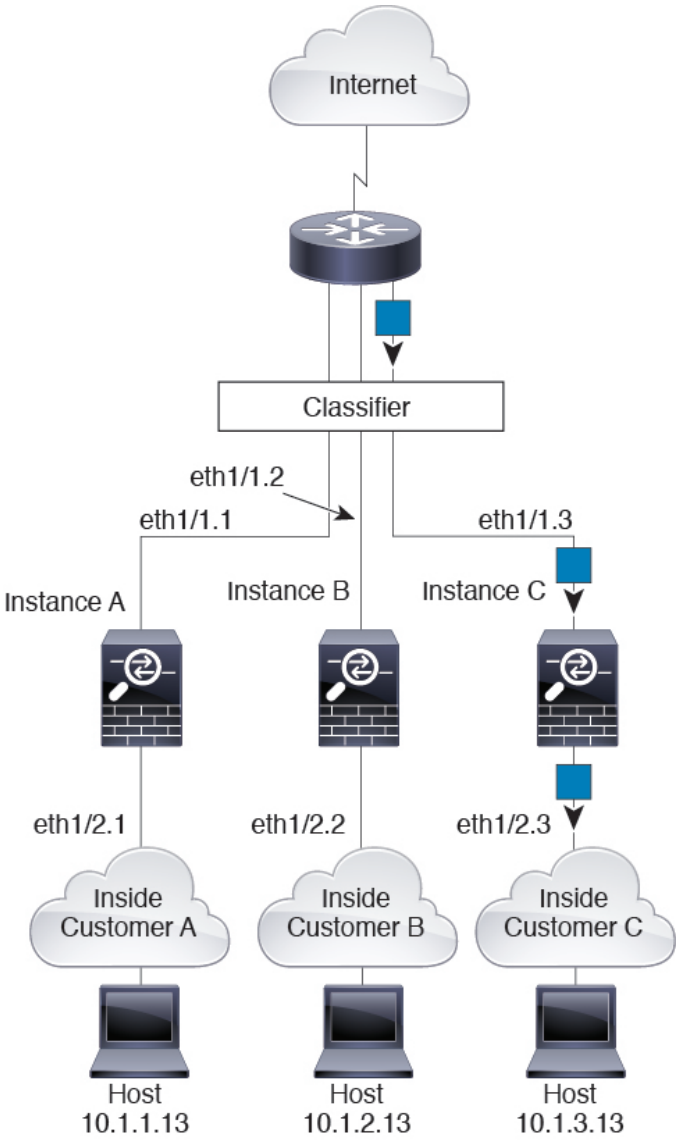
図 7: 内部ネットワークからの着信トラフィック



トランスペアレント ファイアウォール インスタンス

トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のインスタンスCのホスト宛のインターネットからのパケットを示します。分類子は、パケットをインスタンス C に割り当てます。これは、入力インターフェイスがイーサネット 1/2.3 で、このイーサネットがインスタンス C に割り当てられているためです。

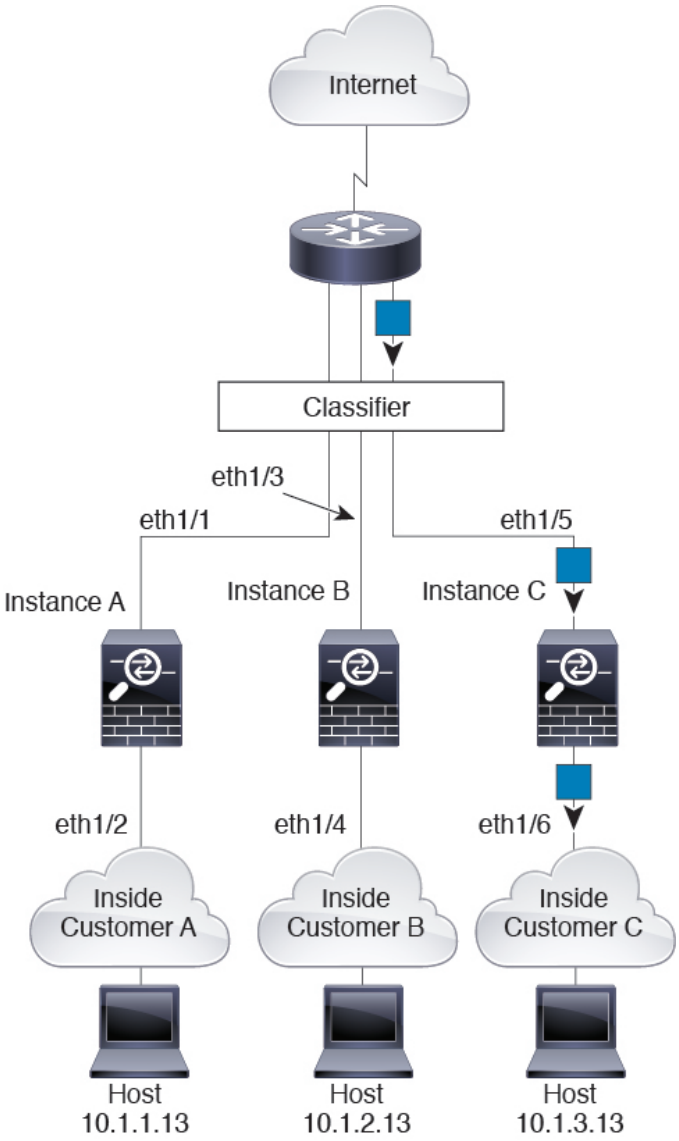
図 *8:* トランスペアレント ファイアウォール インスタンス



インラインセット

インラインセットの場合は一意のインターフェイスを使用する必要があります。また、それらのセットは物理インターフェイスか、またはEtherChannelである必要があります。次の図に、ネットワーク内のインスタンスCのホスト宛のインターネットからのパケットを示します。分類子は、パケットをインスタンスCに割り当てます。これは、入力インターフェイスがイーサネット 1/5 で、このイーサネットがインスタンス C に割り当てられているためです。

図 *9*: インラインセット

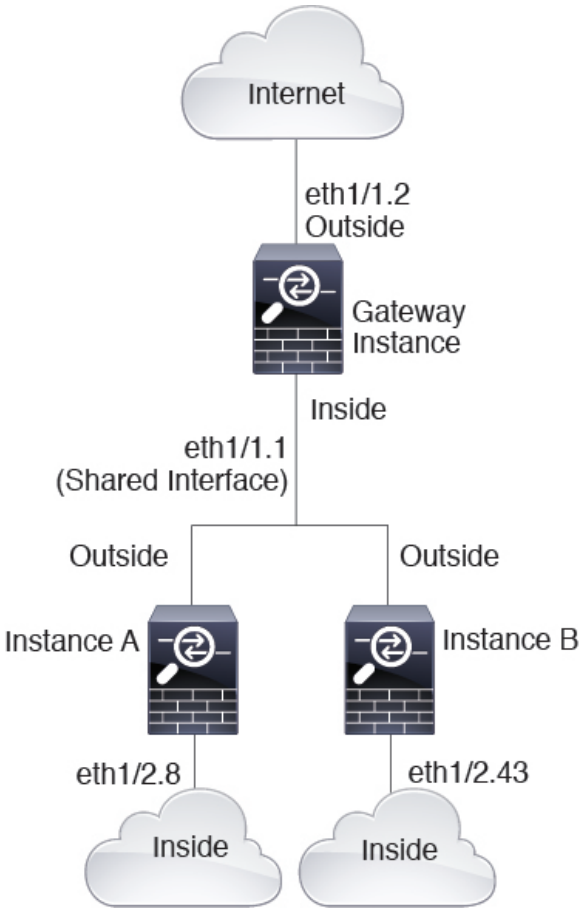


インスタンスのカスケード

別のインスタンスの前にインスタンスを直接配置することをインスタンスのカスケードと呼びます。一方のインスタンスの外部インターフェイスは、もう一方のインスタンスの内部インターフェイスと同じインターフェイスです。いくつかのインスタンスのコンフィギュレーションを単純化する場合、最上位インスタンスの共有パラメータを設定することで、インスタンスをカスケード接続できます。

次の図に、ゲートウェイの背後に2つのインスタンスがあるゲートウェイ インスタンスを示します。

図 *10 :* インスタンスのカスケード



（注） 高可用性を備えたカスケードインスタンス（共有インターフェイスを使用）を使用しないでください。フェールオーバーが発生し、スタンバイユニットが再参加すると、MAC アドレスが一時的に重複し、停止が発生する可能性があります。代わりに、外部スイッチを使用してゲートウェイインスタンスと内部インスタンスに一意のインターフェイスを使用して、それらのインスタンス間でトラフィックを渡す必要があります。

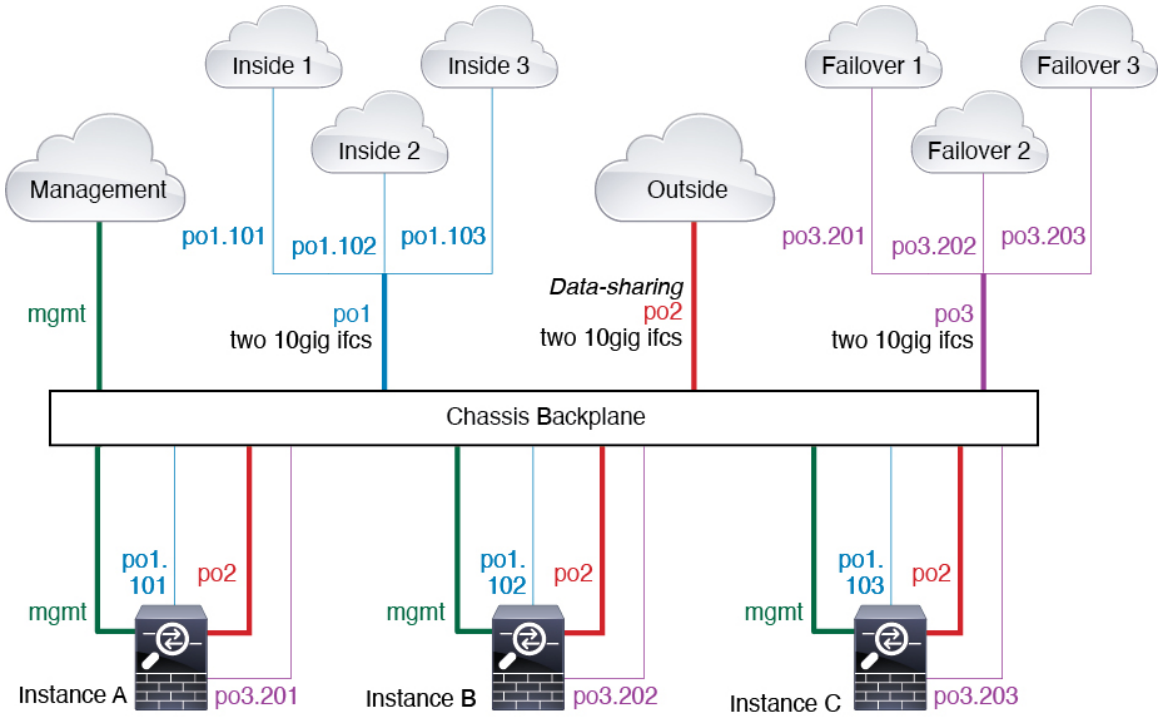
一般的な複数インスタンス展開

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の 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

シャーシは、各インスタンスの共有インターフェイスが一意の MAC アドレスを使用するように、インスタンス インターフェイスの MAC アドレスを自動的に生成します。

インスタンス内の共有インターフェイスに MAC アドレスを手動で割り当てると、手動で割り当てられた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます。生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インスタンス内のインターフェイスの MAC アドレスを手動で設定してください。

自動生成されたアドレスは A2 で始まり、アドレスが重複するリスクがあるため、手動 MAC アドレスの先頭は A2 にしないでください。

シャーシは、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザー定義のプレフィックスまたはシステム定義のプレフィックスであり、*zz.zzzz* はシャーシが生成した内部カウンタです。システム定義のプレフィックスは、IDPROM にプログラムされている Burned-in MAC アドレス内の最初の MAC アドレスの下部 2 バイトと一致します。**connect fxos** を使用し、次に **show module** を使用して、MAC アドレスプールを表示します。たとえば、モジュール 1 について示されている MAC アドレスの範囲が b0aa.772f.f0b0 ～ b0aa.772f.f0bf の場合、システム プレフィックスは f0b0 になります。

ユーザ定義のプレフィックスは、16 進数に変換される整数です。ユーザ定義のプレフィックスの使用方法を示す例を挙げます。プレフィックスとして 77 を指定すると、シャーシは 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスはシャーシネイティブ形式に一致するように逆にされます（*xxyy*）。

A24**D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.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 （17 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

（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

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 Threat Defense ソフトウェアを実行できます。

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い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。

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 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 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
  - Management Center UCAPL/CC モード
  - ハードウェアへのフローオフロード
- CDO クラウド提供 Management Center によるシャーシのプライマリ管理と、オンプレミス 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、CDO 管理対象インスタンスを分析専用のオンプレミス 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対してサブインターフェイスを使用する場合、その親にあるすべてのサブインターフェイスと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

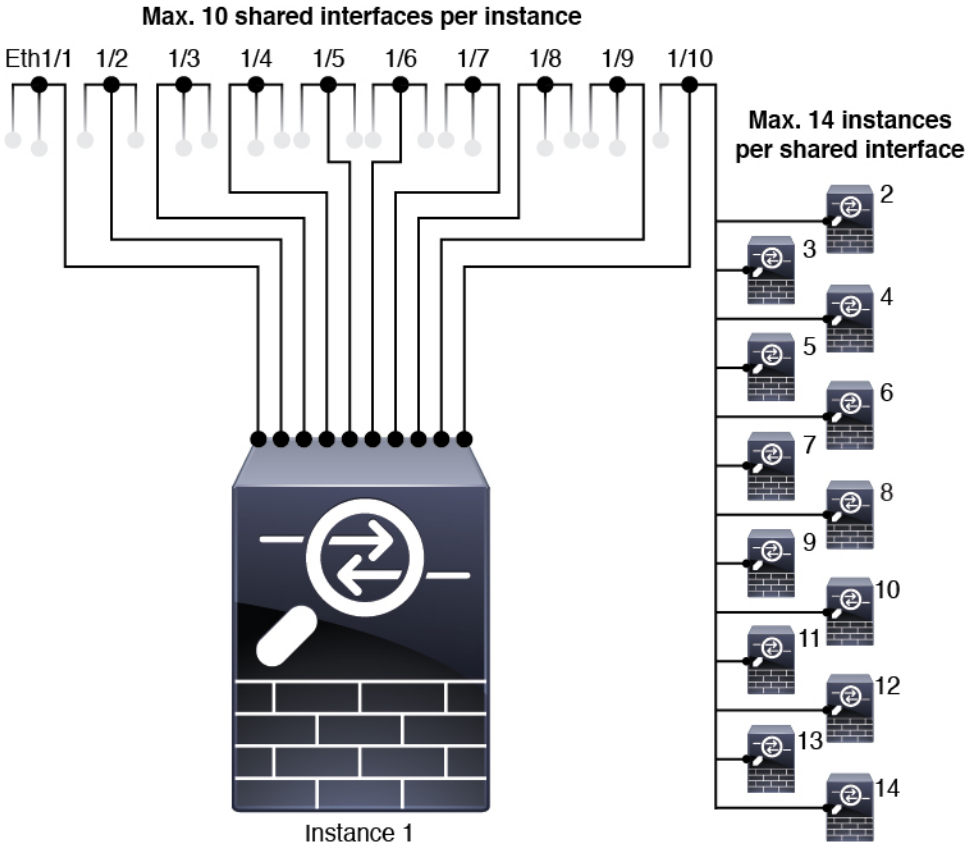
- 最大 48 の EtherChannel を設定できますが、物理インターフェイスの数によって制限されます。
- EtherChannel には、最大 8 つのアクティブ インターフェイスを設定できます。
- EtherChannel 内のすべてのインターフェイスは、同じメディアタイプと速度容量である必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GB と 10GB のインターフェイスなど）を混在させることはできませんが、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、Instance1 ～ Instance14 に Ethernet1/1 を割り当てることができます。

  インスタンスごとの最大共有インターフェイス数：10 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対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。

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では、MAC アドレスを手動で設定する場合、分類が正しく行われるように、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で一意の MAC アドレスを使用します。インスタンスインターフェイスの自動MACアドレス（15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、Management Center にシャーシを追加し、シャーシインターフェイスを設定する必要があります。シャーシ設定をカスタマイズすることもできます。

マルチインスタンスモードの有効化

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 Threat Defense CLI に接続する必要があります。モードを設定したら、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 Threat Defense CLI に接続します。

connect ftd

例：

```
firepower# connect ftd
>
```

ステップ 5 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 のシャーシ管理設定の変更 （67 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、シャーシ管理インターフェイスを設定し、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、設定を消去してリブ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。システムがリブートし、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。シャーシのホスト名は「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**}：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（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 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（-）などがあります。
- *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 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（-）などがあります。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。

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 （67 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...
>
```

Management Center へのマルチインスタンスシャーシの追加

マルチインスタンスシャーシを Management Center に追加します。管理センターとシャーシは、シャーシ MGMT インターフェイスを使用して個々の管理接続を共有します。

Management Center を使用して、すべてのシャーシ設定とインスタンスを設定できます。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。

始める前に

シャーシをマルチインスタンスモードに変換します。マルチインスタンスモードの有効化（21 ページ）を参照してください。

手順

ステップ 1 Management Center で、シャーシ管理 IP アドレスまたはホスト名を使用してシャーシを追加します。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]**の順に選択してから、**[追加（Add）] > [シャーシ（Chassis）]**の順に選択します。

図 *12 :* シャーシの追加

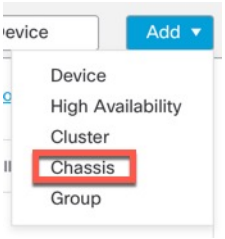
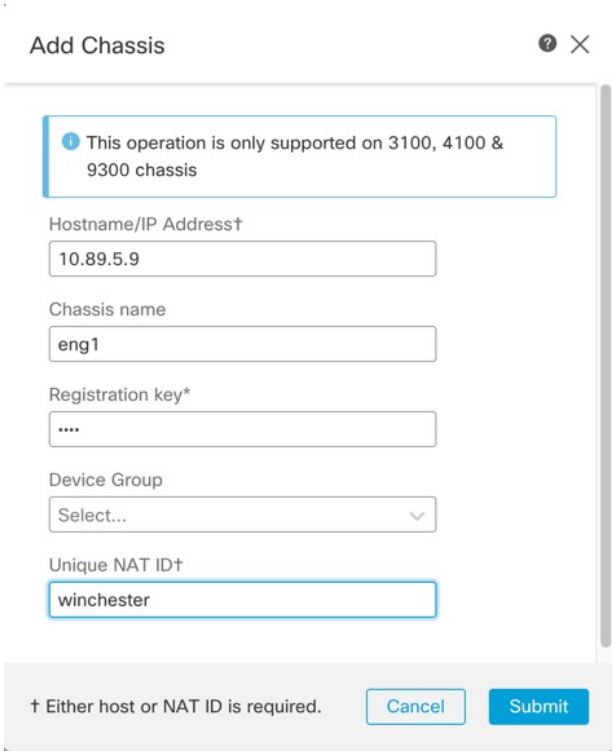


図 *13* : シャーシの追加



b) [ホスト名/IPアドレス（Hostname/IP Address）] フィールドに、追加するシャーシの IP アドレスまたはホスト名を入力します。

ホスト名またはIPアドレスがわからない場合は、このフィールドを空白のままにして、一意の NAT ID を指定できます。

c) [シャーシ名（Chassis Name）] フィールドに、Management Center でのシャーシの表示名を入力します。

d) [登録キー（Registration Key）] フィールドに、Management Center の管理対象としてシャーシを設定したときに使用したのと同じ登録キーを入力します。

登録キーは、1回限り使用可能な共有シークレットです。キーには、英数字とハイフン（-）を含めることができます。

e) マルチドメイン展開では、現在のドメインに関係なく、シャーシをリーフドメインに割り当てます。

現在のドメインがリーフドメインである場合、シャーシは自動的に現在のドメインに追加されます。現在のドメインがリーフドメインでない場合、登録後、シャーシを設定するために、リーフドメインに切り替える必要があります。シャーシは 1 つのドメインにのみ属することができます。

f) （任意） シャーシを**デバイスグループ**に追加します。

g) シャーシの設定時に NAT ID を使用した場合、[一意のNAT ID（Unique NAT ID）] フィールドに同じ NAT ID を入力します。

NAT ID には、英数字とハイフン（-）を含めることができます。

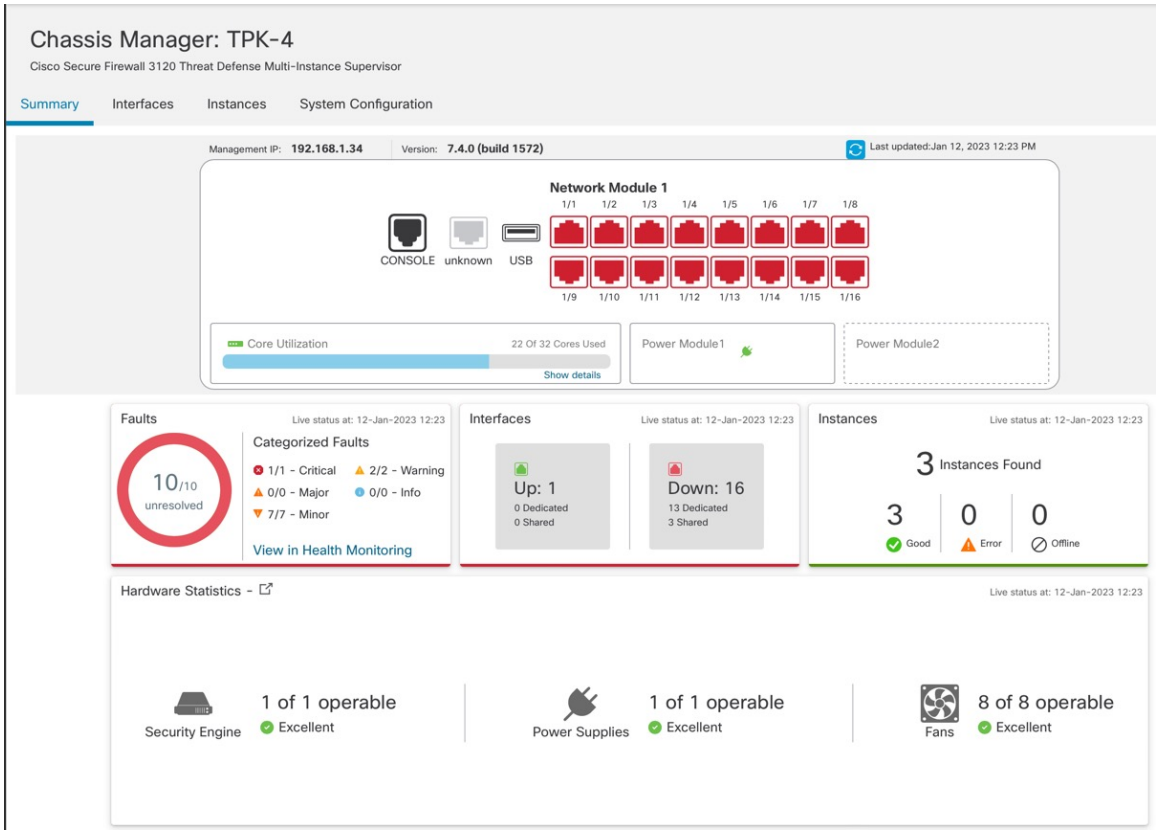
h) **[送信（Submit）]** をクリックします。

シャーシが**[デバイス（Device）]** > **[デバイス管理（Device Management）]**ページに追加されます。

ステップ 2 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、**[編集（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 *14 :* 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 のネットワークモジュールの管理 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、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。

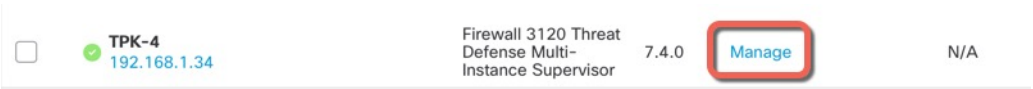
物理インターフェイスの設定

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）]** > **の [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 **[編集（Edit）]** （✎） をクリックします。

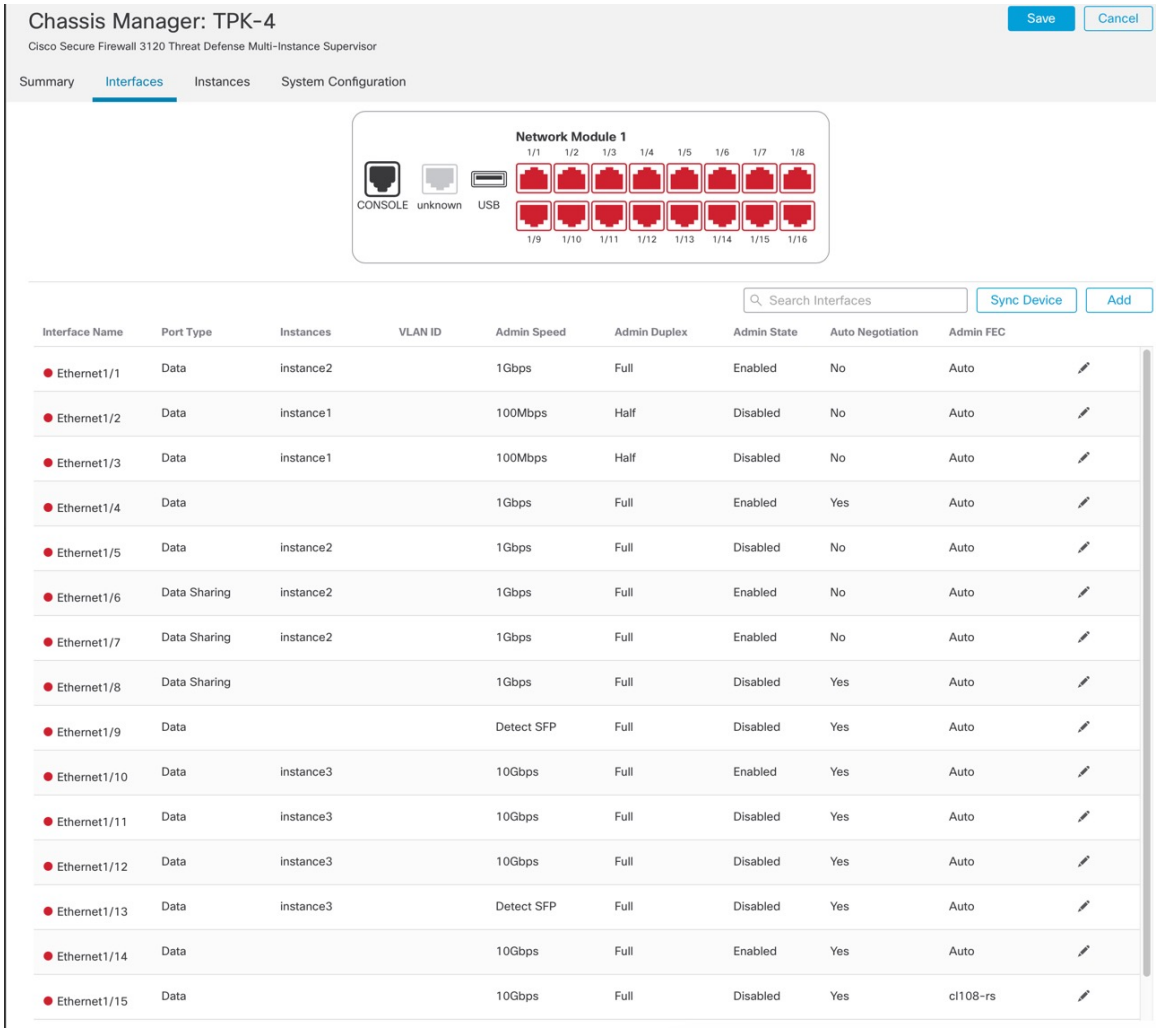
図 *15* : シャーシの管理



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。

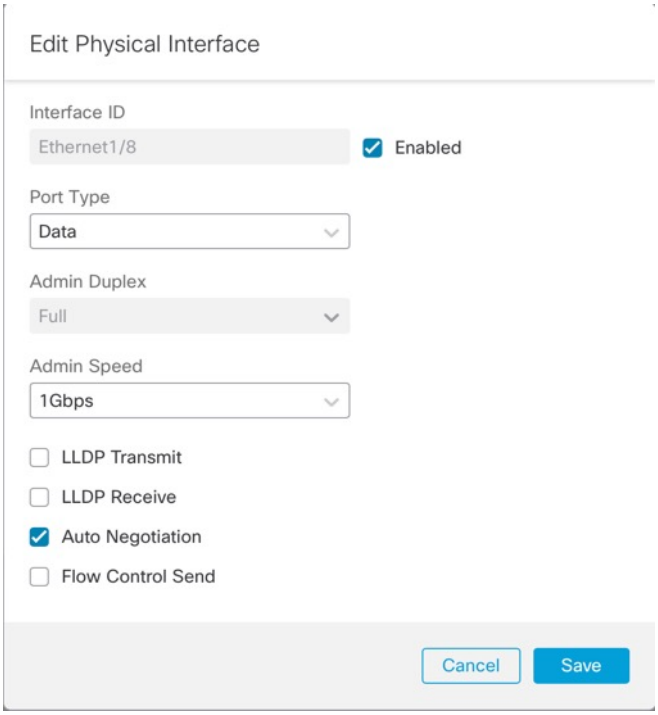
ステップ 2 [インターフェイス（Interfaces）] をクリックします。

図 *16 :* インターフェイス



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

図 *17* : 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 *18* : 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） 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にのみ、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。

EtherChannel の設定

EtherChannel（ポートチャネルとも呼ばれる）は、同じメディアタイプと容量の最大 8 個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。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。

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。

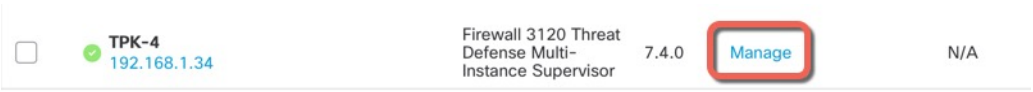
始める前に

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 （27 ページ）を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **の [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 **[編集（Edit）]** （✎） をクリックします。

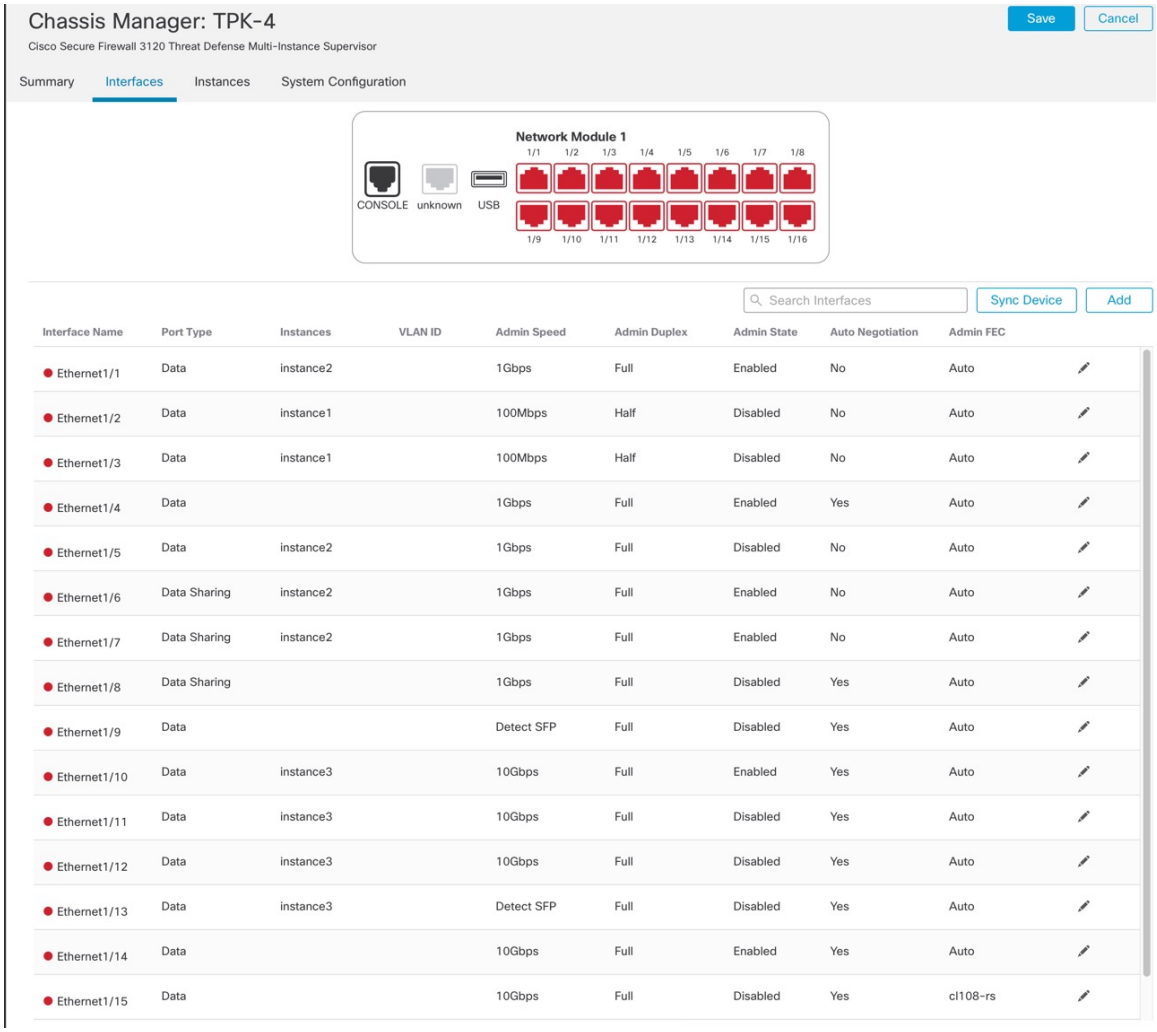
図 *19*：シャーシの管理



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。

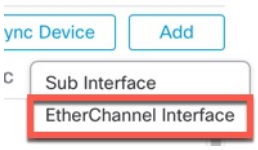
ステップ 2 [インターフェイス（Interfaces）] をクリックします。

図 *20 :* インターフェイス



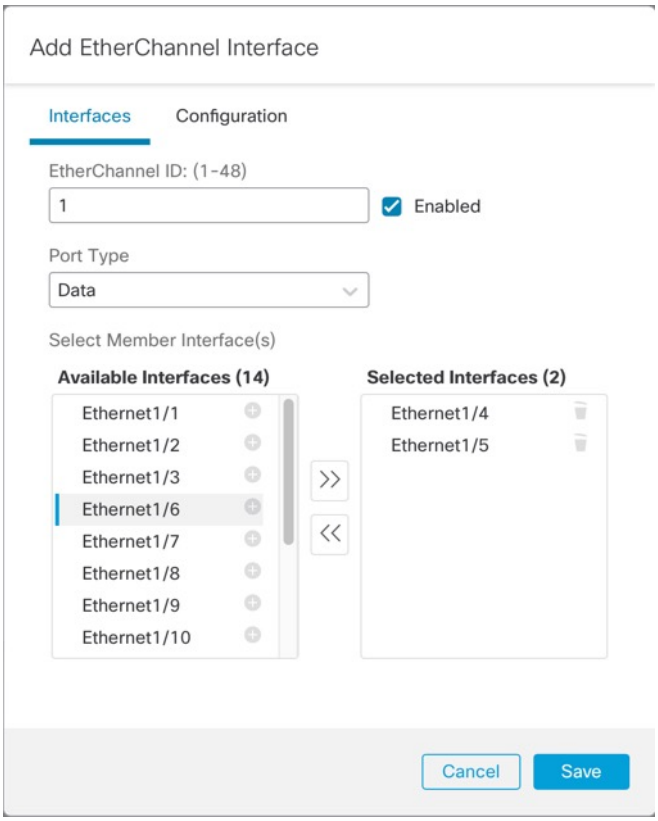
ステップ 3 [追加（Add）]>[EtherChannelインターフェイス（EtherChannel Interface）] をクリックします。>

図 *21 : 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 *22* : 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。

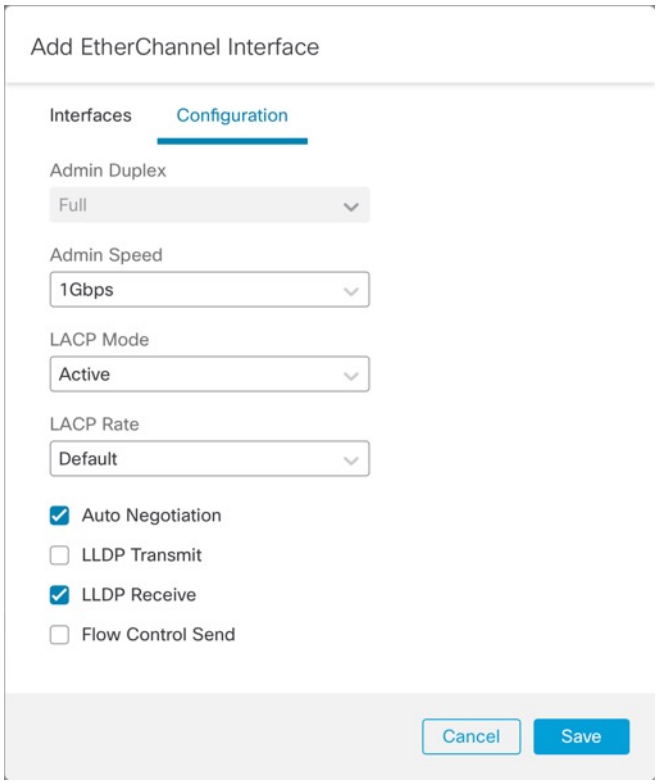
（注） すでにインスタンスに割り当てられているインターフェイスは追加できません。

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 *23 :* コンフィギュレーション設定



a) 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。

b) 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。

c) [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。

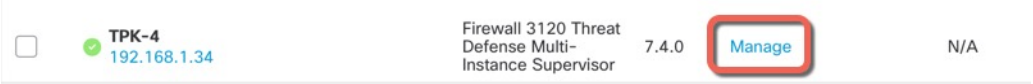
インターフェイスごとの VLAN ID は一意である必要があります。インスタンス内では、VLAN ID は割り当てられたすべてのインターフェイス全体で一意である必要があります。異なるインターフェイスに割り当てられている限り、VLAN ID を別のインターフェイス上で再利用できます。ただし、同じ ID を使用していても、各サブインターフェイスが制限のカウント対象になります。

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）]** > **の [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 **[編集（Edit）]**（✎） をクリックします。

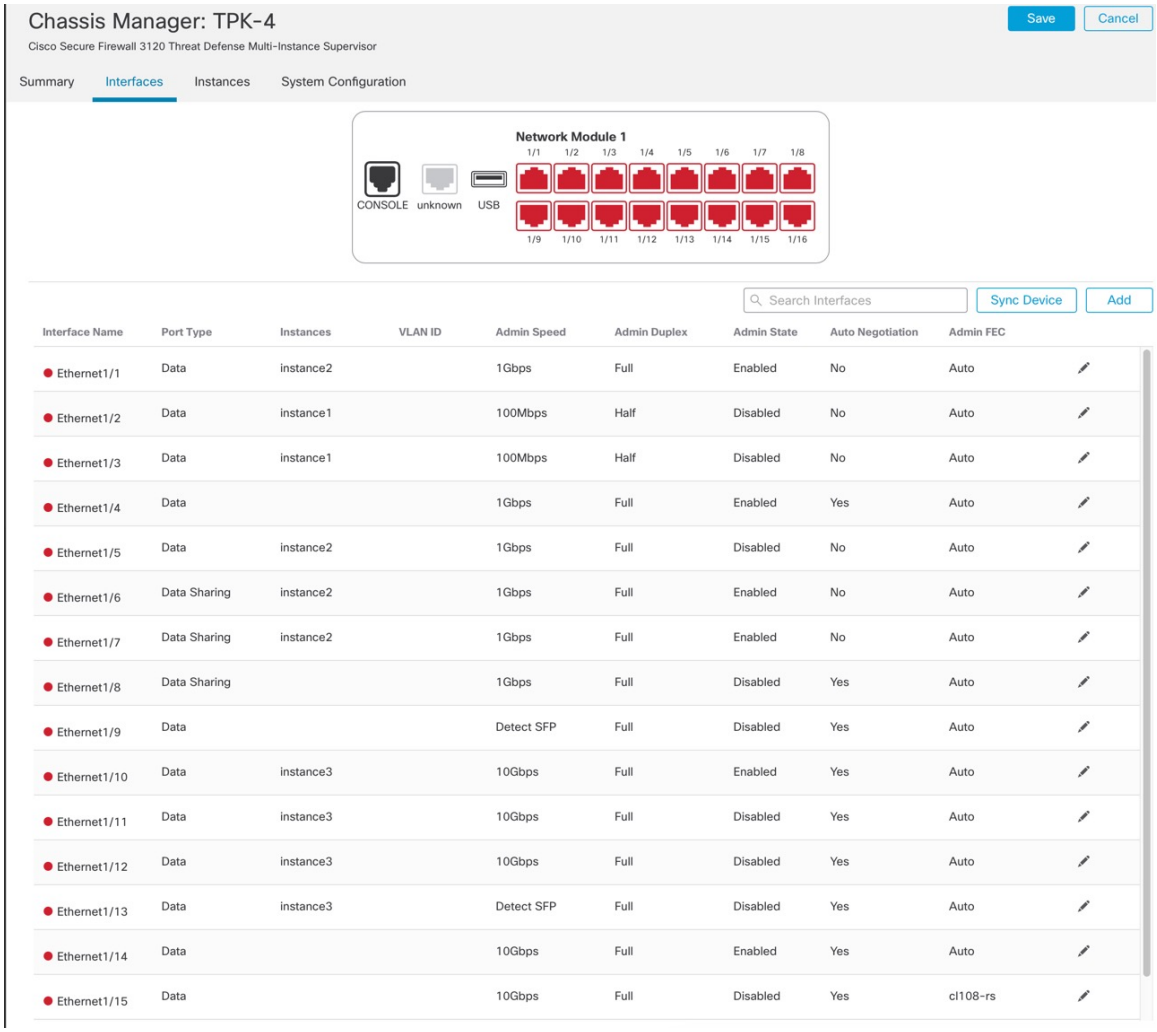
図 *24* : シャーシの管理



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 *25* : インターフェイス

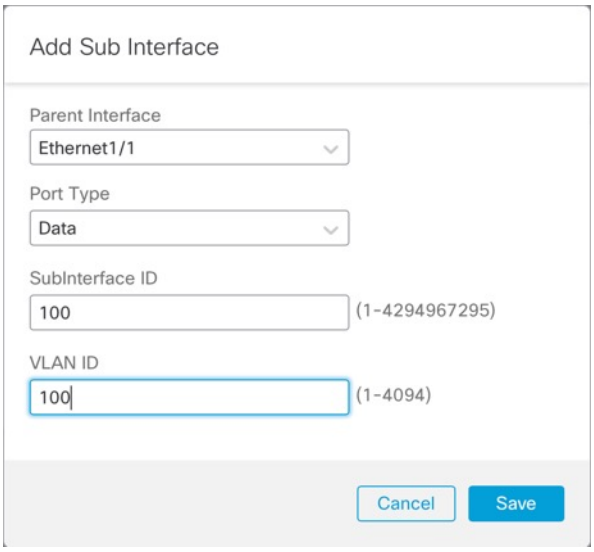


ステップ 3 **[追加（Add）]** > **[サブインターフェイス（Subinterface）]** をクリックします。

図 *26* : 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 *27* : 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（17 ページ） を参照してください。

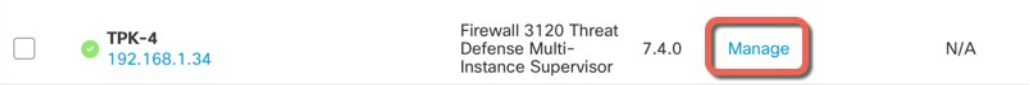
始める前に

マルチインスタンスモードの有効化 （21 ページ） および Management Center へのマルチインスタンスシャーシの追加 （24 ページ）。

手順

ステップ 1 **[デバイス（Devices）]** > **の [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 **[編集（Edit）]** （✎） をクリックします。

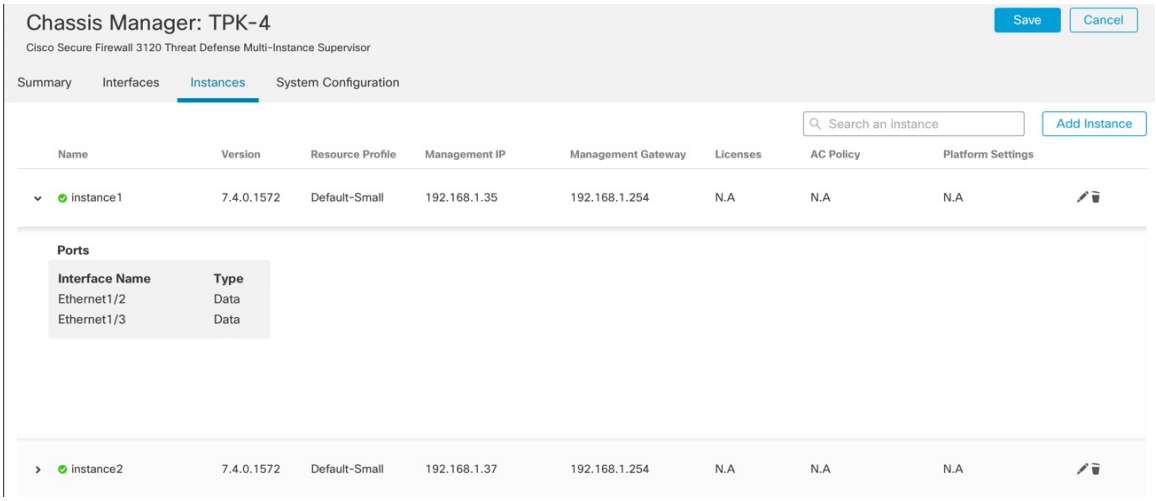
図 *28 :* シャーシの管理



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。

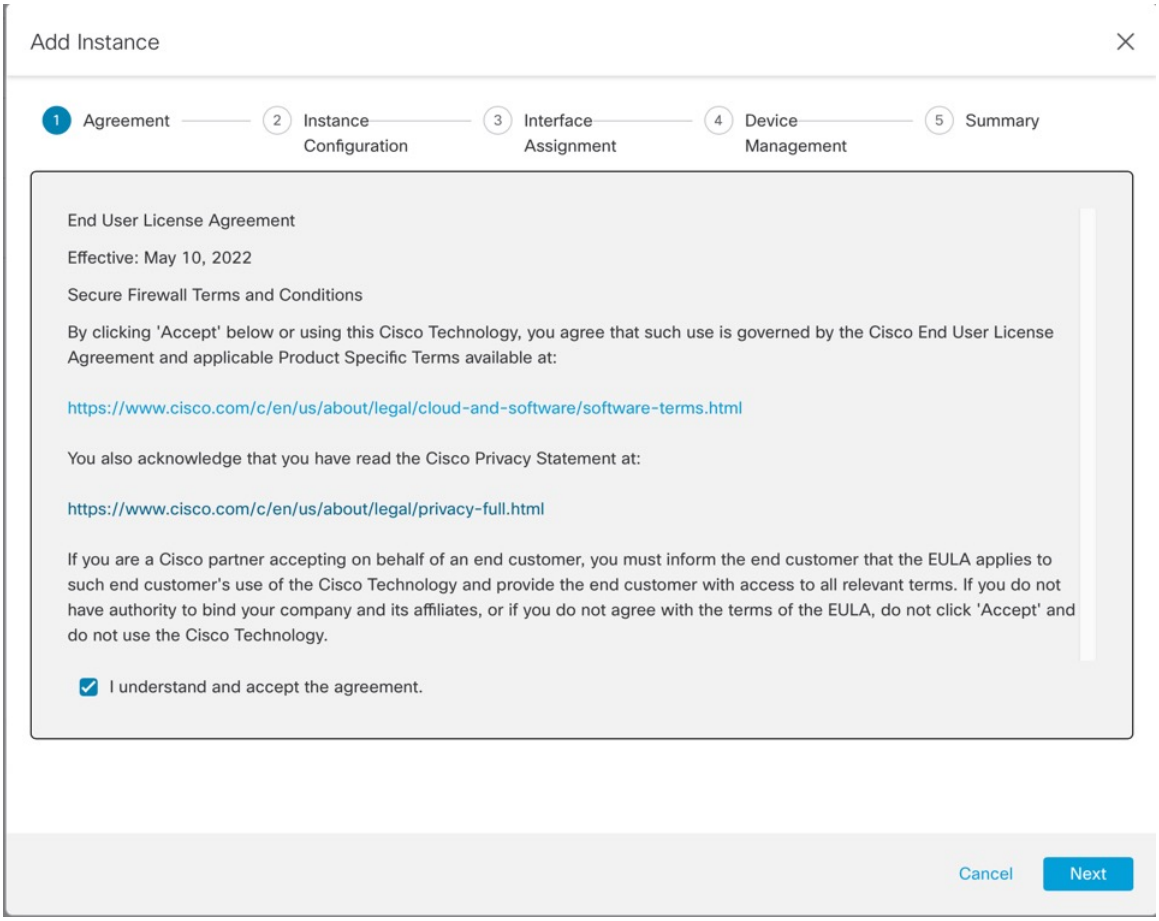
ステップ 2 [インスタンス（Instances）] をクリックし、[インスタンスの追加（Add Instance）] をクリックします。

図 *29 : Instances*



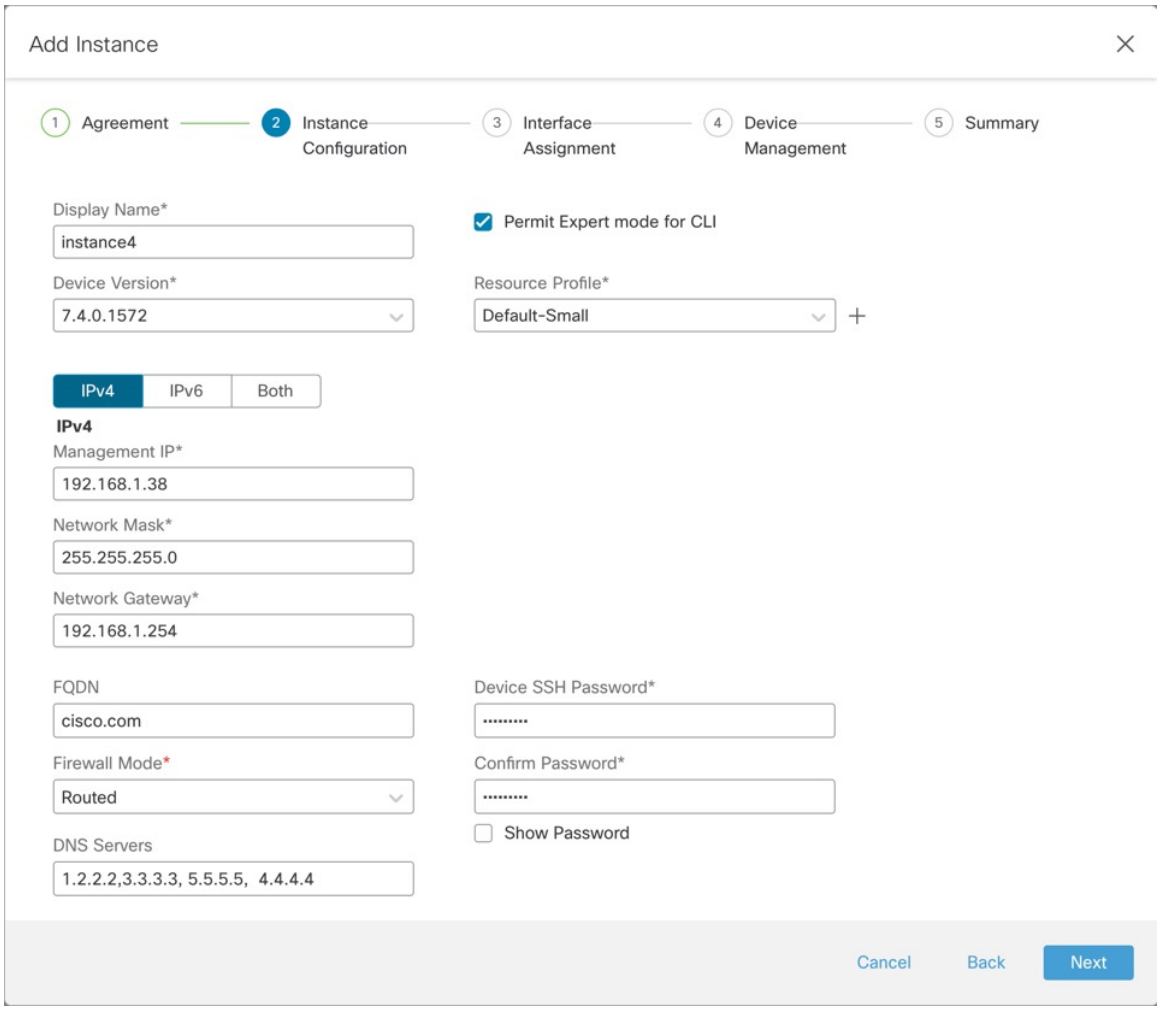
ステップ 3 [契約（Agreement）] で、[契約の内容について理解し、同意します（I understand and accept the agreement）] をオンにし、[次へ（Next）] をクリックします。

図 *30* : 契約



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 *31* : インスタンス設定



- **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。新しいパッケージにアップグレードするには、**[デバイス（Devices）]** > **[シャーシのアップグレード（Chassis Upgrade）]** を参照してください。アップグレードすると、古いバージョンと新しい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、FXOS CLI を使用する必要があります。Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）を参照してください。
- [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

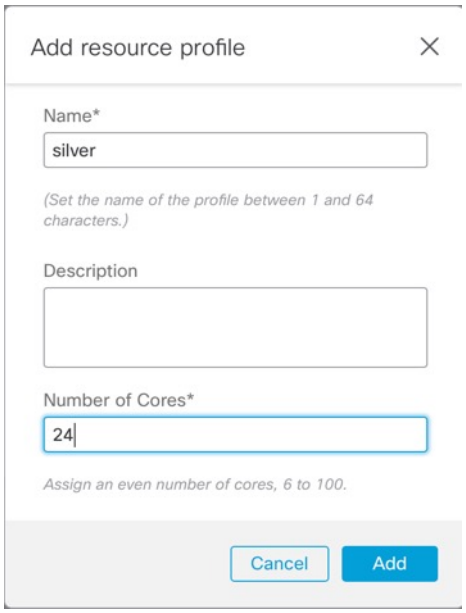
ドレスを持ちます。デフォルトで、この IP アドレスに SSH で接続して Threat Defense CLI にアクセスできます。

- （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 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、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 *32*：リソースプロファイルの追加



- 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。

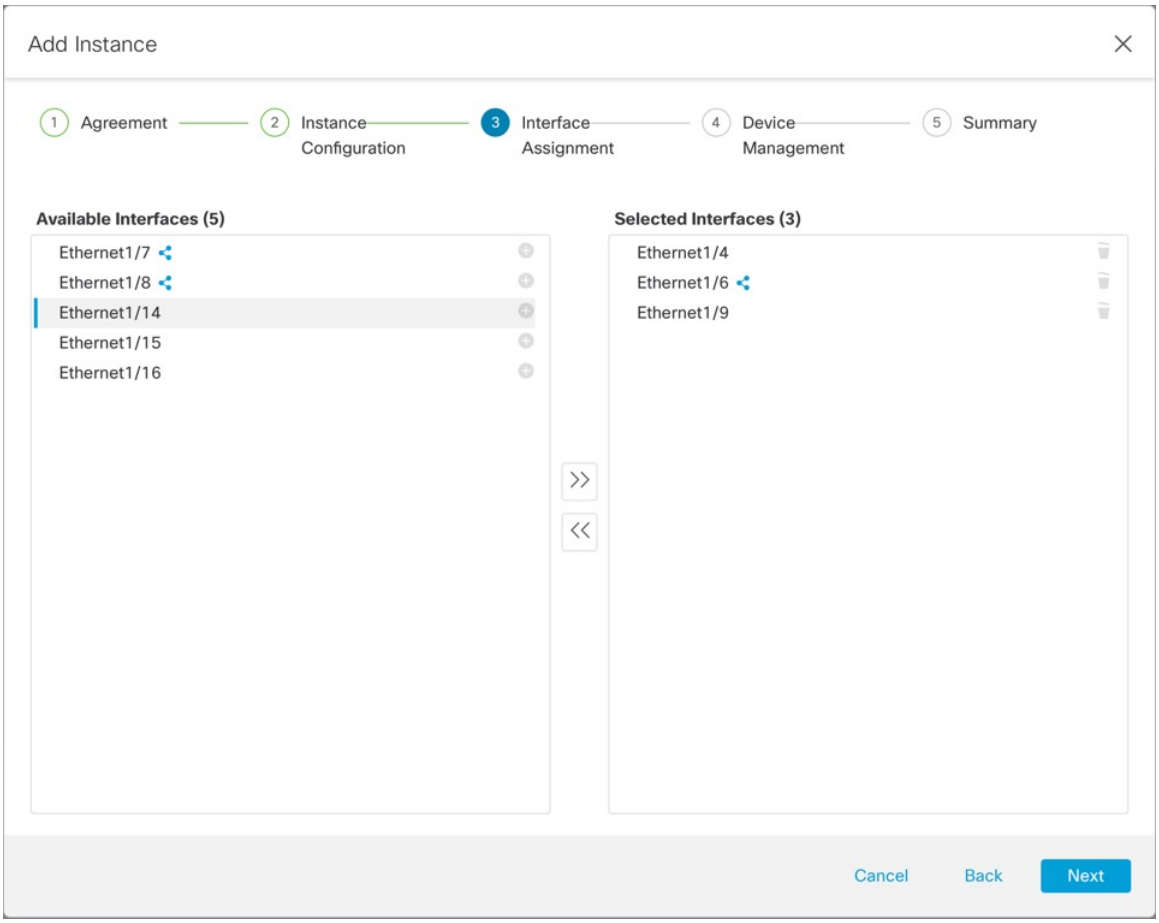
- コアは偶数（6、8、10、12、14 など）で最大値まで割り当てることができます。
- 利用可能な最大コア数は、モデルによって異なります。インスタンスの要件と前提条件 （17 ページ）を参照してください。

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 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、シャーシ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。

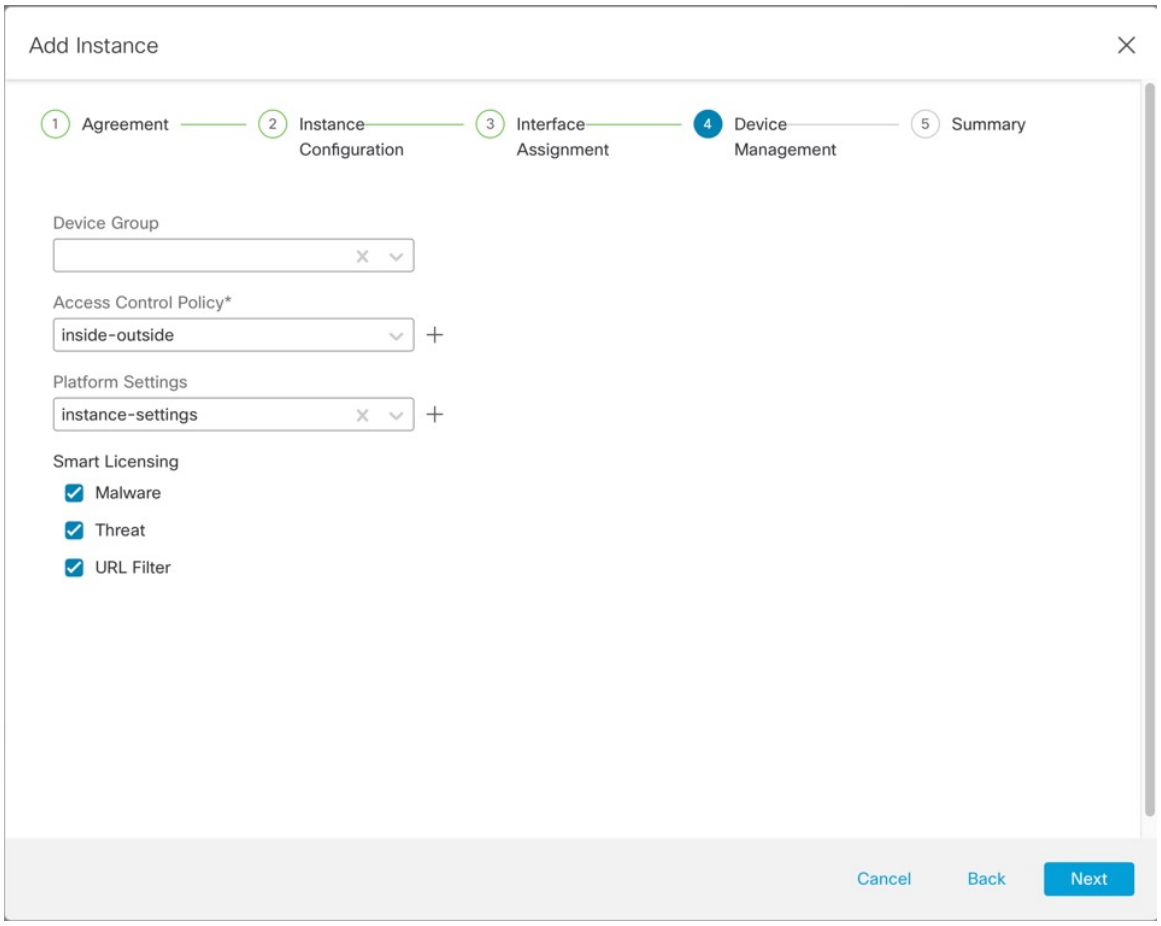
図 *33* : インターフェイスの割り当て



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。

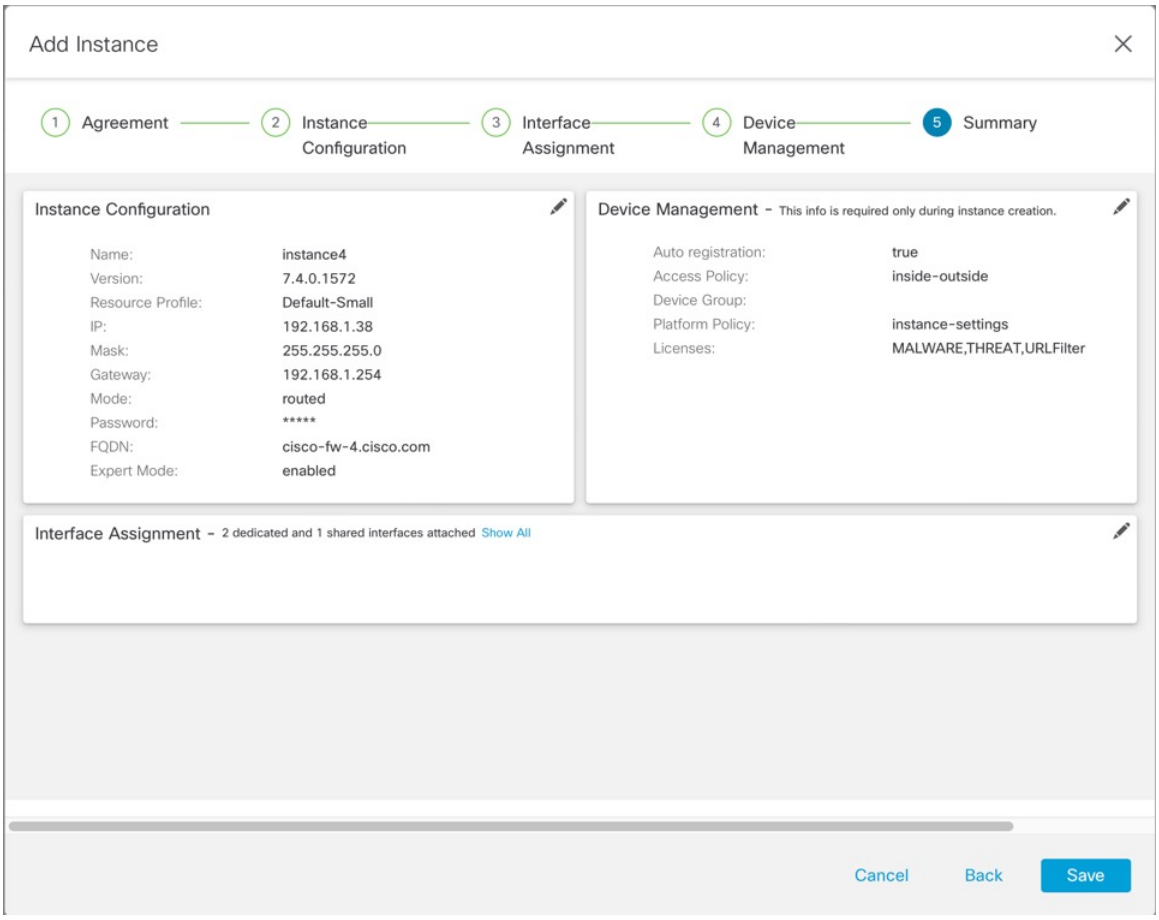
図 *34* : デバイス管理



- **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 *35* : 要約



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 の設定

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。

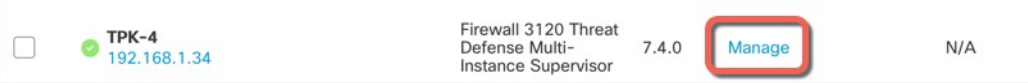
始める前に

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）]** > **の [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 **[編集（Edit）]**（✎） をクリックします。

図 *36* : シャーシの管理

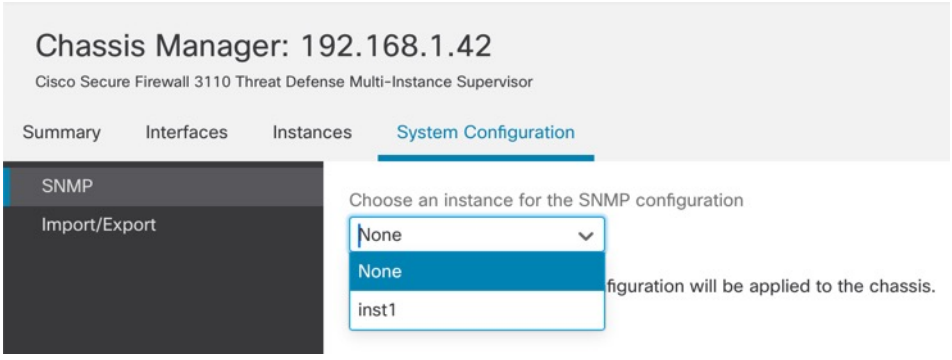


シャーシの [シャーシマネージャ（Chassis Manager）] ページが開き、[要約（Summary）] ページが表示されます。

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 *37* : *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を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

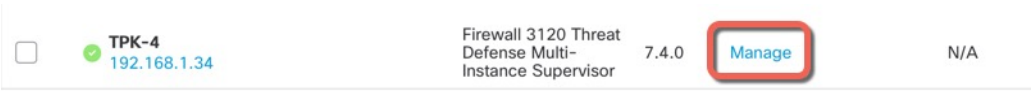
設定をインポートするシャーシでは、以下の特性が一致している必要があります。

- 同じシャーシ ソフトウェア バージョン
- 同じ 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）]** > **の [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 **[編集（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。

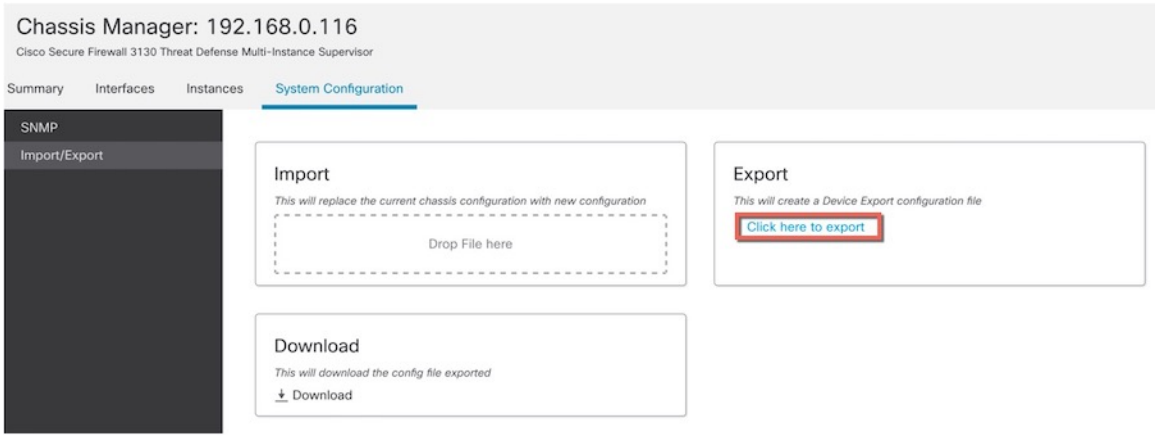
ステップ 2 [システム設定（System Configuration）] をクリックします。

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。

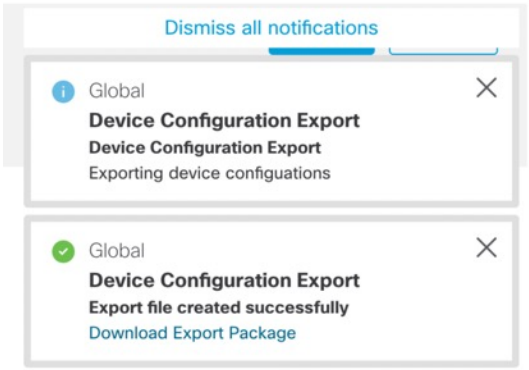
a) [エクスポート（Export）] エリアで、[エクスポートするにはここをクリック（Click here to export）] をクリックします。

図 *39* : エクスポートファイルの作成



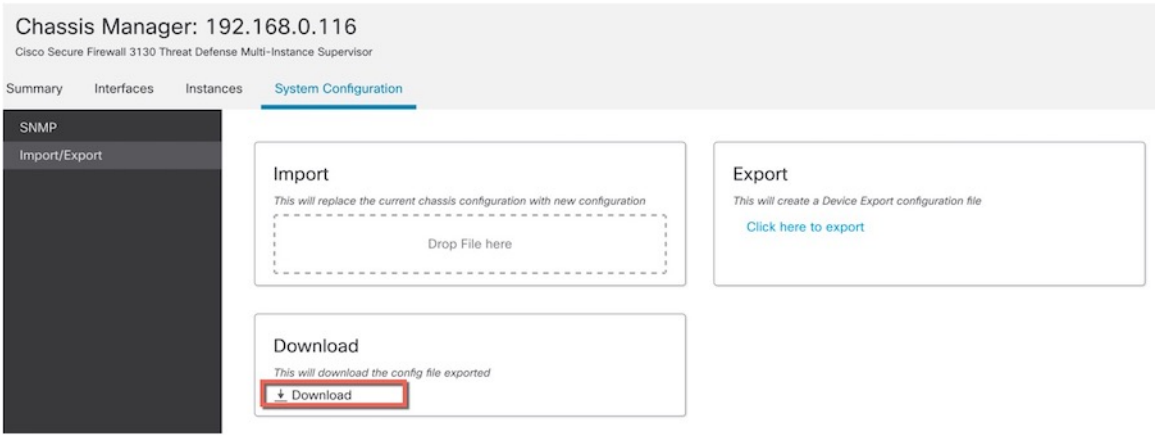
b) [エクスポートファイルが正常に作成されました（Export file created successfully）] という通知をモニタリングします。

図 *40* : 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。

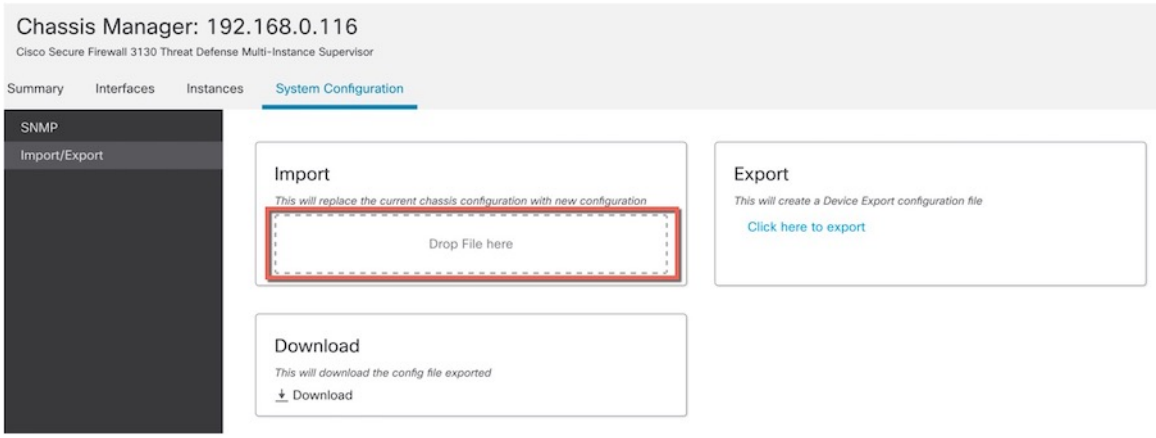
図 *41* : ダウンロード



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 *42* : 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（**[デバイス（Devices）]**>**[プラットフォーム設定（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 **[デバイス（Devices）]** > **[プラットフォーム設定（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[コピー（Copy）]（）、**[編集（Edit）]**（）、または[削除（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。

a) 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。

b) 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。

c) 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。

d) **[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 **[編集（Edit）]**（） をクリックします。

a) [ポリシーの割り当て（Policy Assignment）] をクリックします。

b) 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。

c) 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 [削除（Delete）]（） をクリックします。

d) [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。

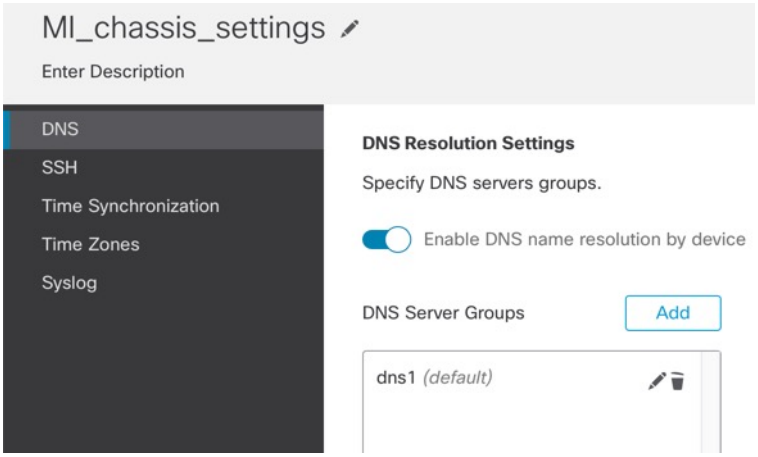
複数の DNS サーバーを設定する場合、シャーシによるサーバーの使用順はランダムになります。4 つの DNS サーバーグループにまたがって最大 4 つのサーバーを設定できます。たとえば、4 台のサーバーで 1 つのサーバーグループを設定したり、それぞれ 1 台のサーバーで 4 つのサーバーグループを設定したりできます。

手順

ステップ 1 **[Devices]** > **[Platform Settings]** を選択し、シャーシポリシーを作成または編集します。

ステップ 2 [DNS] を選択します。

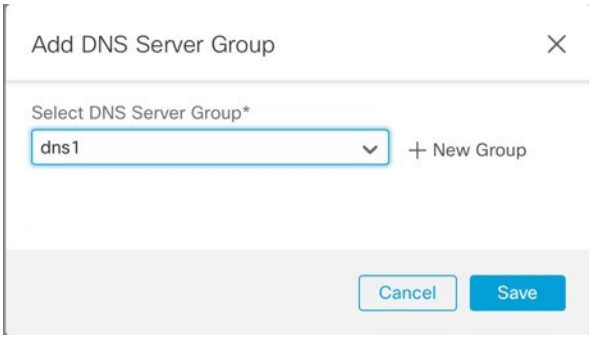
図 *43 : DNS*



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。

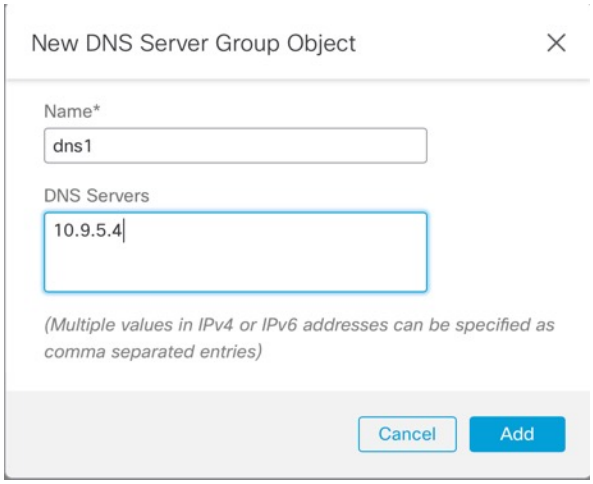
図 *44 : DNS* サーバーグループの追加



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 *45* : 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。

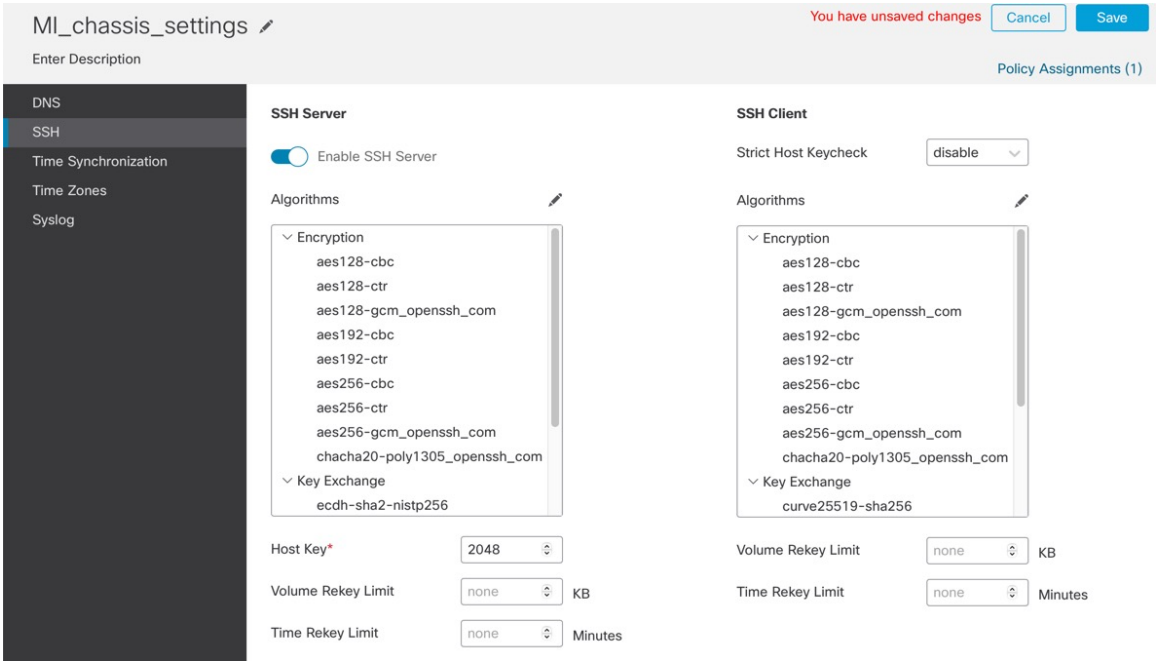
手順

ステップ 1 **[Devices]** > **[Platform Settings]** を選択し、シャーシポリシーを作成または編集します。

ステップ 2 [SSH] を選択します。

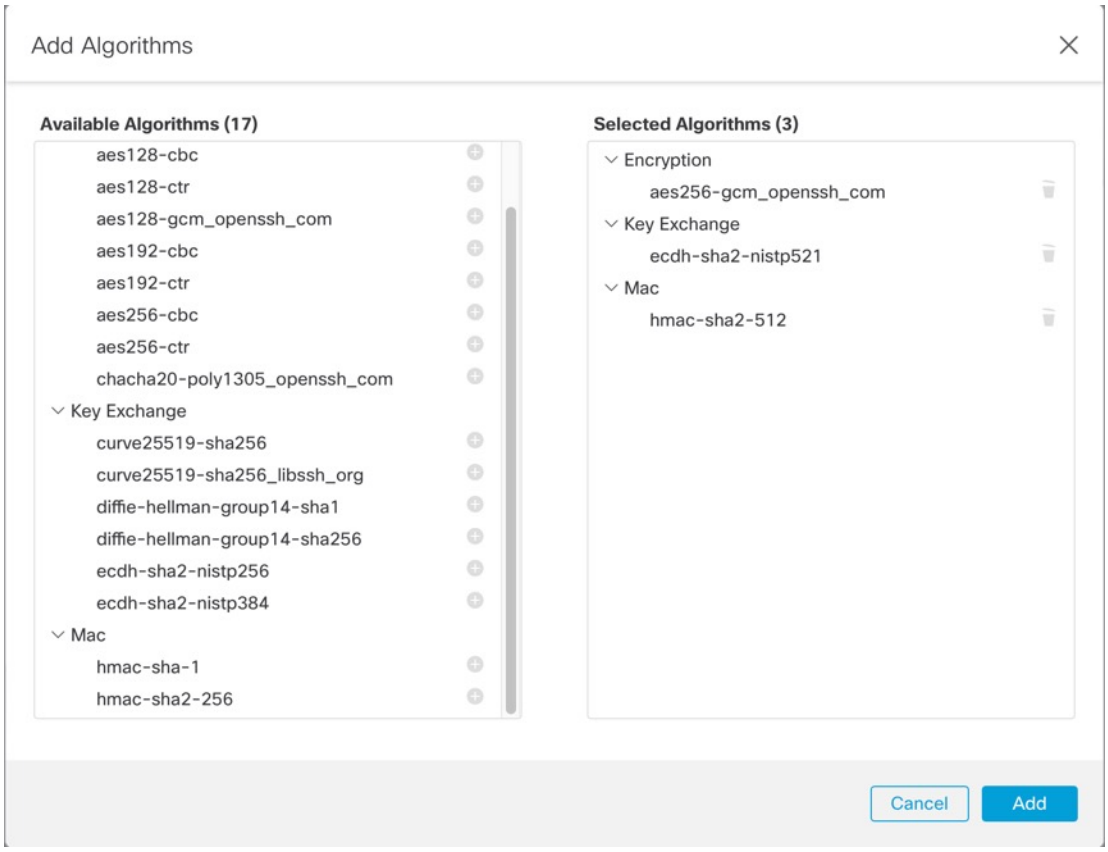
ステップ 3 シャーシへの SSH アクセスを有効にするには、[SSHサーバーの有効化（Enable SSH Server）] スライダを有効にします。

図 *46 : SSH*



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

図 *47*：アルゴリズムの追加



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。

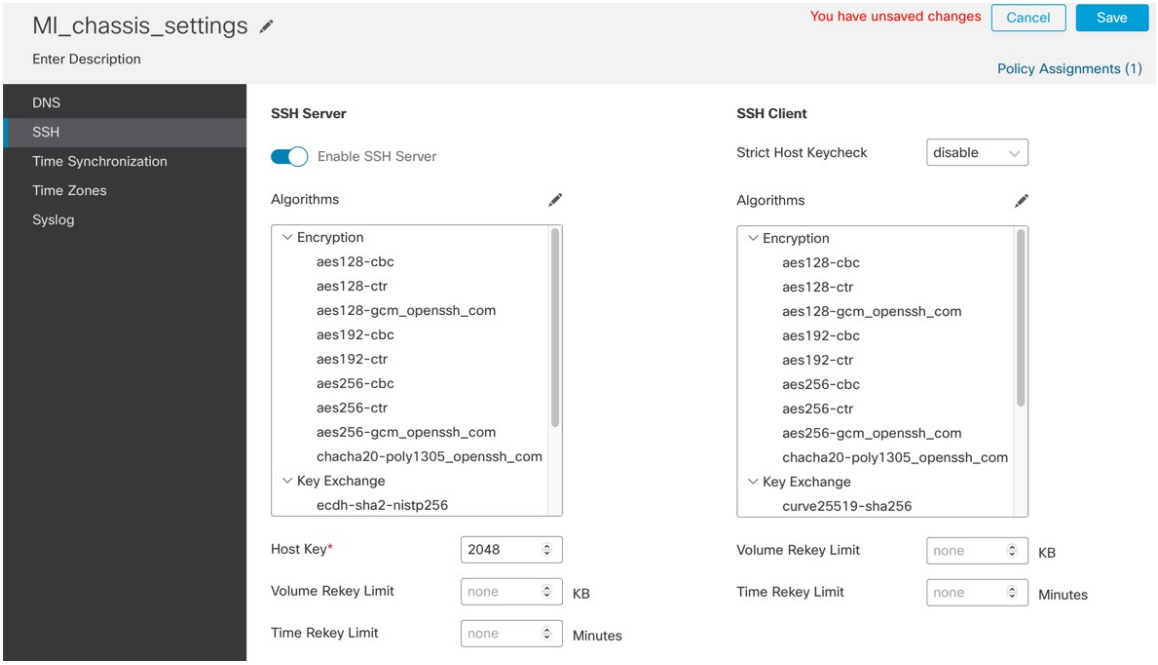
モジュラス値（ビット単位）は、1024 ～ 2048 の範囲内の 8 の倍数です。指定するキー係数のサイズが大きいほど、RSA キー ペアの生成にかかる時間は長くなります。値は 2048 にすることをお勧めします。

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。

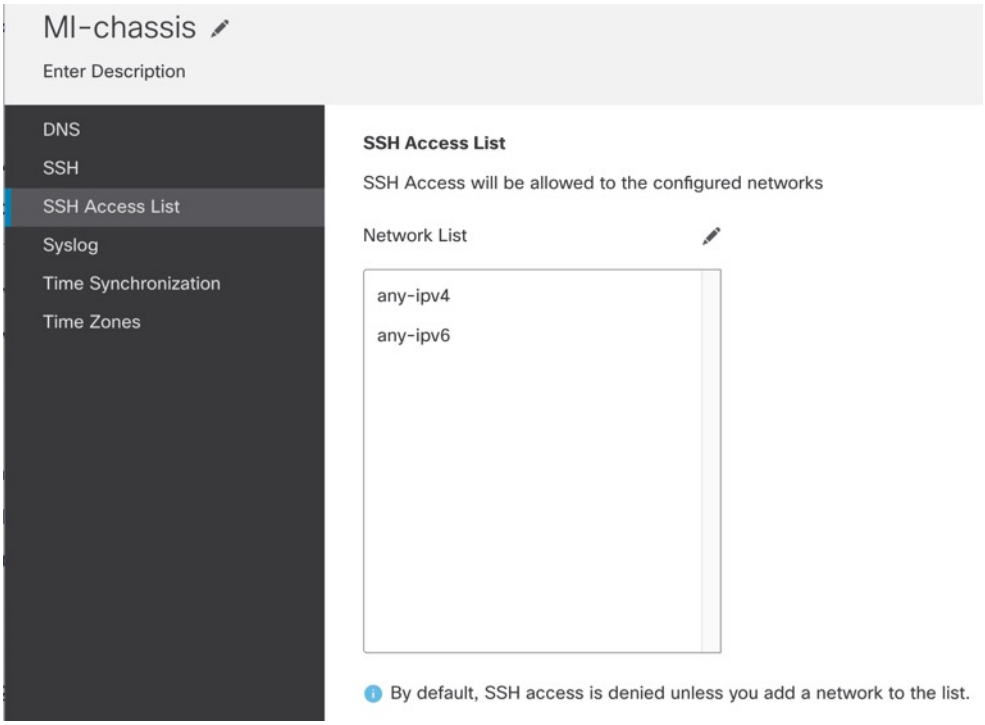
図 *48 : SSH*



- [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）]：**[編集（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。

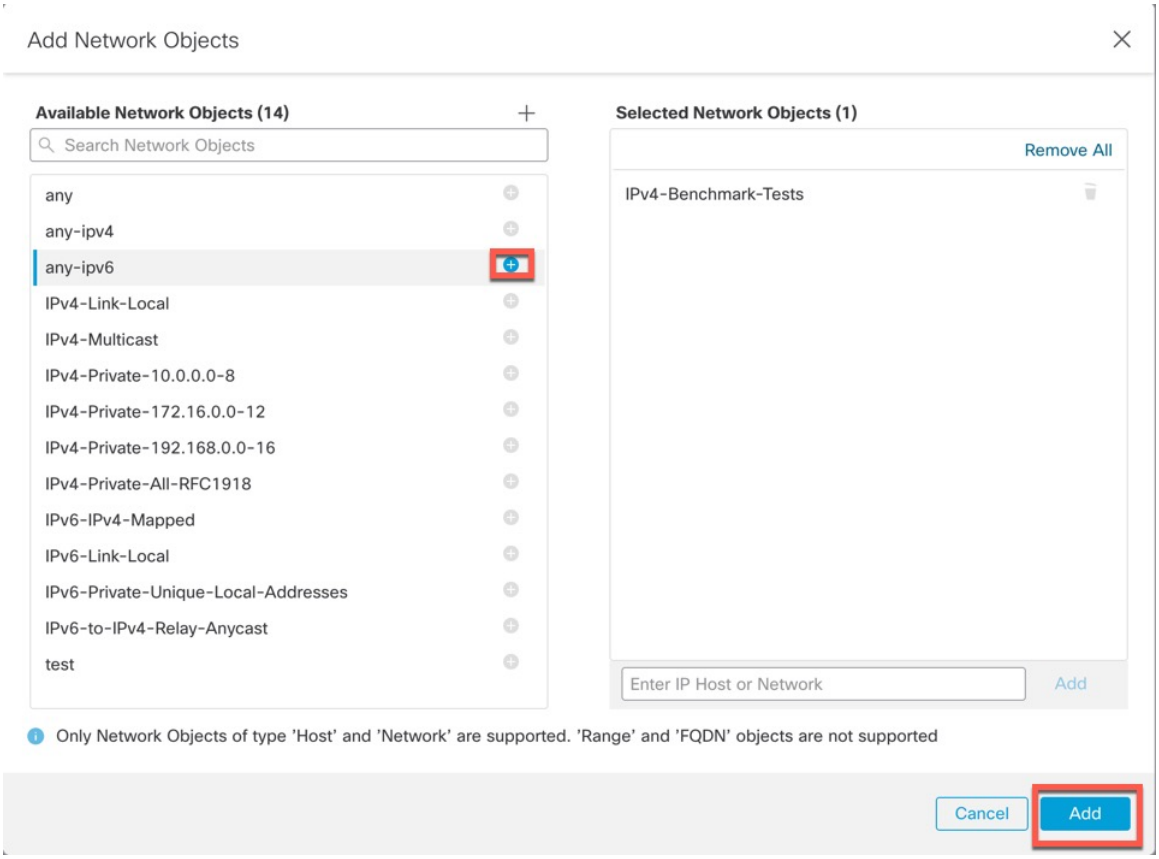
ステップ 9 [SSHアクセスリスト（SSH Access List）] を選択します。SSH を使用するには、IP アドレスまたはネットワークへのアクセスを許可する必要があります。

図 *49 : SSH* アクセスリスト



ステップ 10 **[編集（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 *50* : 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。

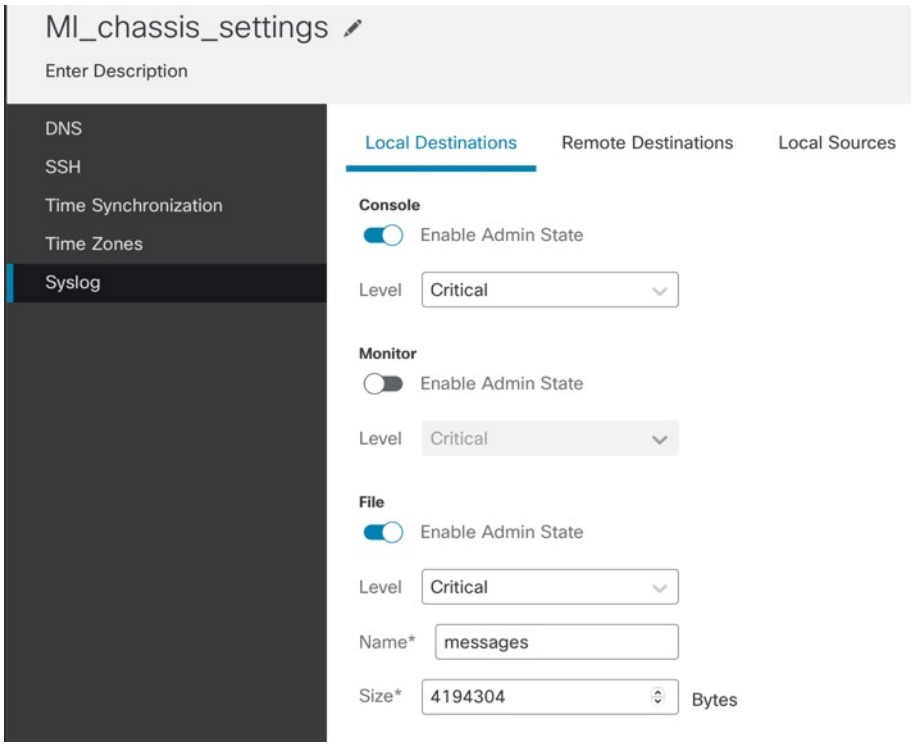
手順

ステップ 1 **[Devices]** > **[Platform Settings]** を選択し、シャーシポリシーを作成または編集します。

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 *51 : Syslog* のローカル接続先

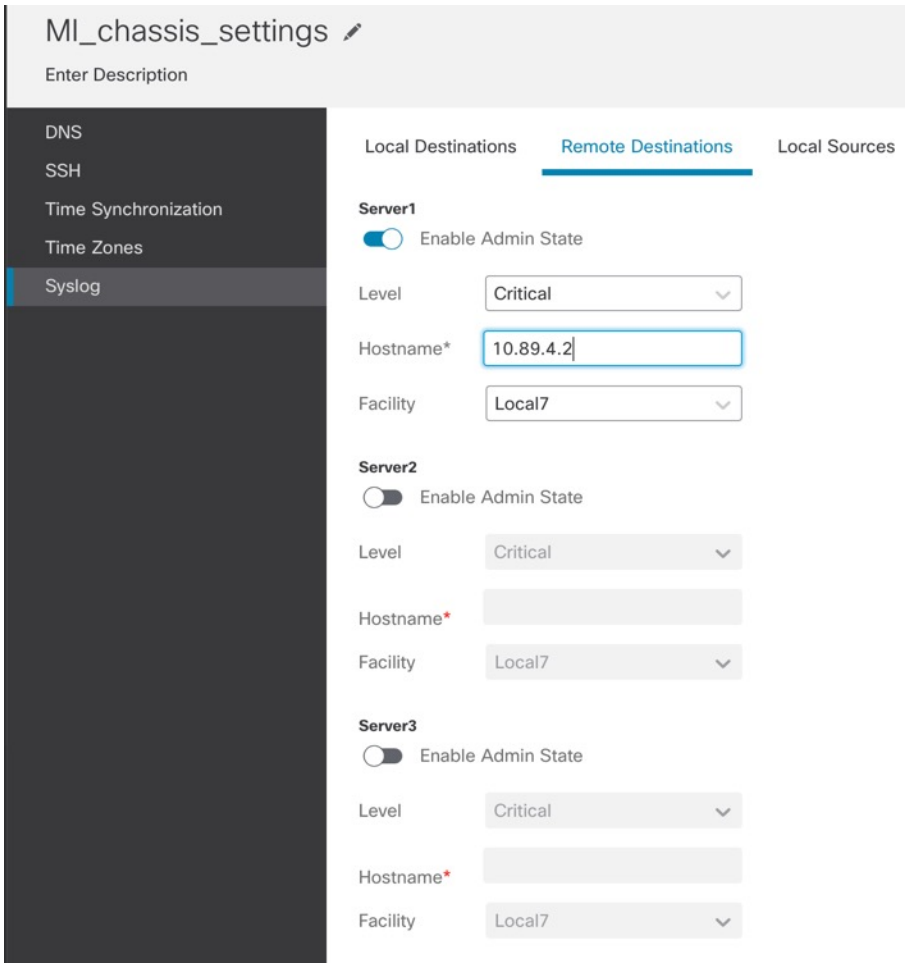


名前	説明
[コンソール（Console）] セクション	
[管理状態（Administrative State）] フィールド	シャーシがコンソールに syslog メッセージを表示するかどうかを指定します。 ログに追加するとともに、コンソールに syslog メッセージを表示する場合は、[有効化（Enable）] チェックボックスをオンにします。[有効化（Enable）] チェックボックスをオフにすると、syslog メッセージはログに追加されますが、コンソールに表示されません。
[レベル（Level）] フィールド	[コンソール（Console）] > [管理状態（Admin State）] 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。シャーシ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。 • **緊急（Emergencies）** • **[Alerts]** • **[Critical]**
[モニタ（Monitor）] セクション	

名前	説明
[管理状態（Administrative State）] フィールド	シャーシがモニタに syslog メッセージを表示するかどうかを指定します。 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。[有効化（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。
[レベル（Level）] ドロップダウン リスト	[モニタ（Monitor）] > [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、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。 • **緊急（Emergencies）** • **[Alerts]** • **[Critical]** • **[Errors]** • **[Warnings]** • **[Notifications]** • **[Information]** • **[Debugging]**

ステップ 4 [リモート接続先（Remote Destinations）] 領域で、シャーシ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 *52 : Syslog* のリモート接続先



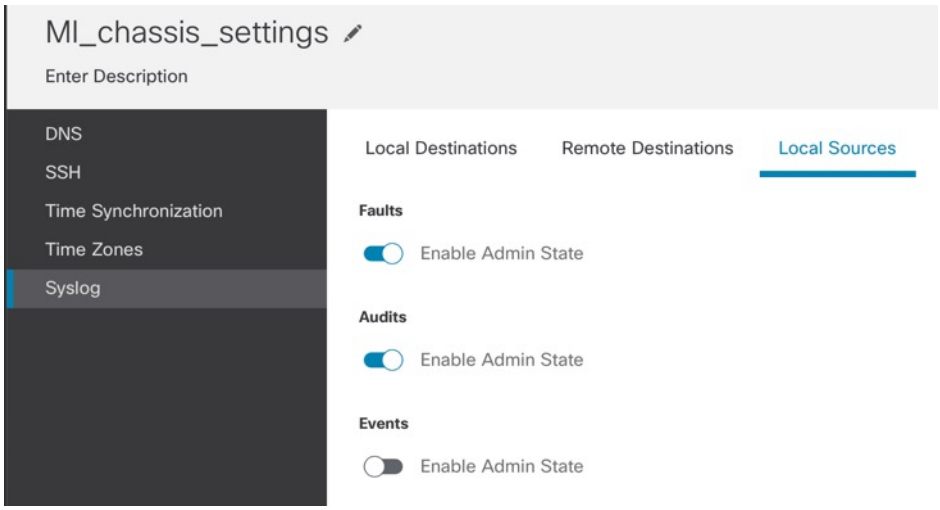
syslog メッセージをリモート宛先に送信することで、外部 syslog サーバで利用可能なディスク領域に応じてメッセージをアーカイブし、保存後にロギング データを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたときに特別なアクションが実行されるように指定したり、ログからデータを抽出してレポート用の別のファイルにその記録を保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

名前	説明
[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。

名前	説明
[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。そのレベル以上のメッセージがリモート ファイルに保存されます。次のいずれかになります。 • **緊急（Emergencies）** • **[Alerts]** • **[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。 • **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 *53 : 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

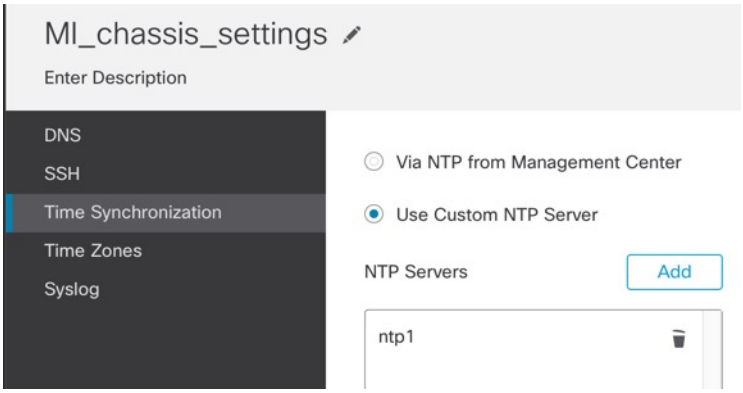
NTP サーバのホスト名を使用する場合は、DNS サーバを設定する必要があります。DNS の設定 （50 ページ）を参照してください。

手順

ステップ 1 **[Devices]** > **[Platform Settings]** を選択し、シャーシポリシーを作成または編集します。

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

図 *54* : 時刻の同期



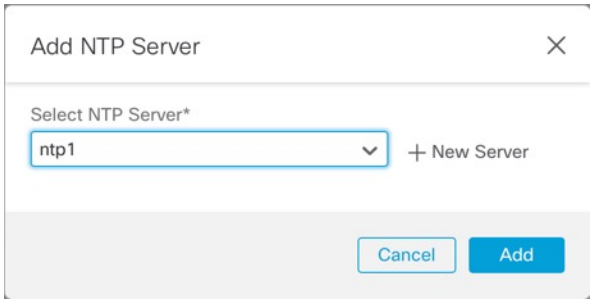
ステップ 3 Management Center から時刻を取得する場合は、[Management CenterのNTP経由（Via NTP from Management Center）] をクリックします。

このオプションにより、シャーシと 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。

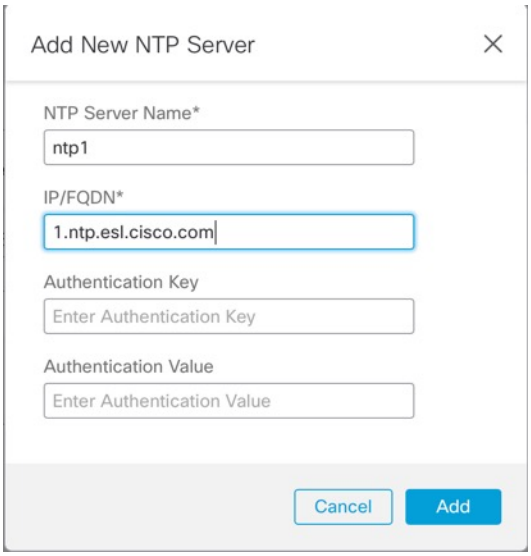
a) [追加（Add）] をクリックしてサーバーを追加します。

図 *55* : *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 *56* : 新しい *NTP* サーバーの追加



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

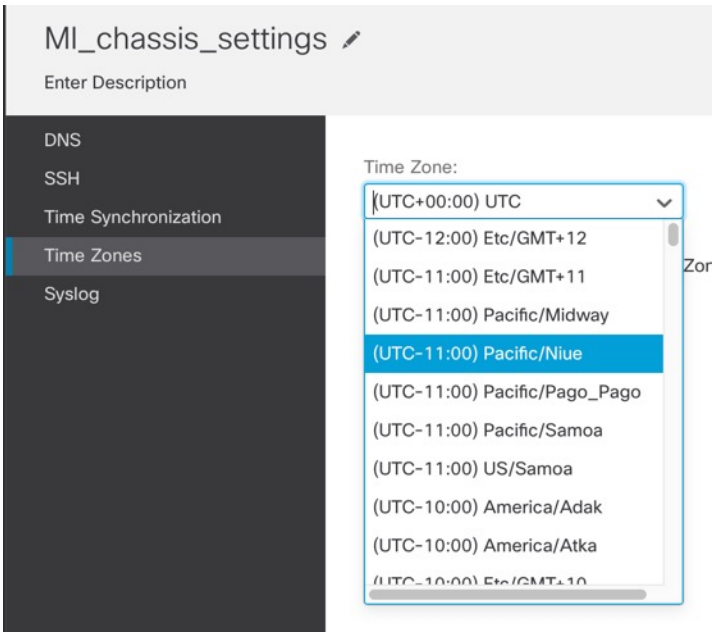
シャーシのタイムゾーンを設定します。

手順

ステップ 1 **[Devices]** > **[Platform Settings]** を選択し、シャーシポリシーを作成または編集します。

ステップ 2 [タイムゾーン（Time Zones）] を選択します。

図 *57* : 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シ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。

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。

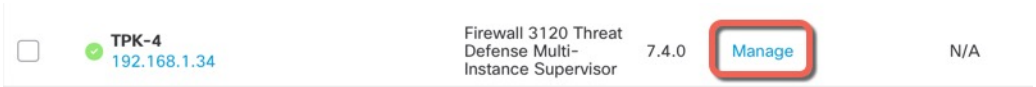
始める前に

- インスタンスの設定 （21 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）]** > の **[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 **[編集（Edit）]** （✎） をクリックします。

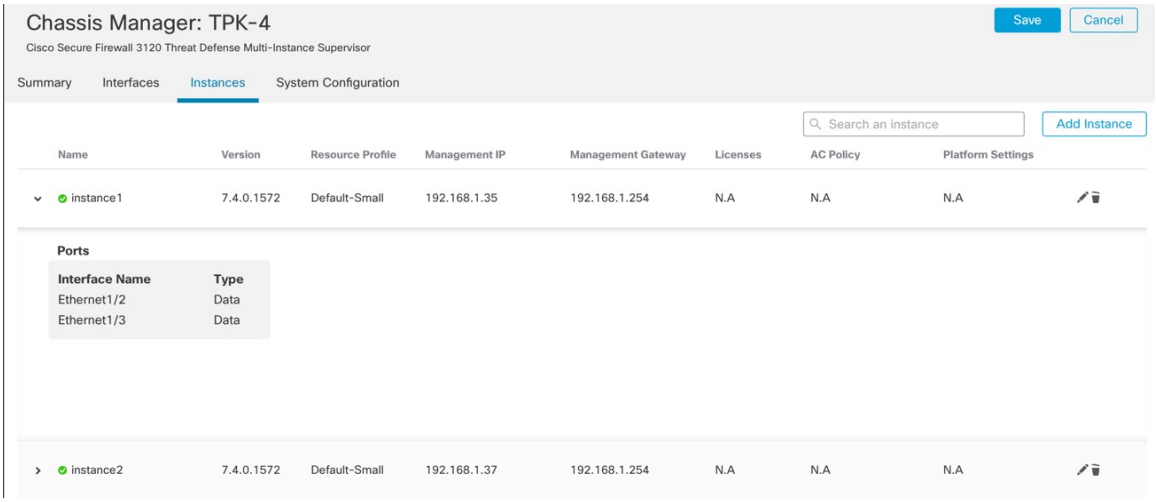
図 *58 :* シャーシの管理



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。

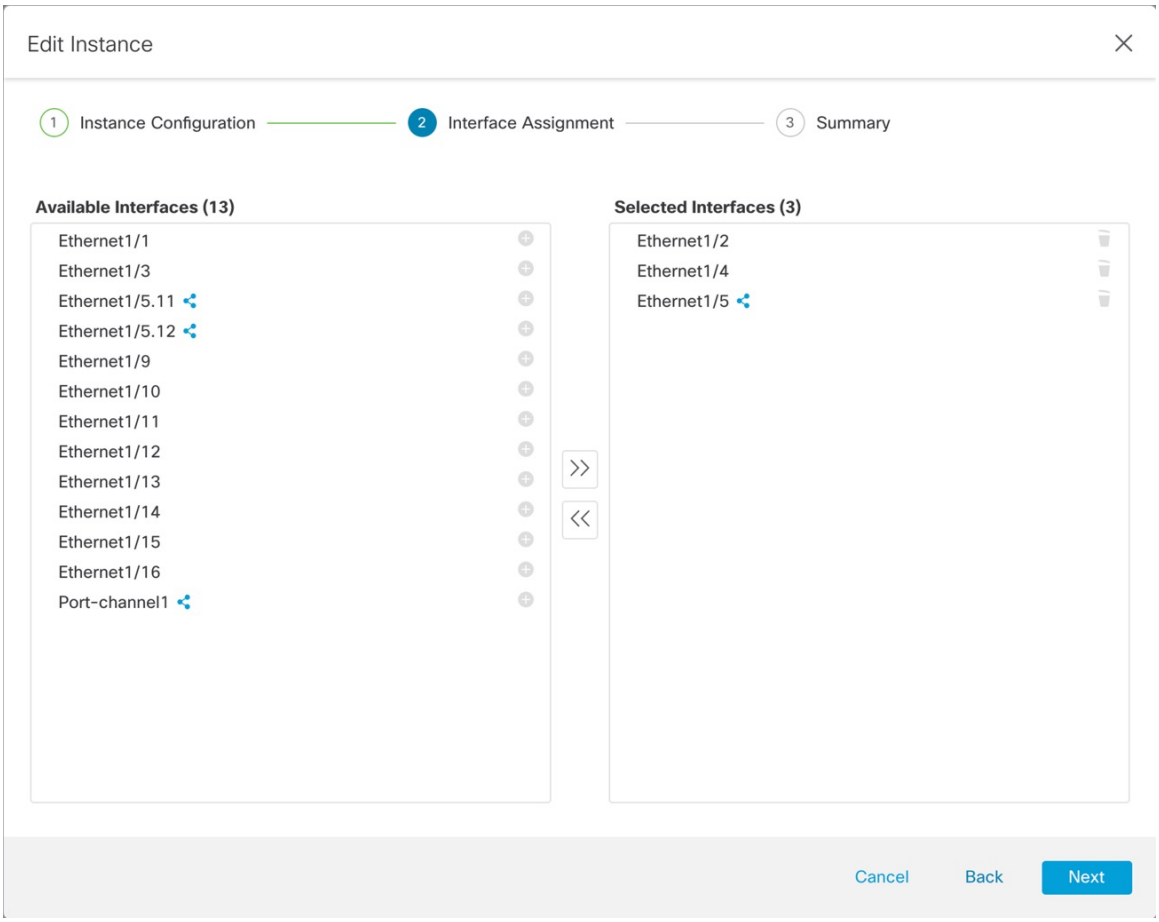
ステップ 2 [インスタンス（Instances）] をクリックし、インターフェイスを変更するインスタンスの横にある **[編集（Edit）]** （✎） をクリックします。

図 *59 : Instances*



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 *60*：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 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、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。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 Management Center を変更します。

最初に、現在の 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*}：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、少なくても 1 台以上のデバイス（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 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 **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（-）などがあります。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。
- **Registration Key:** *reg_key*：シャーシを登録するときに Management Center でも指定する任意のワン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（-）などがあります。

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、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、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 に割り当てられます。

```
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	最小 Management Center	最小 Threat Defense	詳細
Cisco Secure Firewall 3100 のマルチインスタンスモード。	7.4.1	7.4.1	Secure Firewall 3100 は、単一のデバイス（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（マルチインスタンスモード）として展開できます。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では、コンテナインスタンスのアップグレード（*Threat Defense* のアップグレード）とは別に、オペレーティングシステムとファームウェアがアップグレード対象（シャーシのアップグレード）になることに注意してください。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [追加（Add）] > [シャーシ（Chassis）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [シャーシマネージャ（Chassis Manager）]** • **[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [新しいポリシー（New Policy）] > [シャーシプラットフォーム設定（Chassis Platform Settings）]** • **[デバイス（Devices）] > [シャーシのアップグレード（Chassis Upgrade）]** 新規/変更された Threat Defense CLI コマンド：**configure multi-instance network ipv4**、**configure multi-instance network ipv6** 新規/変更された FXOS CLI コマンド：**create device-manager**、**set deploymode** プラットフォームの制限：Cisco Secure Firewall 3105 ではサポートされていません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。