通常のファイアウォール インターフェイス

この章では、 EtherChannel、VLAN サブインターフェイス、IP アドレスなどを含む通常のファイアウォール Firewall Threat Defense インターフェイスの設定について説明します。

（注） Firepower 4100/9300 の最初のインターフェイスの設定については、Configure Interfacesを参照してください。

通常のファイアウォールインターフェイスの要件と前提条件

Model support

Firewall Threat Defense

User roles

- Admin
- Access Admin

- Network Admin

スイッチポートの設定

サポートされているプラットフォームの場合、通常のファイアウォールインターフェイスとしてまたはレイヤ2ハードウェアスイッチポートとして実行するように各インターフェイスを構成できます。この項では、スイッチ モードの有効化と無効化、VLAN インターフェイスの作成、そのインターフェイスのスイッチ ポートへの割り当てなど、スイッチ ポート設定を開始するためのタスクについて説明します。また、サポートされているインターフェイスで Power on Ethernet（PoE）をカスタマイズする方法についても説明します。

About switch ports

This section describes the switch ports for models with Layer 2 switches.

Understanding switch ports and interfaces

Ports and interfaces

For each physical interface, you can set its operation as a firewall interface or as a switch port. See the following information about physical interface and port types as well as logical VLAN interfaces to which you assign switch ports:

- Physical firewall interface—In routed mode, these interfaces forward traffic between networks at Layer 3, using the configured security policy to apply firewall and VPN services. In transparent mode, these interfaces are bridge group members that forward traffic between the interfaces on the same network at Layer 2, using the configured security policy to apply firewall services. In routed mode, you can also use Integrated Routing and Bridging with some interfaces as bridge group members and others as Layer 3 interfaces. By default, the Ethernet 1/1 interface is configured as a firewall interface. You can also configure these interfaces to be IPS-only (inline sets and passive interfaces).
- Physical switch port—Switch ports forward traffic at Layer 2, using the switching function in hardware. Switch ports on the same VLAN can communicate with each other using hardware switching, and traffic is not subject to the Firewall Threat Defense security policy. Access ports accept only untagged traffic, and you can assign them to a single VLAN. Trunk ports accept untagged and tagged traffic, and can belong to more than one VLAN. By default, Ethernet 1/2 and higher are configured as access switch ports on VLAN 1. You cannot configure the Management interface as a switch port.
- Logical VLAN interface—These interfaces operate the same as physical firewall interfaces, with the exception being that you cannot create subinterfaces, IPS-only interfaces (inline sets and passive interfaces), or EtherChannel interfaces. When a switch port needs to communicate with another network, then the Firewall Threat Defense device applies the security policy to the VLAN interface and routes to another logical VLAN interface or firewall interface. You can even use Integrated Routing and Bridging with VLAN interfaces as bridge group members. Traffic between switch ports on the same VLAN are not subject to the Firewall Threat Defense security policy, but traffic between VLANs in a bridge group are subject to the security policy, so you may choose to layer bridge groups and switch ports to enforce the security policy between certain segments.

Power Over Ethernet

PoE is available on the following ports:

- Firepower 1010—Ethernet 1/7 and 1/8 using IEEE 802.3af (PoE) and 802.3at (PoE+) up to 30 watts per port, up to a combined 60 watts.
- Secure Firewall 1210CP—Ethernet 1/5, 1/6, 1/7, and 1/8 using IEEE 802.3af (PoE), 802.3at (PoE+), and 802.3bt (PoE++ and Hi-PoE) up to 90 watts per port, up to a combined 120 watts.

（注） PoE is not supported on the 1010E, 1210CE, and 1220CX.

PoE+ or higher uses Link Layer Discovery Protocol (LLDP) to negotiate the power level. Power is only supplied when needed.

If you shut down the interface, then you disable power to the device.

Auto-MDI/MDIX feature

For all switch ports, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled. When the speed and duplex are set to 1000 and full, then the interface always auto-negotiates; therefore Auto-MDI/MDIX is always enabled and you cannot disable it.

Prerequisites for switch ports

Model support

- Firepower 1010
- Secure Firewall 1210/1220

Guidelines for switch ports

High availability and clustering

- No cluster support.
- You should not use the switch port functionality when using High availability. Because the switch ports operate in hardware, they continue to pass traffic on both the active *and* the standby units. High availability is designed to prevent traffic from passing through the standby unit, but this feature does not extend to switch ports. In a normal High availability network setup, active switch ports on both units will lead to network loops. We suggest that you use external switches for any switching capability. Note that VLAN interfaces can be monitored by failover, while switch ports cannot. Theoretically, you can put a single switch port on a VLAN and successfully use High availability, but a simpler setup is to use physical firewall interfaces instead.

- You can only use a firewall interface as the failover link.

Logical VLAN interfaces (SVIs)

- If you also use VLAN subinterfaces on a firewall interface, you cannot use the same VLAN ID as for a logical VLAN interface. VLAN 1 is reserved for the logical VLAN interface.
- MAC Addresses:
  - Routed firewall mode—All VLAN interfaces share a MAC address. Ensure that any connected switches can support this scenario. If the connected switches require unique MAC addresses, you can manually assign MAC addresses. See MAC アドレスの設定 （78 ページ）.
  - Transparent firewall mode—Each VLAN interface has a unique MAC address. You can override the generated MAC addresses if desired by manually assigning MAC addresses. See MAC アドレスの設定 （78 ページ）.

Bridge groups

You cannot mix logical VLAN interfaces and physical firewall interfaces in the same bridge group.

VLAN interface and switch port unsupported features

VLAN interfaces and switch ports do not support:

- Dynamic routing
- Multicast routing
- Equal-Cost Multi-Path routing (ECMP)
- Inline sets or Passive interfaces
- EtherChannels—Switch ports cannot be part of an EtherChannel. PoE is also not supported on a port in an EtherChannel.
- Failover and state link
- Security group tagging (SGT)

Other Guidelines and Limitations

- You can configure a maximum of 60 named interfaces.
- You cannot configure the Management interface as a switch port.

Default Settings

- Ethernet 1/1 is a firewall interface.
- On 1010, Ethernet 1/2 through Ethernet 1/8 are switch ports assigned to VLAN 1.
- On 1210, Ethernet 1/2 through Ethernet 1/8 are switch ports assigned to VLAN 1.
- On 1220, Ethernet 1/2 through Ethernet 1/10 are switch ports assigned to VLAN 1.

• Default Speed and Duplex—By default, the speed and duplex are set to auto-negotiate.

Configure switch ports and Power Over Ethernet

To configure switch ports and PoE, complete the following tasks.

スイッチ ポート モードの有効化または無効化

各インターフェイスは、ファイアウォール インターフェイスまたはスイッチ ポートのいずれかになるように個別に設定できます。デフォルトでは、イーサネット 1/1 はファイアウォール インターフェイスで、残りのイーサネット インターフェイスはスイッチ ポートとして設定されます。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** ()] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 [スイッチポート（SwitchPort）] 列のスライダをクリックしてスイッチポートモードを設定すると、**Slider enabled** ()または**Slider disabled** ()と表示されます。

デフォルトでは、スイッチ ポートは VLAN 1 のアクセス モードに設定されています。トラフィックをルーティングし、Firewall Threat Defense セキュリティ ポリシーに参加するには、論理 VLAN 1 インターフェイス（またはこれらのスイッチ ポートに設定した任意の VLAN）を手動で追加する必要があります（VLAN インターフェイスを構成する （5 ページ）を参照）。管理インターフェイスをスイッチポートモードに設定することはできません。スイッチポートモードを変更すると、サポートされていないすべての設定が削除されます。

さらに、インターフェイスがすでに有効になっている場合は、無効になります。インターフェイスを再度有効にしたことを確認してください。

VLAN インターフェイスを構成する

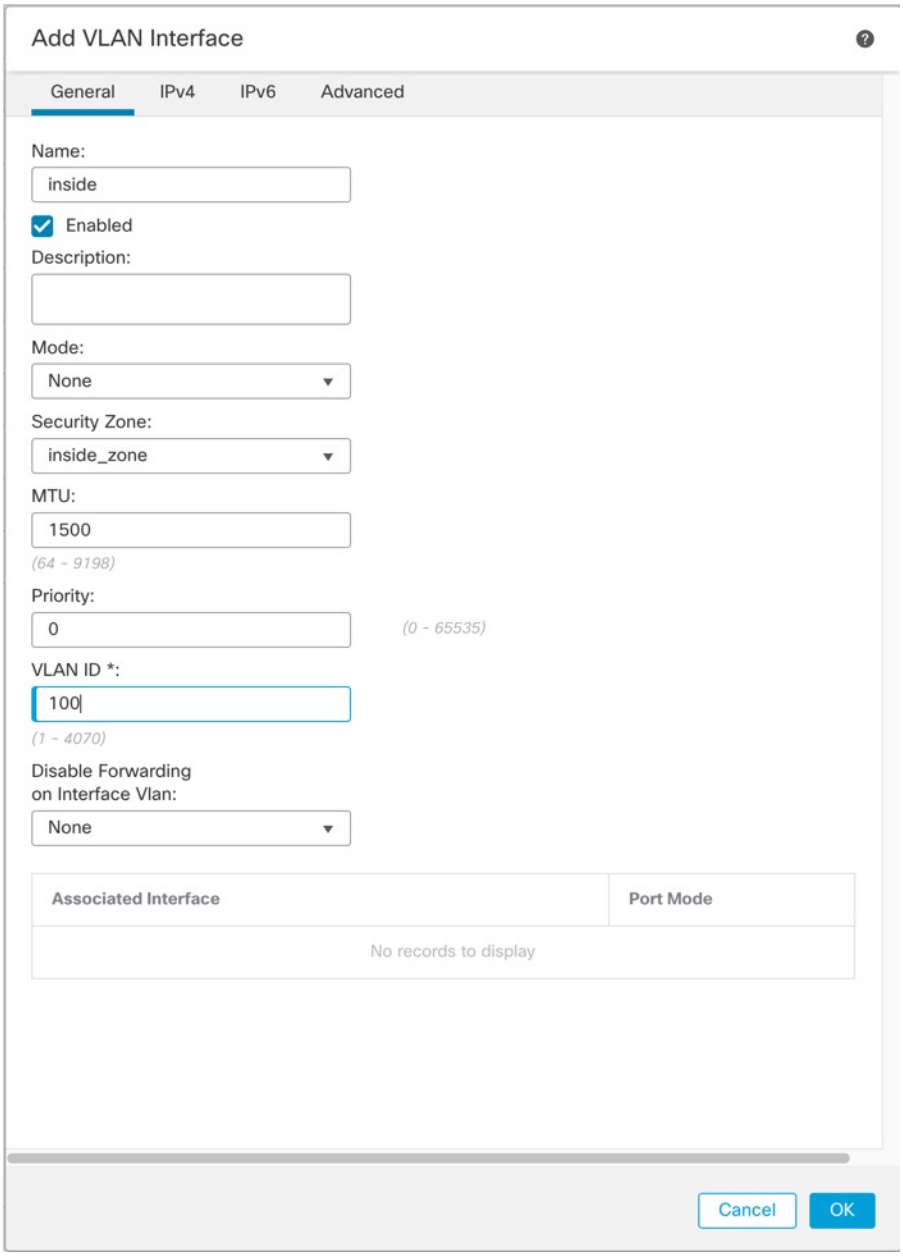
ここでは、関連付けられたスイッチポートで使用するための VLAN インターフェイスの設定方法について説明します。デフォルトでは、スイッチポートは VLAN1 に割り当てられます。トラフィックをルーティングし、Firewall Threat Defense セキュリティポリシーに参加するには、論理 VLAN1 インターフェイス（またはこれらのスイッチポートに設定した任意の VLAN）を手動で追加する必要があります。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 **[インターフェイスの追加（Add Interfaces）]** > **[VLANインターフェイス（VLAN Interface）]** をクリックします。

ステップ 3 [一般（General）] で、次の VLAN 固有のパラメータを設定します。



既存の VLAN インターフェイスを編集している場合、[関連付けられているインターフェイス（Associated Interface）] テーブルには、この VLAN のスイッチ ポートが表示されます。

a) [VLAN ID] を 1 ー 4070 の範囲に設定します。ただし、内部使用のために予約されている 3968 ー 4047 の範囲の ID は除きます。

インターフェイスを保存した後、VLAN ID を変更することはできません。ここでの VLAN ID は、使用される VLAN タグと設定内のインターフェイス ID の両方です。

b) （任意）[インターフェイス VLAN での転送の無効化（Disable Forwarding on Interface VLAN）] の VLAN ID を選択し、別の VLAN への転送を無効にします。

たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。自宅のネットワークはビジネス ネットワークにアクセスする必要がないので、自宅の VLAN で転送を無効にできます。ビジネス ネットワークは自宅のネットワークにアクセスできますが、その反対はできません。

ステップ 4 インターフェイス設定を完了するには、次のいずれかの手順を参照してください。

- ルーテッド モードのインターフェイスの設定 （47 ページ）
- ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定 （54 ページ）

ステップ 5 **[OK]** をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

スイッチ ポートのアクセス ポートとしての構成

1 つの VLAN にスイッチ ポートを割り当てるには、アクセス ポートとして設定します。アクセス ポートは、タグなしのトラフィックのみを受け入れます。スイッチ ポートで有効にされ、VLAN1 に割り当てられているインターフェイスは次のとおりです。

デバイス モデル	スイッチ ポート インターフェイス
Firepower 1010	イーサネット 1/2 ～イーサネット 1/8
Cisco Secure Firewall 1210	イーサネット 1/2 ～イーサネット 1/8
Cisco Secure Firewall 1220	イーサネット 1/2 ～イーサネット 1/10

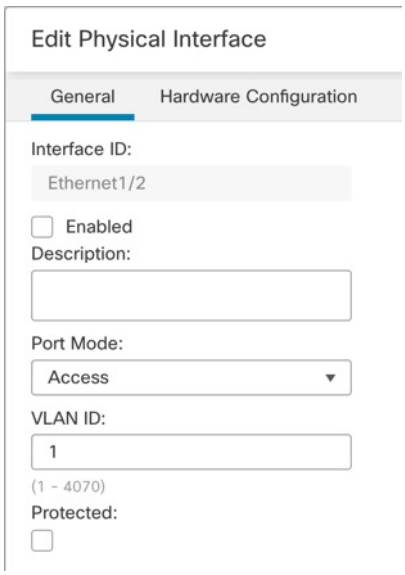
（注） デバイスは、ネットワーク内のループ検出に使用されるスパニングツリープロトコルをサポートしていません。したがって、Firewall Threat Defense とのすべての接続は、ネットワークループ内で終わらないようにする必要があります。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

図 *1:* 物理インターフェイスの編集



ステップ 3 [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 4 （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 5 [ポートモード（Port Mode）] を [アクセス（Access）] に設定します。

ステップ 6 [VLAN ID] フィールドで、このスイッチ ポートの VLAN を 1 ～ 4070 の範囲で設定します。

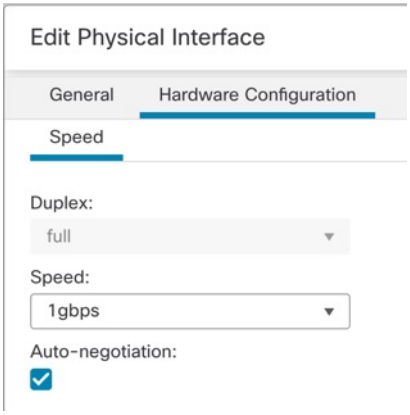
デフォルトの VLAN ID は 1 です。

ステップ 7 （任意） このスイッチ ポートを保護対象として設定するには、[保護済み（Protected）]チェックボックスをオンにします。これにより、スイッチ ポートが同じ VLAN 上の他の保護されたスイッチ ポートと通信するのを防ぐことができます。

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチ ポートで [保護済み（Protected）] を有効にすると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

ステップ 8 （任意）[ハードウェア構成（Hardware Configuration）] をクリックして、デュプレックスと速度を設定します。

図 *2:* ハードウェア構成



[自動ネゴシエーション（Auto-negotiation）] チェックボックス（デフォルト）をオンにして、速度とデュプレックスを自動検出します。このチェックボックスをオフにすると、速度とデュプレックスを手動で設定できます。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。
- [速度（Speed）] : [10mbps]、[100mbps]、または [1gbps] を選択します。

（注）
50G ケーブルを介してポートに接続しているピアスイッチが自動ネゴシエーションをサポートしていない場合は、スイッチと Threat Defense インターフェイスでも自動ネゴシエーションを無効にしてください。たとえば、N9K-C93400LD-H1 は 50G ケーブルでの自動ネゴシエーションをサポートしていません。したがって、ポートを接続するには、プラットフォームとスイッチでデフォルトの自動ネゴシエーションを無効にする必要があります。

ステップ 9 **[OK]** をクリックします。

ステップ 10 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

スイッチ ポートのトランク ポートとしての構成

この手順では、802.1Q タグ付けを使用して複数の VLAN を伝送するトランク ポートの作成方法について説明します。トランクポートは、タグなしトラフィックとタグ付きトラフィックを受け入れます。許可された VLAN のトラフィックは、トランクポートを変更せずに通過します。

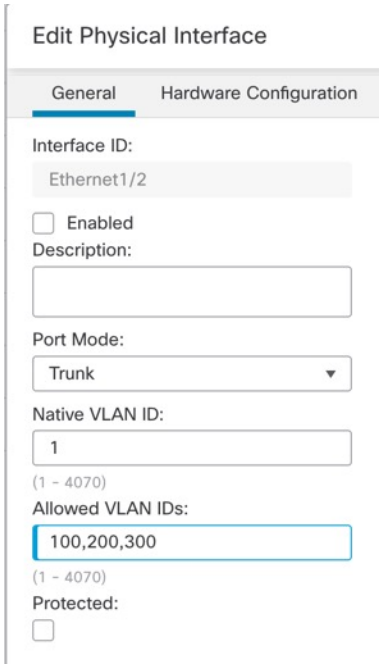
トランクは、タグなしトラフィックを受信すると、そのトラフィックをネイティブ VLAN ID にタグ付けして、Firewall Threat Defense デバイスが正しいスイッチポートにトラフィックを転送したり、別のファイアウォール インターフェイスにルーティングしたりできるようにします。Firewall Threat Defense デバイスは、トランクポートからネイティブ VLAN ID トラフィックを送信する際に VLAN タグを削除します。タグなしトラフィックが同じ VLAN にタグ付けされるように、他のスイッチのトランク ポートに同じネイティブ VLAN を設定してください。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

図 *3:* トランクポートモードの設定



ステップ 3 [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 4 （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 5 [ポートモード（Port Mode）] を [トランク（Trunk）] に設定します。

ステップ 6 [ネイティブVLAN ID（Native VLAN ID）] フィールドで、このスイッチ ポートのネイティブ VLAN を 1 ～ 4070 の範囲で設定します。

デフォルトのネイティブVLANは1です。

各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

ステップ 7 [許可VLAN ID（Allowed VLAN IDs）] フィールドで、このトランク ポートの VLAN を 1 ～ 4070 の範囲で入力します。

次のいずれかの方法で最大 20 個の ID を指定できます。

- 単一の番号（n）
- 範囲（n-x）
- 番号および範囲は、カンマで区切ります。たとえば、次のように指定します。

  5,7-10,13,45-100

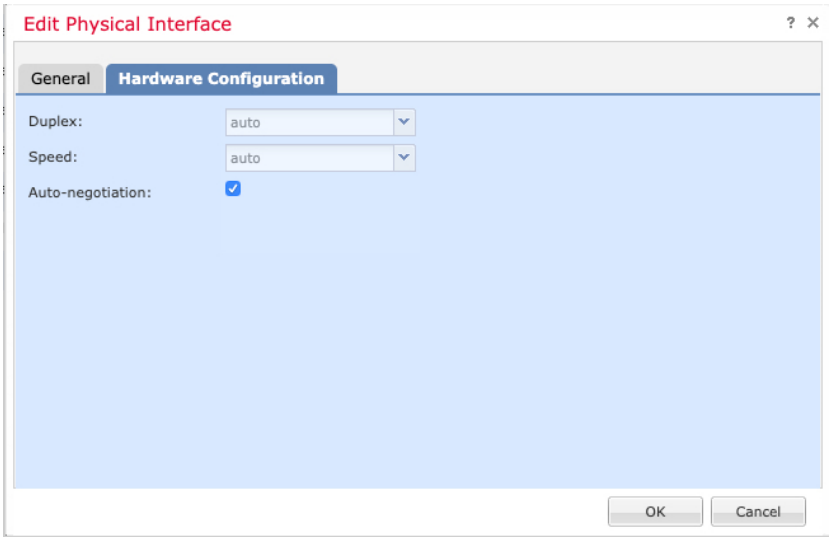
  カンマの代わりスペースを入力できます。

このフィールドにネイティブVLANを含めると、無視されます。トランクポートは、ネイティブVLANトラフィックをポートから送信するときに、常にVLANタグを削除します。さらに、ネイティブ VLAN タグ付きのトラフィックは受信されません。

ステップ 8 （任意）このスイッチ ポートを保護対象として設定するには、[保護済み（Protected）]チェックボックスをオンにします。これにより、スイッチ ポートが同じ VLAN 上の他の保護されたスイッチ ポートと通信するのを防ぐことができます。

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチ ポートで [保護済み（Protected）] を有効にすると、Webサーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

ステップ 9 （任意）[ハードウェア構成（Hardware Configuration）] をクリックして、デュプレックスと速度を設定します。



[自動ネゴシエーション（Auto-negotiation）] チェックボックス（デフォルト）をオンにして、速度とデュプレックスを自動検出します。このチェックボックスをオフにすると、速度とデュプレックスを手動で設定できます。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。
- [速度（Speed）] : [10mbps]、[100mbps]、または [1gbps] を選択します。

50G ケーブルを介してポートに接続しているピアスイッチが自動ネゴシエーションをサポートしていない場合は、スイッチと Threat Defense インターフェイスでも自動ネゴシエーションを無効にしてください。たとえば、N9K-C93400LD-H1 は 50G ケーブルでの自動ネゴシエーションをサポートしていません。したがって、ポートを接続するには、プラットフォームとスイッチでデフォルトの自動ネゴシエーションを無効にする必要があります。

ステップ 10 **[OK]** をクリックします。

ステップ 11 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

Power over Ethernet の設定

Power over Ethernet（PoE）ポートは、IP 電話や無線アクセスポイントなどのデバイスに電力を供給します。PoE はデフォルトでイネーブルです。この手順では、PoE を無効および有効にする方法と、オプションパラメータを設定する方法について説明します。

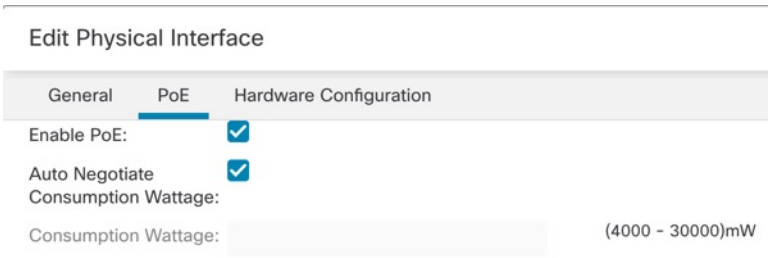
手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 Firepower 1010 の Ethernet 1/7 または 1/8、または Secure Firewall 1210CP の Ethernet 1/5 ～ 1/8 の任意のインターフェイスの **Edit** (✎) をクリックします。

ステップ 3 [PoE] をクリックします。

図 *4 : PoE*



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

PoE はデフォルトでイネーブルです。

ステップ 5 自動ネゴシエーションまたは手動電源を選択します。

- **[消費ワット数の自動ネゴシエート（Auto Negotiate Consumption Wattage）]**：給電先デバイスのクラスに適したワット数を使用して、給電先デバイスに自動的に電力を供給します。ファイアウォールは LLDP を使用して、さらに適切なワット数をネゴシエートします。特定クラスのデバイスを接続すると、より多くの電力を使用する必要がある場合に備えて、そのクラスの最大値までプロビジョニングが行われます。たとえば、12.95W を要求するクラス 4 デバイスを追加した場合、そのデバイスが現在その電力すべてを使用していなくても、30W が割り当てられます。一部のデバイスは、電力要件を再ネゴシエートできます。デバイスに必要な電力が割り当てられている電力よりも少ないことがわかっている場合は、代わりに **[消費ワット数（Consumption Wattage）]** を手動で設定して、他のデバイス用に電力を解放できます。

- **[消費ワット数（Consumption Wattage）]**：**[消費ワット数の自動ネゴシエート（Auto Negotiate Consumption Wattage）]** チェックボックスをオフにして、手動ワット数を設定し、ワット数を（ミリワット単位）で 4000 ～ 30000 （1010）または 90000（1210CP）に手動で指定します。ワット数を手動で設定し、LLDP ネゴシエーションを無効にする場合は、このコマンドを使用します。手動割り当ての場合、 **show power inline** 出力にクラスが **n/a** と表示されます。これは、クラスが消費電力の決定に使用されないためです。

  show power inline コマンドを使用して、現在の PoE ステータスを表示します。

ステップ 6 **[OK]** をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

ループバック インターフェイスの設定

ここでは、ループバック インターフェイスを設定する方法について説明します。

ループバック インターフェイスについて

A loopback interface is a software-only interface that emulates a physical interface. This interface is reachable on IPv4 and IPv6 through multiple physical interfaces. The loopback interface helps to overcome path failures; it is accessible from any physical interface, so if one goes down, you can access the loopback interface from another.

Loopback interfaces can be used for:

- AAA
- BGP
- DNS
- HTTP
- ICMP
- IPsec flow offload—Secure Firewall 1200/3100/4200 only
- NetFlow
- SNMP
- SSH
- Static and dynamic VTI tunnels
- Syslog

The Firewall Threat Defense can distribute the loopback address using dynamic routing protocols, or you can configure a static route on the peer device to reach the loopback IP address through one of the Firewall Threat Defense's physical interfaces. You cannot configure a static route on the Firewall Threat Defense that specifies the loopback interface.

関連トピック

ループバック インターフェイスのガイドラインと制限事項 （15 ページ）
ループバック インターフェイスの設定 （15 ページ）

ループバック インターフェイスのガイドラインと制限事項

Firewall Mode

- Supported in routed mode only.

High availability and Clustering

- No clustering support.

Additional Guidelines and Limitations

- TCP sequence randomization is always disabled for traffic from the physical interface to the loopback interface.

ループバック インターフェイスの設定

デバイスのループバック インターフェイスを追加するには、次の手順を実行します。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 [インターフェイスの追加（Add Interfaces）] ドロップダウンリストから、**[ループバックインターフェイス（Loopback Interface）]** を選択します。

ステップ 3 [一般（General）] タブで、次のパラメータを設定します。

a) [名前（Name）]：ループバック インターフェイスの名前を入力します。

b) [有効（Enabled）]：ループバック インターフェイスを有効にするには、このチェックボックスをオンにします。

c) [ループバック ID（Loopback ID）]：1 ～ 1024 のループバック ID を入力します。

d) [説明（Description）]：ループバック インターフェイスの説明を入力します。

ステップ 4 ルーテッド モード インターフェイスのパラメータを設定します。「ルーテッド モードのインターフェイスの設定 （47 ページ）」を参照してください。

ループバック インターフェイスへのトラフィックのレート制限

始める前に

システムに過剰な負荷がかからないように、ループバック インターフェイス IP アドレスに送信されるトラフィックのレートを制限する必要があります。グローバルサービスポリシーに接続制限ルールを追加できます。

手順

ステップ 1 ループバック インターフェイス IP アドレスへのトラフィックを識別する拡張アクセスリストを作成します。

a) **Objects** > **Object Management** > **Access List** > **Extended**を選択します。

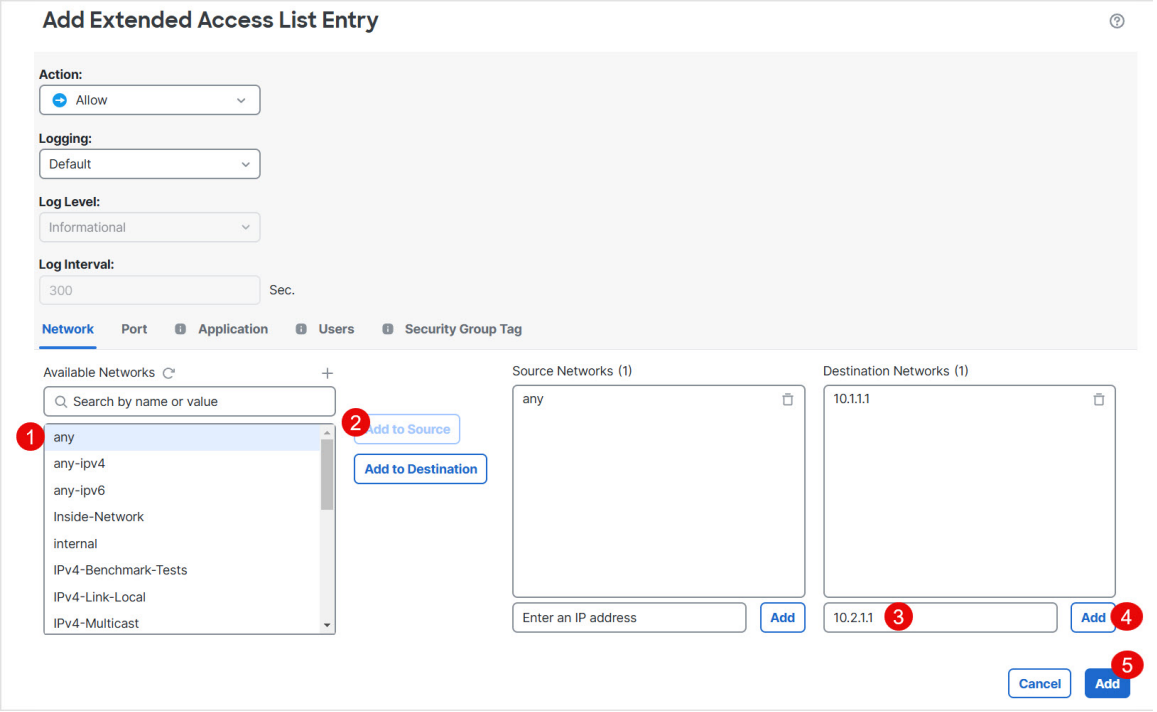
b) [拡張アクセスリストの追加（Add Extended Access List）] をクリックして、新しい ACL を作成します。

c) [新しい拡張アクセスリストオブジェクト（New Extended Access List Object）] ダイアログボックスで、ACL の名前を入力し（スペースは使用不可）、[追加（Add）] をクリックして新しいエントリを作成します。

図 *5: ACL* の命名とエントリの追加

d) [ネットワーク（Network）] タブで、送信元（任意）および宛先アドレス（ループバック IP アドレス）を設定します。

図 *6*：送信元と宛先のネットワーク

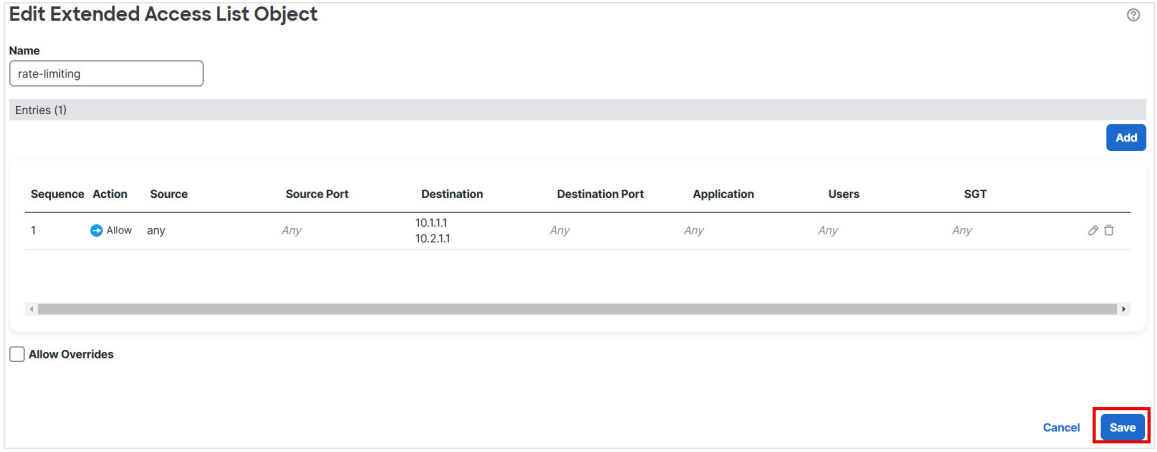


（注）
デフォルトの [アクション（Action）] は [許可（一致）（Allow (match)）] にし、その他の設定はそのままにします。

- [送信元（Source）]：[使用可能なネットワーク（Available Networks）] リストから **any** を選択し、[送信元に追加（Add to Source）] をクリックします。**any** の代わりに送信元 IP アドレスを指定して、このアクセスリストを絞り込むこともできます。
- [宛先（Destination）]：[宛先ネットワーク（Destination Networks）] リストの下の編集ボックスにアドレスを入力し、[追加（Add）] をクリックします。ループバックインターフェイスごとに手順を繰り返します。

e) [追加（Add）] をクリックして、エントリを ACL に追加します。
f) [保存（Save）] をクリックして、ACL を保存します。

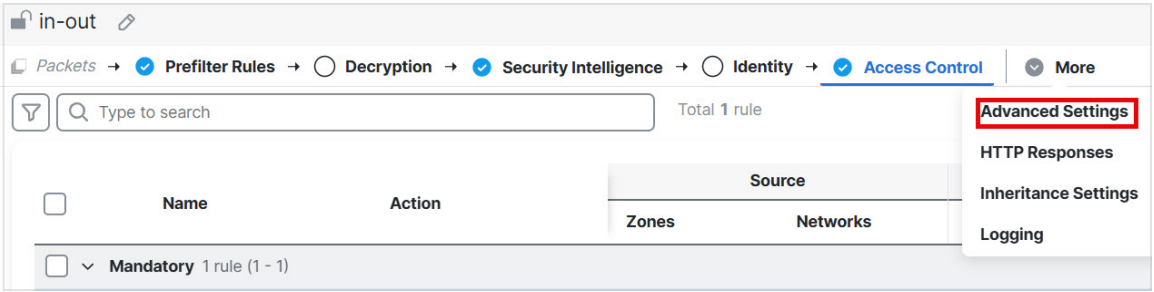
図 *7* : *ACL* の保存



ステップ 2 **Policies** > **Access Control heading** > **Access Control** を選択し、デバイスに割り当てられているアクセス コントロール ポリシーの **Edit** (✎)をクリックします。

ステップ 3 パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックします。

図 *8* : 詳細設定

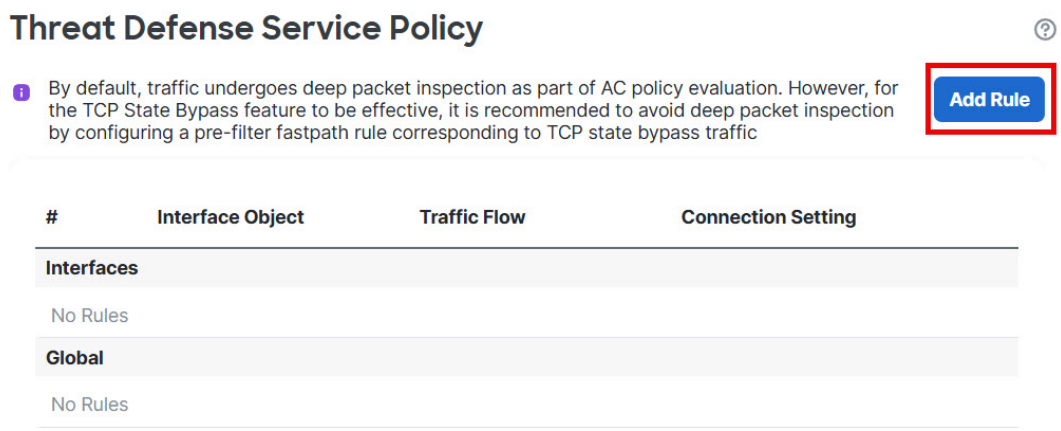


ステップ 4 [Threat Defenseサービスポリシー（Threat Defense Service Policy）] グループで **Edit** (✎) をクリックします。

図 *9* : *Threat Defense* サービス ポリシー

ステップ 5 [ルールの追加（Add Rule）] をクリックして、新しいルールを作成します。

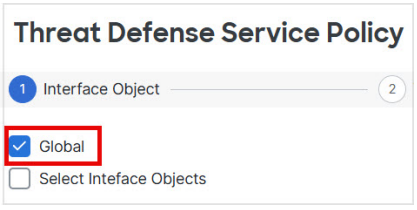
図 *10* : *[*ルールの追加（***Add Rule***）*]*



サービス ポリシー ルール ウィザードが開き、ルールの設定プロセスの手順が表示されます。

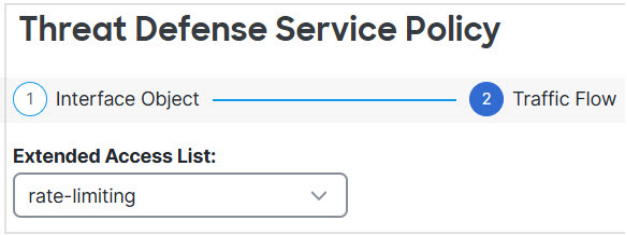
ステップ 6 [インターフェイス オブジェクト（Interface Object）] ステップで、[グローバル（Global）] をクリックしてすべてのインターフェイスに適用されるグローバルルールを作成し、[次へ（Next）] をクリックします。

図 *11* : グローバルポリシー



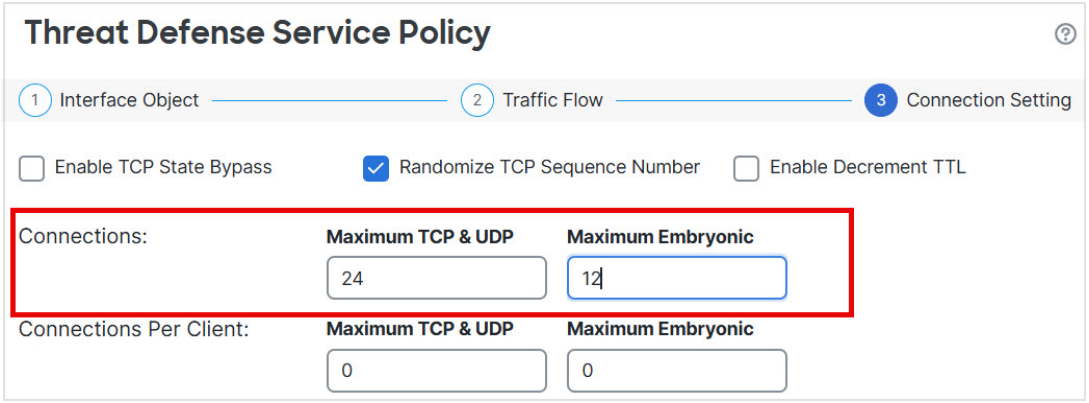
ステップ 7 [トラフィックフロー（Traffic Flow）] ステップで、ステップ 1 （16 ページ） で作成した拡張アクセスリストオブジェクトを選択し、[次へ（Next）] をクリックします。

図 *12* : 拡張アクセスリストの選択



ステップ 8 [接続設定（Connection Setting）] ステップで、[接続制限（Connections limit）] を設定します。

図 *13 :* 接続制限の設定



[最大TCPおよびUDP（Maximum TCP & UDP）] 接続数をループバック インターフェイスの予期される接続数に設定し、[最大初期接続数（Maximum Embryonic）] の接続数をそれよりも低い数に設定します。予期される必要なループバック インターフェイスセッション数に応じて、たとえば、5/2、10/5、または 1024/512 に設定できます。

初期接続制限を設定すると TCP 代行受信が有効になります。この代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃からシステムを保護します。

ステップ 9 [終了（Finish）] をクリックして変更を保存します。

ステップ 10 [OK] をクリックします。

ステップ 11 [詳細設定（Advanced Settings）] ウィンドウで [保存（Save）] をクリックします。

ステップ 12 これで、影響を受けるデバイスに変更を展開できます。

VLAN サブインターフェイスおよび 802.1Q トランキング

VLAN サブインターフェイスを使用すると、1 つの物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたはデバイスを追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。

VLAN サブインターフェイスのガイドラインと制限事項

モデルのサポート

- 1010/1210/1220：スイッチ ポートまたは VLAN インターフェイスの VLAN サブインターフェイスはサポートされていません。.

高可用性とクラスタリング

フェールオーバーリンクまたは状態リンクやクラスタ制御リンクのサブインターフェイスを使用することはできません。例外はマルチインスタンスモードの場合です。その場合、これらのリンクにはシャーシ定義サブインターフェイスを使用できます。

その他のガイドライン

- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、冗長インターフェイスペアのアクティブな物理インターフェイスと EtherChannel リンクにも当てはまります。サブインターフェイスでトラフィックを通過させるにはその物理、冗長、または EtherChannel インターフェイスを有効にする必要があるため、インターフェイスに名前を設定しないことで物理、冗長、または EtherChannel インターフェイスがトラフィックを通過させないようにします。物理インターフェイス、冗長インターフェイス、または EtherChannel インターフェイスでタグのないパケットを通過させる場合は、通常通り名前を設定できます。
- CLI で設定された専用の管理インターフェイスでも、マネージャアクセスに使用されるデータインターフェイスでも、管理インターフェイスにサブインターフェイスを設定することはできません。
- 同じ親インターフェイスのすべてのサブインターフェイスは、ブリッジグループメンバーかルーテッドインターフェイスのいずれかである必要があります。混在および一致はできません。
- Firewall Threat Defense はダイナミック トランキング プロトコル（DTP）をサポートしないため、接続されているスイッチポートを無条件にトランキングするように設定する必要があります。
- 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、Firewall Threat Defense で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、Firewall Threat Defense で特定のインスタンスでのトラフィックの中断を避けることができます。

（注） MAC アドレスを手動で割り当てる場合は、予期しない動作や停止を避けるために、同じ物理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 MAC アドレスを割り当てるようにしてください。

Maximum number of VLAN subinterfaces by device model

The device model limits the maximum number of VLAN subinterfaces that you can configure. Note that you can configure subinterfaces on data interfaces only, you cannot configure them on the management interface.

The following table explains the limits for each device model.

Model	Maximum VLAN Subinterfaces
Firepower 1010	60
Firepower 1120	512
Firepower 1140, 1150	1024
Secure Firewall 1200	1024
Secure Firewall 3100	1024
Secure Firewall 4200	1024
Firepower 4100	1024
Firepower 9300	1024
Firewall Threat Defense Virtual	50
ISA 3000	100

サブインターフェイスの追加

1 つ以上のサブインターフェイスを物理インターフェイス、冗長インターフェイス、または PortChannel インターフェイスに追加します。

Firepower 4100/9300 の場合、コンテナインターフェイスで使用するためのサブインターフェイスを FXOS で作成します。Add a VLAN Subinterface for Container Instancesを参照してください。これらのサブインターフェイスは Firewall Management Center のインターフェイスリストに表示されます。Firewall Management Center にサブインターフェイスを追加することもできますが、FXOS にサブインターフェイスが定義されていない親インターフェイス上に限ります。

（注） 親の物理インターフェイスがタグなしのパケットを渡します。タグなしのパケットを渡さない場合は、セキュリティ ポリシーの親インターフェイスが含まれていないことを確認します。

手順

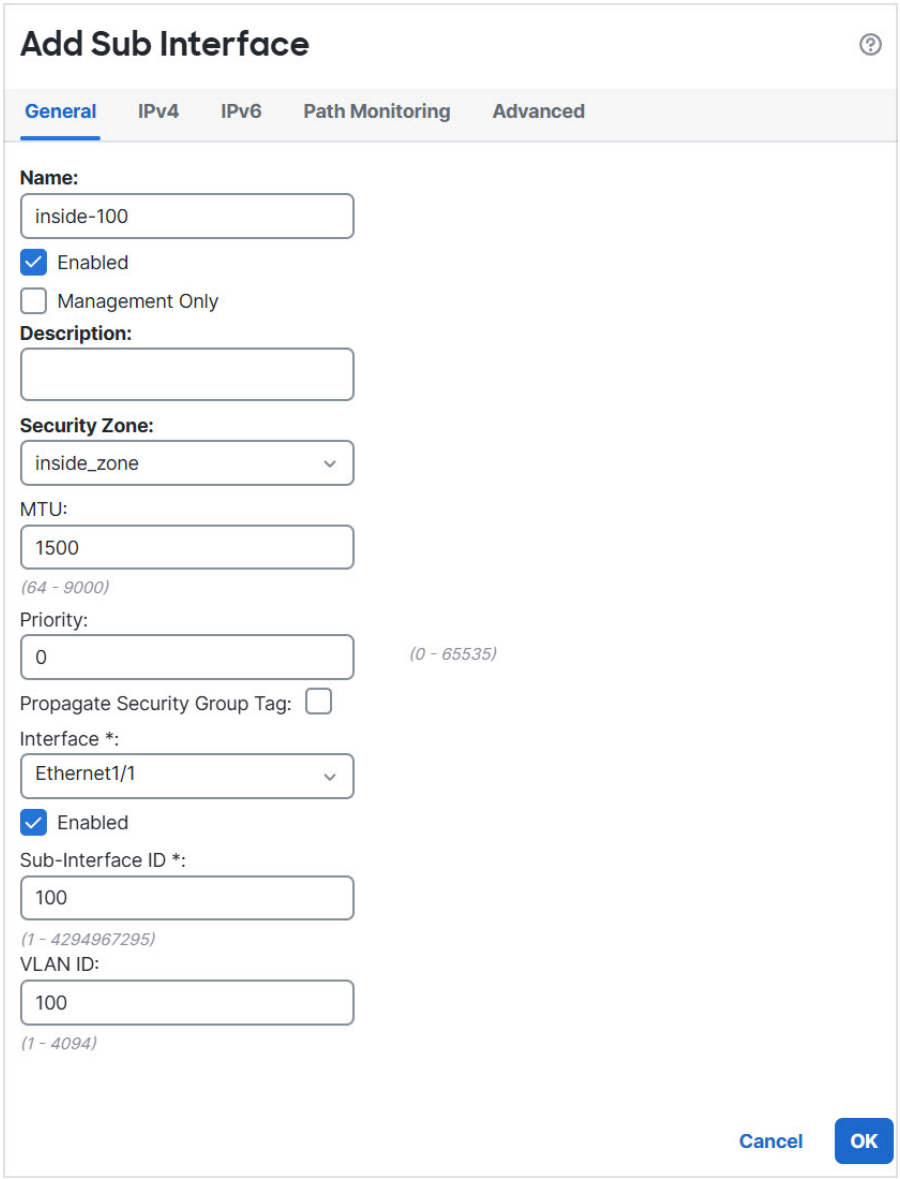
ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** ()] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 物理インターフェイスの有効化およびイーサネット設定の構成に従って、親インターフェイスを有効にします。

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

ステップ 4 [全般（General）] で、次のパラメータを設定します。

図 *14* : サブインターフェイスの追加



a) [インターフェイス（Interface）]：サブインターフェイスを追加する物理、冗長、またはポートチャネル インターフェイスを選択します。

b) [サブインターフェイス ID（Sub-Interface ID）]：サブインターフェイス ID を 1 ～ 4294967295 の範囲の整数で入力します。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。設定後は ID を変更できません。

c) [VLAN ID]：VLAN ID を 1 ～ 4094 の範囲で入力します。これは、このサブインターフェイス上のパケットにタグを付けるために使用されます。

この VLAN ID は一意である必要があります。 1010/1210/1220 の場合は、VLAN 1 を使用できません。VLAN 1 は、スイッチポートの論理的な VLAN インターフェイス用に予約されています。

ステップ 5 [OK] をクリックします。

ステップ 6 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

ステップ 7 ルーテッドまたはトランスペアレント モード インターフェイスのパラメータを設定します。ルーテッドモードのインターフェイスの設定（47 ページ）またはブリッジ グループ インターフェイスの設定 （53 ページ）を参照してください。

VXLAN インターフェイスの設定

この章では、仮想拡張 LAN（VXLAN） インターフェイスの設定方法について説明します。VXLAN インターフェイスは、レイヤ 2 ネットワークを拡張するために、レイヤ 3 物理ネットワーク上のレイヤ 2 仮想ネットワークとして機能します。

VXLAN インターフェイスについて

VXLAN は、VLAN の場合と同じイーサネットレイヤ 2 ネットワークサービスを提供しますが、より優れた拡張性と柔軟性を備えています。VLAN と比較して、VXLAN には次の利点があります。

- データセンター全体でのマルチテナントセグメントの柔軟な配置。
- より多くのレイヤ 2 セグメント（最大 1600 万の VXLAN セグメント）に対応するための高度なスケーラビリティ。

ここでは、VXLAN の動作について説明します。VXLAN の詳細については、RFC 7348 を参照してください。Geneve の詳細については、RFC 8926 を参照してください。

カプセル化

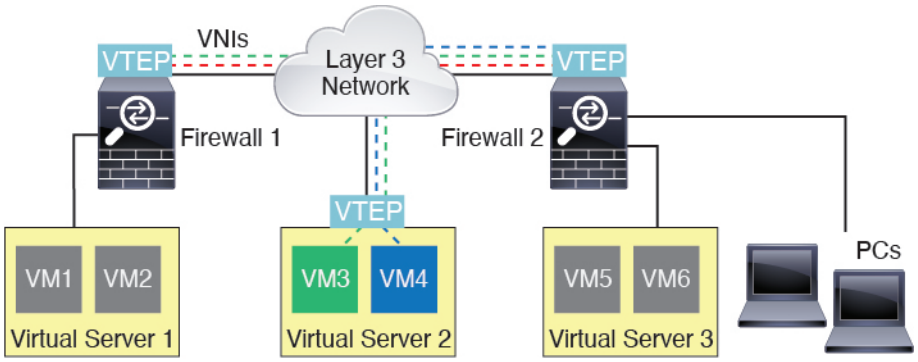
Firewall Threat Defense は、次の 2 種類の VXLAN カプセル化をサポートしています。

- VXLAN（すべてのモデル）：VXLAN は、MAC Address-in-User Datagram Protocol（MAC-in-UDP）のカプセル化を使用します。元のレイヤ 2 フレームに VXLAN ヘッダーが追加され、UDP-IP パケットに置かれます。
- Geneve（Firewall Threat Defense Virtual のみ）：Geneve には、MAC アドレスに限定されない柔軟な内部ヘッダーがあります。Geneve カプセル化は、Amazon Web Services（AWS）ゲートウェイロードバランサとアプライアンス間のパケットの透過的なルーティング、および追加情報の送信に必要です。

VXLAN トンネル エンドポイント

VXLAN トンネルエンドポイント（VTEP）デバイスは、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP には 2 つのインターフェイス タイプ（セキュリティ ポリシーを適用する VXLAN Network Identifier（VNI）インターフェイスと呼ばれる 1 つ以上の仮想インターフェイスと、 VTEP 間に VNI をトンネリングする VTEP 送信元インターフェイスと呼ばれる通常のインターフェイス）があります。VTEP 送信元インターフェイスは、VTEP 間通信のトランスポート IP ネットワークに接続されます。

次の図は、2 つの Firewall Threat Defense と、レイヤ 3 ネットワークを介して VTEP として機能し、サイト間の VNI 1、2、3 を拡張する仮想サーバ 2 を示します。Firewall Threat Defense は、VXLAN ネットワークと非 VXLAN ネットワーク間のブリッジまたはゲートウェイとして機能します。



VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。カプセル化されたパケットは、発信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてルーティングされます。VXLAN カプセル化の場合：宛先 IP アドレスは、リモート VTEP が不明な場合、マルチキャストグループにすることができます。Geneve では、Firewall Threat Defense はスタティックピアのみをサポートします。デフォルトでは、 VXLAN の宛先ポートは UDP ポート 4789 です（ユーザーが設定可能）。Geneve の宛先ポートは 6081 です。

VTEP 送信元インターフェイス

VTEP 送信元インターフェイスは、すべての VNI インターフェイスに関連付けられる通常のインターフェイス（物理、EtherChannel、または VLAN）です。Firewall Threat Defense Virtual ごとに 1 つの VTEP 送信元インターフェイスを設定できます。設定できる VTEP 送信元インターフェイスは 1 つだけであるため、VXLAN インターフェイスと Geneve インターフェイスの両方を同じデバイスに設定することはできません。AWS または Azure での Firewall Threat Defense Virtual クラスタリングには例外があり、2 つの VTEP ソースインターフェイスを使用することができます。VXLAN インターフェイスはクラスタ制御リンクに使用され、Geneve（AWS）または VXLAN（Azure）インターフェイスはゲートウェイロードバランサに使用できます。

VTEP 送信元インターフェイスは、VXLAN トラフィック専用にすることができますが、その使用に制限されません。必要に応じて、インターフェイスを通常のトラフィックに使用し、そのトラフィックのインターフェイスにセキュリティ ポリシーを適用できます。ただし、VXLAN

トラフィックの場合は、すべてのセキュリティポリシーを VNI インターフェイスに適用する必要があります。VTEP インターフェイスは、物理ポートとしてのみ機能します。

トランスペアレントファイアウォールモードでは、VTEP送信元インターフェイスは、BVIの一部ではないため、そのIPアドレスを設定しません。このインターフェイスは、管理インターフェイスが処理される方法に似ています。

VNI インターフェイス

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワーク トラフィックの分割を維持する仮想インターフェイスです。各VNI インターフェイスにセキュリティ ポリシーを直接適用します。

追加できる VTEP インターフェイスは 1 つだけで、すべての VNI インターフェイスは、同じ VTEP インターフェイスに関連付けられます。AWS または Azure での Firewall Threat Defense Virtual クラスタリングには例外があります。AWS クラスタリングの場合、2 つの VTEP ソースインターフェイスを使用することができます。VXLAN インターフェイスはクラスタ制御リンクに使用され、Geneve インターフェイスは AWS ゲートウェイロードバランサに使用できます。Azure クラスタリングの場合、2 つの VTEP ソースインターフェイスを使用することができます。VXLAN インターフェイスはクラスタ制御リンクに使用され、2 つ目の VXLAN インターフェイスは Azure ゲートウェイロードバランサに使用できます。

VXLAN パケット処理

VXLAN

VTEP 送信元インターフェイスを出入りするトラフィックは、VXLAN 処理、特にカプセル化または非カプセル化の対象となります。

カプセル化処理には、次のタスクが含まれます。

- VTEP送信元インターフェイスにより、VXLANヘッダーが含まれている内部MACフレームがカプセル化されます。
- UDP チェックサム フィールドがゼロに設定されます。
- 外部フレームの送信元 IP がVTEP インターフェイスの IP に設定されます。
- 外部フレームの宛先 IP がリモート VTEP IP ルックアップによって決定されます。

カプセル化解除については、次の場合に Firewall Threat Defense によって VXLAN パケットのみがカプセル化解除されます。

- これが、宛先ポートが 4789 に設定された UDP パケットである場合（この値はユーザー設定可能です）。
- 入力インターフェイスが VTEP 送信元インターフェイスである場合。
- 入力インターフェイスの IP アドレスが宛先 IP アドレスと同じになります。

- VXLAN パケット形式が標準に準拠します。

Geneve

VTEP送信元インターフェイスを出入りするトラフィックは、Geneve処理、特にカプセル化または非カプセル化の対象となります。

カプセル化処理には、次のタスクが含まれます。

- VTEP 送信元インターフェイスにより、Geneve ヘッダーが含まれている内部 MAC フレームがカプセル化されます。
- UDP チェックサム フィールドがゼロに設定されます。
- 外部フレームの送信元 IP がVTEP インターフェイスの IP に設定されます。
- 外部フレームの宛先 IP には、設定したピア IP アドレスが設定されます。

カプセル化解除：Firewall Threat Defense は次の場合に Geneve パケットのみをカプセル化解除します。

- これが、宛先ポートが 6081 に設定された UDP パケットである場合（この値はユーザー設定可能です）。
- 入力インターフェイスが VTEP 送信元インターフェイスである場合。
- 入力インターフェイスの IP アドレスが宛先 IP アドレスと同じになります。
- Geneve パケット形式が標準に準拠します。

ピア VTEP

Firewall Threat Defense がピア VTEP の背後にあるデバイスにパケットを送信する場合、Firewall Threat Defense には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

Firewall Threat Defense はVNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

VXLAN ピア

Firewall Threat Defense がこの情報を検出するには 2 つの方法あります。

- 単一のピア VTEP IP アドレスを Firewall Threat Defense に静的に設定できます。

  IPv4 の場合：Firewall Threat Defense が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンドノードの MAC アドレスを取得します。

IPv6 の場合：Firewall Threat Defense は IPv6 ネイバー要請メッセージを IPv6 要請ノード マルチキャストアドレスに送信します。ピア VTEP は、そのリンクローカルアドレスを使用して IPv6 ネイバー アドバタイズメント メッセージで応答します。

- ピア VTEP IP アドレスのグループを Firewall Threat Defense に静的に設定できます。

  IPv4 の場合：Firewall Threat Defense が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンドノードの MAC アドレスを取得します。

  IPv6 の場合：Firewall Threat Defense は IPv6 ネイバー要請メッセージを IPv6 要請ノード マルチキャストアドレスに送信します。ピア VTEP は、そのリンクローカルアドレスを使用して IPv6 ネイバー アドバタイズメント メッセージで応答します。

- マルチキャスト グループは、VNI インターフェイスごとに（または VTEP 全体に）設定できます。

  IPv4 の場合：Firewall Threat Defense は、IP マルチキャストパケット内の VXLAN カプセル化 ARP ブロードキャストパケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、Firewall Threat Defense はリモート VTEP の IP アドレスと、リモート エンド ノードの宛先 MAC アドレスの両方を取得することができます。

  IPv6 の場合：Firewall Threat Defense は、VTEP 送信元インターフェイスを経由してマルチキャストリスナー検出（MLD）レポートメッセージを送信し、Firewall Threat Defense が VTEP インターフェイスでマルチキャストアドレス トラフィックをリッスンしていることを示します。

  このオプションは、Geneve ではサポートされていません。

Geneve ピア

Firewall Threat Defense Virtual は、静的に定義されたピアのみをサポートします。AWS ゲートウェイロードバランサで Firewall Threat Defense Virtual ピアの IP アドレスを定義できます。Firewall Threat Defense Virtual はゲートウェイロードバランサへのトラフィックを開始しないため、Firewall Threat Defense Virtual でゲートウェイロードバランサの IP アドレスを指定する必要はありません。Geneve トラフィックを受信すると、ピア IP アドレスを学習します。マルチキャストグループは、Geneve ではサポートされていません。

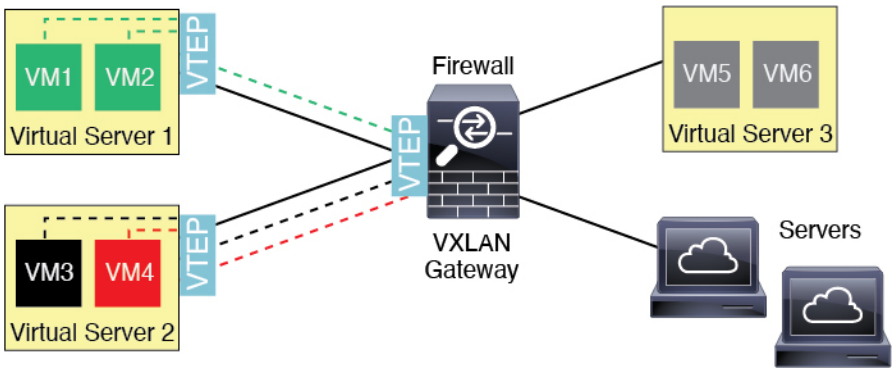
VXLAN 使用例

ここでは、Firewall Threat Defense での VXLAN の実装の使用例について説明します。

VXLAN ブリッジまたはゲートウェイの概要

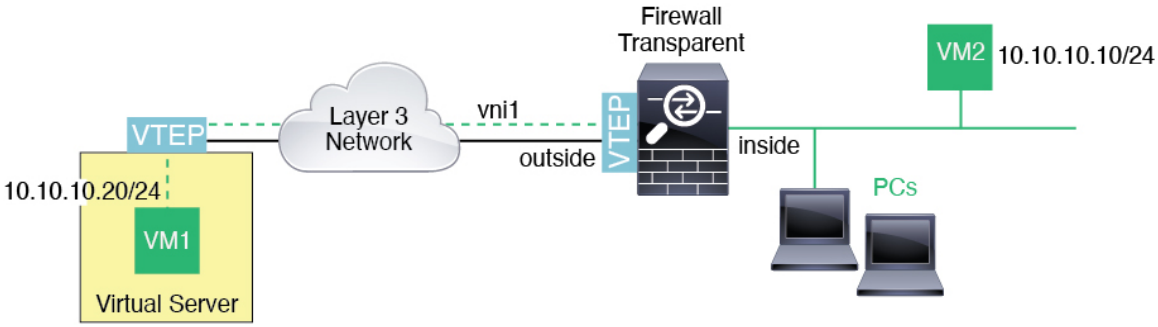
Each Firewall Threat Defense VTEP acts as a bridge or gateway between end nodes such as VMs, servers, and PCs and the VXLAN overlay network. For incoming frames received with VXLAN encapsulation over the VTEP source interface, the Firewall Threat Defense strips out the VXLAN header and forwards it to a physical interface connected to a non-VXLAN network based on the destination MAC address of the inner Ethernet frame.

The Firewall Threat Defense always processes VXLAN packets; it does not just forward VXLAN packets untouched between two other VTEPs.



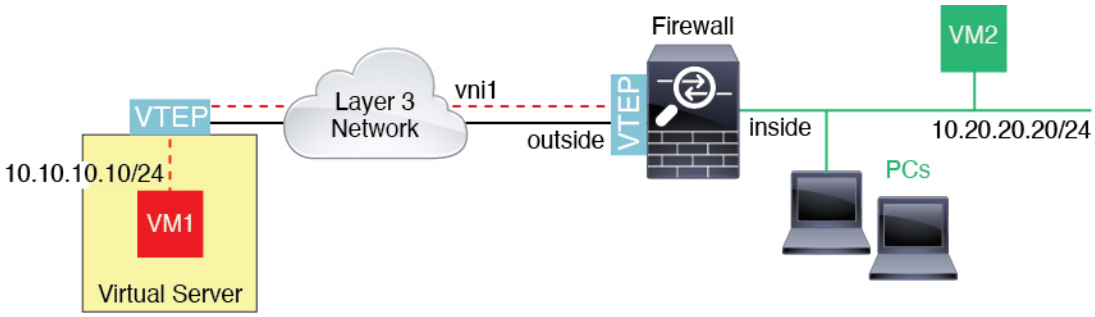
VXLAN ブリッジ

When you use a bridge group (transparent firewall mode, or optionally routed mode), the Firewall Threat Defense can serve as a VXLAN bridge between a (remote) VXLAN segment and a local segment where both are in the same network. In this case, one member of the bridge group is a regular interface while the other member is a VNI interface.



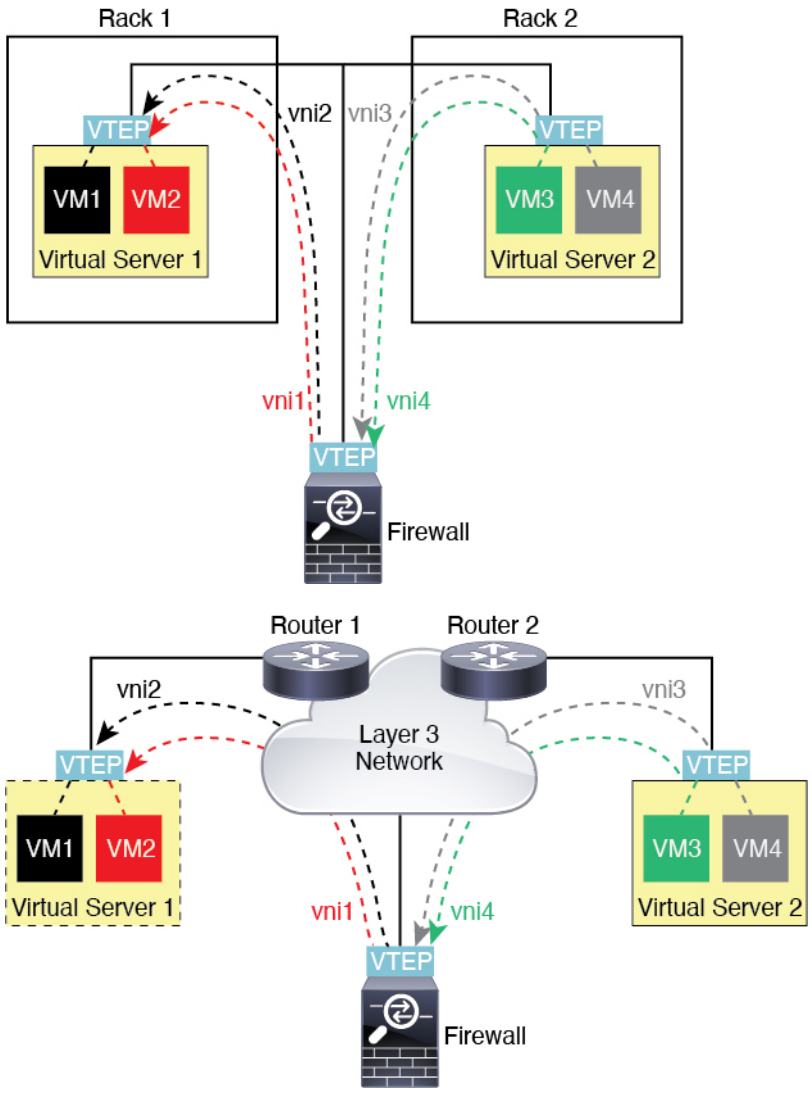
VXLAN ゲートウェイ（ルーテッド モード）

The Firewall Threat Defense can serve as a router between VXLAN and non-VXLAN domains, connecting devices on different networks.



VXLAN ドメイン間のルータ

With a VXLAN-stretched Layer 2 domain, a VM can point to an Firewall Threat Defense as its gateway while the Firewall Threat Defense is not on the same rack, or even when the Firewall Threat Defense is far away over the Layer 3 network.



See the following notes about this scenario:

1. For packets from VM3 to VM1, the destination MAC address is the Firewall Threat Defense MAC address, because the Firewall Threat Defense is the default gateway.
2. The VTEP source interface on Virtual Server 2 receives packets from VM3, then encapsulates the packets with VNI 3's VXLAN tag and sends them to the Firewall Threat Defense.
3. When the Firewall Threat Defense receives the packets, it decapsulates the packets to get the inner frames.
4. The Firewall Threat Defense uses the inner frames for route lookup, then finds that the destination is on VNI 2. If it does not already have a mapping for VM1, the Firewall Threat Defense sends an encapsulated ARP broadcast on the multicast group IP on VNI 2.

（注） The Firewall Threat Defense must use dynamic VTEP peer discovery because it has multiple VTEP peers in this scenario.

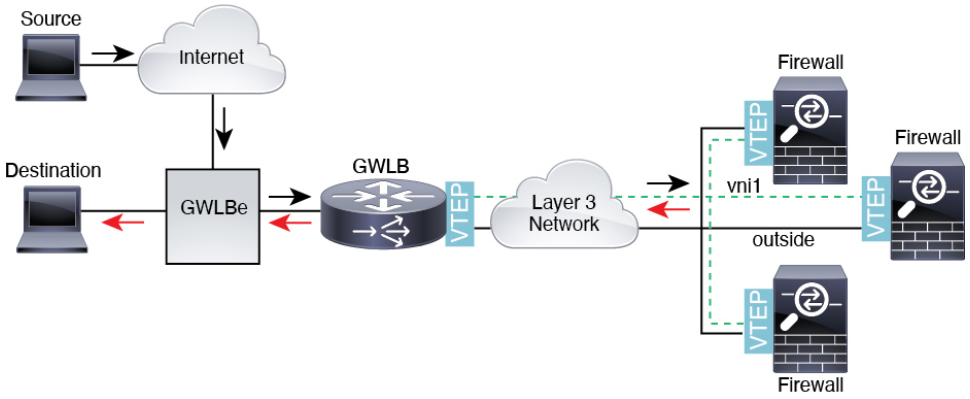
5. The Firewall Threat Defense encapsulates the packets again with the VXLAN tag for VNI 2 and sends the packets to Virtual Server 1. Before encapsulation, the Firewall Threat Defense changes the inner frame destination MAC address to be the MAC of VM1 (multicast-encapsulated ARP might be needed for the Firewall Threat Defense to learn the VM1 MAC address).
6. When Virtual Server 1 receives the VXLAN packets, it decapsulates the packets and delivers the inner frames to VM1.

Geneve シングルアームプロキシの使用例

（注） This use case is the only currently supported use case for Geneve interfaces.

The AWS Gateway Load Balancer combines a transparent network gateway and a load balancer that distributes traffic and scales virtual appliances on demand. The Firewall Threat Defense Virtual supports the Gateway Load Balancer centralized control plane with a distributed data plane (Gateway Load Balancer endpoint). The following figure shows traffic forwarded to the Gateway Load Balancer from the Gateway Load Balancer endpoint. The Gateway Load Balancer balances traffic among multiple Firewall Threat Defense Virtuals, which inspect the traffic before either dropping it or sending it back to the Gateway Load Balancer (U-turn traffic). The Gateway Load Balancer then sends the traffic back to the Gateway Load Balancer endpoint and to the destination.

図 *15 : Geneve Single-Arm Proxy*



AWS ゲートウェイロードバランサおよび Geneve デュアルアームプロキシ

（注） この使用例は、サポートされている Geneve インターフェイスの唯一の使用例です。

Firewall Threat Defense Virtual は、シングルアームまたはデュアルアームモードの分散データプレーン（ゲートウェイ ロード バランサ エンドポイント）を備えたゲートウェイロードバラン

サ集中型コントロールプレーンをサポートします。次の図は、GWLB および GWLB エンドポイントへのトラフィックホップを必要とせずに宛先（インターネット）に直接転送されるアウトバウンドトラフィック（Firewall Threat Defense Virtual によって検査されるトラフィック）を示しています。 Firewall Threat Defense Virtual はアウトバウンドトラフィックを検査し、NAT を実行してから、トラフィックをドロップするか、NAT ゲートウェイを介してインターネットに送り返します。デュアルアームプロキシは、マルチ VPC 展開に共通の出力パスを提供します。ファイアウォールは、複数の VPC からのアウトバウンドトラフィックを検査し、トラフィックは単一のポイントからインターネットに出るため、費用対効果の高いインフラストラクチャ ソリューションです。

図 *16 : Geneve* デュアルアームプロキシ：単一 *VPC* からの出力トラフィック

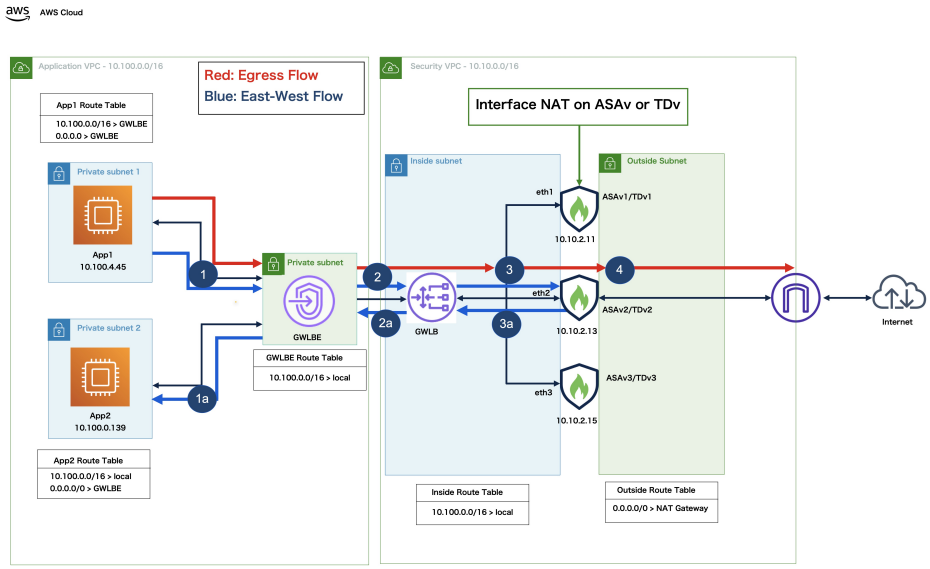
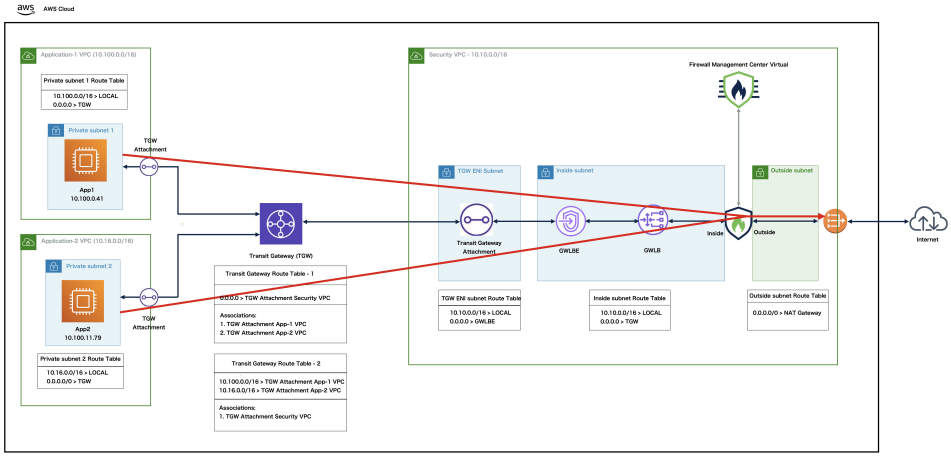


図 *17 : Geneve* デュアルアームプロキシ：複数の *VPC* からの出力トラフィック

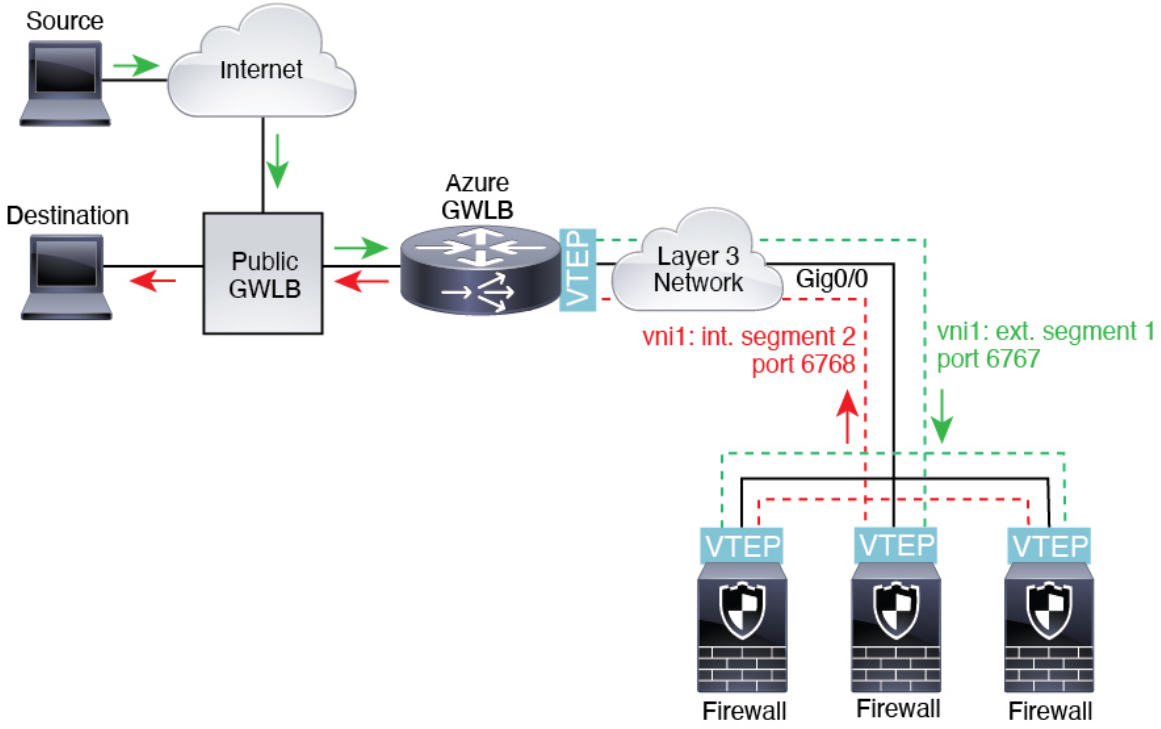


Azure ゲートウェイロードバランサおよびペアプロキシ

Azure サービスチェーンでは、Firewall Threat Defense Virtual がインターネットと顧客サービス間のパケットをインターセプトできる透過的なゲートウェイとして機能します。Firewall Threat Defense Virtual は、ペアリングされたプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。

次の図は、外部 VXLAN セグメント上のパブリックゲートウェイロードバランサから Azure ゲートウェイロードバランサに転送されるトラフィックを示しています。ゲートウェイロードバランサは、複数の Firewall Threat Defense Virtual の間でトラフィックのバランスをとり、トラフィックをドロップするか、外部 VXLAN セグメント上のゲートウェイロードバランサに送り返す前に検査します。Azure ゲートウェイロードバランサは、トラフィックをパブリックゲートウェイロードバランサと宛先に送り返します。

図 *18* : ペアリングされたプロキシを使用した *Azure Gateway* ロードバランサ



VXLAN インターフェイスの要件と前提条件

モデルの要件

- VXLAN カプセル化は、すべてのモデルでサポートされます。
- Geneve カプセル化は、次のモデルでサポートされます。
  - Amazon Web Services（AWS）の Firewall Threat Defense Virtual
- ペアプロキシモードの VXLAN は、次のモデルでサポートされています。
  - Azure の Firewall Threat Defense Virtual
- Firepower 1010 および Cisco Secure Firewall 1210/1220：スイッチポートおよび VLAN インターフェイスは、VTEP インターフェイスとしてサポートされていません。

VXLAN インターフェイスのガイドライン

ファイアウォール モード

- Geneve インターフェイスは、ルーテッド ファイアウォール モードでのみサポートされています。
- ペアプロキシの VXLAN インターフェイスは、ルーテッド ファイアウォール モードでのみサポートされています。

IPv6

- VNI インターフェイスは、IPv4 と IPv6 の両方のトラフィックをサポートします。
- VXLAN カプセル化の場合、VTEP 送信元インターフェイスは IPv4 と IPv6 の両方をサポートします。Firewall Threat Defense Virtual クラスタ制御リンクの VTEP 送信元インターフェイスは、IPv4 のみをサポートします。

  Geneve の場合、VTEP 送信元インターフェイスは IPv4 のみをサポートします。

クラスタ

- クラスタリングは、クラスタ制御リンク（Firewall Threat Defense Virtual のみ）を除いて、個別インターフェイスモードの VXLAN をサポートしていません。スパンド EtherChannel モードだけが VXLAN をサポートしています。

  GWLB で使用する追加の Geneve インターフェイスを使用できる AWS と、GWLB で使用する追加のペアプロキシの VXLAN インターフェイスを使用できる Azure の場合は例外です。

Routing

- VNI インターフェイスでは、スタティック ルーティングまたはポリシー ベース ルーティングのみをサポートします。ダイナミック ルーティング プロトコルはサポートされません。

[VPN]

VPN に VTEP 送信元インターフェイスを構成したり、VTI として使用したりすることはできません。

MTU

- VXLAN カプセル化：送信元インターフェイスの MTU が 1,554 バイト（IPv4 の場合）または 1,574 バイト（IPv6 の場合）未満の場合、Firewall Threat Defense は自動的に MTU を 1,554 バイトまたは 1,574 バイトに増やします。この場合、イーサネット データグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。他のデバイスが使用する MTU の方が大きい場合、送信元インターフェ

イス MTU を、ネットワーク MTU＋54 バイト（IPv4 の場合）または＋64 バイト（IPv6 の場合）に設定する必要があります。Firewall Threat Defense Virtual の場合、この MTU は、ジャンボフレーム予約を有効にするためにリスタートする必要があります。

- Geneve カプセル化：送信元インターフェイスの MTU が 1,806 バイト未満の場合、Firewall Threat Defense は自動的に MTU を 1,806 バイトに増やします。この場合、イーサネットデータグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。他のデバイスが使用する MTU の方が大きい場合、送信元インターフェイス MTU を、ネットワーク MTU＋306 バイトに設定する必要があります。この MTU は、ジャンボフレーム予約を有効にするためにリスタートする必要があります。

VXLAN または Geneve インターフェイスの設定

VXLAN または Geneve インターフェイスを設定できます。

VXLAN インターフェイスの設定

VXLAN を設定するには、次の手順を実行します。

（注） VXLAN または Geneve を設定できます（Firewall Threat Defense Virtual のみ）。Geneve インターフェイスについては、Geneve インターフェイスの設定 （40 ページ）を参照してください。

（注） Azure GWLB の場合、ARM テンプレートを使用して VM を展開するときに、VXLAN インターフェイスが設定されます。このセクションを使用して、設定を変更できます。

1. VTEP 送信元インターフェイスの設定 （37 ページ）。
2. VNI インターフェイスの設定 （39 ページ）。
3. （Azure GWLB）ゲートウェイロードバランサのヘルスチェックの許可 （42 ページ）。

VTEP 送信元インターフェイスの設定

Firewall Threat Defense デバイスごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント（NVE）として定義されます。VXLAN は、デフォルトのカプセル化タイプです。Azure のFirewall Threat Defense Virtual でのクラスタリングには例外があり、1 つの VTEP ソースインターフェイスをクラスタ制御リンクに使用し、2 つ目のソースインターフェイスを Azure GWLB に接続されたデータインターフェイスに使用できます。

手順

ステップ 1 ピア VTEP のグループを指定する場合は、ピア IP アドレスを持つネットワークオブジェクトを追加します。ネットワーク オブジェクトの作成 を参照してください。

ステップ 2 **Devices** > **Device Management**を選択します。

ステップ 3 VXLAN を設定するデバイスの横にある **Edit** (✎) をクリックします。

ステップ 4 （任意） 送信元インターフェイスが NVE 専用であることを指定します。

ルーテッドモードでは、この設定はオプションです。設定した場合、トラフィックはこのインターフェイスの VXLAN および共通の管理トラフィックのみに制限されます。トランスペアレント ファイアウォール モードでは、この設定は自動的に有効になります。

a) [インターフェイス（Interfaces）] をクリックします。
b) VTEP 送信元インターフェイスの **Edit** (✎) をクリックします。
c) [全般（General）] ページで、[NVEのみ（NVE Only）] チェックボックスをオンにします。

ステップ 5 まだ表示されていない場合は、[VTEP] をクリックします。

ステップ 6 [NVEの有効化（Enable NVE）] をオンにします。

ステップ 7 [VTEPの追加（Add VTEP）] をクリックします。

ステップ 8 [カプセル化タイプ（Encapsulation Type）] で、[VxLAN] を選択します。

AWS の場合、[VxLAN] と [Geneve] のどちらかを選択できます。他のプラットフォームでは、[VxLAN] が自動的に選択されます。

ステップ 9 [カプセル化ポート（Encapsulation port）] に指定された範囲内で値を入力します。

デフォルト値は 4789 です。

ステップ 10 [VTEP送信元インターフェイス（VTEP Source Interface）] を選択します。

デバイス上にある使用可能な物理インターフェイスのリストから選択します。送信元インターフェイスの MTU が 1554 バイト（IPv4 の場合）または 1574 バイト（IPv6 の場合）未満の場合、Firewall Management Center は自動的に MTU を 1554 バイトまたは 1574 バイトに増やします。

ステップ 11 [ネイバーアドレス（Neighbor Address）] を選択します。次のオプションを使用できます。

- [なし（None）] : ネイバーアドレスを指定しません。
- [ピアVTEP（Peer VTEP）] : ピア VTP アドレスを指定します。
- [ピアグループ（Peer Group ）] : ピア IP アドレスを持つネットワークオブジェクトを指定します。
- [デフォルトマルチキャスト（Default Multicast）] : 関連するすべての VNI インターフェイスのデフォルト マルチキャスト グループを指定します。VNI インターフェイスごとにマルチキャスト グループを設定していない場合は、このグループが使用されます。その VNI

インターフェイス レベルでグループを設定している場合は、そのグループがこの設定よりも優先されます。

ステップ 12 [OK] をクリックします。

ステップ 13 **[保存（Save）]** をクリックします。

ステップ 14 ルーテッドインターフェイスのパラメータを設定します。「ルーテッドモードのインターフェイスの設定」を参照してください。

VNI インターフェイスの設定

VNI インターフェイスを追加してそれを VTEP 送信元インターフェイスに関連付けて、基本インターフェイス パラメータを設定します。

Azure Firewall Threat Defense Virtual の場合、通常の VXLAN インターフェイスを設定するか、Azure GWLB で使用するペアプロキシモードの VXLAN インターフェイスを設定できます。ペアプロキシモードは、クラスタリングでサポートされる唯一のモードです。

手順

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

ステップ 2 VXLAN を設定するデバイスの横にある **Edit** (✎) をクリックします。

ステップ 3 [インターフェイス（Interfaces）] をクリックします。

ステップ 4 [インターフェイスの追加（Add Interfaces）] をクリックし、[VNIインターフェイス（VNI Interface）] を選択します。

ステップ 5 [名前（Name）] と [説明（Description）] にインターフェイスの名前と説明をそれぞれ入力します。.

ステップ 6 [セキュリティゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティゾーンを追加します。

ステップ 7 指定された範囲内で、[優先度（Priority）] フィールドの値を入力します。デフォルトでは、0 が選択されています。

ステップ 8 [VNI ID] には 1 ～ 10000 の間で値を入力します。

この ID は内部インターフェイス識別子です。

ステップ 9 （Azure GWLB のペアプロキシ VXLAN）プロキシペアモードを有効にして、必要なパラメータを設定します。

a) **プロキシのペアリング**を確認します。
b) **内部ポート**を 1024 ～ 65535 に設定します。
c) **内部セグメント ID** を 1 ～ 16777215 の範囲で設定します。
d) **外部ポート**を 1024 ～ 65535 に設定します。
e) **外部セグメント ID** を 1 ～ 16777215 の範囲で設定します。

ステップ 10 （通常の VXLAN）**[VNIセグメントID（VNI Segment ID）]** には 1 ～ 16777215 の間の値を入力します。

セグメント ID は VXLAN タギングに使用されます。

ステップ 11 [マルチキャストグループアドレス（Multicast Group IP Address）] を入力します。

VNI インターフェイスに対してマルチキャスト グループを設定しない場合は、VTEP 送信元インターフェイス設定のデフォルト グループが使用されます（使用可能な場合）。VTEP 送信元インターフェイスに対して手動でVTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャスト グループを指定することはできません。

ステップ 12 [VTEPインターフェイスにマッピングされているNVE（NVE Mapped to VTEP Interface）] をオンにします。

このオプションにより、インターフェイスが VTEP 送信元インターフェイスに関連付けられます。

ステップ 13 [OK] をクリックします。

ステップ 14 [保存（Save）] をクリックして、インターフェイス設定を保存します。

ステップ 15 ルーテッドまたはトランスペアレント インターフェイスのパラメータを設定します。「ルーテッド モードとトランス ペアレント モードのインターフェイスの設定 （43 ページ）」を参照してください。

Geneve インターフェイスの設定

Firewall Threat Defense Virtual の Geneve インターフェイスを設定するには、次の手順を実行します。

（注） VXLAN または Geneve を設定できます。VXLAN インターフェイスの詳細については、「VXLAN インターフェイスの設定 （37 ページ）」を参照してください。

1. VTEP 送信元インターフェイスの設定 （40 ページ）。
2. VNI の設定 （41 ページ）。
3. ゲートウェイロードバランサのヘルスチェックの許可 （42 ページ）。

VTEP 送信元インターフェイスの設定

Firewall Threat Defense Virtual デバイスごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント（NVE）として定義されます。。

手順

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

ステップ 2 Geneve を設定するデバイスの横にある **Edit** (✎) をクリックします。

ステップ 3 [VTEP] をクリックします。

ステップ 4 [NVEの有効化（Enable NVE）] をオンにします。

ステップ 5 [VTEPの追加（Add VTEP）] をクリックします。

ステップ 6 [カプセル化タイプ（Encapsulation Type）] で、[Geneve] を選択します。

ステップ 7 [カプセル化ポート（Encapsulation port）] に指定された範囲内で値を入力します。

[Geneveポート（Geneve Port）] を変更することは推奨しません。AWS にはポート 6081 が必要です。

ステップ 8 [VTEP送信元インターフェイス（VTEP Source Interface）] を選択します。

デバイス上にある使用可能な物理インターフェイスのリストから選択できます。送信元インターフェイスの MTU が 1806 バイト未満の場合、Firewall Management Center は自動的に MTU を 1806 バイトに増やします。

ステップ 9 [OK] をクリックします。

ステップ 10 **[保存（Save）]** をクリックします。

ステップ 11 ルーテッドインターフェイスのパラメータを設定します。「ルーテッドモードのインターフェイスの設定」を参照してください。

VNI の設定

VNI を追加し、その VNI を（VTEP）送信元インターフェイスに関連付けて、基本インターフェイスパラメータを設定します。

手順

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

ステップ 2 Geneve を設定するデバイスの横にある **Edit** (✎) をクリックします。

ステップ 3 [インターフェイス（Interfaces）] をクリックします。

ステップ 4 [インターフェイスの追加（Add Interfaces）] をクリックし、[VNIインターフェイス（VNI Interface）] を選択します。

ステップ 5 [名前（Name）] フィールドと [説明（Description）] フィールドに、関連情報を入力します。

ステップ 6 [VNI ID] フィールドには 1 ～ 10000 の値を入力します。

（注）
この ID は内部インターフェイス識別子です。

ステップ 7 [プロキシの有効化（Enable Proxy] チェックボックスをオンにします。

（注）
デバイスの VNI インターフェイスで AWS プロキシが有効になっている場合、NAT の設定は許可されません。

このオプションにより、シングルアーム プロキシ モードまたはデュアルアーム プロキシ モードが有効になります。シングルアーム プロキシ モードでは、トラフィックは入ったときと同じインターフェイスから出る（U ターントラフィック）ことができますが、デュアルアーム プロキシ モードでは、仮想デバイスが、検査されたトラフィックの NAT を実行し、その後にアウトバウンドトラフィックをインターネットに直接転送でき、トラフィックを GWLB および GWLB エンドポイントに返す必要がありません。後でインターフェイスを編集する場合は、シングルアーム プロキシ モードまたはデュアルアーム プロキシ モードを無効にできません。無効にするには、既存のインターフェイスを削除して、新しい VNI を作成する必要があります。

このオプションは、Geneve VTEP でのみ使用できます。

ステップ 8 [プロキシタイプ（Proxy type）] ドロップダウンリストから、インターフェイスに対して有効にするプロキシモードを選択します。インターフェイスのプロキシモードを指定しない場合、デフォルトではシングルアーム プロキシ モードが考慮されます。

ステップ 9 [VTEPインターフェイスにマッピングされているNVE（NVE Mapped to VTEP Interface）] を選択します。

このオプションにより、インターフェイスが VTEP 送信元インターフェイスに関連付けられます。

ステップ 10 [OK] をクリックします。

ステップ 11 **[保存（Save）]** をクリックします。

次のタスク

ルーテッドインターフェイスのパラメータを設定します。「ルーテッドモードのインターフェイスの設定」を参照してください。

ゲートウェイロードバランサのヘルスチェックの許可

AWS または Azure GWLB では、アプライアンスがヘルスチェックに正しく応答する必要があります。GWLBは、正常と見なされるアプライアンスにのみトラフィックを送信します。SSH、HTTP、または HTTPS のヘルスチェックに応答するように Firewall Threat Defense Virtual を設定する必要があります。

次のいずれかの方法を設定します。

手順

ステップ 1 SSH を設定します。「セキュアシェルの設定」を参照してください。

GWLB IP アドレスからの SSH を許可します。GWLB は、Firewall Threat Defense Virtual への接続の確立を試行し、ログインの Firewall Threat Defense Virtual のプロンプトが正常性の証拠として取得されます。SSH ログインの試行は 1 分後にタイムアウトします。このタイムアウトに対応するには、GWLB でより長いヘルスチェック間隔を設定する必要があります。

ステップ 2 ポート変換機能を備えたスタティック インターフェイス NAT を使用した HTTP(S) リダイレクトの設定

ヘルスチェックをメタデータ HTTP(S) サーバーにリダイレクトするように Firewall Threat Defense Virtual を設定できます。HTTP（S）ヘルスチェックの場合、HTTP（S）サーバーは 200 ー 399 の範囲のステータスコードで GWLB に応答する必要があります。Firewall Threat Defense Virtual では同時管理接続の数に制限があるため、ヘルスチェックを外部サーバーにオフロードすることもできます。

ポート変換を設定したスタティック インターフェイス NAT を使用すると、ポート（ポート 80 など）への接続を別の IP アドレスにリダイレクトできます。たとえば、Firewall Threat Defense Virtual 外部インターフェイスの宛先を持つ GWLB からの HTTP パケットを、HTTP サーバーの宛先を持つ Firewall Threat Defense Virtual 外部インターフェイスからのように変換します。次に Firewall Threat Defense Virtual はパケットをマッピングされた宛先アドレスに転送します。HTTP サーバーは Firewall Threat Defense Virtual 外部インターフェイスに応答し、Firewall Threat Defense Virtual は GWLB に応答を転送します。GWLB から HTTP サーバーへのトラフィックを許可するアクセスルールが必要です。

a) GWLB ネットワークから送られた外部インターフェイスの HTTP(S) トラフィックをアクセスルールで許可します。アクセス コントロール ルール を参照してください。
b) HTTP(S) の場合、送信元 GWLB の IP アドレスを Firewall Threat Defense Virtual 外部インターフェイスの IP アドレスに変換します。次に、外部インターフェイスの IP アドレスの宛先を HTTP(S) サーバーの IP アドレスに変換します。「静的手動 NAT の構成」を参照してください。

ルーテッド モードとトランス ペアレント モードのインターフェイスの設定

この項では、ルーテッド ファイアウォール モードおよびトランスペアレント ファイアウォール モードで、すべてのモデルに対応する標準のインターフェイス設定を完了するためのタスクについて説明します。

ルーテッド モード インターフェイスとトランスペアレント モード インターフェイスについて

ファイアウォール モードのインターフェイスでは、トラフィックが、フローの維持、IP レイヤおよび TCP レイヤの両方でのフロー状態の追跡、IP 最適化、TCP の正規化などのファイアウォール機能の対象となります。オプションで、セキュリティ ポリシーに従ってこのトラフィックに IPS 機能を設定することもできます。

設定できるファイアウォール インターフェイスのタイプは、ルーテッド モードとトランスペアレント モードのどちらのファイアウォール モードがそのデバイスに設定されているかによって異なります。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。

- ルーテッド モード インターフェイス（ルーテッド ファイアウォール モードのみ）：ルーティングを行う各インターフェイスは異なるサブネット上にあります。
- ブリッジグループ インターフェイス（ルーテッドおよびトランスペアレント ファイアウォール モード）：複数のインターフェイスをネットワーク上でグループ化することができ、Firepower Threat Defense デバイスはブリッジング技術を使用してインターフェイス間のトラフィックを通過させることができます。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。ルーテッド モードでは、Firepower Threat Defense デバイスは BVI と通常のルーテッド インターフェイス間をルーティングします。トランスペアレント モードでは、各ブリッジグループは分離されていて、相互通信できません。

Dual IP Stack (IPv4 and IPv6)

The Firewall Threat Defense device supports both IPv6 and IPv4 addresses on an interface. Make sure you configure a default route for both IPv4 and IPv6.

31-Bit Subnet Mask

For routed interfaces, you can configure an IP address on a 31-bit subnet for point-to-point connections. The 31-bit subnet includes only 2 addresses; normally, the first and last address in the subnet is reserved for the network and broadcast, so a 2-address subnet is not usable. However, if you have a point-to-point connection and do not need network or broadcast addresses, a 31-bit subnet is a useful way to preserve addresses in IPv4. For example, the failover link between 2 Firewall Threat Defenses only requires 2 addresses; any packet that is transmitted by one end of the link is always received by the other, and broadcasting is unnecessary. You can also have a directly-connected management station running SNMP or Syslog.

31-Bit Subnet and Clustering

You can use a 31-bit subnet mask for cluster interfaces, excluding the management interface and the Cluster Control Link.

31-Bit Subnet and Failover

For failover, when you use a 31-bit subnet for the Firewall Threat Defense interface IP address, you cannot configure a standby IP address for the interface because there are not enough addresses. Normally, an

interface for failover should have a standby IP address so the active unit can perform interface tests to ensure standby interface health. Without a standby IP address, the Firewall Threat Defense cannot perform any network tests; only the link state can be tracked.

For the failover and optional separate state link, which are point-to-point connections, you can also use a 31-bit subnet.

31-Bit Subnet and Management

If you have a directly-connected management station, you can use a point-to-point connection for SSH or HTTP on the Firewall Threat Defense, or for SNMP or Syslog on the management station.

31-Bit Subnet Unsupported Features

The following features do not support the 31-Bit subnet:

- BVI interfaces for bridge groups—The bridge group requires at least 3 host addresses: the BVI, and two hosts connected to two bridge group member interfaces. you must use a /29 subnet or smaller.
- Multicast Routing

Guidelines and Limitations for Routed and Transparent Mode Interfaces

High availability, Clustering, and Multi-Instance

- Do not configure failover links with the procedures in this chapter. See the High availability chapter for more information.
- For cluster interfaces, see the clustering chapter for requirements.
- For multi-instance mode, shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode).
- When you use High availability, you must set the IP address and standby address for data interfaces manually; DHCP and PPPoE are not supported. Set the standby IP addresses on the **Devices** > **Device Management** > **High Availability** tab in the **Monitored Interfaces** area. See the High availability chapter for more information.

IPv6

- IPv6 is supported on all interfaces.
- You can only configure IPv6 addresses manually in transparent mode.
- The Firewall Threat Defense device does not support IPv6 anycast addresses.
- DHCPv6 and prefix delegation options are not supported with transparent mode, clustering, or High availability.

Model Guidelines

- For the Firewall Threat Defense Virtual on VMware with bridged ixgbevf interfaces, bridge groups are not supported.

Transparent Mode and Bridge Group Guidelines

- You can create up to 250 bridge groups, with 64 interfaces per bridge group.
- Each directly-connected network must be on the same subnet.
- The Firewall Threat Defense device does not support traffic on secondary networks; only traffic on the same network as the BVI IP address is supported.
- An IP address for the BVI is required for each bridge group for to-the-device and from-the-device management traffic, as well as for data traffic to pass through the Firewall Threat Defense device. For IPv4 traffic, specify an IPv4 address. For IPv6 traffic, specify an IPv6 address.
- You can only configure IPv6 addresses manually.
- The BVI IP address must be on the same subnet as the connected network. You cannot set the subnet to a host subnet (255.255.255.255).
- Management interfaces are not supported as bridge group members.
- For multi-instance mode, shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode).
- For the Firewall Threat Defense Virtual on VMware with bridged ixgbevf interfaces, transparent mode is not supported, and bridge groups are not supported in routed mode.
- For the / 1010/ 1210// 1220, you cannot mix logical VLAN interfaces and physical firewall interfaces in the same bridge group.
- For the Firepower 4100/9300, data-sharing interfaces are not supported as bridge group members.
- In transparent mode, you must use at least 1 bridge group; data interfaces must belong to a bridge group.
- In transparent mode, do not specify the BVI IP address as the default gateway for connected devices; devices need to specify the router on the other side of the Firewall Threat Defense as the default gateway.
- In transparent mode, the *default* route, which is required to provide a return path for management traffic, is only applied to management traffic from one bridge group network. This is because the default route specifies an interface in the bridge group as well as the router IP address on the bridge group network, and you can only define one default route. If you have management traffic from more than one bridge group network, you need to specify a regular static route that identifies the network from which you expect management traffic.
- Transparent mode is not supported on threat defense virtual instances deployed on Amazon Web Services, Microsoft Azure, Google Cloud Platform, and Oracle Cloud Infrastructure.
- In routed mode, to route between bridge groups and other routed interfaces, you must name the BVI.
- In routed mode, Firewall Threat Defense-defined EtherChannel interfaces are not supported as bridge group members. EtherChannels on the Firepower 4100/9300 can be bridge group members.
- Bidirectional Forwarding Detection (BFD) echo packets are not allowed through the Firewall Threat Defense when using bridge group members. If there are two neighbors on either side of the Firewall Threat Defense running BFD, then the Firewall Threat Defense will drop BFD echo packets because they have the same source and destination IP address and appear to be part of a LAND attack.

Additional Guidelines and Requirements

- The Firewall Threat Defense supports only one 802.1Q header in a packet and does not support multiple headers (known as Q-in-Q support) for firewall interfaces.**Note:** For inline sets and passive interfaces, the FTD supports Q-in-Q up to two 802.1Q headers in a packet, with the exception of the Firepower 4100/9300, which only supports one 802.1Q header.
- Interface problems, such as frequent up/down status changes, can prevent the floating connection timer from applying correctly to the connections going through the interface. If you have problems with an interface's status, consider clearing all connections after the status becomes stable to clear invalid connections.

ルーテッド モードのインターフェイスの設定

この手順では、名前、セキュリティ ゾーン、および IPv4 アドレスを設定する方法について説明します。

（注） すべてのインターフェイスタイプですべてのフィールドがサポートされているわけではありません。

始める前に

- **Firepower 4100/9300**
  1. Configure a Physical Interface
  2. （任意）特別なインターフェイスを設定します。
     - Add an EtherChannel (Port Channel)
     - Add a VLAN Subinterface for Container Instances FXOS で次を実行します。
     - ループバック インターフェイスの設定 （15 ページ）
     - Firewall Management Center でのサブインターフェイスの追加 （22 ページ）
     - VXLAN インターフェイスの設定 （37 ページ）

- （任意）**他のすべてのモデル**：
  - EtherChannel の設定
  - ループバック インターフェイスの設定 （15 ページ）
  - サブインターフェイスの追加 （22 ページ）
  - VXLAN インターフェイスの設定 （37 ページ）
  - AWS 上の Firewall Threat Defense Virtual：Geneve インターフェイスの設定 （40 ページ）

- Firepower 1010 および Cisco Secure Firewall 1210/1220：VLAN インターフェイスを構成する （5 ページ）

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

ステップ 3 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

この名前を「cluster」という語句で始めることはできません。その名前は内部で使用するために予約されています。

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 （任意） このインターフェイスを [管理専用（Management Only）] に設定してトラフィックを管理トラフィックに制限します。through-the-box トラフィックは許可されていません。

ステップ 6 （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 7 [モード（Mode）] ドロップダウン リストで、[なし（None）] を選択します。

通常のファイアウォール インターフェイスのモードは [なし（None）] に設定されています。他のモードは IPS 専用インターフェイス タイプ向けです。

ステップ 8 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ルーテッド インターフェイスは、ルーテッド タイプ インターフェイスであり、ルーテッド タイプのゾーンにのみ属することができます。

ステップ 9 **MTU** についてはMTU の設定 （77 ページ）を参照してください。

ステップ 10 [優先度（Priority）] フィールドに、0 ～ 65535 の範囲の数値を入力します。

この値は、ポリシーベースのルーティング構成で使用されます。優先度は、複数の出力インターフェイス間でトラフィックをルーティングする方法を決定するために使用されます。詳細については、「ポリシーベース ルーティング ポリシーの設定」を参照してください。

ステップ 11 [IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ（IP Type）] ドロップダウン リストにある次のオプションのいずれかを使用します。

高可用性、クラスタリング、およびループバック インターフェイスは、静的 IP アドレス構成のみをサポートします。DHCP および PPPoE はサポートされていません。

- [静的 IP を使用する（Use Static IP）]：IP アドレスおよびサブネット マスクを入力します。ポイントツーポイント接続の場合、31 ビットのサブネットマスク（255.255.255.254 または /31）を指定できます。この場合、ネットワークまたはブロードキャスト アドレス用の IP

アドレスは予約されません。この場合、スタンバイ IP アドレスを設定できません。高可用性の場合は、静的 IP アドレスのみを使用できます。**Devices** > **Device Management** ページでスタンバイ IP アドレスを設定し、**[監視対象インターフェイス（Monitored Interfaces）]** 領域で、**[高可用性（HA）（High Availability）]** をクリックします。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニターできず、リンク ステートをトラックすることしかできません。

- [DHCP の使用（Use DHCP）]：次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバーからデフォルト ルートを取得します。
  - [DHCPルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。
- [PPPoE を使用（Use PPPoE）]：インターフェイスが DSL、ケーブル モデム、またはその他の手段で ISP に接続されていて、ISP が PPPoE を使用して IP アドレスを割り当てる場合は、次のパラメータを設定します。
  - [VPDN グループ名（VPDN Group Name）]：この接続を表すために選択するグループ名を指定します。
  - [PPPoE ユーザ名（PPPoE User Name）]：ISP によって提供されたユーザ名を指定します。
  - [PPPoE パスワード/パスワードの確認（PPPoE Password/Confirm Password）]：ISP によって提供されたパスワードを指定し、確認します。
  - [PPP 認証（PPP Authentication）]：[PAP]、[CHAP]、または [MSCHAP] を選択します。

    PAP は認証時にクリアテキストのユーザ名とパスワードを渡すため、セキュアではありません。CHAP では、サーバのチャレンジに対して、クライアントは暗号化された「チャレンジとパスワード」およびクリアテキストのユーザ名を返します。CHAP は PAP よりセキュアですが、データを暗号化しません。MSCHAP は CHAP に似ていますが、サーバが CHAP のようにクリア テキスト パスワードを扱わず、暗号化されたパスワードだけを保存、比較するため、CHAP よりセキュアです。また、MSCHAP では MPPE によるデータの暗号化のためのキーを生成します。
  - [PPPoE ルート メトリック（PPPoE route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます。有効な値は 1 ～ 255 です。デフォルトでは、学習したルートのアドミニストレーティブ ディスタンスは 1 です。
  - [ルート設定の有効化（Enable Route Settings）]：手動で PPPoE の IP アドレスを設定するには、このチェックボックスをオンにして、[IP アドレス（IP Address）] を入力します。

[ルート設定を有効化（Enable Route Settings）] チェックボックスをオンにして、[IPアドレス（IP Address）] を空欄にした場合、**ip address pppoe setroute** コマンドが次のように適用されます。

```
interface GigabitEthernet0/2
nameif inside2_pppoe
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
pppoe client vpdn group test
pppoe client route distance 10
ip address pppoe setroute
```

- [フラッシュにユーザー名とパスワードを保存（Store Username and Password in Flash）]：フラッシュ メモリにユーザー名とパスワードを保存します。

  Firewall Threat Defense デバイスは、NVRAM の特定の場所にユーザー名とパスワードを保存します。

ステップ 12 （任意） IPv6 アドレスの設定 （58 ページ）を参照して [IPv6] タブでの IPv6 アドレスを設定します。

ステップ 13 （任意） MAC アドレスの設定 （78 ページ）を参照して [詳細設定（Advanced）] タブで MAC アドレスを手動で設定します。

ステップ 14 （任意） **[ハードウェア構成（Hardware Configuration）]** > **[速度（Speed）]**をクリックして、デュプレックスと速度を設定します。

- [デュプレックス（Duplex）]：[全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。SFP インターフェイスは [全二重（Full）] のみをサポートします。
- [速度（Speed）]：速度を選択します（モデルによって異なります）。SFP の場合は、**[SFP を検出（Detect SFP）]** を選択して、インストールされた 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および FEC は常に有効です。デュアルスピード トランシーバの場合、低い方の速度が使用されます。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。一部のスイッチおよびトランシーバは、特に高速のインターフェイスの場合、自動ネゴシエーションをサポートしていません。この場合、Firewall Threat Defense のインターフェイスを手動速度に設定し、 **自動ネゴシエーション** も無効にして、リンクがアップ状態になるようにします。

  （注）
  高可用性（HA）またはクラウド制御リンク インターフェイスの速度は変更できません。

- **[自動ネゴシエーション（Auto-negotiation）]**：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。

  1100 を除き、自動ネゴシエーションは速度とは別に設定します。一部のスイッチは、特に高速のインターフェイスの場合、自動ネゴシエーションをサポートしていません。この場合、 Firewall Threat Defense のインターフェイスを手動速度に設定し、 **自動ネゴシエーション** も無効にして、リンクがアップ状態になるようにします。

- **前方誤り訂正モード**：25Gbps 以上のインターフェイスの場合、[前方誤り訂正（FEC）（Forward Error Correction (FEC)）]を有効にします。

  EtherChannel メンバーインターフェイスの場合は、EtherChannel に追加する前に FEC を設定する必要があります。EtherChannelからインターフェイスを削除する場合は、再起動後にインターフェイスの FEC を再設定する必要があります。

  一部のスイッチでは、特に大規模なインターフェイスの場合、FECの自動モードをサポートしていません。スイッチのサポートに応じて、FECを無効にするか、手動で設定してください。

  自動を使用する場合に選択する設定は、トランシーバのタイプと、インターフェイスが固定（内蔵）かネットワークモジュールかによって異なります。

表 *1*：自動設定のデフォルト *FEC*

トランシーバ タイプ	固定ポートのデフォルト FEC（イーサネット 1/9 ～ 1/16）	ネットワークモジュールのデフォルト FEC
25G-SR	第 108 条 RS-FEC	第 108 条 RS-FEC
25G-LR	第 108 条 RS-FEC	第 108 条 RS-FEC
10/25G-CSR	第 108 条 RS-FEC	第 74 条 FC-FEC
25G-AOC*x*M	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-CU2.5/3M	自動ネゴシエーション	自動ネゴシエーション
25G-CU4/5M	自動ネゴシエーション	自動ネゴシエーション
25/50/100G	第 91 条 RS-FEC	第 91 条 RS-FEC

ステップ 15 （任意）[マネージャアクセス（Manager Access）]ページのデータインターフェイスで Firewall Management Center 管理アクセスを有効にします。

Firewall Threat Defense を最初にセットアップするときに、データインターフェイスからマネージャアクセスを有効にできます。Firewall Threat Defense を Firewall Management Center に追加した後にマネージャアクセスを有効または無効にする場合は、次を参照してください。

- マネージャアクセスの有効化：管理アクセスインターフェイスの管理からデータへの変更

  （注）
  管理インターフェイスからデータインターフェイスへのマネージャインターフェイスの移行を最初に開始しないと、マネージャアクセスを有効にすることはできません。移行を開始したら、[マネージャアクセス（Manager Access）] ページでマネージャアクセスを有効にし、設定を保存できます。

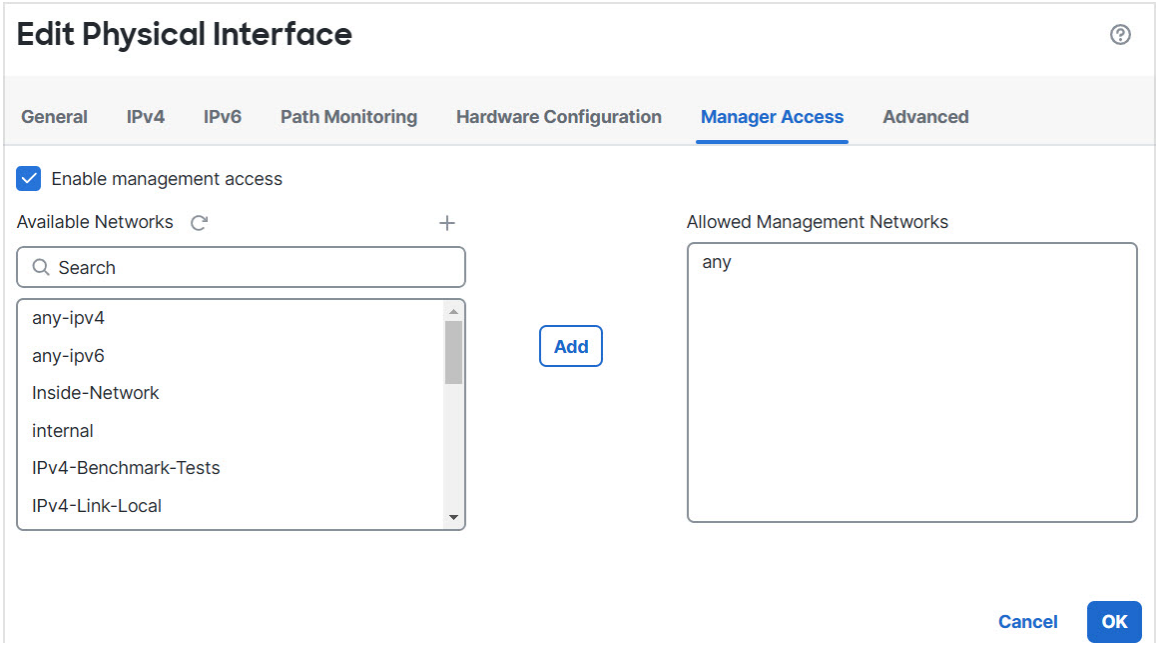
- マネージャアクセスの無効化：マネージャ アクセス インターフェイスをデータから管理に変更する

マネージャアクセスインターフェイスをあるデータインターフェイスから別のデータインターフェイスに変更する場合は、元のデータインターフェイスでマネージャアクセスを無効にする必要がありますが、インターフェイス自体はまだ無効にしないでください。展開を実行するには、元のデータインターフェイスを使用する必要があります。新しいマネージャ アクセス インターフェイスで同じ IP アドレスを使用する場合は、元のインターフェイスの IP 設定を削除または変更できます。この変更は展開に影響しません。新しいインターフェイスに別の IP アドレスを使用する場合は、Firewall Management Center に表示されるデバイスの IP アドレスも変更します。Firewall Management Center でのホスト名または IP アドレスの更新を参照してください。スタティックルート、DDNS、DNS 設定などの新しいインターフェイスを使用するように、関連する構成も更新してください。

データインターフェイスからのマネージャアクセスには、次の制限があります。

- マネージャアクセスを有効にできるのは、1 つの物理的なデータインターフェイスのみです。サブインターフェイスまたは EtherChannel を使用することはできません。マネージャアクセスインターフェイスでサブインターフェイスを作成することもできません。冗長性を目的として、Firewall Management Center の単一のセカンダリインターフェイスでマネージャアクセスを有効にすることもできます。
- このインターフェイスは管理専用にできません。
- ルーテッドインターフェイスを使用するルーテッドファイアウォールモードのみです。
- PPPoE はサポートされていません。ISP で PPPoE が必要な場合は、PPPoE をサポートするルータを Firewall Threat Defense と WAN モデムの間に配置する必要があります。
- インターフェイスを配置する必要があるのはグローバル VRF のみです。
- SSH はデータインターフェイスではデフォルトで有効になっていないため、後で Firewall Management Center を使用して SSH を有効にする必要があります。また、管理インターフェイス ゲートウェイがデータインターフェイスに変更されるため、**configure network static-routes** コマンドを使用して管理インターフェイス用の静的ルートを追加しない限り、リモートネットワークから管理インターフェイスに SSH 接続することはできません。Amazon Web Services の Firewall Threat Defense Virtual の場合、コンソールポートは使用できないため、管理インターフェイスへの SSH アクセスを維持する必要があります。設定を続行する前に、管理用の静的ルートを追加します。または、マネージャアクセス用のデータインターフェイスを設定する前に、すべての CLI 構成（**configure manager add** コマンドを含む）を終了してから接続を切断します。
- 管理インターフェイスとイベント専用インターフェイスを別々に使用することはできません。
- クラスタリングはサポートされません。この場合、管理インターフェイスを使用する必要があります。

図 *19* : マネージャアクセス



- Firepower Management Center が専用の管理インターフェイスの代わりにこのデータインターフェイスを管理に使用するには、[このインターフェイス上の管理をマネージャに対して有効にする（Enable management on this interface for the manager） をオンにします。
- （オプション）[許可された管理ネットワーク（Allowed Management Networks）] ボックスで、マネージャアクセスを許可するネットワークを追加します。デフォルトでは、すべてのネットワークが許可されます。

ステップ 16 **[OK]** をクリックします。

ステップ 17 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

ブリッジ グループ インターフェイスの設定

ブリッジ グループは、Secure Firewall Threat Defense device がルーティングではなくブリッジするインターフェイスのグループです。ブリッジグループはトランスペアレント ファイアウォール モード、ルーテッド ファイアウォール モードの両方でサポートされています。ブリッジグループの詳細については、About Bridge Groupsを参照してください。

ブリッジグループと関連インターフェイスを設定するには、次の手順を実行します。

ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定

この手順は、ブリッジ グループ メンバー インターフェイスの名前とセキュリティ ゾーンを設定する方法について説明します。同じブリッジグループで、さまざまな種類のインターフェイス（物理インターフェイス、VLAN サブインターフェイス、Firepower 1010 および Cisco Secure Firewall 1210/1220 VLAN インターフェイス、EtherChannel、冗長インターフェイス）を含めることができます。管理インターフェイスはサポートされていません。ルーテッドモードでは、EtherChannel はサポートされません。Firepower 4100/9300 では、データ共有タイプのインターフェイスはサポートされていません。

始める前に

- **Firepower 4100/9300**
  1. Configure a Physical Interface
  2. （任意）特別なインターフェイスを設定します。
     - Add an EtherChannel (Port Channel)
     - Add a VLAN Subinterface for Container Instances FXOS で次を実行します。
     - Firewall Management Center でのサブインターフェイスの追加 （22 ページ）

- （任意）**他のすべてのモデル**：
  - EtherChannel の設定
  - サブインターフェイスの追加 （22 ページ）
  - Firepower 1010 および Cisco Secure Firewall 1210/1220：VLAN インターフェイスを構成する （5 ページ）

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

ステップ 3 [名前（Name）] フィールドに、48 文字以内で名前を入力します。

この名前を「cluster」という語句で始めることはできません。その名前は内部で使用するために予約されています。

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 （任意） このインターフェイスを [管理専用（Management Only）] に設定してトラフィックを管理トラフィックに制限します。through-the-box トラフィックは許可されていません。

ステップ 6 （任意） [Description] フィールドに説明を追加します。

説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 7 [モード（Mode）] ドロップダウン リストで、[なし（None）] を選択します。

通常のファイアウォール インターフェイスのモードは [なし（None）] に設定されています。他のモードは IPS 専用インターフェイス タイプ向けです。このインターフェイスをブリッジ グループに割り当てると、[スイッチド（Switched）] がモードに表示されます。

ステップ 8 [セキュリティ ゾーン（Security Zone）] ドロップダウン リストからセキュリティ ゾーンを選択するか、[新規（New）] をクリックして、新しいセキュリティ ゾーンを追加します。

ブリッジ グループ メンバー インターフェイスは、スイッチドタイプ インターフェイスであり、スイッチドタイプのゾーンにのみ属することができます。このインターフェイスに対して IP アドレス設定は行わないでください。ブリッジ仮想インターフェイス（BVI）に対してのみ IP アドレスを設定します。BVI はゾーンに属しておらず、BVI にはアクセス コントロール ポリシーを適用できないことに注意してください。

ステップ 9 **MTU** についてはMTU の設定 （77 ページ）を参照してください。

ステップ 10 （任意） **[ハードウェア構成（Hardware Configuration）]** > **[速度（Speed）]**をクリックして、デュプレックスと速度を設定します。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）] を選択します。SFP インターフェイスは [全二重（Full）] のみをサポートします。
- [速度（Speed）] : 速度を選択します（モデルによって異なります）。SFP の場合は、**[SFP を検出（Detect SFP）]** を選択して、インストールされた 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および FEC は常に有効です。デュアルスピード トランシーバの場合、低い方の速度が使用されます。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。一部のスイッチおよびトランシーバは、特に高速のインターフェイスの場合、自動ネゴシエーションをサポートしていません。この場合、Firewall Threat Defense のインターフェイスを手動速度に設定し、 **自動ネゴシエーション** も無効にして、リンクがアップ状態になるようにします。

  （注）
  高可用性（HA）またはクラウド制御リンク インターフェイスの速度は変更できません。

- **[自動ネゴシエーション（Auto-negotiation）]** : 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。

  1100 を除き、自動ネゴシエーションは速度とは別に設定します。一部のスイッチは、特に高速のインターフェイスの場合、自動ネゴシエーションをサポートしていません。この場合、 Firewall Threat Defense のインターフェイスを手動速度に設定し、 **自動ネゴシエーション** も無効にして、リンクがアップ状態になるようにします。

- **前方誤り訂正モード** : 25Gbps 以上のインターフェイスの場合、[前方誤り訂正（FEC）（Forward Error Correction (FEC)）]を有効にします。

  EtherChannel メンバーインターフェイスの場合は、EtherChannel に追加する前に FEC を設定する必要があります。EtherChannelからインターフェイスを削除する場合は、再起動後にインターフェイスの FEC を再設定する必要があります。

一部のスイッチでは、特に大規模なインターフェイスの場合、FECの自動モードをサポートしていません。スイッチのサポートに応じて、FECを無効にするか、手動で設定してください。

自動を使用する場合に選択する設定は、トランシーバのタイプと、インターフェイスが固定（内蔵）かネットワークモジュールかによって異なります。

表 *2*：自動設定のデフォルト *FEC*

トランシーバ タイプ	固定ポートのデフォルト FEC（イーサネット 1/9 ～ 1/16）	ネットワークモジュールのデフォルト FEC
25G-SR	第 108 条 RS-FEC	第 108 条 RS-FEC
25G-LR	第 108 条 RS-FEC	第 108 条 RS-FEC
10/25G-CSR	第 108 条 RS-FEC	第 74 条 FC-FEC
25G-AOC*x*M	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-CU2.5/3M	自動ネゴシエーション	自動ネゴシエーション
25G-CU4/5M	自動ネゴシエーション	自動ネゴシエーション
25/50/100G	第 91 条 RS-FEC	第 91 条 RS-FEC

ステップ 11 （任意） IPv6 アドレスの設定 （58 ページ）を参照して [IPv6] タブでの IPv6 アドレスを設定します。

ステップ 12 （任意） MAC アドレスの設定 （78 ページ）を参照して [詳細設定（Advanced）] タブで MAC アドレスを手動で設定します。

ステップ 13 **[OK]** をクリックします。

ステップ 14 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

ブリッジ仮想インターフェイス（BVI）の設定

ブリッジ グループごとに、IP アドレスを設定する BVI が必要です。Firewall Threat Defense はブリッジ グループが発信元になるパケットの送信元アドレスとして、この IP アドレスを使用します。BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、BVI IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカルアドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。

ルーテッドモードの場合、BVIに名前を指定すると、BVIがルーティングに参加します。名前を指定しなければ、ブリッジ グループはトランスペアレント ファイアウォール モードの場合と同じように隔離されたままになります。

始める前に

セキュリティ ゾーンに BVI を追加することはできません。そのため、BVI にアクセス コントロール ポリシーを適用することはできません。ゾーンに基づいてブリッジ グループのメンバー インターフェイスにポリシーを適用する必要があります。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 **[インターフェイスの追加（Add Interfaces）]** > **[ブリッジ グループ インターフェイス（Bridge Group Interface）]** を選択します。

ステップ 3 （ルーテッド モード）[名前（Name）] フィールドに、名前を 48 文字以内で入力します。

トラフィックをブリッジ グループ メンバーの外部（たとえば、外部インターフェイスや他のブリッジグループのメンバー）にルーティングする必要がある場合は、BVIに名前を付ける必要があります。名前は大文字と小文字が区別されません。

ステップ 4 [ブリッジ グループ ID（Bridge Group ID）] フィールドに、1 ～ 250 の間のブリッジ グループ ID を入力します。

ステップ 5 （オプション）[説明（Description）] フィールドに、このブリッジ グループの説明を入力します。

ステップ 6 [インターフェイス（Interfaces）] タブでインターフェイスをクリックし、[追加（Add）] をクリックして [選択したインターフェイス（Selected Interfaces）] 領域にそのインターフェイスを移動します。ブリッジグループのメンバーにするすべてのインターフェイスに対して繰り返します。

ステップ 7 （トランスペアレント モード）[IPv4] タブをクリックします。[IP アドレス（IP Address）] フィールドに IPv4 アドレスおよびサブネット マスクを入力します。

BVI にはホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30 サブネットなど（255.255.255.252）、ホスト アドレスが 3 つ未満（アップストリーム ルータ、ダウンストリーム ルータ、トランスペアレント ファイアウォールにそれぞれ 1 つずつ）の他のサブネットを使用しないでください。Firewall Threat Defense デバイスは、サブネットの先頭アドレスと最終アドレスで送受信されるすべての ARP パケットをドロップします。たとえば、/30 サブネットを使用し、そのサブネットからアップストリーム ルータへの予約済みアドレスを割り当てた場合、Firewall Threat Defense デバイスはダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。

高可用性の場合は、**Devices** > **Device Management** ページの **[モニター対象インターフェイス（Monitored Interfaces）]** エリアの **[高可用性（High Availability）]** タブで、スタンバイ IP アドレスを設定します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネッ

トワーク テストを使用してスタンバイ インターフェイスをモニターできず、リンク ステートをトラックすることしかできません。

ステップ 8 （ルーテッド モード）[IPv4] タブをクリックします。IP アドレスを設定するには、[IP タイプ（IP Type）] ドロップダウン リストにある次のオプションのいずれかを使用します。

高可用性およびクラスタリング インターフェイスは、静的 IP アドレス設定のみをサポートします。DHCP はサポートされていません。

- [静的 IP を使用する（Use Static IP）]：IP アドレスおよびサブネット マスクを入力します。高可用性の場合は、静的 IP アドレスのみを使用できます。**Devices** > **Device Management** でスタンバイ IP アドレスを設定し、**[監視対象インターフェイス（Monitored Interfaces）]** エリアで、**[高可用性（HA）（High Availability）]** タブをクリックします。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニターできず、リンク ステートをトラックすることしかできません。
- [DHCP の使用（Use DHCP）]：次のオプションのパラメータを設定します。
  - [DHCP を使用してデフォルト ルートを取得（Obtain default route using DHCP）]：DHCP サーバーからデフォルト ルートを取得します。
  - [DHCPルートメトリック（DHCP route metric）]：アドミニストレーティブ ディスタンスを学習したルートに割り当てます（1 ～ 255）。学習したルートのデフォルトのアドミニストレーティブ ディスタンスは 1 です。

ステップ 9 （任意） IPv6 アドレッシングの設定については、IPv6 アドレスの設定 （58 ページ）を参照してください。

ステップ 10 （任意） スタティック ARP エントリの追加 （79 ページ）および静的 MAC アドレスの追加とブリッジグループの MAC 学習の無効化 （80 ページ）（トランスペアレント モードの場合のみ）を参照して **ARP** と **MAC** を設定します。

ステップ 11 **[OK]** をクリックします。

ステップ 12 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

IPv6 アドレスの設定

ここでは、ルーテッド モードおよびトランスペアレント モードで IPv6 アドレッシングを設定する方法について説明します。

About IPv6

This section includes information about IPv6.

IPv6 Addressing

You can configure two types of unicast addresses for IPv6:

- Global—The global address is a public address that you can use on the public network. For a bridge group, this address needs to be configured for the BVI, and not per member interface. You can also configure a global IPv6 address for the management interface in transparent mode.
- Link-local—The link-local address is a private address that you can only use on the directly-connected network. Routers do not forward packets using link-local addresses; they are only for communication on a particular physical network segment. They can be used for address configuration or for the Neighbor Discovery functions such as address resolution. In a bridge group, only member interfaces have link-local addresses; the BVI does not have a link-local address.

At a minimum, you need to configure a link-local address for IPv6 to operate. If you configure a global address, a link-local address is automatically configured on the interface, so you do not also need to specifically configure a link-local address. For bridge group member interfaces, when you configure the global address on the BVI, the Firewall Threat Defense device automatically generates link-local addresses for member interfaces. If you do not configure a global address, then you need to configure the link-local address, either automatically or manually.

Modified EUI-64 Interface IDs

RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture requires that the interface identifier portion of all unicast IPv6 addresses, except those that start with binary value 000, be 64 bits long and be constructed in Modified EUI-64 format. The Firewall Threat Defense device can enforce this requirement for hosts attached to the local link.

When this feature is enabled on an interface, the source addresses of IPv6 packets received on that interface are verified against the source MAC addresses to ensure that the interface identifiers use the Modified EUI-64 format. If the IPv6 packets do not use the Modified EUI-64 format for the interface identifier, the packets are dropped and the following system log message is generated:

```
325003: EUI-64 source address check failed.
```

The address format verification is only performed when a flow is created. Packets from an existing flow are not checked. Additionally, the address verification can only be performed for hosts on the local link.

Configure the IPv6 Prefix Delegation Client

The Firewall Threat Defense can act as a DHPCv6 Prefix Delegation client so that the client interface, for example the outside interface connected to a cable modem, can receive one or more IPv6 prefixes that the Firewall Threat Defense can then subnet and assign to its inside interfaces.

About IPv6 Prefix Delegation

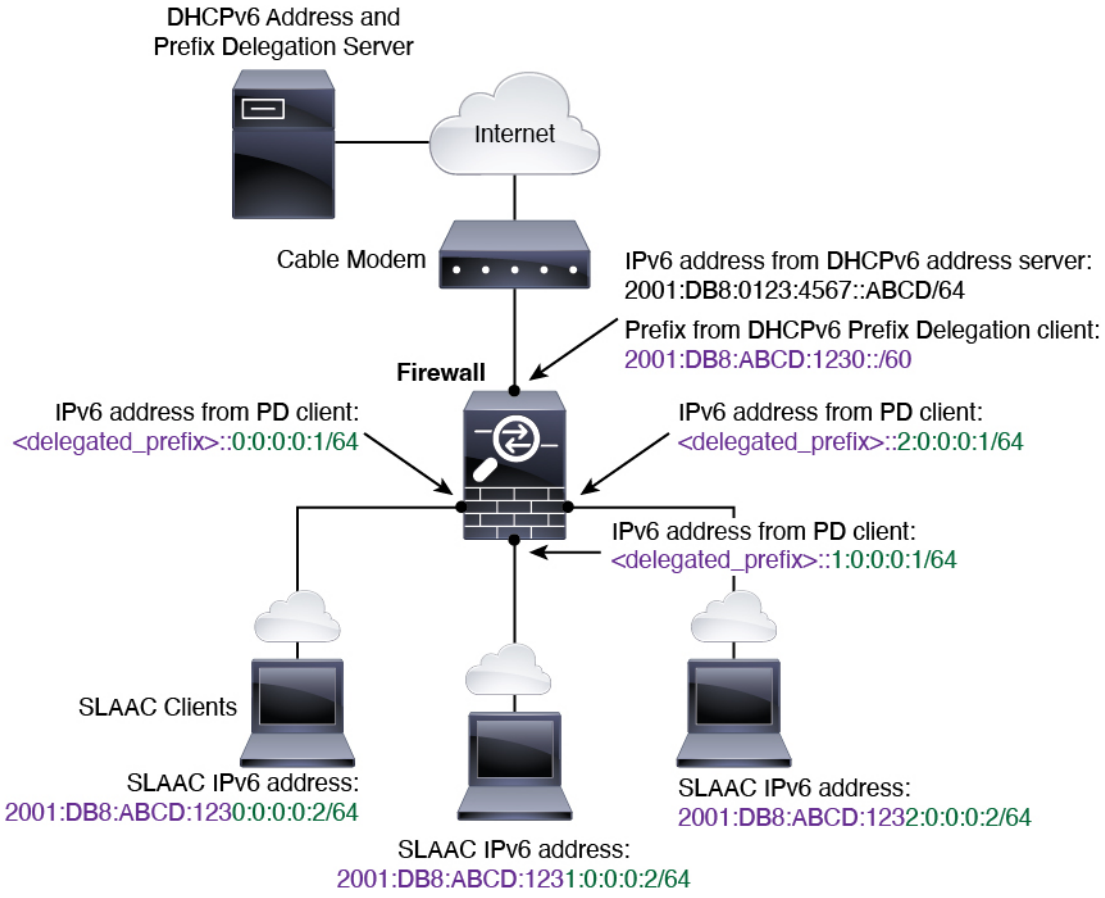
The Firewall Threat Defense can act as a DHPCv6 Prefix Delegation client so that the client interface, for example the outside interface connected to a cable modem, can receive one or more IPv6 prefixes that the Firewall Threat Defense can then subnet and assign to its inside interfaces. Hosts connected to the inside interfaces can then use StateLess Address Auto Configuration (SLAAC) to obtain global IPv6 addresses. Note that the inside Firewall Threat Defense interfaces do not in turn act as Prefix Delegation servers; the Firewall Threat Defense can only provide global IP addresses to SLAAC clients. For example, if a router is connected to the Firewall Threat Defense, it can act as a SLAAC client to obtain its IP address. But if

you want to use a subnet of the delegated prefix for the networks behind the router, you must manually configure those addresses on the router's inside interfaces.

The Firewall Threat Defense includes a light DHCPv6 server so the Firewall Threat Defense can provide information such as the DNS server and domain name to SLAAC clients when they send Information Request (IR) packets to the Firewall Threat Defense. The Firewall Threat Defense only accepts IR packets, and does not assign addresses to the clients. You will configure the client to generate its own IPv6 address by enabling IPv6 autoconfiguration on the client. Enabling stateless autoconfiguration on a client configures IPv6 addresses based on prefixes received in Router Advertisement messages; in other words, based on the prefix that the Firewall Threat Defense received using Prefix Delegation.

IPv6 Prefix Delegation /64 Subnet Example

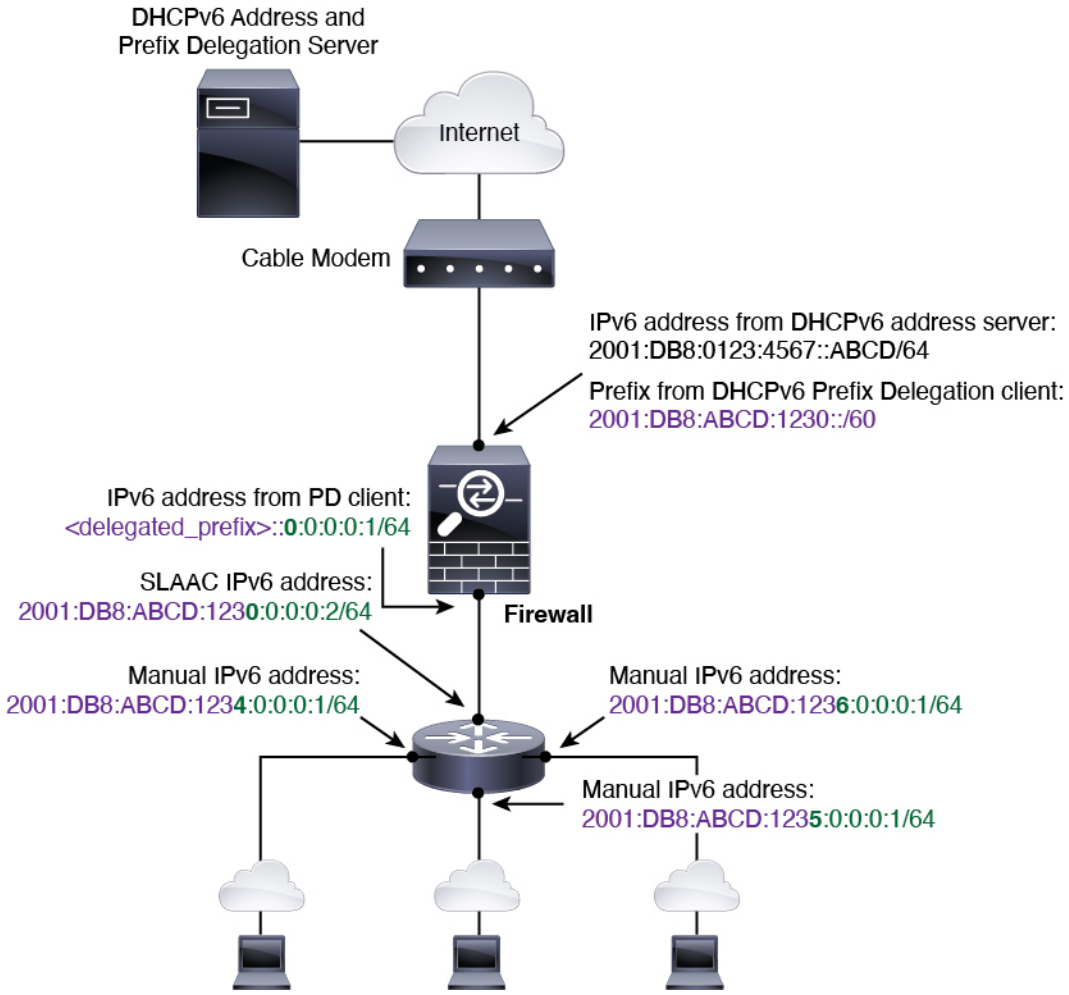
The following example shows the Firewall Threat Defense receiving an IP address on the outside interface using the DHCPv6 address client. It also gets a delegated prefix using the DHCPv6 Prefix Delegation client. The Firewall Threat Defense subnets the delegated prefix into /64 networks and assigns global IPv6 addresses to its inside interfaces dynamically using the delegated prefix plus a manually configured subnet (::0, ::1, or ::2) and IPv6 address (0:0:0:1) per interface. SLAAC clients connected to those inside interfaces obtain IPv6 addresses on each /64 subnet.



IPv6 Prefix Delegation /62 Subnet Example

The following example shows the Firewall Threat Defense subnetting the prefix into 4 /62 subnets: 2001:DB8:ABCD:123**0**::/62, 2001:DB8:ABCD:123**4**::/62, 2001:DB8:ABCD:123**8**::/62, and

2001:DB8:ABCD:123**C**::/62. The Firewall Threat Defense uses one of 4 available /64 subnets on 2001:DB8:ABCD:1230::/62 for its inside network (::0). You can then manually use additional /62 subnets for downstream routers. The router shown uses 3 of 4 available /64 subnets on 2001:DB8:ABCD:1234::/62 for its inside interfaces (::4, ::5, and ::6). In this case, the inside router interfaces cannot dynamically obtain the delegated prefix, so you need to view the delegated prefix on the Firewall Threat Defense, and then use that prefix for your router configuration. Usually, ISPs delegate the same prefix to a given client when the lease expires, but if the Firewall Threat Defense receives a new prefix, you will have to modify the router configuration to use the new prefix. The DHCP unique identifier (DUID) is persistent across reboots.



IPv6 プレフィックス委任クライアントの有効化

1 つ以上のインターフェイスで DHCPv6 プレフィクス委任クライアントをイネーブルにします。Firewall Threat Defense は、サブネット化して内部ネットワークに割り当てることができる 1 つ以上の IPv6 プレフィックスを取得します。通常、プレフィックス委任クライアントを有効にしたインターフェイスは DHCPv6 アドレスクライアントを使用して IP アドレスを取得し、その他の Firewall Threat Defense インターフェイスだけが、委任されたプレフィックスから取得されるアドレスを使用します。

この機能は、ルーテッドモードでのみサポートされます。この機能は、クラスタリングまたはハイアベイラビリティではサポートされません。

始める前に

プレフィックス委任を使用する場合は、IPv6 トラフィックの中断を防ぐために、Firewall Threat Defense IPv6 ネイバー探索のルータアドバタイズメント間隔を DHCPv6 サーバーによって割り当てられるプレフィックスの推奨有効期間よりもはるかに小さい値に設定する必要があります。たとえば、DHCPv6 サーバーでプレフィックス委任の推奨有効期間を 300 秒に設定している場合は、Firewall Threat Defense RA の間隔を 150 秒に設定する必要があります。推奨有効期間を設定するには、**show ipv6 general-prefix** コマンドを使用します。Firewall Threat Defense RA の間隔を設定するには、「IPv6 ネイバー探索の設定 （68 ページ）」を参照してください。デフォルトは 200 秒です。

手順

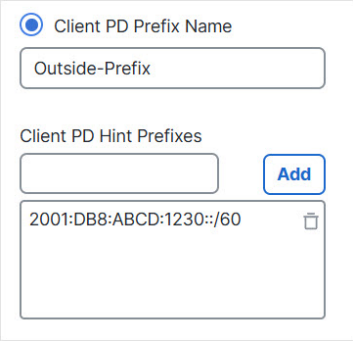
ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

ステップ 3 [IPv6] ページをクリックしてから、[DHCP] をクリックします。

ステップ 4 [クライアントPDプレフィックス名（Client PD Prefix Name）] をクリックし、このプレフィックスの名前を入力します。

図 *20*: プレフィックス委任クライアントの有効化



名前には最大 200 文字を使用できます。

ステップ 5 （任意）[クライアントPDヒントプレフィックス（Client PD Hint Prefixes）] フィールドにプレフィックスとプレフィックス長を入力し、受信する委任されたプレフィックスに関する DHCP サーバーへのヒントを 1 つ以上指定して [追加（Add）] をクリックします。

通常、特定のプレフィクス長（::/60 など）を要求しますが、以前に特定のプレフィックスを受信しており、リースの期限が切れるときにそれを確実に再取得したい場合は、そのプレフィックスの全体をヒントとして入力できます。複数のヒント（異なるプレフィックスまたはプレ

フィックス長）を入力すると、どのヒントに従うのか、またはそもそもヒントに従うのかどうかが DHCP サーバによって決定されます。

ステップ 6 **[OK]** をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

グローバル IPv6 アドレスの設定

ルーテッド モードの任意のインターフェイスとトランスペアレント モードまたはルーテッド モードの BVI に対してグローバル IPv6 アドレスを設定するには、次の手順を実行します。

（注） グローバルアドレスを設定すると、リンクローカルアドレスは自動的に設定されるため、別々に設定する必要はありません。ブリッジ グループについて、BVI でグローバル アドレスを設定すると、すべてのメンバー インターフェイスのリンクローカル アドレスが自動的に設定されます。

Firewall Threat Defense で定義されているサブインターフェイスの場合、親インターフェイスの同じ Burned-In MAC Address を使用するので、MAC アドレスも手動で設定することをお勧めします。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、Firewall Threat Defense で特定のインスタンスでのトラフィックの中断を避けることができます。MAC アドレスの設定 （78 ページ）を参照してください。

始める前に

ブリッジグループの IPv6 ネイバー探索では、双方向アクセスルールを使用して、Firewall Threat Defense ブリッジ グループ メンバー インターフェイスでネイバー送信要求（ICMPv6 タイプ 135）およびネイバーアドバタイズメント（ICMPv6 タイプ 136）パケットを明示的に許可する必要があります。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

ステップ 3 [IPv6] ページをクリックします。

ルーテッドモードでは、[基本（Basic）]ページがデフォルトで選択されています。トランスペアレントモードでは、[アドレス（Address）] ページがデフォルトで選択されています。

ステップ 4 （任意）[基本（Basic）] ページで、[IPv6を有効にする（Enable IPv6）] をオンにします。

リンクローカルアドレスのみを設定する場合は、このオプションを使用します。それ以外の場合、IPv6 アドレスを設定すると、IPv6 処理が自動的に有効になります。

ステップ 5 グローバル IPv6 アドレスを次のいずれかの方法で設定します。

フェールオーバーやクラスタリング、およびループバック インターフェイスの場合は、IP アドレスを手動で設定する必要がありますクラスタリングの場合、リンクローカルアドレスの手動設定もサポートされていません。

- （ルーテッドインターフェイス）ステートレス自動設定：[自動設定（Autoconfiguration）] チェックボックスをオンにします。

  インターフェイス上でステートレス自動設定を有効にすると、受信したルータ アドバタイズメント メッセージのプレフィックスに基づいて IPv6 アドレスを設定します。ステートレスな自動設定が有効になっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

  RFC 4862 では、ステートレス自動設定用に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定されていますが、この場合は、Firewall Threat Defense デバイスがルータ アドバタイズメント メッセージを送信します。**[設定（Settings）]** タブをクリックし、**[IPv6]** タブをクリックして、**[RA の有効化（Enable RA）]** チェック ボックスをオフにして、メッセージを抑止します。

- 手動設定：グローバル IPv6 アドレスを手動で設定するには、次の手順を実行します。

  1. [アドレス（Address）] ページ、[アドレスの追加（Add Address）] (+) の順にクリックします。

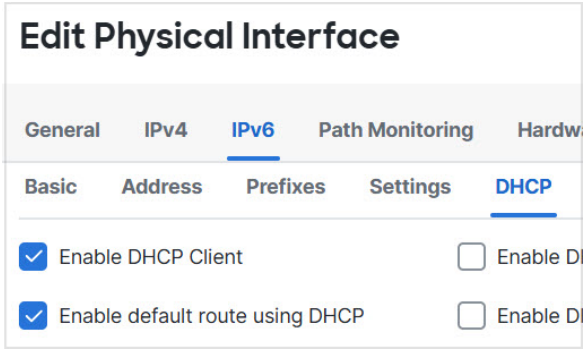
     [アドレスの追加（Add Address）] ダイアログボックスが表示されます。

  2. [アドレス（Address）] フィールドに、インターフェイス ID を含む完全なグローバル IPv6 アドレス、または IPv6 プレフィックス長と IPv6 プレフィックスのいずれかを入力します。（ルーテッドモード）プレフィックスだけを入力した場合は、必ず [EUI-64 を適用（Enforce EUI 64）] チェックボックスをオンにして、Modified EUI-64 形式を使用してインターフェイス ID を生成するようにしてください。たとえば、2001:0DB8::BA98:0:3210/48（完全なアドレス）または 2001:0DB8::/48（プレフィックス、[EUI 64] はオン）。

     （**[EUI 64の適用（Enforce EUI 64）]** を設定しなかった場合は）**Devices** > **Device Management** ページでスタンバイ IP アドレスを設定し、**[モニター対象インターフェイス（Monitored Interfaces）]** エリアの **[高可用性（High Availability）]** をクリックします。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステートをトラックすることしかできません。

- （ルーテッドインターフェイス）DHCPv6 を使用してアドレスを取得する：DHCPv6 を使用するには、次の手順を実行します。

図 *21 : DHCPv6* クライアントの有効化



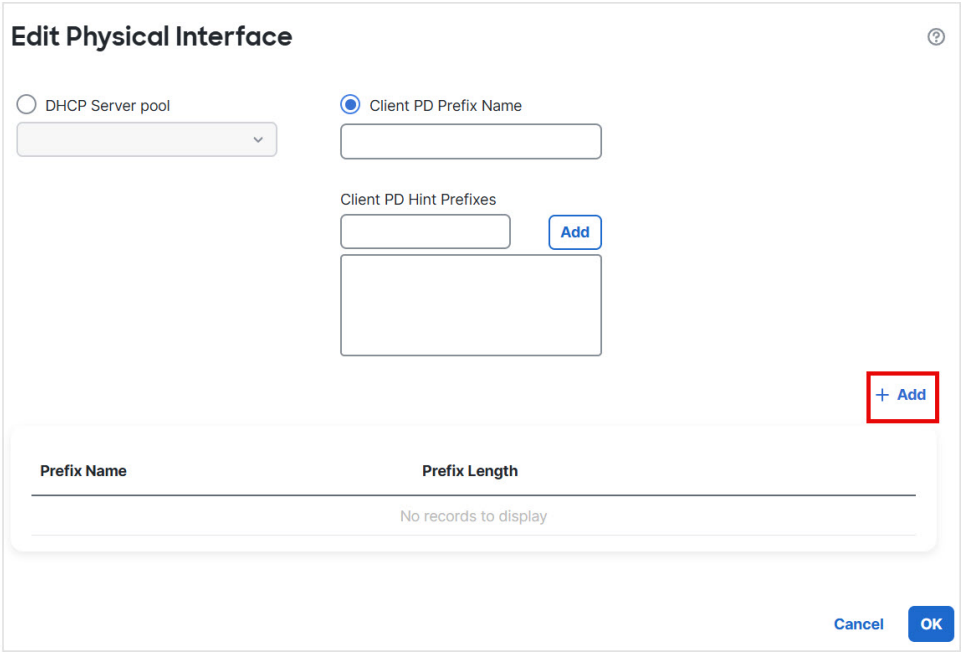
1. [DHCP] ページをクリックします。
2. [DHCPクライアントの有効化（Enable DHCP Client）] チェックボックスをオンにします。
3. （オプション）ルータアドバタイズメントからデフォルトルートを取得するには、[DHCPを使用してデフォルトルートを有効にする（Enable default route using DHCP）] チェックボックスをクリックします。

- （ルーテッドインターフェイス）委任されたプレフィックスを使用する：委任されたプレフィックスを使用して IPv6 アドレスを割り当てるには、次の手順を実行します。

  この機能は、Firewall Threat Defense に別のインターフェイスで DHCPv6 プレフィックス委任クライアントを有効にさせるために必要です。IPv6プレフィックス委任クライアントの有効化 （61 ページ） を参照してください。

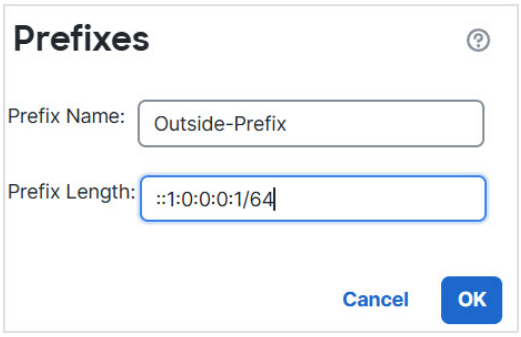
  1. [DHCP] ページをクリックします。
  2. (+) をクリックします。

図 *22*: 委任されたプレフィックスの使用



3. 別のインターフェイスでプレフィックス委任クライアントに指定した**プレフィックス名**を入力します（「IPv6 プレフィックス委任クライアントの有効化 （61 ページ）」を参照）。

図 *23*: プレフィックス名とアドレスの指定



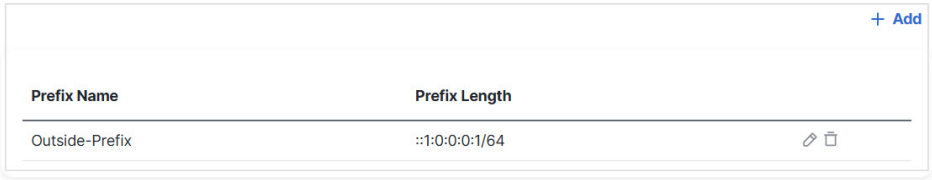
4. IPv6 アドレスと**プレフィックス長**を入力します。

   通常、委任されたプレフィクスは /60 以下であるため、複数 /64 ネットワークにサブネット化できます。接続されるクライアント用に SLAAC をサポートする必要がある場合は、/64 がサポートされるサブネット長です。/60 サブネットを補完するアドレス（1:0:0:0:1 など）を指定する必要があります。プレフィックスが /60 未満の場合は、アドレスの前に :: を入力します。たとえば、委任されたプレフィクスが 2001:DB8:1234:5670::/60 である場合、このインターフェイスに割り当てられるグローバル IP アドレスは 2001:DB8:1234:5671::1/64 です。ルータ アドバタイズメントでアドバタイズされるプレフィクスは 2001:DB8:1234:5671::/64 です。この例では、プレフィ

クスが /60 未満である場合、プレフィックスの残りのビットは、前に配置される :: によって示されるように、0になります。たとえば、プレフィクスが 2001:DB8:1234::/48 である場合、IPv6 アドレスは 2001:DB8:1234::1:0:0:0:1/64 になります。

5. [OK] をクリックします。

図 *24:* プレフィックス委任テーブル



6. 必要に応じて、このインターフェイスで DHCPv6 ステートレスサーバーを有効にします（「DHCPv6 ステートレスサーバーの有効化」を参照）。その場合は、[アドレス以外の設定でDHCPを有効にする（Enable DHCP for non-address config）] オプションもオンにすることをお勧めします。

ステップ 6 ルーテッドインターフェイスの場合は、必要に応じて [基本（Basic）] ページで次の値を設定できます。

- ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[EUI-64 を適用（Enforce EUI-64）] チェックボックスをオンにします。
- リンクローカル アドレスを手動で設定するには、[リンクローカル アドレス（Link-Local address）] フィールドにアドレスを入力します。

  リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feee:6a82。グローバル アドレスを設定する必要がなく、リンクローカル アドレスだけを設定する必要がある場合は、リンクローカル アドレスを手動で定義できます。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、その他のデバイスで Modified EUI-64 形式の使用が強制される場合、手動で割り当てたリンクローカルアドレスによりパケットがドロップされることがあります。

  クラスタリングは、手動のリンクローカルアドレスをサポートしていません。

ステップ 7 ルーテッドインターフェイスの場合は、必要に応じて [DHCP] ページで次の値を設定できます。

- [アドレス設定の DHCP を有効化（Enable DHCP for address config）] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Managed Address Config フラグを設定します。

  IPv6 ルータ アドバタイズメント内のこのフラグは、取得されるステートレス自動設定のアドレス以外のアドレスの取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。

- [アドレス設定の DHCP を有効化（Enable DHCP for address config）] チェックボックスをオンにして、IPv6 ルータ アドバタイズメント パケットの Other Address Config フラグを設定します。

  IPv6 ルータ アドバタイズメント内のこのフラグは、DHCPv6 から DNS サーバー アドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを、IPv6 自動設定クライアントに通知します。DHCPv6 プレフィックス委任で DHCPv6 ステートレスサーバーを使用する場合は、このオプションを使用します。

ステップ 8 ルーテッドインターフェイスの場合は、[プレフィックス（Prefixes）] ページと [設定（Settings）] ページでの設定について「IPv6 ネイバー探索の設定 （68 ページ）」を参照してください。BVI インターフェイスの場合は、[設定（Settings）] ページの以下のパラメータを参照してください。

- [DAD 試行（DAD attempts）]：DAD 試行の最大数（1 ～ 600）。重複アドレス検出（DAD）プロセスをディセーブルにするには、この値を 0 に設定します。この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。デフォルトでは 1 になっています。
- [NS 間隔（NS Interval）]：インターフェイスでの IPv6 ネイバー要請再送信の間隔（1000 ～ 3600000 ms）。デフォルト値は 1000 ミリ秒です。
- [到達可能時間（Reachable Time）]：到達可能性確認イベントが発生した後でリモートの IPv6 ノードを到達可能とみなす時間（0 ～ 3600000 ms）。デフォルト値は 0 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

ステップ 9 **[OK]** をクリックします。

ステップ 10 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

IPv6 ネイバー探索の設定

IPv6 ネイバー探索プロセスは、ICMPv6 メッセージおよび要請ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを特定し、ネイバーの読み出し可能性を確認し、隣接ルータを追跡します。

ノード（ホスト）はネイバー探索を使用して、接続リンク上に存在することがわかっているネイバーのリンク層アドレスの特定や、無効になったキャッシュ値の迅速なパージを行います。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送しようとしている

隣接ルータを検出します。さらに、ノードはこのプロトコルを使用して、どのネイバーが到達可能でどのネイバーがそうでないかをアクティブに追跡するとともに、変更されたリンク層アドレスを検出します。ルータまたはルータへのパスが失われると、ホストは機能している代替ルータまたは代替パスをアクティブに検索します。

始める前に

ルーテッドモードのみでサポートされます。トランスペアレントモードでサポートされるIPv6ネイバー設定については、「グローバル IPv6 アドレスの設定 （63 ページ）」を参照してください。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

ステップ 3 [IPv6]、[プレフィックス（Prefixes）] の順にクリックします。

ステップ 4 （任意） IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定するには、次の手順を実行します。

a) [プレフィックスの追加（Add Prefix）] をクリックします。 (+)

b) [アドレス（Address）] フィールドに、プレフィックス長の IPv6 アドレスを入力するか、または [デフォルト（Default）] チェックボックスをオンにして、デフォルトのプレフィックスを使用します。

c) （任意） IPv6 プレフィックスをアドバタイズしない場合は、[アドバタイズメント（Advertisement）] チェックボックスをオフにします。**デフォルトの** プレフィックスの場合、この設定はオンリンク プレフィックスにのみ適用されます。特定のオフリンク プレフィックスの **[アドバタイズメント（Advertisement）]** をオフにしない限り、オフリンク プレフィックスは引き続きアドバタイズされます。

d) [オフ リンク（Off Link）] チェックボックスをオンにして、指定したプレフィックスがリンクに割り当てられたことを示します。指定したプレフィックスを含むアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。このプレフィックスは、オンリンクの判別には使用しないでください。

e) 指定されているプレフィックスを自動設定に使用する場合、[自動設定（Autoconfiguration）] チェックボックスをオンにします。

f) [プレフィックス ライフタイム（Prefix Lifetime）] で、[期間（Duration）] または [失効日（Expiration Date）] をクリックします。

- [期間（Duration）] : プレフィックスの [優先ライフタイム（Preferred Lifetime）] を秒単位で入力します。この設定は、指定の IPv6 プレフィックスが有効なものとしてアドバタイズする時間です。最大値は無限大です。有効な値は、0 ～ 4294967295 です。デフォルトは 2592000（30 日間）です。プレフィックスの [有効ライフタイム（Valid Lifetime）] を秒単位で入力します。この設定は、指定の IPv6 プレフィックスが優先であるとしてアドバタイズする時間です。最大値は無限大です。有効な値は、0 ～

4294967295 です。デフォルト設定は、604800（7 日）です。または、[無限大（Infinite）] チェックボックスをオンにして、時間無制限を設定します。

- [失効日（Expiration Date）] : [有効（Valid）]、[優先（Preferred）] 日時を選択します。

g) [OK] をクリックします。

ステップ 5 [設定（Settings）] をクリックします。

ステップ 6 （任意） [DAD 試行（DAD attempts）] の最大数、1 ～ 600 を設定します。デフォルトでは 1 になっています。重複アドレス検出（DAD）プロセスをディセーブルにするには、この値を 0 に設定します。

この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。

ステートレス自動設定プロセス中に、重複アドレス検出は、アドレスがインターフェイスに割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を確認します。

重複アドレスが検出されると、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用対象外となり、次のエラー メッセージが生成されます。

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカル アドレスであれば、インターフェイスで IPv6 パケットの処理はディセーブルになります。重複アドレスがグローバル アドレスであれば、そのアドレスは使用されません。

ステップ 7 （任意） [NS インターバル（NS Interval）] フィールドで、IPv6 ネイバー勧誘再送信の時間の間隔を、1000 ～ 3600000ms で設定します。

デフォルト値は 1000 ミリ秒です。

ローカル リンク上にある他のノードのリンクレイヤ アドレスを検出するため、ノードからネイバー送信要求メッセージ（ICMPv6 Type 135）がローカル リンクに送信されます。ネイバー送信要求メッセージを受信すると、宛先ノードは、ネイバー アドバタイズメント メッセージ（ICPMv6 Type 136）をローカル リンク上に送信して応答します。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがあるネイバーの到達可能性を検証する場合、ネイバー送信要求メッセージ内の宛先アドレスとして、そのネイバーのユニキャスト アドレスを使用します。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。

ステップ 8 （任意） 到達可能性確認イベントが発生した後でリモート IPv6 ノードが到達可能であると見なされる時間を、[到達可能時間（Reachable Time）] フィールドにて、0 ～ 3600000ms で設定します。

デフォルト値は 0 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

ステップ 9 （任意）ルータ アドバタイズメントの伝送を抑制にするには、[RA を有効にする（Enable RA）]チェックボックスをオフにします。ルータ アドバタイズメントの伝送を有効にすると、RA ライフタイムと時間間隔を設定できます。

ルータ要請メッセージ（ICMPv6 Type 133）に応答して、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）が自動的に送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

Firewall Threat Defenseで IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージを無効化できます。

- [RA ライフタイム（RA Lifetime）]：IPv6 ルータ アドバタイズメントのルータのライフタイム値を、0 ～ 9000 秒で設定します。

  デフォルトは 1800 秒です。

- [RA インターバル（RA Interval）]：IPv6 ルータ アドバタイズメントの伝送の間の時間間隔を、3 ～ 1800 秒で設定します。

  デフォルトは 200 秒です。

  他の IPv6 ノードとの同期を防ぐために、ファイアウォールは、設定した値（ジッター）をランダムに調整します。

ステップ 10 **[OK]** をクリックします。

ステップ 11 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

高度なインターフェイスの設定

この項では、通常のファイアウォール モードのインターフェイスの MAC アドレスの設定方法、最大伝送ユニット（MTU）の設定方法、およびその他の詳細パラメータの設定方法について説明します。

About Advanced Interface Configuration

This section describes advanced interface settings.

About MAC Addresses

You can manually assign MAC addresses to override the default. For container instances, the FXOS chassis automatically generates unique MAC addresses for all interfaces.

（注） You might want to assign unique MAC addresses to subinterfaces defined on the Firewall Threat Defense, because they use the same burned-in MAC address of the parent interface. For example, your service provider might perform access control based on the MAC address. Also, because IPv6 link-local addresses are generated based on the MAC address, assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses, which can avoid traffic disruption in certain instances on the Firewall Threat Defense device.

（注） For container instances, even if you are not sharing a subinterface, if you manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification.

Default MAC Addresses

For native instances:

Default MAC address assignments depend on the type of interface.

- Physical interfaces—The physical interface uses the burned-in MAC address.
- VLAN interfaces (Firepower 1010 and Secure Firewall 1210/1220)—Routed firewall mode: All VLAN interfaces share a MAC address. Ensure that any connected switches can support this scenario. If the connected switches require unique MAC addresses, you can manually assign MAC addresses. See MAC アドレスの設定 （78 ページ）.

  Transparent firewall mode: Each VLAN interface has a unique MAC address. You can override the generated MAC addresses if desired by manually assigning MAC addresses. See MAC アドレスの設定 （78 ページ）.
- EtherChannels (Firepower Models)—For an EtherChannel, all interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links. The port-channel interface uses a unique MAC address from a pool; interface membership does not affect the MAC address.
- EtherChannels (ASA Models)—The port-channel interface uses the lowest-numbered channel group interface MAC address as the port-channel MAC address. Alternatively you can configure a MAC address for the port-channel interface. We recommend configuring a unique MAC address in case the group channel interface membership changes. If you remove the interface that was providing the port-channel MAC address, then the port-channel MAC address changes to the next lowest numbered interface, thus causing traffic disruption.

- Subinterfaces (Firewall Threat Defense-defined)—All subinterfaces of a physical interface use the same burned-in MAC address. You might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address. Also, because IPv6 link-local addresses are generated based on the MAC address, assigning unique MAC addresses to subinterfaces allows for unique IPv6 link-local addresses, which can avoid traffic disruption in certain instances on the Firewall Threat Defense.

For container instances:

- MAC addresses for all interfaces are taken from a MAC address pool. For subinterfaces, if you decide to manually configure MAC addresses, make sure you use unique MAC addresses for all subinterfaces on the same parent interface to ensure proper classification. See Automatic MAC Addresses for Container Instance Interfaces.

About the MTU

The MTU specifies the maximum frame *payload* size that the Firewall Threat Defense device can transmit on a given Ethernet interface. The MTU value is the frame size *without* Ethernet headers, VLAN tagging, or other overhead. For example, when you set the MTU to 1500, the expected frame size is 1518 bytes including the headers, or 1522 when using VLAN. Do not set the MTU value higher to accommodate these headers.

For Geneve, the entire Ethernet datagram is being encapsulated, so the new IP packet is larger and requires a larger MTU: you should set the Firewall Threat Defense device VTEP source interface MTU to be the network MTU + 306 bytes.

Path MTU Discovery

The Firewall Threat Defense device supports Path MTU Discovery (as defined in RFC 1191), which lets all devices in a network path between two hosts coordinate the MTU so they can standardize on the lowest MTU in the path.

Default MTU

The default MTU on the Firewall Threat Defense device is 1500 bytes. This value does not include the 18-22 bytes for the Ethernet header, VLAN tagging, or other overhead.

MTU and Fragmentation

For IPv4, if an outgoing IP packet is larger than the specified MTU, it is fragmented into 2 or more frames. Fragments are reassembled at the destination (and sometimes at intermediate hops), and fragmentation can cause performance degradation. For IPv6, packets are typically not allowed to be fragmented at all. Therefore, your IP packets should fit within the MTU size to avoid fragmentation.

For TCP packets, the endpoints typically use their MTU to determine the TCP maximum segment size (MTU - 40, for example). If additional TCP headers are added along the way, for example for site-to-site VPN tunnels, then the TCP MSS might need to be adjusted down by the tunneling entity. See About the TCP MSS （74 ページ）.

For UDP or ICMP, the application should take the MTU into account to avoid fragmentation.

（注） The Firewall Threat Defense device can receive frames larger than the configured MTU as long as there is room in memory.

MTU and Jumbo Frames

A larger MTU lets you send larger packets. Larger packets might be more efficient for your network. See the following guidelines:

- Matching MTUs on the traffic path—We recommend that you set the MTU on all Firewall Threat Defense interfaces and other device interfaces along the traffic path to be the same. Matching MTUs prevents intermediate devices from fragmenting the packets.
- Accommodating jumbo frames—You can set the MTU 9000 bytes or higher when you enable jumbo frames. The maximum depends on the model.

About the TCP MSS

The TCP maximum segment size (MSS) is the size of the TCP payload *before* any TCP and IP headers are added. UDP packets are not affected. The client and the server exchange TCP MSS values during the three-way handshake when establishing the connection.

You can set the TCP MSS on the Firewall Threat Defense device for through traffic using the Sysopt_Basic object in FlexConfig; see FlexConfig ポリシー; by default, the maximum TCP MSS is set to 1380 bytes. This setting is useful when the Firewall Threat Defense device needs to add to the size of the packet for IPsec VPN encapsulation. However, for non-IPsec endpoints, you should disable the maximum TCP MSS on the Firewall Threat Defense device.

If you set a maximum TCP MSS, if either endpoint of a connection requests a TCP MSS that is larger than the value set on the Firewall Threat Defense device, then the Firewall Threat Defense device overwrites the TCP MSS in the request packet with the Firewall Threat Defense device maximum. If the host or server does not request a TCP MSS, then the Firewall Threat Defense device assumes the RFC 793-default value of 536 bytes (IPv4) or 1220 bytes (IPv6), but does not modify the packet. For example, you leave the default MTU as 1500 bytes. A host requests an MSS of 1500 minus the TCP and IP header length, which sets the MSS to 1460. If the Firewall Threat Defense device maximum TCP MSS is 1380 (the default), then the Firewall Threat Defense device changes the MSS value in the TCP request packet to 1380. The server then sends packets with 1380-byte payloads. The Firewall Threat Defense device can then add up to 120 bytes of headers to the packet and still fit in the MTU size of 1500.

You can also configure the minimum TCP MSS; if a host or server requests a very small TCP MSS, the Firewall Threat Defense device can adjust the value up. By default, the minimum TCP MSS is not enabled.

For to-the-box traffic, including for SSL VPN connections, this setting does not apply. The Firewall Threat Defense device uses the MTU to derive the TCP MSS: MTU - 40 (IPv4) or MTU - 60 (IPv6).

Default TCP MSS

By default, the maximum TCP MSS on the Firewall Threat Defense device is 1380 bytes. This default accommodates IPv4 IPsec VPN connections where the headers can equal up to 120 bytes; this value fits within the default MTU of 1500 bytes.

Suggested Maximum TCP MSS Setting

The default TCP MSS assumes the Firewall Threat Defense device acts as an IPv4 IPsec VPN endpoint and has an MTU of 1500. When the Firewall Threat Defense device acts as an IPv4 IPsec VPN endpoint, it needs to accommodate up to 120 bytes for TCP and IP headers.

If you change the MTU value, use IPv6, or do not use the Firewall Threat Defense device as an IPsec VPN endpoint, then you should change the TCP MSS setting using the Sysopt_Basic object in FlexConfig.

（注） Even if you explicitly set an MSS, if a component such as TLS/SSL decryption or server discovery needs a particular MSS, it will set that MSS based on the interface MTU and ignore your MSS setting.

See the following guidelines:

- Normal traffic—Disable the TCP MSS limit and accept the value established between connection endpoints. Because connection endpoints typically derive the TCP MSS from the MTU, non-IPsec packets usually fit this TCP MSS.
- IPv4 IPsec endpoint traffic—Set the maximum TCP MSS to the MTU - 120. For example, if you use jumbo frames and set the MTU to 9000, then you need to set the TCP MSS to 8880 to take advantage of the new MTU.
- IPv6 IPsec endpoint traffic—Set the maximum TCP MSS to the MTU - 140.

ARP Inspection for Bridge Group Traffic

By default, all ARP packets are allowed between bridge group members. You can control the flow of ARP packets by enabling ARP inspection.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.

When you enable ARP inspection, the Firewall Threat Defense device compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
- If there is a mismatch between the MAC address, the IP address, or the interface, then the Firewall Threat Defense device drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the Firewall Threat Defense device to either forward the packet out all interfaces (flood), or to drop the packet.

（注） The dedicated Management interface never floods packets even if this parameter is set to flood.

MAC Address Table

When you use bridge groups, the Firewall Threat Defense learns and builds a MAC address table in a similar way as a normal bridge or switch: when a device sends a packet through the bridge group, the Firewall Threat Defense adds the MAC address to its table. The table associates the MAC address with the source interface so that the Firewall Threat Defense knows to send any packets addressed to the device out the correct interface. Because traffic between bridge group members is subject to the Firewall Threat Defense security policy, if the destination MAC address of a packet is not in the table, the Firewall Threat Defense does not flood the original packet on all interfaces as a normal bridge does. Instead, it generates the following packets for directly-connected devices or for remote devices:

- Packets for directly-connected devices—The Firewall Threat Defense generates an ARP request for the destination IP address, so that it can learn which interface receives the ARP response.
- Packets for remote devices—The Firewall Threat Defense generates a ping to the destination IP address so that it can learn which interface receives the ping reply.

The original packet is dropped.

Default Settings

- If you enable ARP inspection, the default setting is to flood non-matching packets.
- The default timeout value for dynamic MAC address table entries is 5 minutes.
- By default, each interface automatically learns the MAC addresses of entering traffic, and the Firewall Threat Defense device adds corresponding entries to the MAC address table.

（注） Secure Firewall Threat Defense device generates a reset packet to reset a connection that is denied by a stateful inspection engine. Here, the destination MAC address of the packet is not determined based on the ARP table lookup but instead it is taken directly from the packets (connections) that are being denied.

Guidelines for ARP Inspection and the MAC Address Table

- ARP inspection is only supported for bridge groups.
- MAC address table configuration is only supported for bridge groups.

MTU の設定

たとえば、ジャンボ フレームを許可するようにインターフェイスの MTU をカスタマイズします。

、ISA 3000、Firewall Threat Defense Virtualの場合：1500 バイトを超える MTU を変更すると、jumbo-frame reservation が自動的に有効になります。ジャンボフレームを使用するには、システムを再起動する必要があります。クラスタリングをサポートする Firewall Threat Defense Virtual では、Day0 構成で jumbo-frame reservation を有効にすることができるため、その場合は再起動する必要はありません。再起動後、disable jumbo-frame reservation を無効にすることはできません。Firewall Threat Defense Virtual の場合は例外で、サポートされている場合は Day0 構成で jumbo-frame reservation を無効にできます。インライン セットでインターフェイスを使用する場合、MTU 設定は使用されません。ただし、jumbo-frame reservation の設定はインラインセットに関連します。ジャンボフレームによりインラインインターフェイスは最大 9000 バイトのパケットを受信できます。 jumbo-frame reservation を有効にするには、すべてのインターフェイスの MTU を 1500 バイトより大きい値に設定する必要があります。

ジャンボフレームは、他のプラットフォームではデフォルトで有効化されます。

注意 デバイス上でデータインターフェイスの最大 MTU 値を変更し、設定の変更を展開すると、Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。インスペクションは、変更したインターフェイスだけでなく、すべてのデータインターフェイスで中断されます。この中断でトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイス タイプに応じて異なります。この注意は、管理専用のインターフェイスには適用されません。詳細については、Snort の再起動によるトラフィックの動作を参照してください。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

ステップ 3 [全般（General）] タブで [MTU] を設定します。最小値と最大値は、プラットフォームによって異なります。

デフォルト値は 1500 バイトです。

ステップ 4 **[OK]** をクリックします。

ステップ 5 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

ステップ 6 ISA 3000、および Firewall Threat Defense Virtual で MTU を 1,500 バイト超に設定する場合は、システムを再起動して jumbo-frame reservation を有効にします。「デバイスのシャットダウンまたは再起動」を参照してください。

MAC アドレスの設定

MAC アドレスを手動で割り当てることが必要となる場合があります。**[追加（Add）]** ドロップダウンリストで **[高可用性（HA）（High Availability）]** を選択して、**Devices** > **Device Management** ウィンドウで、アクティブおよびスタンバイ MAC アドレスを設定することもできます。両方の画面でインターフェイスの MAC アドレスを設定した場合は、**[インターフェイス（Interfaces）]** > **[詳細（Advanced）]** タブのアドレスが優先されます。

（注） コンテナ インスタンスでは、MAC アドレスを手動で設定すると、サブインターフェイスを共有していない場合でも、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。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックします。
[情報（Information）] タブが選択されています。

ステップ 4 （個別インターフェイスモードでのクラスタリングの場合）ドロップダウンリストから MAC アドレスプールを選択します。

アドレス プールに従って MAC アドレスプールを追加できます。

ステップ 5 （他のモードの場合）アクティブおよびスタンバイの MAC アドレスを設定します。

a) [アクティブな MAC アドレス（Active MAC Address）] フィールドに、MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。

たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

b) [スタンバイMACアドレス（Standby MAC Address）] フィールドに、ハイ アベイラビリティで使用する MAC アドレスを入力します。

アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 6 **[OK]** をクリックします。

ステップ 7 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

スタティック ARP エントリの追加

デフォルトでは、ブリッジグループのメンバーの間ですべての ARP パケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションを有効にします（ARP インスペクション 参照）。ARP インスペクションは、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。

ルーテッド インターフェイスの場合、スタティック ARP エントリを入力できますが、通常はダイナミック エントリで十分です。ルーテッド インターフェイスの場合、直接接続されたホストにパケットを配送するために ARP テーブルが使用されます。送信者は IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、新しい情報で更新される前にこのエントリがタイムアウトする必要があります。

トランスペアレント モードの場合、管理トラフィックなどの Firewall Threat Defense デバイスとの間のトラフィックに、Firewall Threat Defense は ARP テーブルのダイナミック ARP エントリのみを使用します。

始める前に

この画面は、名前付きインターフェイスについてのみ使用できます。

手順

ステップ 1 **[Devices** > **Device Management]** を選択して、Firewall Threat Defense デバイスに対して **[Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックして、[ARP] タブをクリックします（トランスペアレント モードでは、[ARP と MAC（ARP and MAC）]）。

ステップ 4 [ARP 設定を追加（Add ARP Config）] (＋) をクリックします。
[ARP 設定を追加（Add ARP Config）] ダイアログボックスが表示されます。

ステップ 5 [IP アドレス（IP Address）] フィールドに、ホストの IP アドレスを入力します。

ステップ 6 [MAC アドレス（MAC Address）] フィールドに、ホストの MAC アドレスを入力します。たとえば、「00e0.1e4e.3d8b」のように入力します。

ステップ 7 このアドレスでプロキシ ARP を実行するには、[エイリアスを有効にする（Enable Alias）] チェックボックスをオンにします。

Firewall Threat Defense デバイスは、指定された IP アドレスの ARP 要求を受信すると、指定された MAC アドレスで応答します。

ステップ 8 [OK] をクリックし、次にもう一度 [OK] をクリックして、[詳細設定（Advanced settings）] を閉じます。

ステップ 9 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

静的 MAC アドレスの追加とブリッジグループの MAC 学習の無効化

通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。MAC アドレス ラーニングを無効にすることができます。ただし、MAC アドレスをスタティックにテーブルに追加しないかぎり、トラフィックは Firewall Threat Defense デバイスを通過できません。スタティック MAC アドレスは、MAC アドレス テーブルに追加することもできます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、Firewall Threat Defense デバイスはトラフィックをドロップし、システム メッセージを生成します。スタティック ARP エントリを追加するときに（スタティック ARP エントリの追加 （79 ページ） を参照）、スタティック MAC アドレス エントリは MAC アドレス テーブルに自動的に追加されます。

始める前に

この画面は、トランスペアレントモードの名前付き BVI でのみ使用できます。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックして、[ARP と MAC（ARP and MAC）] タブをクリックします。

ステップ 4 （任意）[MAC ラーニングを有効にする（Enable MAC Learning）] チェックボックスをオフにして MAC ラーニングを無効にします。

ステップ 5 スタティック MAC アドレスを追加するには、[MAC 設定を追加（Add MAC Config）] をクリックします。
[MAC 設定を追加（Add MAC Config）] ダイアログボックスが表示されます。

ステップ 6 [MAC アドレス（MAC Address）] フィールドに、ホストの MAC アドレスを入力します。たとえば、「00e0.1e4e.3d8b」のように入力します。[OK] をクリックします。

ステップ 7 [OK] をクリックして詳細設定を終了します。

ステップ 8 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

セキュリティの設定パラメータの設定

この項では、IP スプーフィングの防止方法、完全フラグメント リアセンブルの許可方法、および [プラットフォーム設定（Platform Settings）] でデバイス レベルで設定されるデフォルトのフラグメント設定のオーバーライド方法について説明します。

アンチ スプーフィング

この項では、インターフェイスでユニキャスト リバース パス フォワーディング（ユニキャスト RPF）を有効にします。ユニキャスト RPF は、ルーティング テーブルに従って、すべてのパケットが正しい送信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護します。

通常、Firewall Threat Defense デバイスは、パケットの転送先を判定するときに宛先アドレスだけを調べます。ユニキャスト RPF は、送信元アドレスも調べるようにデバイスに指示します。そのため、リバース パス フォワーディング（Reverse Path Forwarding）と呼ばれます。Firewall Threat Defense デバイスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートをデバイスのルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、Firewall Threat Defense デバイスはデフォルト ルートを使用してユニキャスト RPF 保護の条件を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティング テーブルにない場合、デバイスはデフォルト ルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく識別します。

ルーティング テーブルにあるアドレスから外部インターフェイスにトラフィックが入り、このアドレスが内部インターフェイスに関連付けられている場合、Firewall Threat Defense デバイスはパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合は、一致するルート（デフォルト ルート）が外部インターフェイスを示しているため、デバイスはパケットをドロップします。

ユニキャスト RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションが含まれているため、初期パケットには逆ルートのルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

パケットあたりのフラグメント

デフォルトでは、Firewall Threat Defense デバイスは 1 つの IP パケットにつき最大 24 のフラグメントを許可し、最大 200 のフラグメントのリアセンブリ待ちを許可します。NFS over UDP など、アプリケーションが日常的にパケットをフラグメント化する場合は、ネットワークでフラグメント化を許可する必要があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、フラグメントが Firewall Threat Defense デバイスを通過できないようにすることをお勧めします。フラグメント化されたパケットは、DoS 攻撃によく使われます。

フラグメントのリアセンブル

Firewall Threat Defense デバイスは、次に示すフラグメント リアセンブル プロセスを実行します。

- IP フラグメントは、フラグメント セットが作成されるまで、またはタイムアウト間隔が経過するまで収集されます。
- フラグメントセットが作成されると、セットに対して整合性チェックが実行されます。これらのチェックには、重複、テール オーバーフロー、チェーン オーバーフローはいずれも含まれません。
- Firewall Threat Defense デバイスで終端する IP フラグメントは、常に完全にリアセンブルされます。
- [完全フラグメント リアセンブル（Full Fragment Reassembly）] が無効化されている場合（デフォルト）、フラグメントセットは、さらに処理するためにトランスポート層に転送されます。
- [完全フラグメント リアセンブル（Full Fragment Reassembly）] が有効化されている場合、フラグメント セットは、最初に単一の IP パケットに結合されます。この単一の IP パケットは、さらに処理するためにトランスポート層に転送されます。

始める前に

この画面は、名前付きインターフェイスでのみ使用できます。

手順

ステップ 1 [**Devices** > **Device Management**] を選択して、Firewall Threat Defense デバイスに対して [**Edit** (✎)] をクリックします。[インターフェイス（Interfaces）] タブがデフォルトで選択されます。

ステップ 2 編集するインターフェイス **Edit** (✎) をクリックします。

ステップ 3 [詳細（Advanced）] タブをクリックして、[セキュリティ設定（Security Configuration）] タブをクリックします。

ステップ 4 ユニキャストリバース パス フォワーディングを有効にするには、[アンチスプーフィングの有効化（Enable Anti Spoofing）] チェックボックスをオンにします。

ステップ 5 完全フラグメントリアセンブルを有効化するには、[完全フラグメントリアセンブルを許可（Allow Full Fragment Reassembly）] チェックボックスをオンにします。

ステップ 6 パケットごとに許容するフラグメント数を変更するには、[デフォルトフラグメント設定のオーバーライド（Override Default Fragment Setting）] チェックボックスをオンにして、次に示す値を設定します。

- サイズ（Size）：リアセンブルを待機する IP リアセンブル データベースに格納可能なパケットの最大数を設定します。デフォルトは 200 です。この値を 1 に設定すると、フラグメントが無効化されます。
- チェーン（Chain）：1 つの完全な IP パケットにフラグメント化できる最大パケット数を指定します。デフォルトは 24 パケットです。
- タイムアウト（Timeout）：フラグメント化されたパケット全体が到着するまで待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントの到着後に開始されます。指定した秒数までに到着しなかったパケットフラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。デフォルトは 5 秒です。

ステップ 7 **[OK]** をクリックします。

ステップ 8 **[Save（保存）]** をクリックします。

これで、**Deploy** > **Deploy** に移動して、ポリシーを割り当てたデバイスにデプロイします。変更内容は導入するまで適用されません。

通常のファイアウォール インターフェイスの履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Cisco Secure Firewall 1210CP IEEE 802.3bt のサポート（PoE++および Hi-PoE）	7.7.0	7.7.0	IEEE 802.3bt のサポートに関連する次の改善を確認してください。 • PoE++ と Hi-PoE：ポートあたり最大 90 W。 • シングルシグネチャおよびデュアルシグネチャの受電デバイス（PD）。 • パワーバジェットが先着順で行われます。 • **show power inline** にパワーバジェットフィールドが追加されました。 新規/変更された画面：**[デバイス（Devices）]**> **[デバイス管理（Device Management）]** > **[インターフェイス（Interfaces）]** > **[物理インターフェイスの編集（Edit Physical Interface）]** > **[PoE]** 新規/変更されたコマンド： **show power inline**
組み込みスイッチを搭載したモデルの場合、サブインターフェイスでは VLAN 1 を使用できません。	7.6	7.6	組み込みスイッチのあるモデルでは、 VLAN 1 を使用してサブインターフェイスを作成できません。VLAN 1 は、スイッチポートの論理的な VLAN インターフェイス用に予約されています。 1010 を 7.6 以降にアップグレードし、 VLAN 1 をサブインターフェイスに割り当てている場合は、サブインターフェイスのVLAN ID を新しいVLANに変更する必要があります。VLAN 1 を使用して設定を展開することはできません。
Cisco Secure Firewall による GWLB を使用した AWS でのデュアルアーム展開モードのサポート	7.6	7.6	Cisco Secure Firewall は、GWLB を使用した AWS でのデュアルアーム展開モードをサポートします。このモードでは、ファイアウォールは、トラフィックインスペクション後にインターネットに向かうトラフィックをインターネットゲートウェイを介してインターネットに直接転送すると同時に、ネットワークアドレス変換（NAT）も実行できます。
Cisco Secure Firewall 1210/1220 ハードウェアスイッチのサポート	7.6	7.6	Cisco Secure Firewall 1210/1220 では、各イーサネット インターフェイスをスイッチポートまたはファイアウォールインターフェイスとして設定できます

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Cisco Secure Firewall 1210CP PoE+ は、イーサネットポート 1/5 ～ 1/8 でサポートされます	7.6	7.6	Cisco Secure Firewall 1210CP は、イーサネットポート 1/5 ～ 1/8 で Power over Ethernet+（PoE+）をサポートします。
VXLAN VTEP IPv6 のサポート	7.4	任意（Any）	VXLAN VTEP インターフェイスに IPv6 アドレスを指定できるようになりました。IPv6 は、Threat Defense Virtual クラスタ制御リンクまたは Geneve カプセル化ではサポートされていません。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [VTEP] > [VTEPの追加（Add VTEP）]** **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [VNIインターフェイス（VNI Interface）]** Firewall Threat Defense バージョン 7.4 が必要です。
BGP と管理トラフィックのループバック インターフェイスをサポート	7.4	任意（Any）	ループバック インターフェイスは、次の目的で使用できます。 • AAA • BGP • DNS • HTTP • ICMP • IPsec フローのオフロード • NetFlow • SNMP • SSH • Syslog Firewall Threat Defense バージョン 7.4 が必要です。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
VTI のループバック インターフェイス サポート	7.3	任意（Any）	ループバック インターフェイスを追加できるようになりました。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバック インターフェイスに割り当てられた IP アドレスを使用してすべてのインターフェイスにアクセスできます。VTI の場合、送信元インターフェイスとしてループバック インターフェイスを設定するのに加えて、静的に設定された IP アドレスの代わりに、ループバック インターフェイスから IP アドレスを継承するサポートも追加されています。 新しい/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [ループバック インターフェイスの追加（Add Loopback Interface）]**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
IPv6 DHCP	7.3	任意（Any）	Firewall Threat Defense で IPv6 アドレッシングの次の機能がサポートされるようになりました。 • DHCPv6 アドレスクライアント：Firewall Threat Defense は DHCPv6 サーバーから IPv6 グローバルアドレスとオプションのデフォルトルートを取得します。 • DHCPv6 プレフィックス委任クライアント：Firewall Threat Defense は DHCPv6 サーバーから委任プレフィックスを取得します。Firewall Threat Defense は、委任プレフィックスを使用して他の Firewall Threat Defense インターフェイスのアドレスを設定し、ステートレスアドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータ アドバタイズメント • DHCPv6 ステートレスサーバー：SLAAC クライアントが Firewall Threat Defense に情報要求（IR）パケットを送信すると、Firewall Threat Defense はドメイン名などの他の情報を SLAAC クライアントに提供します。Firewall Threat Defense は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスの追加/編集（Add/Edit Interfaces）] > [IPv6] > [DHCP]** • **[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [DHCP IPv6プール（DHCP IPv6 Pool）]** 新規/変更されたコマンド：**show bgp ipv6 unicast、show ipv6 dhcp、show ipv6 general-prefix**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Azure ゲートウェイロードバランサの Firewall Threat Defense Virtual のペアプロキシ VXLAN	7.3	任意（Any）	Azure ゲートウェイロードバランサ（GWLB）で使用するために、Azure で Firewall Threat Defense Virtual 用のペアプロキシモード VXLAN インターフェイスを設定できます。Firewall Threat Defense Virtual は、ペアリングされたプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [VNIインターフェイス（VNI Interface）]** サポートされているプラットフォーム：Azure の Firewall Threat Defense Virtual
VXLAN のサポート	7.2	任意（Any）	VXLAN カプセル化のサポートが追加されました。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [VTEP]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [VNIインターフェイス（VNI Interface）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [インターフェイス（Interfaces）]** [物理インターフェイスの編集（edit physical interface）] > [全般（General）] サポートされているプラットフォーム：すべて。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Firewall Threat Defense Virtual の Geneve サポート	7.1	任意（Any）	Amazon Web Services（AWS）ゲートウェイロードバランサのシングルアームプロキシをサポートするために、Geneve カプセル化サポートが Firewall Threat Defense Virtual に追加されました。AWS ゲートウェイロードバランサは、透過的なネットワークゲートウェイ（全トラフィックの唯一の出入口）と、トラフィックを分散し、トラフィックの需要に合わせて Firewall Threat Defense Virtual を拡張するロードバランサを組み合わせます。 この機能には Snort 3 が必要です。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [VTEP]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interfaces）] > [VNIインターフェイス（VNI Interface）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイス（Device）] > [インターフェイス（Interfaces）]** [物理インターフェイスの編集（edit physical interface）] > [全般（General）] サポートされているプラットフォーム：AWS の Firewall Threat Defense Virtual

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
31 ビット サブネット マスク	7.0	任意（Any）	ルーテッドインターフェイスに関しては、ポイントツーポイント接続向けの 31 ビットのサブネットに IP アドレスを設定できます。31 ビット サブネットには 2 つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2 アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの FTD 間のフェールオーバーリンクに必要なアドレスは 2 つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP や Syslog を実行する管理ステーションを直接接続することもできます。この機能は、ブリッジグループ用の BVI、またはマルチキャストルーティングではサポートされていません。 新しい/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
Firepower 4100/9300 の Firewall Threat Defense 動作リンク状態と物理リンク状態の同期	6.7	任意（Any）	Firepower 4100/9300 シャーシで、Firewall Threat Defense 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS 管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。Firewall Threat Defense アプリケーション インターフェイスの管理状態は考慮されません。Firewall Threat Defense からの同期がない場合は、たとえば、Firewall Threat Defense アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、Firewall Threat Defense のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、 Firewall Threat Defense が処理できるようになる前に外部ルータが Firewall Threat Defense へのトラフィックの送信を開始することがあるためです。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。 （注） この機能は、クラスタリング、コンテナインスタンス、またはRadware vDP デコレータを使用する Firewall Threat Defense ではサポートされていません。ASA でもサポートされていません。 新規/変更された [Firepower Chassis Manager] 画面：**[論理デバイス（Logical Devices）] > [リンク状態の有効化（Enable Link State）]** 新規/変更された FXOS コマンド：**set link-state-sync enabled**、**show interface expand detail** サポートされているプラットフォーム：Firepower 4100/9300
Firepower 1010 ハードウェア スイッチのサポート	6.5	すべて	Firepower 1010 では、各イーサネット インターフェイスをスイッチポートまたはファイアウォール インターフェイスとして設定できます。 新しい/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [VLANインターフェイスの追加（Add VLAN Interface）]**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
イーサネット 1/7 およびイーサネット 1/8 での Firepower 1010 PoE+ のサポート	6.5	すべて	Firepower 1010 は、スイッチ ポートとして設定されている場合、イーサネット 1/7 およびイーサネット 1/8 の Power on Ethernet+（PoE+）をサポートします。 新しい/変更された画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）] > [PoE]**
コンテナインスタンスで使用される VLAN サブインターフェイス	6.3.0	いずれか	柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。 新規/変更された Secure Firewall Management Center 画面： **[デバイス（Devices）] > [デバイス管理（Device Management）] > [編集（Edit）]** アイコン **> [インターフェイス（Interfaces）]** タブ 新規/変更された Secure Firewall Chassis Manager 画面： **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [新規追加（Add New）]** ドロップダウン メニューの **[サブインターフェイス（Subinterface）]** 新規/変更された FXOS コマンド：**create subinterface、set vlan、show interface、show subinterface** サポートされるプラットフォーム：Firepower 4100/9300
コンテナインスタンスのデータ共有インターフェイス	6.3.0	いずれか	柔軟な物理インターフェイスの使用を可能にするため、複数のインスタンス間でインターフェイスを共有することができます。 新規/変更された Secure Firewall Chassis Manager 画面： **[インターフェイス（Interfaces）] > [すべてのインターフェイス（All Interfaces）] > [タイプ（Type）]** 新規/変更された FXOS コマンド：**set port-type data-sharing、show interface** サポートされるプラットフォーム：Firepower 4100/9300

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
統合ルーティングおよびブリッジング	6.2.0	いずれか	統合ルーティングおよびブリッジングによって、ブリッジグループとルーテッドインターフェイスの間でルーティングする機能が提供されます。ブリッジグループは、Firewall Threat Defense がルーティングではなくブリッジするインターフェイスのグループです。Firewall Threat Defense は、Firewall Threat Defense がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレントファイアウォールモードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジ グループの設定と、ブリッジグループ間およびブリッジグループとルーテッド インターフェイス間のルーティングを実行できます。ブリッジグループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジ グループのゲートウェイとして機能することによってルーティングに参加します。Firewall Threat Defense にブリッジ グループを割り当てるための追加インターフェイスがある場合、統合ルーティングおよびブリッジングによって、外部のレイヤ 2 スイッチを使用するのではない別の方法が提供されます。ルーテッド モードでは、BVI は名前付きインターフェイスとなり、アクセス ルールや DHCP サーバなどの一部の機能に、メンバー インターフェイスとは個別に参加できます。 トランスペアレント モードでサポートされるクラスタリングの機能は、ルーテッドモードではサポートされません。マルチキャスト ルーティングとダイナミック ルーティングの機能も、BVI ではサポートされません。 新規/変更された画面： • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [物理インターフェイスの編集（Edit Physical Interface）]** • **[デバイス（Devices）] > [デバイス管理（Device Management）] > [インターフェイス（Interfaces）] > [インターフェイスを追加（Add Interfaces）] > [ブリッジ グループ インターフェイス（Bridge Group Interface）]** サポートされているプラットフォーム：すべて（Firepower 2100 と Firewall Threat Defense Virtual を除く）

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。