



# 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、[インターフェイスの設定](#)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](#) (1 ページ)
- [Firepower 1010 のスイッチポートの設定](#) (2 ページ)
- [ループバック インターフェイスの設定](#) (14 ページ)
- [VLAN サブインターフェイスと 802.1Q トランッキングの設定](#) (20 ページ)
- [VXLAN インターフェイスの設定](#) (25 ページ)
- [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](#) (41 ページ)
- [高度なインターフェイスの設定](#) (69 ページ)
- [通常のファイアウォール インターフェイスの履歴](#) (83 ページ)

## 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

モデルのサポート

Threat Defense

ユーザの役割

- 管理者
- アクセス管理者

- ネットワーク管理者

## Firepower 1010 のスイッチポートの設定

Firepower 1010 の各インターフェイスは、通常ファイアウォール 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設定できます。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。

### スイッチポートについて

この項では、Firepower 1010 のスイッチポートについて説明します。

### スイッチポートおよびインターフェイスについて

#### ポートとインターフェイス

1010 の物理インターフェイスごとに、その動作をファイアウォール インターフェイスまたはスイッチポートとして設定できます。物理インターフェイスとポートタイプ、およびスイッチポートを割り当てる論理VLAN インターフェイスについては、次の情報を参照してください。

- 物理ファイアウォールインターフェイス：ルーテッドモードでは、これらのインターフェイスは、設定済みのセキュリティポリシーを使用してファイアウォールとVPNサービスを適用することによって、レイヤ3のネットワーク間でトラフィックを転送します。トランスパレントモードでは、これらのインターフェイスは、設定済みのセキュリティポリシーを使用してファイアウォールサービスを適用することによって、レイヤ2の同じネットワーク上のインターフェイス間でトラフィックを転送するブリッジグループメンバーです。ルーテッドモードでは、一部のインターフェイスでブリッジグループメンバーとして、その他のインターフェイスでレイヤ3インターフェイスとして、統合ルーティングおよびブリッジングを使用することもできます。デフォルトでは、イーサネット1/1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として設定されます。また、これらのインターフェイスをIPS専用（インラインセットとパッシブインターフェイス）に設定することもできます。
- 物理スイッチポート：スイッチポートは、ハードウェアのスイッチ機能を使用して、レイヤ2でトラフィックを転送します。同じVLAN上のスイッチポートは、ハードウェアスイッチングを使用して相互に通信できます。トラフィックには、Firewall Threat Defenseセキュリティポリシーは適用されません。アクセスポートはタグなしトラフィックのみを受け入れ、それらを単一のVLANに割り当てることができます。トランクポートはタグなしおよびタグ付きトラフィックを受け入れ、複数のVLANに属することができます。デフォルトでは、イーサネット1/2～1/8はVLAN1のアクセススイッチポートとして設定され

ています。Diagnostic インターフェイスをスイッチポートとして設定することはできません。

- 論理 VLAN インターフェイス：これらのインターフェイスは物理ファイアウォール インターフェイスと同じように動作しますが、サブインターフェイス、IPS 専用インターフェイス（インラインセットおよびパッシブインターフェイス）、または EtherChannel インターフェイスを作成できないという例外があります。スイッチポートが別のネットワークと通信する必要がある場合、Firewall Threat Defense デバイスは VLAN インターフェイスにセキュリティポリシーを適用し、別の論理 VLAN インターフェイスまたはファイアウォール インターフェイスにルーティングします。ブリッジグループメンバーとして VLAN インターフェイスで統合ルーティングおよびブリッジングを使用することもできます。同じ VLAN 上のスイッチポート間のトラフィックに Firewall Threat Defense セキュリティポリシーは適用されませんが、ブリッジグループ内の VLAN 間のトラフィックにはセキュリティポリシーが適用されるため、ブリッジグループとスイッチポートを階層化して特定のセグメント間にセキュリティポリシーを適用できます。

### Power Over Ethernet

PoE は、IEEE 802.3af (PoE) および 802.3at (PoE+) を使用して、イーサネット 1/7 およびイーサネット 1/8 でポートあたり最大 30 ワットまで供給できます。

PoE+ では、リンク層検出プロトコル (Link Layer Discovery Protocol, LLDP) を使用して、電力レベルをネゴシエートします。電力は必要な場合にのみ提供されます。

インターフェイスをシャットダウンすると、デバイスへの電源がディセーブルになります。

## Auto-MDI/MDIX 機能

すべてのスイッチポートで、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーションフェーズでストレートケーブルを検出すると、内部クロスオーバーを実行することでクロスケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常に有効になり、無効にできません。

## スイッチポートの注意事項および制約事項

### 高可用性 と クラスタリング

- クラスタはサポートされません。
- 高可用性を使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。高可用性は、トラフィックがスタンバイユニットを通過

するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の 高可用性 のネットワーク設定では、両方のユニットのアクティブなスイッチポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLAN インターフェイスはフェールオーバーによってモニタできますが、スイッチポートはモニタできません。理論的には、1つのスイッチポートを VLAN に配置して、高可用性 を正常に使用することができますが、代わりに物理ファイアウォール インターフェイスを使用する設定の方が簡単です。

- ファイアウォール インターフェイスはフェールオーバー リンクとしてのみ使用できます。

### 論理 VLAN インターフェイス (SVI)

- 最大 60 個の VLAN インターフェイスを作成できます。
- また、ファイアウォール インターフェイスで VLAN サブインターフェイスを使用する場合、論理 VLAN インターフェイスと同じ VLAN ID は使用できません。
- MAC アドレス :
  - ルーテッドファイアウォール モード : すべての VLAN インターフェイスが 1 つの MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。 [MAC アドレスの設定 \(77 ページ\)](#) を参照してください。
  - トランスペアレント ファイアウォール モード : 各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。 [MAC アドレスの設定 \(77 ページ\)](#) を参照してください。

### ブリッジ グループ

同じブリッジ グループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。

### VLAN インターフェイスおよびスイッチ ポートでサポートされていない機能

VLAN インターフェイスおよびスイッチポートは、次の機能をサポートしていません。

- ダイナミック ルーティング
- マルチキャスト ルーティング
- 等コストマルチパス (ECMP) ルーティング
- インラインセットまたはパッシブインターフェイス
- EtherChannel : スwitchのポートを EtherChannel の一部にはできません。PoE も、EtherChannel のポートではサポートされません。

- フェールオーバーおよびステートリンク
- セキュリティグループタグ (SGT)

#### その他の注意事項と制約事項

- Firepower 1010 には、最大 60 個の名前付きインターフェイスを設定できます。
- Diagnostic インターフェイスをスイッチポートとして設定することはできません。

#### デフォルト設定

- 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す。
- イーサネット 1/2 ~ 1/8 が、VLAN 1 に割り当てられたスイッチ ポートです。
- デフォルトの速度とデュプレックス：デフォルトでは、速度とデュプレックスは自動ネゴシエーションに設定されます。


## スイッチ ポートと Power Over Ethernet の設定



スイッチ ポートおよび PoE を設定するには、次のタスクを実行します。

### スイッチ ポート モードの有効化または無効化

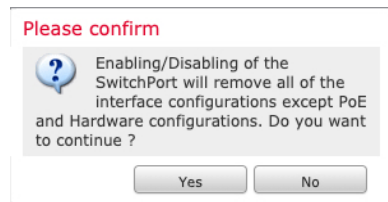
各インターフェイスは、ファイアウォール インターフェイスまたはスイッチ ポートのいずれかになるように個別に設定できます。デフォルトでは、イーサネット 1/1 はファイアウォール インターフェイスで、残りのイーサネット インターフェイスはスイッチ ポートとして設定されます。

#### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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、[有効なスライダ (Slider enabled)] () または[無効なスライダ (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 インターフェイスの設定 \(6 ページ\)](#) 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 インターフェイスの設定

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 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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。

### Add VLAN Interface

General

IPv4

IPv6

Advanced

Name:

inside

☒ Enabled

Description:

Mode:

None

Security Zone:

inside\_zone

MTU:

1500

(64 - 9198)

Priority:

0

(0 - 65535)

VLAN ID \*:

100

(1 - 4070)

Disable Forwarding  
on Interface Vlan:

None

Associated Interface	Port Mode
No records to display	

Cancel

OK

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 ～ 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 ～ 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、VLANID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 \(45 ページ\)](#)
- [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 \(52 ページ\)](#)

**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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## スイッチ ポートのアクセス ポートとしての設定

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。では、イーサネット 1/2 ~ 1/8 は、デフォルトで VLAN 1 に割り当てられています。



(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** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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 [編集 (Edit)] (✎) をクリックします。



図 1: 物理インターフェイスの編集

Edit Physical Interface

General Hardware Configuration

Interface ID:  
Ethernet1/2

☐ Enabled

Description:

Port Mode:  
Access ▼

VLAN ID:  
1  
(1 - 4070)

Protected:  
☐

**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ある場合、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

The screenshot shows the 'Edit Physical Interface' window with the 'Hardware Configuration' tab selected. Under the 'Speed' section, the 'Duplex' dropdown is set to 'full' and the 'Speed' dropdown is set to '1gbps'. The 'Auto-negotiation' checkbox is checked.

[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。

**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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## スイッチポートのトランクポートとしての設定

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、ASA 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。ASA 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** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス [編集 (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 [編集 (Edit)] (✎) をクリックします。

図 3: トランクポートモードの設定

Edit Physical Interface

General Hardware Configuration

Interface ID:  
Ethernet1/2

☐ Enabled

Description:

Port Mode:  
Trunk

Native VLAN ID:  
1  
(1 - 4070)

Allowed VLAN IDs:  
100,200,300  
(1 - 4070)

Protected:  
☐

**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

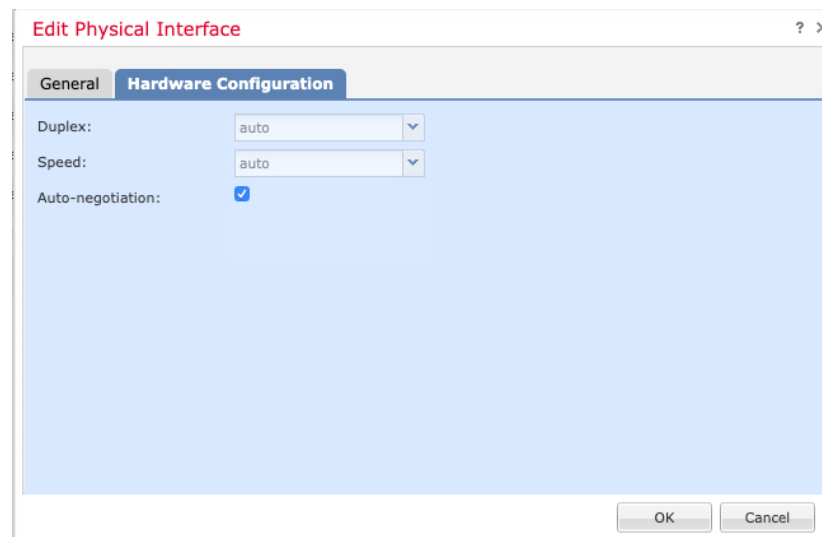
カンマの代わりスペースを入力できます。

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ある場合、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。

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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## 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。

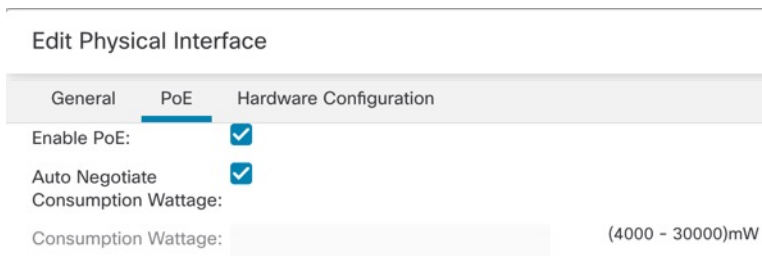
### 手順

ステップ 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス [編集 (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 の [編集 (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



General	PoE	Hardware Configuration
Enable PoE: <input checked="" type="checkbox"/>		
Auto Negotiate Consumption Wattage: <input checked="" type="checkbox"/>		
Consumption Wattage: (4000 - 30000)mW		

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 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、**[展開 (Deploy)]** > **[展開 (Deployment)]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## 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

ループバック インターフェイスは、物理インターフェイスをエミュレートするソフトウェア専用インターフェイスであり、複数の物理インターフェイスを介して IPv4 および IPv6 に到達できます。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。任意の物理インターフェイスからアクセスできるため、1 つがダウンした場合、別のインターフェイスからループバック インターフェイスにアクセスできます。

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。

- スタティックおよびダイナミック VTI トンネル

Firewall Threat Defense は、ダイナミック ルーティング プロトコルを使用してループバックアドレスを配布できます。または、ピアデバイスでスタティックルートを設定して、Firewall Threat Defense のいずれかの物理インターフェイスを介してループバック IP アドレスに到達できます。Firewall Threat Defense では、ループバック インターフェイスを指定するスタティックルートを設定できません。

### 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

### ファイアウォール モード

- ルータモードのみでサポートされます。

### 高可用性 とクラスターリング

- クラスターリングはサポートされません。

### その他のガイドラインと制限事項

- 物理インターフェイスからループバック インターフェイスへのトラフィックでは、TCP シーケンスのランダム化は常に無効になっています。

## 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 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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 ルータモード インターフェイスのパラメータを設定します。「[ルータモードのインターフェイスの設定](#) (45 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) [オブジェクト (Objects)] > [オブジェクト管理 (Object Management)] を選択し、コンテンツテーブルから [アクセスコントロールリスト (Access Control Lists)] > [拡張 (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

New Extended Access List Object

Name  
rate-limiting

Entries (0)

?

Add

- 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

Edit Extended Access List Object

Name  
rate-limiting

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	any	Any	10.1.1.1 10.2.1.1	Any	Any	Any	Any

☐ Allow Overrides

Cancel Save

**ステップ 2** [ポリシー (Policy)] > [アクセス制御 (Access Control)] > [アクセス制御 (Access Control)] の順に選択し、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[編集 (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

in-out ✎

Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control → More

Advanced Settings  
HTTP Responses  
Inheritance Settings  
Logging

Name	Action	Zones	Source	Networks
Mandatory (1 - 1)				

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

図 9: Threat Defense サービス ポリシー

Threat Defense Service Policy

Threat Defense Service Rule(s)

0

**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: [ルールを追加 (Add Rule)]

Threat Defense Service Policy

By default, traffic undergoes deep packet inspection as part of AC policy evaluation. However, for the TCP State Bypass feature to be effective, it is recommended to avoid deep packet inspection by configuring a pre-filter fastpath rule corresponding to TCP state bypass traffic

**Add Rule**

#	Interface Object	Traffic Flow	Connection Setting
<b>Interfaces</b>			
	No Rules		
<b>Global</b>			
	No Rules		

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

Threat Defense Service Policy

1 Interface Object

☒ Global

☐ Select Interface Objects

- 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

Threat Defense Service Policy

1 Interface Object 2 Traffic Flow

Extended Access List:

rate-limiting

- 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

Threat Defense Service Policy

1 Interface Object 2 Traffic Flow 3 Connection Setting

☐ Enable TCP State Bypass ☒ Randomize TCP Sequence Number ☐ Enable Decrement TTL

Connections:

	Maximum TCP & UDP	Maximum Embryonic
	24	12

Connections Per Client:

	Maximum TCP & UDP	Maximum Embryonic
	0	0

[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と 802.1Q トランキングの設定

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

- Firepower 1010 : VLAN サブインターフェイスは、スイッチポートおよび VLAN インターフェイスで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カ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 トランッキング 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ッ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。

## デバイス モデルによる VLAN サブインターフェイスの最大数

デバイス モデルにより、設定できる VLAN サブインターフェイスの最大数が制限されます。データ インターフェイスでのみサブインターフェイスを設定することができ、管理インターフェイスでは設定できないことに注意してください。

次の表で、各デバイス モデルの制限について説明します。

モデル	VLAN サブインターフェイスの最大数
Firepower 1010	60
Firepower 1120	512
Firepower 1140、1150	1024
Firepower 2100	1024
Cisco Secure Firewall 3100	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。[コンテナ インスタンスの VLAN サブインターフェイスの追加](#)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 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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

**Add Sub Interface**

General IPv4 IPv6 Path Monitoring Advanced

Name:  
inside-100

☒ Enabled  
☐ Management Only

Description:

Security Zone:  
inside\_zone

MTU:  
1500  
(64 - 9198)

Priority:  
0  
(0 - 65535)

Propagate Security Group Tag: ☐

Interface \*:  
Ethernet1/1

☒ Enabled

Sub-Interface ID \*:  
100  
(1 - 4294967295)

VLAN ID:  
100  
(1 - 4094)

Cancel OK

- [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。
- [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。
- [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。

**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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

**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 \(45 ページ\)](#) または [ブリッジグループインターフェイスの設定 \(51 ページ\)](#) 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。

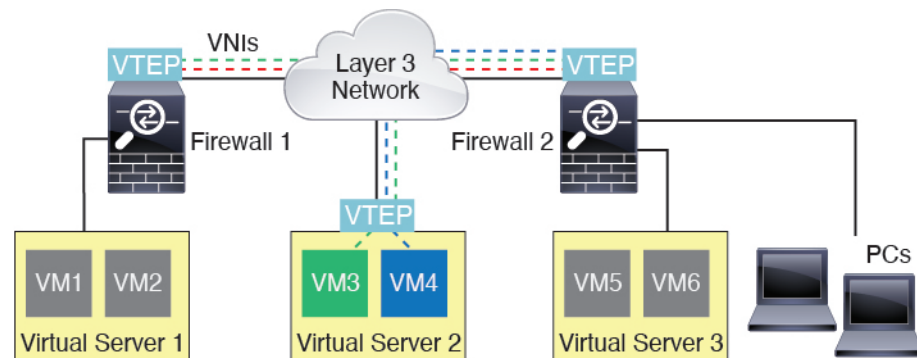
- **VXLAN (すべてのモデル)** : VXLAN は、MAC Address-in-User Datagram Protocol (MAC-in-UDP) のカプセル化を使用します。元のレイヤ 2 フレームに VXLAN ヘッダーが追加され、UDP-IP パケットに置かれます。
- **Geneve (Firewall Threat Defense Virtual のみ)** : Geneve には、MAC アドレスに限定されない柔軟な内部ヘッダーがあります。Geneve カプセル化は、Amazon Web Services (AWS) ゲートウェイロードバランサとアプライアンス間の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

カプセル化解除については、次の場合に ASA によって Geneve 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 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。  
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。
- 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。  
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。
- 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。

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。

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。

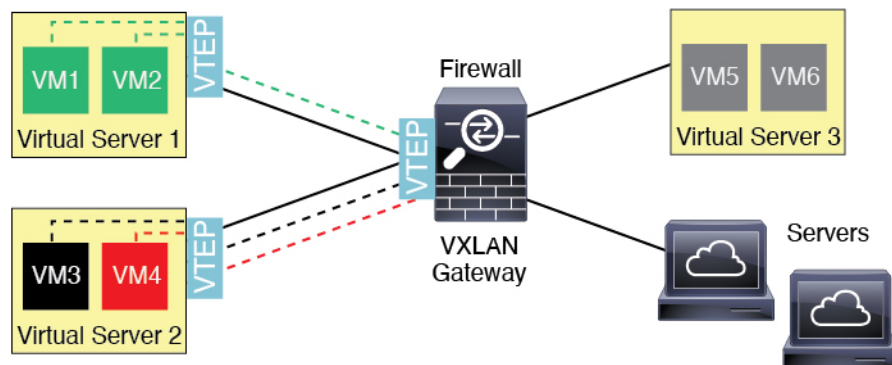
## VXLAN 使用例

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

各 Firewall Threat Defense の VTEP は、VM、サーバ、PC、VXLAN のオーバーレイ ネットワークなどのエンドノード間のブリッジまたはゲートウェイとして機能します。VTEP 送信元インターフェイスを介して VXLAN カプセル化で受信した受信フレームの場合、Firewall Threat Defense は VXLAN ヘッダーを除去して、内部イーサネット フレームの宛先 MAC アドレスに基づいて非 VXLAN ネットワークに接続されている物理インターフェイスに転送します。

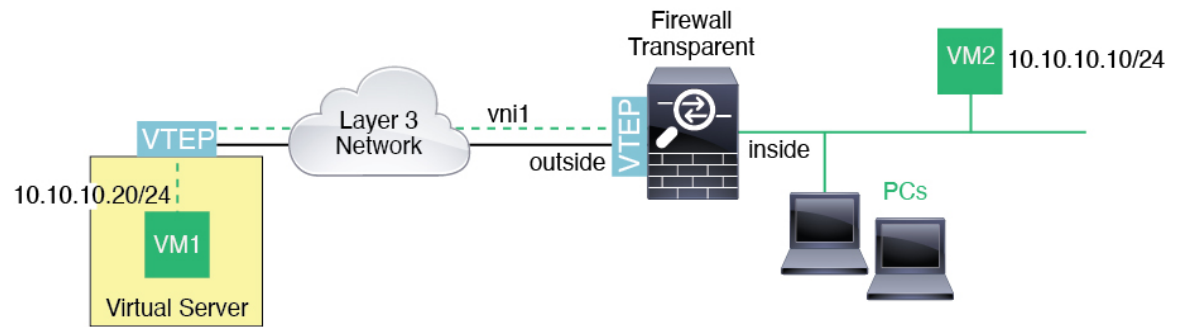
Firewall Threat Defense は、常に VXLAN パケットを処理します。つまり、他の 2 つの VTEP 間で VXLAN パケットをそのまま転送する訳ではありません。



### VXLAN ブリッジ

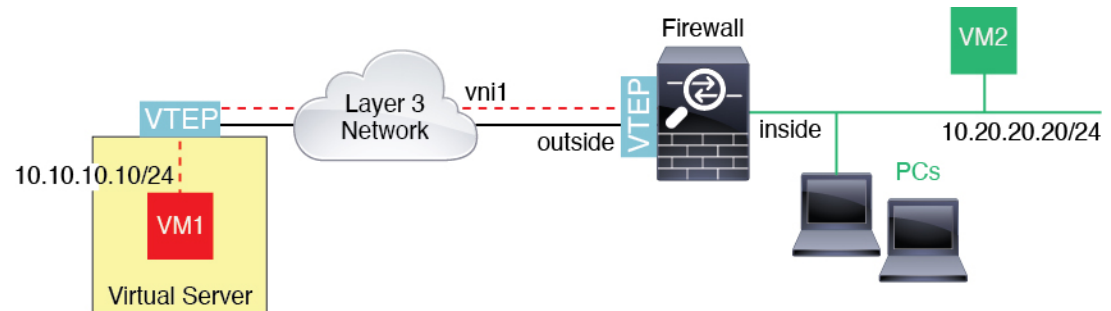
ブリッジグループ（トランスパレント ファイアウォール モードまたは任意ルーテッドモード）を使用する場合、Firewall Threat Defense は、同じネットワークに存在する（リモート）VXLAN セグメントとローカルセグメント間の VXLAN ブリッジとして機能できます。この場合、ブリッジグループのメンバーは通常インターフェイス 1 つのメンバーが通常のインターフェイスで、もう 1 つのメンバーが VNI インターフェイスです。

## VXLAN ゲートウェイ (ルーテッドモード)



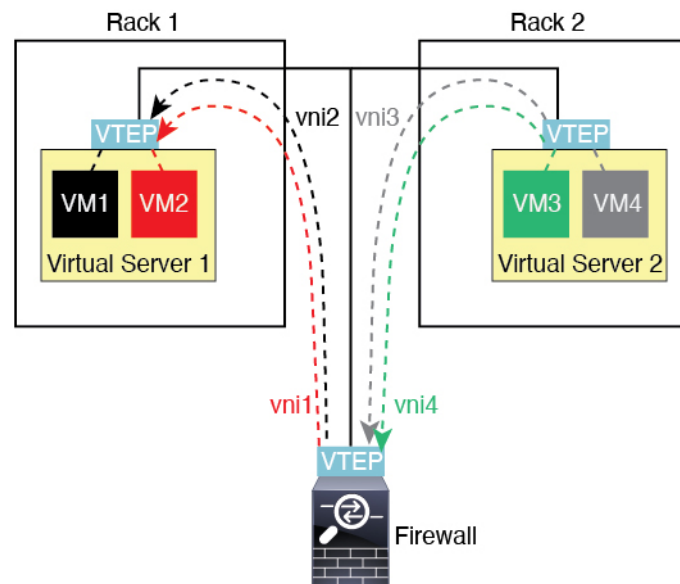
## VXLAN ゲートウェイ (ルーテッドモード)

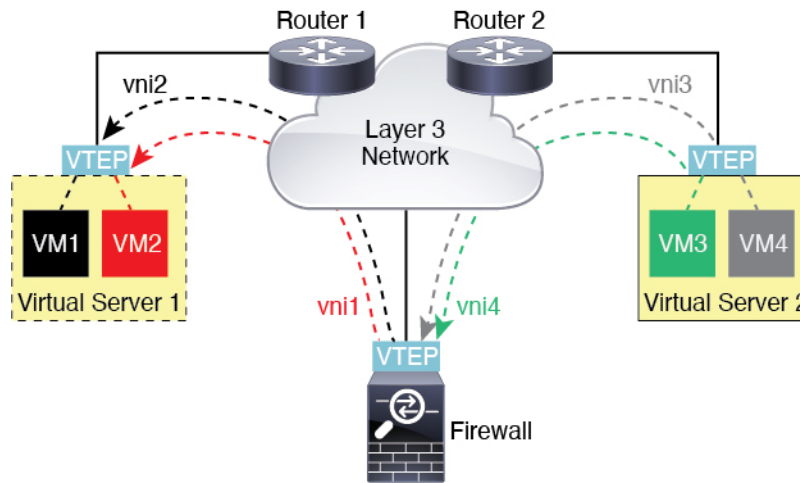
Firewall Threat Defense は、VXLAN ドメインと非 VXLAN ドメイン間のルータとして機能し、異なるネットワーク上のデバイスを接続します。



## VXLAN ドメイン間のルータ

VXLAN 拡張 レイヤ 2 ドメインを使用すると、VM は、Firewall Threat Defense が同じラックにないとき、あるいは Firewall Threat Defense がレイヤ 3 ネットワーク上の離れた場所にあるときに s のゲートウェイとして Firewall Threat Defense を指し示すことができます。





このシナリオに関する次の注意事項を参照してください。

1. VM3 から VM1 へのパケットでは、Firewall Threat Defense がデフォルトゲートウェイであるため、宛先 MAC アドレスは Firewall Threat Defense の MAC アドレスです。
2. 仮想サーバー 2 の VTEP 送信元インターフェイスは、VM3 からパケットを受信してから、VNI 3 の VXLAN タグでパケットをカプセル化して Firewall Threat Defense に送信します。
3. Firewall Threat Defense は、パケットを受信すると、そのパケットをカプセル化解除して内部フレームを取得します。
4. Firewall Threat Defense は、ルートルックアップに内部フレームを使用して、宛先が VNI 2 上であることを認識します。VM1 のマッピングがまだない場合、Firewall Threat Defense は、VNI 2 カプセル化された ARP ブロードキャストを VNI 2 のマルチキャストグループ IP で送信します。



(注) このシナリオでは複数の VTEP ピアがあるため、Firewall Threat Defense は、複数のダイナミック VTEP ピア ディスカバリを使用する必要があります。

5. Firewall Threat Defense は、VNI 2 の VXLAN タグでパケットを再度カプセル化し、仮想サーバー 1 に送信します。カプセル化の前に、Firewall Threat Defense は、内部フレームの宛先 MAC アドレスを変更して VM1 の MAC にします (Firewall Threat Defense で VM1 の MAC アドレスを取得するためにマルチキャスト カプセル化 ARP が必要な場合があります)。
6. 仮想サーバー 1 は、VXLAN パケットを受信すると、パケットをカプセル化解除して内部フレームを VM1 に配信します。

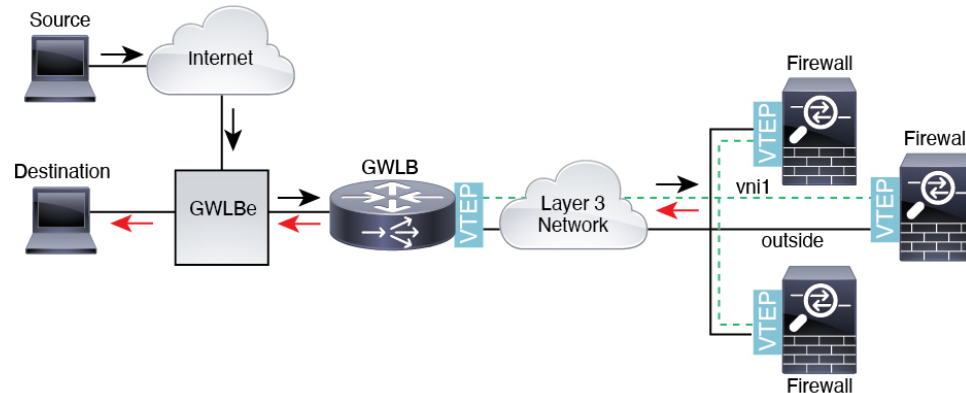
## Geneve シングルアームプロキシの使用例



(注) この使用例は、現在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。

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と、トラフィックを分散し、仮想アプライアンスをオンデマンドで拡張するロードバランサを組み合わせます。Firewall Threat Defense Virtual は、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、ゲートウェイロードバランサのエンドポイントから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、ゲートウェイロードバランサに送り返す（U ターントラフィック）前に検査します。ゲートウェイロードバランサは、トラフィックをゲートウェイロードバランサのエンドポイントと宛先に送り返します。

図 15: Geneve シングルアームプロキシ

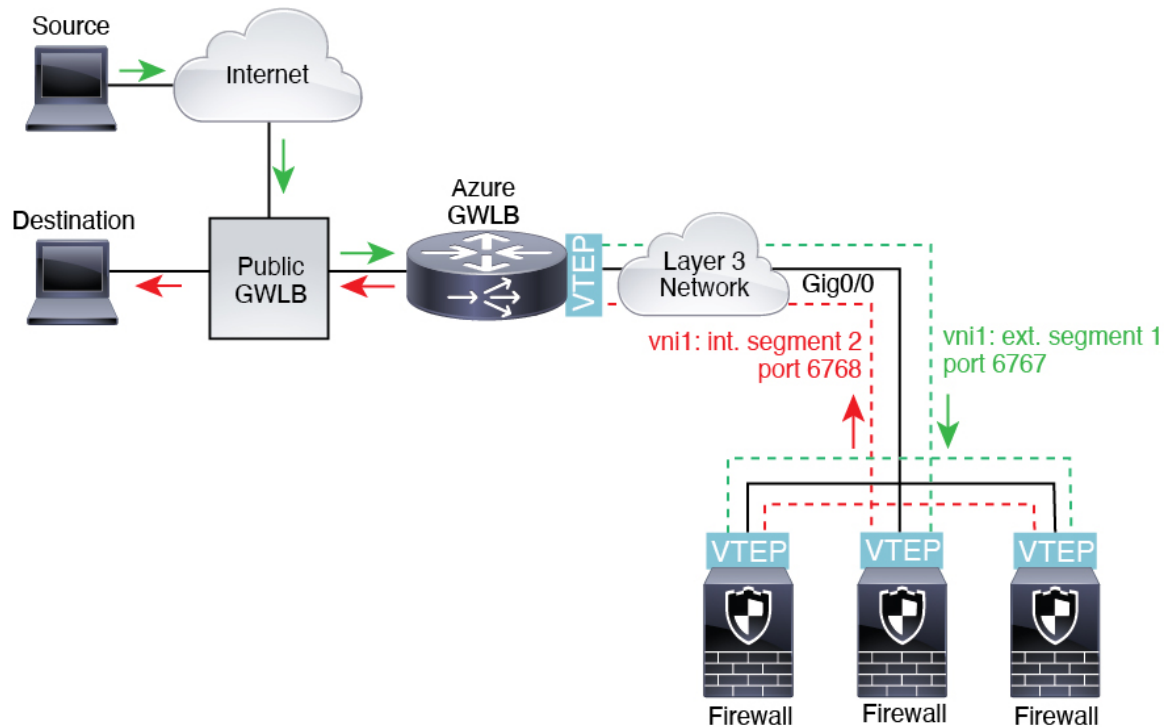


## Azure ゲートウェイロードバランサおよびペアプロキシ

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 16: 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 : 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。
- VTEP 送信元インターフェイス IP アドレスは、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 バイト未満の場合、Firewall Threat Defense は自動的に MTU を 1,554 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 \(38 ページ\)](#) 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 \(35 ページ\)](#)。
2. [VNI インターフェイスの設定 \(37 ページ\)](#)。
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 \(40 ページ\)](#)。

### 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** [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。

**ステップ 3** VXLAN を設定するデバイスの横にある [編集 (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 [編集 (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 バイト未満の場合、Firewall Management Center は自動的に MTU を 1554 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 VTEP 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** [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。
- ステップ 2** VXLAN を設定するデバイスの横にある [編集 (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 \(41 ページ\)](#)」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 \(35 ページ\)](#)」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 \(38 ページ\)](#)。
2. [VNI の設定 \(39 ページ\)](#)。
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 \(40 ページ\)](#)。

### 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** [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。

**ステップ 2** Geneve を設定するデバイスの横にある [編集 (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** [デバイス (Devices)] > [デバイス管理 (Device Management)] の順に選択します。
- ステップ 2** Geneve を設定するデバイスの横にある [編集 (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が有効になり、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ことができます (Uターントラフィック)。後でインターフェ

イスを編集する場合、シングルアームプロキシを無効にすることはできません。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 インターフェイス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** [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 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。

---

### 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 ～ 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。「[スタティック手動 NAT の設定](#)」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。

## デュアル IP スタック (IPv4 および IPv6)

Firewall Threat Defense デバイスは、インターフェイスで IPv6 アドレスと IPv4 アドレスの両方をサポートしています。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

## 31 ビット サブネット マスク

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 Firewall Threat Defense 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、ブロードキャストは必要ありません。また、SNMP または 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。

### 31 ビットのサブネットとクラスタリング

管理インターフェイスとクラスタ制御リンクを除き、クラスタインターフェイスの 31 ビットのサブネットマスクを使用できます。

### 31 ビットのサブネットとフェールオーバー

フェールオーバーに関しては、Firewall Threat Defense インターフェイスの IP アドレスに 31 ビットのサブネットを使用した場合、アドレスが不足しているため、インターフェイス用のスタンバイ IP アドレスは設定できません。通常、アクティブなユニットがインターフェイスのテストを実行し、スタンバイのインターフェイスの健全性を保証できるよう、フェールオーバー インターフェイスはスタンバイ IP アドレスを必要とします。スタンバイ IP アドレスがないと、Firewall Threat Defense はネットワークのテストを実行できず、リンクステートのみしか追跡できません。

ポイントツーポイント接続であるフェールオーバーと任意のステートリンクでは、31 ビットのサブネットも使用できます。

### 31 ビットのサブネットと管理

直接接続される管理ステーションがあれば、Firewall Threat Defense 上で SSH または HTTP にポイントツーポイント接続を、または管理ステーション上で SNMP または Syslog にポイントツーポイント接続をそれぞれ使用できます。

### 31 ビットのサブネットをサポートしていない機能

次の機能は、31 ビットのサブネットをサポートしていません。

- ブリッジグループ用 BVI インターフェイス - ブリッジグループには BVI、2 つのブリッジグループ メンバーに接続された 2 つのホスト用に、少なくとも 3 つのホスト アドレスが必要です。/29 サブネット以下を使用する必要があります。
- マルチキャスト ルーティング

## ルーテッドモードおよびトランスペアレントモードのインターフェイスに関するガイドラインと制限事項

### 高可用性、クラスタリング、およびマルチインスタンス

- フェールオーバー リンクは、この章の手順で設定しないでください。詳細については、「高可用性」の章を参照してください。
- クラスターインターフェイスの場合は、クラスタリングの章で要件を確認してください。
- マルチインスタンスモードの場合、共有インターフェイスはブリッジグループ メンバー インターフェイス（トランスペアレントモードまたはルーテッドモード）ではサポートされません。
- 高可用性を使用する場合、データ インターフェイスの IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。[モニター対象インターフェイス (Monitored Interfaces)] 領域の [デバイス (Devices)] > [デバイス管理 (Device Management)] > [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。詳細については、高可用性の章も参照してください。

### IPv6

- IPv6 はすべてのインターフェイスでサポートされます。
- トランスペアレント モードでは、IPv6 アドレスは手動でのみ設定できます。
- Firewall Threat Defense デバイスは、IPv6 エニーキャスト アドレスはサポートしません。
- DHCPv6 およびプレフィックス委任オプションは、トランスペアレントモード、クラスタリング、または 高可用性 ではサポートされません。

### モデルのガイドライン

- ブリッジされた ixgbevf インターフェイスを持つ VMware 上の Firewall Threat Defense Virtual では、のブリッジグループはサポートされません。
- FirePOWER 2100 シリーズでは、ルーテッドモードのブリッジグループはサポートされません。

## トランスペアレントモードとブリッジグループのガイドライン

- 64のインターフェイスをもつブリッジグループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- Firewall Threat Defense デバイスでは、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVIIP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- デバイスとデバイス間の管理トラフィック、および Firewall Threat Defense デバイス を通過するデータトラフィックの各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv4 トラフィックの場合は、IPv4 アドレスを指定します。IPv6 トラフィックの場合は、IPv6 アドレスを指定します。
- IPv6 アドレスは手動でのみ設定できます。
- BVIIP 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。サブネットにホスト サブネット (255.255.255.255) を設定することはできません。
- 管理インターフェイスはブリッジグループのメンバーとしてサポートされません。
- マルチインスタンスモードの場合、共有インターフェイスはブリッジグループ メンバー インターフェイス (トランスペアレントモードまたはルーテッドモード) ではサポートされません。
- ブリッジされた ixgbevf インターフェイスを備えた VMware の Firewall Threat Defense Virtual の場合、トランスペアレントモードはサポートされておらず、ブリッジグループはルーテッドモードではサポートされていません。
- Firepower 2100 シリーズ では、ルーテッド モードのブリッジグループはサポートされません。
- Firepower 1010 では、同じブリッジグループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。
- Firepower 4100/9300 では、データ共有インターフェイスはブリッジグループのメンバーとしてサポートされません。
- トランスペアレントモードでは、少なくとも 1 つのブリッジグループを使用し、データインターフェイスがブリッジグループに属している必要があります。
- トランスペアレントモードでは、接続されたデバイス用のデフォルトゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは Firewall Threat Defense の他方側のルータをデフォルトゲートウェイとして指定する必要があります。
- トランスペアレントモードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジグループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジグループのインターフェイスとブリッジグループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジグループ ネットワークから

の管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。

- トランスペアレントモードでは、PPPoE は Diagnostic インターフェイスでサポートされません。
- 透過モードは、Amazon Web Services、Microsoft Azure、Google Cloud Platform、および Oracle Cloud Infrastructure にデプロイされた脅威防御仮想インスタンスではサポートされていません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッドモードでは、Firewall Threat Defense 定義の EtherChannel インターフェイスがブリッジグループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジグループメンバーにすることができます。
- Bidirectional Forwarding Detection (BFD) エコー パケットは、ブリッジグループ メンバを使用するときに、Firewall Threat Defense を介して許可されません。BFD を実行している Firewall Threat Defense の両側に 2 つのネイバーがある場合、Firewall Threat Defense は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

#### その他のガイドラインと要件

- Firewall Threat Defense では、ファイアウォールインターフェイスについては、パケットで 802.1Q ヘッダーが 1 つだけサポートされ、複数のヘッダー (Q-in-Q) はサポートされません。注：インラインセットとパッシブインターフェイスについては、FTD で Q-in-Q がサポートされ、パケットで 802.1Q ヘッダーが 2 つまでサポートされます。ただし、Firepower 4100/9300 は例外で、802.1Q ヘッダーは 1 つだけサポートされます。
- 頻繁なアップ/ダウンステータスの変化などのインターフェイスの問題があると、フローティング接続タイマーが、インターフェイスを通過する接続に正しく適用されない場合があります。インターフェイスのステータスに問題がある場合は、無効な接続をクリアするため、ステータスが安定した後にすべての接続をクリアすることを検討してください。

## ルーテッドモードのインターフェイスの設定

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. 物理インターフェイスの設定

## 2. (任意) 特別なインターフェイスを設定します。

- [EtherChannel \(ポート チャンネル\) の追加](#)
  - [コンテナ インスタンスの VLAN サブインターフェイスの追加](#) 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 \(35 ページ\)](#)
- (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 \(35 ページ\)](#)
  - AWS 上の Firewall Threat Defense Virtual : [Geneve インターフェイスの設定 \(38 ページ\)](#)
  - Firepower 1010 : [VLAN インターフェイスの設定 \(6 ページ\)](#)

## 手順

- 
- ステップ 1** [デバイス (Devices) ]>[デバイス管理 (Device Management) ]を選択し、Firewall Threat Defense デバイス[編集 (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 [編集 (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 \(75 ページ\)](#) 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。[モニター対象インターフェイス (Monitored Interfaces) ] エリアの [デバイス (Devices) ] > [デバイス管理 (Device Management) ] > [ハイスレディビリティ (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 ユニティはネットワーク 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 ステータスをトラッキング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 \(56 ページ\)](#) 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 \(77 ページ\)](#) 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)。(Cisco Secure Firewall 3100 のみ) [SFPを検出 (Detect SFP)] を選択してインストールされている SFP モジュールの速度を検出し、適切な速度を使用します。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。

(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)] : 速度、リンクステータス、およびフロー制御をネゴシエートするようにインターフェイスを設定します。
- [前方誤り訂正モード (Forward Error Correction Mode)] : (Cisco Secure Firewall 3100 のみ) 25 Gbps 以上のインターフェイスの場合は、前方誤り訂正 (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。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 74 条 FC-FEC	第 108 条 RS-FEC
25G-LR	第 74 条 FC-FEC	第 108 条 RS-FEC
10/25G-CSR	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-AOCxM	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

**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、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。
- ハイアベイラビリティ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 17: 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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## 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 デバイス 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、[ブリッジグループについて](#)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 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. [物理インターフェイスの設定](#)
  2. （任意）特別なインターフェイスを設定します。
    - [EtherChannel（ポートチャネル）の追加](#)
    - [コンテナインスタンスのVLANサブインターフェイスの追加](#) 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 : VLAN インターフェイスの設定（6 ページ）](#)

### 手順

- 
- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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 [編集 (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 \(75 ページ\)](#) 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)。(Cisco Secure Firewall 3100 のみ) [SFPを検出 (Detect SFP)] を選択してインストールされている SFP モジュールの速度を検出し、適切な速度を使用します。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。

(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)] : 速度、リンクステータス、およびフロー制御をネゴシエートするようにインターフェイスを設定します。
- [前方誤り訂正モード (Forward Error Correction Mode)] : (Cisco Secure Firewall 3100 のみ) 25 Gbps 以上のインターフェイスの場合は、前方誤り訂正 (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。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 74 条 FC-FEC	第 108 条 RS-FEC
25G-LR	第 74 条 FC-FEC	第 108 条 RS-FEC
10/25G-CSR	第 74 条 FC-FEC	第 74 条 FC-FEC
25G-AOCxM	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

- ステップ 11 (任意) [IPv6 アドレスの設定 \(56 ページ\)](#) 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 \(77 ページ\)](#) 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、**[展開 (Deploy)]** > **[展開 (Deployment)]** をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## 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。BVIIP 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、BVIIP 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。




(注) 個別の Diagnostic インターフェイスでは、設定できないブリッジグループ (ID 301) は、設定に自動的に追加されます。このブリッジグループはブリッジグループの制限に含まれません。



## 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 [デバイス (Devices) ]>[デバイス管理 (Device Management) ] を選択し、Firewall Threat Defense デバイス[編集 (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、[モニター対象インターフェイス (Monitored Interfaces) ] エリアの [デバイス (Devices) ]>[デバイス管理 (Device Management) ]>[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 ユニットのネットワーク 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 ステータスをトラッキング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。[モニター対象インターフェイス (Monitored Interfaces)] エリアの [デバイス (Devices)] > [デバイス管理 (Device Management)] > [ハイアベイラビリティ (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キング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 \(56 ページ\)](#) 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 \(78 ページ\)](#) 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 \(79 ページ\)](#) (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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## 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。

### IPv6 について

このセクションには、IPv6 に関する情報が含まれています。

#### IPv6 アドレッシング

IPv6 に対して次の 2 種類のユニキャストアドレスを設定できます。



- **グローバル**：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。ブリッジ グループの場合、このアドレスは各メンバー インターフェイスごとに設定するのではなく、BVI用に設定する必要があります。また、トランスペアレント モードで管理インターフェイスのグローバルな IPv6 アドレスを設定することもできます。
- **リンクローカル**：リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワークセグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決などのネイバー探索機能に使用できます。ブリッジ グループでは、メンバー インターフェイスのみがリンクローカル アドレスを所有しています。BVI にはリンクローカル アドレスはありません。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に設定する必要はありません。ブリッジ グループ インターフェイスでは、BVI でグローバル アドレスを設定した場合、Firewall Threat Defense デバイスが自動的にメンバー インターフェイスのリンクローカル アドレスを生成します。グローバル アドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

## Modified EUI-64 インターフェイス ID

RFC 3513 「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネット プロトコルバージョン6 アドレッシングアーキテクチャ）では、バイナリ値 000 で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。Firewall Threat Defense デバイスでは、ローカル リンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスで有効化されていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

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

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカルリンク上のホストに対してのみ実行できます。

## IPv6 プレフィックス委任クライアントの設定

Firewall Threat Defense は、（ケーブルモデムに接続された外部インターフェイスなどの）クライアント インターフェイスが 1 つ以上の IPv6 プレフィックスを受け取れるように DHCPv6 プレフィックス委任クライアントとして機能することができ、Firewall Threat Defense はそのプレフィックスをサブネット化して内部インターフェイスに割り当てることが可能です。

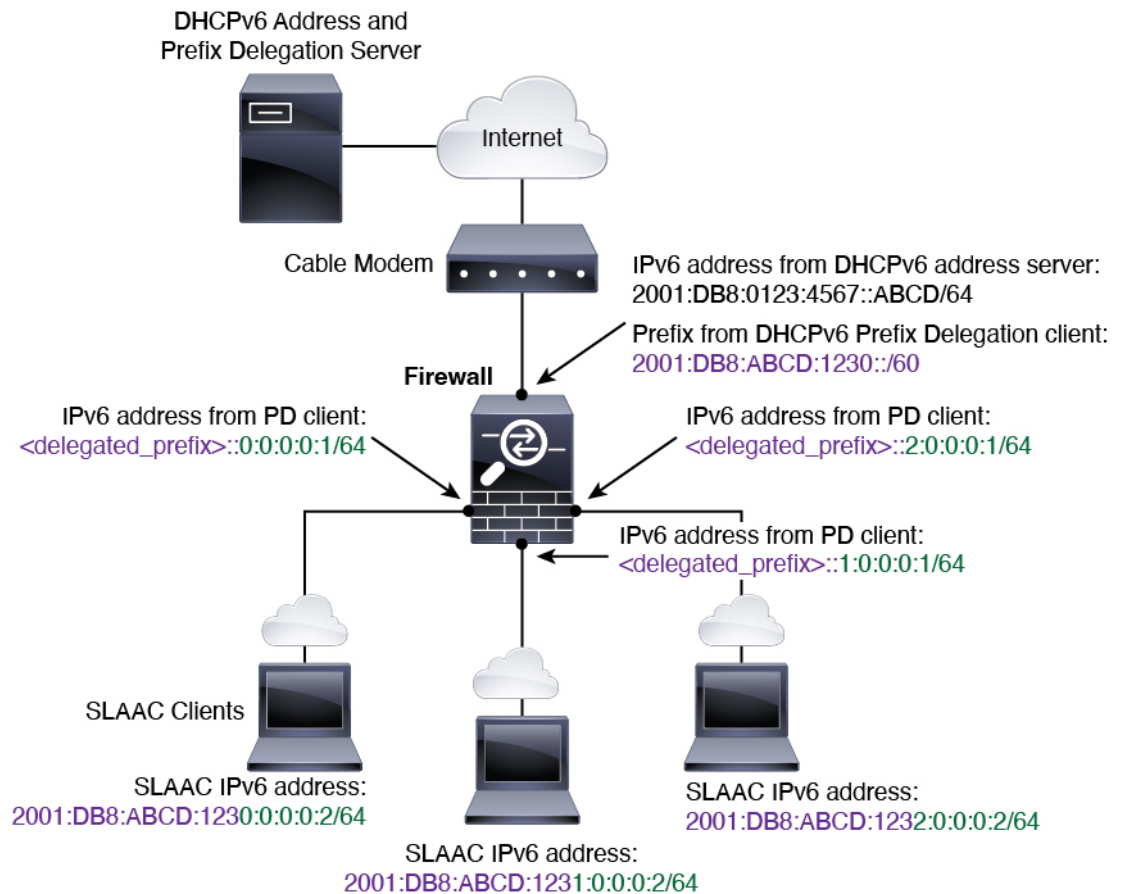
## IPv6 プレフィックス委任の概要

Firewall Threat Defense は、（ケーブルモデムに接続された外部インターフェイスなどの）クライアントインターフェイスが 1 つ以上の IPv6 プレフィックスを受け取れるように DHCPv6 プレフィックス委任クライアントとして機能することができ、Firewall Threat Defense はそのプレフィックスをサブネット化して内部インターフェイスに割り当てることが可能です。これにより、内部インターフェイスに接続されているホストは、StateLess Address Auto Configuration（SLAAC）を使用してグローバル IPv6 アドレスを取得できます。ただし、内部 Firewall Threat Defense インターフェイスはプレフィックス委任サーバーとして機能しないため注意してください。Firewall Threat Defense は、SLAAC クライアントにグローバル IP アドレスを提供することしかできません。たとえば、ルータが Firewall Threat Defense に接続されている場合、ASA は SLAAC クライアントとして機能し、IP アドレスを取得できます。しかし、ルータの背後のネットワークに代理プレフィックスのサブネットを使用したい場合、ルータの内部インターフェイス上でそれらのアドレスを手動で設定する必要があります。

Firewall Threat Defense には軽量 DHCPv6 サーバーが含まれており、SLAAC クライアントが情報要求（IR）パケットを Firewall Threat Defense に送信した場合、Firewall Threat Defense は DNS サーバーやドメイン名などの情報を SLAAC クライアントに提供できます。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。クライアントが独自の IPv6 アドレスを生成するように設定するには、クライアントで IPv6 自動設定を有効にします。クライアントでステートレスな自動設定を有効にすると、ルータアドバタイズメントメッセージで受信したプレフィックス（Firewall Threat Defense がプレフィックス委任を使用して受信したプレフィックス）に基づいて IPv6 アドレスが設定されます。

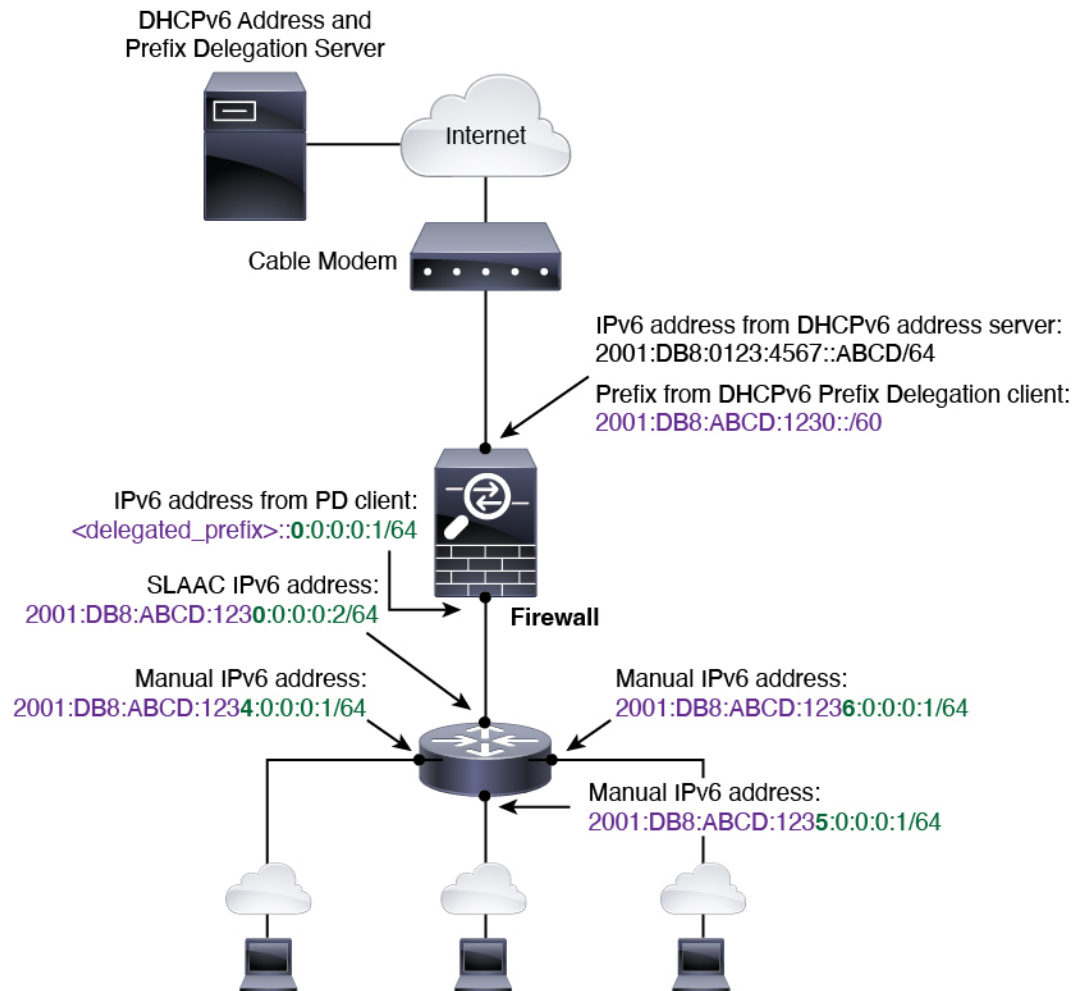
### IPv6 プレフィックス委任 /64 サブネットの例

次の例では、Firewall Threat Defense が DHCPv6 アドレスクライアントを使用して、外部インターフェイス上で IP アドレスを受け取ることを示しています。また、ASA は DHCPv6 プレフィックス委任クライアントを使用して代理プレフィックスを取得します。Firewall Threat Defense は、委任されたプレフィックスを /64 ネットワークにサブネット化し、委任されたプレフィックスと手動で設定されたサブネット（::0、::1、または ::2）と各インターフェイスの IPv6 アドレス（0:0:0:1）を使用して、動的に内部インターフェイスにグローバル IPv6 アドレスを割り当てます。これらの内部インターフェイスに接続されている SLAAC クライアントは、各 /64 サブネットの IPv6 アドレスを取得します。



#### IPv6 プレフィックス委任 /62 サブネットの例

次の例は、Firewall Threat Defense が 4/62 サブネットにプレフィックスをサブネット化するところを示しています。2001:DB8:ABCD:1230::/62、2001:DB8:ABCD:1234::/62、2001:DB8:ABCD:1238::/62、2001:DB8:ABCD:123C::/62。Firewall Threat Defense は、内部ネットワーク (::0) に 2001:DB8:ABCD:1230::/62 の利用可能な 64 サブネット 4 つのいずれかを使用します。ダウンストリーム ルータには、手動で追加の /62 サブネットを使用できます。図のルータは、内部インターフェイス (::4, ::5, and ::6) に 2001:DB8:ABCD:1234::/62 の利用可能な 4 つの /64 サブネットのうちの 3 つを使用します。この場合、内部ルータインターフェイスは委任されたプレフィックスを動的に取得できないため、Firewall Threat Defense 上で委任されたプレフィックスを表示し、ルータ設定にそのプレフィックスを使用する必要があります。通常、リースが期限切れになった場合、ISP は既定のクライアントに同じプレフィックスを委任しますが、Firewall Threat Defense が新しいプレフィックスを受け取った場合、新しいプレフィックスを使用するようルータ設定を変更する必要があります。DHCP の一意識別子 (DUID) は、再起動後も存続します。



## 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 プレフィッ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（66 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** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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 [編集 (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 18: プレフィックス委任クライアントの有効化

● Client PD Prefix Name

Outside-Prefix

Client PD Hint Prefixes

2001:DB8:ABCD:1230::/60

Add

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、特定のプレフィックス長 (::/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 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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## 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 \(77 ページ\)](#) 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** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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 [編集 (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。[IPv6]>[設定 (Settings)]>[RA の有効化 (Enable RA)] チェックボックスをオフにして、メッセージを抑制します。

- 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) 高可用性のために、[モニター対象インターフェイス (Monitored Interfaces)] 領域の [デバイス (Devices)]>[デバイス管理 (Device Management)]>[高可用性 (High Availability)] ページでスタンバイ 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 ユニットのネットワーク 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 ステートをトラッキング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 19: DHCPv6 クライアントの有効化

Edit Physical Interface					
General		IPv4	IPv6	Path Monitoring	Hardware
Basic		Address	Prefixes	Settings	DHCP
<input checked="" type="checkbox"/>	Enable DHCP Client				<input type="checkbox"/> Enable
<input checked="" type="checkbox"/>	Enable default route using DHCP				<input type="checkbox"/> Enable

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の有効にする (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 (60 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 20: 委任されたプレフィックスの使用

The screenshot shows the 'Edit Physical Interface' configuration page. The 'IPv6' tab is selected, and the 'DHCP' sub-tab is active. A table is present with columns 'Prefix Name' and 'Prefix Length'. A red box highlights the '+ Add' button in the bottom right corner of the table area. Below the table, it says 'No records to display'.



3. 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ックスは /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ックスが 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ックスは 2001:DB8:1234:5671::/64 です。この例では、プレフィックスが /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、プレフィックスが 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。



## 4. [OK] をクリックします。

図 21: プレフィックス委任テーブル

+ Add		
Prefix Name	Prefix Length	
Outside-Prefix	::1:0:0:0:1/64	 

5. 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:feec: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 \(66 ページ\)](#)」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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## 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 \(62 ページ\)](#)」を参照してください。

## 手順

- ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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 [編集 (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せん。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、インターフェイス上で IPv6 パケットの処理は無効になります。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 (ICMPv6 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あるインターフェイス (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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## 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。

## インターフェイスの詳細設定について

ここでは、インターフェイスの詳細設定について説明します。

## MAC アドレスについて

手動でMACアドレスを割り当てて、デフォルトを上書きすることができます。コンテナインスタンスの場合、FXOS シャーシはすべてのインターフェイスに対して一意の MAC アドレスを自動的に生成します。



- (注) 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ができます。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て、一意の IPv6 リンクローカルアドレスが可能になり、Firewall Threat Defense デバイスで特定のインスタンスでのトラフィックの中断を回避できます。



- (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。

### デフォルトの MAC アドレス

#### ネイティブインスタンスの場合：

デフォルトのMACアドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスでは、Burned-In MAC Address を使用します。
- VLAN インターフェイス（Firepower 1010 および）：ルーテッドファイアウォールモード：すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。[MAC アドレスの設定（77 ページ）](#) を参照してください。

トランスペアレントファイアウォールモード：各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。[MAC アドレスの設定（77 ページ）](#) を参照してください。

- EtherChannel（Firepower モデル）：EtherChannel の場合、そのチャネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対して透過的になります。ネットワークアプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないからです。ポートチャネルインターフェイスは、プールにある一意の MAC アドレスを使用します。インターフェイス メンバーシップは MAC アドレスに影響しません。

- **EtherChannel (ASA モデル)** : ポートチャネルインターフェイスは、最も小さいチャネルグループ インターフェイスの MAC アドレスをポートチャネル MAC アドレスとして使用します。または、ポートチャネルインターフェイスの MAC アドレスを設定することもできます。グループ チャネル インターフェイスのメンバーシップが変更された場合に備えて、一意の MAC アドレスを設定することをお勧めします。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。
- **サブインターフェイス(Firewall Threat Defense 定義)**: 物理インターフェイスのすべてのサブインターフェイスは同じ Burned-In MAC Address を使用します。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必要がある場合があります。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。

#### コンテナインスタンスの場合 :

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

## MTU について

MTU は、Firewall Threat Defense デバイスが特定のイーサネットインターフェイスで送信可能な最大フレームペイロードサイズを指定します。MTU の値は、イーサネットヘッダー、VLAN タギング、またはその他のオーバーヘッドを含まないフレーム サイズです。たとえば、MTU を 1500 に設定すると、予想されるフレーム サイズはヘッダーを含めて 1518 バイトで、VLAN を使用する場合は 1522 です。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

Geneve については、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 IP パケットは大きくなり、より大きな MTU が必要となります。そのため、ASA VTEP 送信元インターフェイスの 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。

#### パス MTU ディスカバリ

Firewall Threat Defense デバイスは、Path MTU Discovery (RFC 1191 の定義に従う) をサポートします。つまり、2 台のホスト間のネットワーク パス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

#### デフォルト MTU

Firewall Threat Defense デバイスのデフォルト MTU は、1500 バイトです。この値には、イーサネットヘッダー、VLAN タギングや他のオーバーヘッド分の 18~22 バイトは含まれません。



## MTU とフラグメンテーション

IPv4 の場合、出力 IP パケットが、指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは送信先（場合によっては中継先）で組立て直されます。フラグメント化はパフォーマンス低下の原因となります。IPv6 の場合、通常、パケットのフラグメント化は許可されません。したがってフラグメント化を避けるために、IP パケットを MTU サイズ以内におさめる必要があります。

TCP パケットの場合、通常、エンドポイントが MTU を使用して、TCP 最大セグメントサイズ（たとえば、MTU - 40 など）を判別します。途中で TCP ヘッダーが追加される場合（たとえば、サイト間 VPN トンネルなど）、トンネリング エンティティによって TCP MSS を調整する必要があります。TCP MSS について（72 ページ）を参照してください。

UDP または ICMP の場合、アプリケーションは、フラグメンテーションを避けるために、MTU を考慮する必要があります。



（注） Firewall Threat Defense デバイスはメモリに空きがある限り、設定された MTU よりも大きいフレームを受信します。

## MTU とジャンボ フレーム

MTU が大きくなると、より大きなパケットを送信できます。大きなパケットはネットワークにとってより効率的です。次のガイドラインを参照してください。

- トラフィックパスの MTU の一致：すべての Firewall Threat Defense インターフェイスの MTU と、トラフィックパス上のその他のデバイスインターフェイスの MTU を同じ値に設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボフレームへの対応：ジャンボフレームが有効な場合、MTU を 9,000 バイト以上に設定できます。最大値はモデルによって異なります。

## TCP MSS について

TCP 最大セグメントサイズ (MSS) とは、あらゆる TCP と IP ヘッダーが追加される前の TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイ ハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

FlexConfig の Sysopt\_Basic オブジェクトを使用して」を参照してください。「FlexConfig ポリシー」を参照してください。デフォルトで、最大 TCP MSS は 1,380 バイトに設定されます。この設定は、Firewall Threat Defense デバイスが IPsec VPN カプセル化のパケットサイズを大きくする必要がある場合に役立ちます。ただし、非 IPsec エンドポイントでは、Firewall Threat Defense デバイスの最大 TCP MSS を無効化する必要があります。

最大 TCP MSS を設定すると、接続のいずれかのエンドポイントが Firewall Threat Defense デバイスで設定した値よりも大きな TCP MSS を要求した場合に、Firewall Threat Defense デバイスは要求パケットの TCP MSS を Firewall Threat Defense デバイスの最大値で上書きします。ホストやサーバが TCP MSS を要求しない場合、Firewall Threat Defense デバイスは RFC 793 のデ



フォルト値 536 バイト (IPv4) または 1220 バイト (IPv6) を想定しますが、パケットを変更することはありません。たとえば、MTU をデフォルトの 1500 バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。Firewall Threat Defense デバイスの最大 TCP MSS が 1380 (デフォルト) の場合は、Firewall Threat Defense デバイスは TCP 要求パケットの MSS 値を 1380 に変更します。サーバは、1380 バイトのペイロードを含むパケットを送信します。Firewall Threat Defense デバイスはさらに 120 バイトのヘッダーをパケットに追加しますが、それでも 1500 の MTU サイズに収まります。

TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、Firewall Threat Defense デバイスは値を調整します。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN 接続用を含む to-the-box トラフィックには、この設定は適用されません。Firewall Threat Defense デバイスは MTU を使用して、TCP MSS を導き出します。MTU - 40 (IPv4) または MTU - 60 (IPv6) となります。

## デフォルト TCP MSS

デフォルトでは、Firewall Threat Defense デバイスの最大 TCP MSS は 1380 バイトです。このデフォルトは、ヘッダーが最大 120 バイトの IPv4 IPsec VPN 接続に対応しています。この値は、MTU のデフォルトの 1500 バイト内にも収まっています。

## TCP MSS の推奨最大設定

デフォルトでは TCP MSS は、Firewall Threat Defense デバイスが IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。Firewall Threat Defense デバイスが IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして Firewall Threat Defense デバイスを使用しない場合は、FlexConfig の Sysopt\_Basic オブジェクトを使用して TCP MSS 設定を変更する必要があります。



- (注) MSS を明示的に設定した場合でも、TLS/SSL 復号やサーバ検出などのコンポーネントが特定の MSS を必要とする場合、その MSS はインターフェイス MTU に基づいて設定され、MSS 設定は無視されます。

次のガイドラインを参照してください。

- 通常のトラフィック：TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。一般に接続エンドポイントは MTU から TCP MSS を取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。
- IPv4 IPsec エンドポイントトラフィック：最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボフレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。

- IPv6 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 140 に設定します。

## ブリッジグループ トラフィックの ARP インспекション

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спекションをイネーブルにします。

ARP インспекションによって、悪意のあるユーザが他のホストやルータになります（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インспекションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARP インспекションを有効化すると、Firewall Threat Defense デバイスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、Firewall Threat Defense デバイスはパケットをドロップします。
- ARP パケットがスタティック ARP テーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッド）するか、またはドロップするように Firewall Threat Defense デバイスを設定できます。



(注) 専用の Diagnostic インターフェイスは、このパラメータが flood に設定されている場合でもパケットをフラッドしません。

## MAC アドレス テーブル

ブリッジグループを使用する場合、Firewall Threat Defense は、通常のブリッジまたはスイッチと同様に、MAC アドレスを学習して MAC アドレステーブルを作成します。デバイスがブリッジグループ経由でパケットを送信すると、Firewall Threat Defense が MAC アドレスをアドレステーブルに追加します。テーブルで MAC アドレスと発信元インターフェイスが関連付けられているため、Firewall Threat Defense は、パケットが正しいインターフェイスからデバイスにアドレス指定されていることがわかります。ブリッジグループ メンバー間のトラフィックには Firewall Threat Defense セキュリティ ポリシーが適用されるため、パケットの宛先 MAC アドレスがテーブルに含まれていなくても、通常のブリッジのように、すべてのインターフェイスに

元のパケットを Firewall Threat Defense がフラッディングすることはありません。代わりに、直接接続されたデバイスまたはリモート デバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット：Firewall Threat Defense は宛先 IP アドレスに対して ARP 要求を生成し、ARP 応答を受信したインターフェイスを学習します。
- リモート デバイスへのパケット：Firewall Threat Defense は宛先 IP アドレスへの ping を生成し、ping 応答を受信したインターフェイスを学習します。

元のパケットはドロップされます。

## デフォルト設定

- ARP インスペクションを有効にした場合、デフォルト設定では、一致しないパケットはフラッディングします。
- ダイナミック MAC アドレス テーブル エントリのデフォルトのタイムアウト値は 5 分です。
- デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、Firewall Threat Defense デバイスは対応するエントリを MAC アドレス テーブルに追加します。



- (注) Secure Firewall Threat Defense デバイスはリセットパケットを生成し、ステートフル検査エンジンによって拒否された接続をリセットします。リセットパケットでは、パケットの宛先 MAC アドレスが ARP テーブルのルックアップに基づいて決定されるのではなく、拒否されるパケット（接続）から直接取得されます。

## ARP インスペクションと MAC アドレス テーブルのガイドライン

- ARP インスペクションは、ブリッジ グループでのみサポートされます。
- MAC アドレス テーブル構成は、ブリッジ グループでのみサポートされます。

## 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、診断インターフェイスまた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** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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 [編集 (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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

**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必要がある場合があります。また、[デバイス (Devices)] > [デバイス管理 (Device Management)] > [ハイアベイラビリティ (High Availability)] タブで、アクティブ MAC アドレスとスタンバイ 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的な MAC アドレスを使用します。

### 手順

**ステップ 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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 [編集 (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** 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 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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## 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спекションを有効にします（[ARP インспекション](#) 参照）。ARP インспек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 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス[編集 (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 [編集 (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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## 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 \(78 ページ\)](#) 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** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス [編集 (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 [編集 (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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

## 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が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** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択し、Firewall Threat Defense デバイス [編集 (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 [編集 (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、[展開 (Deploy)] > [展開 (Deployment)] をクリックし、割り当てたデバイスにポリシーを展開できるようになりました。変更を展開するまで、変更は有効ではありません。

---

# 通常ファイアウォール インターフェイスの履歴

機能	最小 Firewall Management Center	最小 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)	<p>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。</p> <p>新しい/変更された画面：</p> <p>[デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [インターフェイス (Interfaces)] &gt; [インターフェイスの追加 (Add Interfaces)] &gt; [ループバック インターフェイスの追加 (Add Loopback Interface)]</p>

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
IPv6 DHCP	7.3	任意 (Any)	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 委任プレフィックスの BGP ルータ アドバタイズメント</li> <li>• 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。</li> </ul> <p>新しい/変更された画面 :</p> <ul style="list-style-type: none"> <li>• [デバイス (Devices) ] &gt; [デバイス管理 (Device Management) ] &gt; [インターフェイス (Interfaces) ] &gt; [インターフェイスの追加/編集 (Add/Edit Interfaces) ] &gt; [IPv6] &gt; [DHCP]</li> <li>• [オブジェクト (Objects) ] &gt; [オブジェクト管理 (Object Management) ] &gt; [DHCP IPv6 プール (DHCP IPv6 Pool) ]</li> </ul> <p>新規/変更されたコマンド : <code>show bgp ipv6 unicast</code>、<code>show ipv6 dhcp</code>、<code>show ipv6 general-prefix</code></p>

機能	最小 Firewall Management Center	最小 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)	<p>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。</p> <p>新しい/変更された画面：</p> <ul style="list-style-type: none"> <li>• [デバイス（Devices）] &gt; [デバイス管理（Device Management）] &gt; [デバイス（Device）] &gt; [インターフェイス（Interfaces）] &gt; [インターフェイスの追加（Add Interfaces）] &gt; [VNI インターフェイス（VNI Interface）]</li> </ul> <p>サポートされているプラットフォーム：Azure の Firewall Threat Defense Virtual</p>
VXLAN のサポート	7.2	任意 (Any)	<p>VXLAN カプセル化のサポートが追加されました。</p> <p>新しい/変更された画面：</p> <ul style="list-style-type: none"> <li>• [デバイス（Devices）] &gt; [デバイス管理（Device Management）] &gt; [デバイス（Device）] &gt; [VTEP]</li> <li>• [デバイス（Devices）] &gt; [デバイス管理（Device Management）] &gt; [デバイス（Device）] &gt; [インターフェイス（Interfaces）] &gt; [インターフェイスの追加（Add Interfaces）] &gt; [VNI インターフェイス（VNI Interface）]</li> <li>• [デバイス（Devices）] &gt; [デバイス管理（Device Management）] &gt; [デバイス（Device）] &gt; [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）] &gt; [全般（General）]</li> </ul> <p>サポートされているプラットフォーム：すべて。</p>

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
Firewall Threat Defense Virtual の Geneve サポート	7.1	任意 (Any)	<p>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。</p> <p>この機能には Snort 3 が必要です。</p> <p>新しい/変更された画面：</p> <ul style="list-style-type: none"> <li>• [デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [デバイス (Device)] &gt; [VTEP]</li> <li>• [デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [デバイス (Device)] &gt; [インターフェイス (Interfaces)] &gt; [インターフェイスの追加 (Add Interfaces)] &gt; [VNI インターフェイス (VNI Interface)]</li> <li>• [デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [デバイス (Device)] &gt; [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)] &gt; [全般 (General)]</li> </ul> <p>サポートされているプラットフォーム：AWS の Firewall Threat Defense Virtual</p>

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
31 ビット サブネット マスク	7.0	任意 (Any)	<p>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、ブロードキャストは必要ありません。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。</p> <p>新しい/変更された画面：</p> <p>[デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [インターフェイス (Interfaces)]</p>

機能	最小 Firewall Management Center	最小 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	いずれか	<p>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。</p> <p>(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。</p> <p>新規/変更された [Firepower Chassis Manager] 画面 : [論理デバイス (Logical Devices)] &gt; [リンク状態の有効化 (Enable Link State)]</p> <p>新規/変更された FXOS コマンド : <b>set link-state-sync enabled、show interface expand detail</b></p> <p>サポートされているプラットフォーム : Firepower 4100/9300</p>
Firepower 1010 ハードウェア スイッチのサポート	6.5	任意 (Any)	<p>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。</p> <p>新しい/変更された画面 :</p> <ul style="list-style-type: none"> <li>• [デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [インターフェイス (Interfaces)]</li> <li>• [デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [インターフェイス (Interfaces)] &gt; [物理インターフェイスの編集 (Edit Physical Interface)]</li> <li>• [デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [インターフェイス (Interfaces)] &gt; [VLAN インターフェイスの追加 (Add VLAN Interface)]</li> </ul>



機能	最小 Firewall Management Center	最小 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	任意 (Any)	<p>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。</p> <p>新しい/変更された画面：</p> <p>[デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [インターフェイス (Interfaces)] &gt; [物理インターフェイスの編集 (Edit Physical Interface)] &gt; [PoE]</p>
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	<p>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。</p> <p>新規/変更された Secure Firewall Management Center 画面：</p> <p>[デバイス (Devices)] &gt; [デバイス管理 (Device Management)] &gt; [編集 (Edit)] アイコン &gt; [インターフェイス (Interfaces)] タブ</p> <p>新規/変更された Secure Firewall シャーシマネージャ 画面：</p> <p>[インターフェイス (Interfaces)] &gt; [すべてのインターフェイス (All Interfaces)] &gt; [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)]</p> <p>新規/変更された FXOS コマンド：create subinterface、set vlan、show interface、show subinterface</p> <p>サポートされるプラットフォーム：Firepower 4100/9300</p>
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	<p>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。</p> <p>新規/変更された Secure Firewall シャーシマネージャ 画面：</p> <p>[インターフェイス (Interfaces)] &gt; [すべてのインターフェイス (All Interfaces)] &gt; [タイプ (Type)]</p> <p>新規/変更された FXOS コマンド：set port-type data-sharing、show interface</p> <p>サポートされるプラットフォーム：Firepower 4100/9300</p>

機能	最小 Firewall Management Center	最小 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	<p>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。</p> <p>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。</p> <p>新規/変更された画面：</p> <ul style="list-style-type: none"> <li>• [デバイス（Devices）] &gt; [デバイス管理（Device Management）] &gt; [インターフェイス（Interfaces）] &gt; [物理インターフェイスの編集（Edit Physical Interface）]</li> <li>• [デバイス（Devices）] &gt; [デバイス管理（Device Management）] &gt; [インターフェイス（Interfaces）] &gt; [インターフェイスを追加（Add Interfaces）] &gt; [ブリッジグループ インターフェイス（Bridge Group Interface）]</li> </ul> <p>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）</p>

## 翻訳について

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