



インターフェイス

ここでは、脅威に対する防御デバイスでのインターフェイスの設定方法について説明します。

- [Threat Defense インターフェイスについて \(1 ページ\)](#)
- [インターフェイスに関する注意事項と制約事項 \(6 ページ\)](#)
- [物理インターフェイスの設定 \(7 ページ\)](#)
- [管理インターフェイスの設定 \(14 ページ\)](#)
- [ブリッジグループの設定 \(16 ページ\)](#)
- [EtherChannel の設定 \(21 ページ\)](#)
- [VLAN インターフェイスおよびスイッチポートの設定 \(Firepower 1010\) \(34 ページ\)](#)
- [VLAN サブインターフェイスと 802.1Q トランキングの設定 \(48 ページ\)](#)
- [パッシブ インターフェイスの設定 \(54 ページ\)](#)
- [インラインセットの設定 \(59 ページ\)](#)
- [高度なインターフェイス オプションの設定 \(62 ページ\)](#)
- [インターフェイスの変更のスキャンとインターフェイスの移行 \(68 ページ\)](#)
- [Secure Firewall 3100 のネットワークモジュールの管理 \(73 ページ\)](#)
- [管理インターフェイスと診断インターフェイスのマージ \(83 ページ\)](#)
- [停電時のハードウェアバイパスの設定 \(ISA 3000\) \(92 ページ\)](#)
- [モニタリング インターフェイス \(94 ページ\)](#)
- [インターフェイスの例 \(96 ページ\)](#)

Threat Defense インターフェイスについて

Threat Defense には、データインターフェイスやManagementインターフェイスが組み込まれています。

インターフェイス接続（物理的または仮想）のためにケーブルを接続するとき、インターフェイスを設定する必要があります。最小限の作業として、トラフィックを通過させることができるようにインターフェイスを指定して有効化します。インターフェイスがブリッジグループのメンバーである場合、これで十分です。ブリッジグループのメンバーでない場合、インターフェイスにIPアドレスを割り当てる必要があります。単一の物理インターフェイスではなく、VLAN サブインターフェイスを特定のポートで作成する場合、通常、物理インターフェイスで

はなくサブインターフェイス上で IP アドレスを設定します。VLAN サブインターフェイスを使用すると、物理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。これは、スイッチのトランクポートに接続する場合に役立ちます。パッシブインターフェイスでは IP アドレスを設定しません。

[インターフェイス (Interfaces)] ページには、インターフェイスタイプのサブページが含まれます ([インターフェイス (Interfaces)] (物理インターフェイスの場合)、[ブリッジグループ (Bridge Groups)]、[仮想トンネルインターフェイス (Virtual Tunnel Interfaces)]、[EtherChannel (EtherChannels)]、[VLAN] (Firepower 1010 の場合))。Firepower 4100/9300 EtherChannel は [インターフェイス (Interfaces)] ページには表示されますが、[EtherChannel] ページには表示されないことに注意してください。これは、Device Manager ではなく FXOS の EtherChannel パラメータのみを変更できるためです。各ページに、利用可能なインターフェイスとそれぞれの名前、アドレス、モード、状態が表示されます。インターフェイスのステータスは、インターフェイスのリストで直接オン/オフを変更できます。このリストは、設定に基づいたインターフェイス特性を示します。メンバーインターフェイスを参照するには、ブリッジグループ、EtherChannel、または VLAN インターフェイス上で [開く/閉じる (open/close)] 矢印を使用します。メンバーインターフェイスは対応するリストにも表示されます。サポートされている親インターフェイスのサブインターフェイスを表示することもできます。これらのインターフェイスが仮想インターフェイスおよびネットワークアダプタにどのようにマッピングされるかについては、[Threat Defense の物理インターフェイスへの VMware ネットワークアダプタとインターフェイスのマッピング方法](#)を参照してください。

以下の各トピックでは、Device Manager を使用してインターフェイスを設定する場合の制限事項、およびインターフェイス管理に関するその他の概念について説明します。

インターフェイスモード

インターフェイスごとに次のモードのいずれかを設定できます。

ルーテッド

各レイヤ 3 ルーテッドインターフェイスに、固有のサブネット上の IP アドレスが必要です。通常、これらのインターフェイスをスイッチ、別のルータ上のポート、または ISP/WAN ゲートウェイに接続します。

インライン

インターフェイスをインラインセットに追加すると、モードがインラインに変更されます。インラインをモードとして直接選択することはできません。

パッシブ

パッシブインターフェイスは、スイッチ SPAN (スイッチドポートアナライザ) またはミラーポートを使用してネットワーク全体を流れるトラフィックをモニターします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワークトラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション (トラフィックのブロッキングやシェーピングなど) を実行することができませ

ん。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。

スイッチポート (Firepower 1010)

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、脅威に対する防御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、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。管理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。

BridgeGroupMember

ブリッジグループは、脅威に対する防御 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。すべてのインターフェイスは同じネットワーク上にあります。ブリッジグループはブリッジ ネットワークに IP アドレスを持つブリッジ仮想インターフェイス (BVI) によって表されます。

BVI に名前を付けると、ルーテッドインターフェイスと BVI の間のルーティングを実行できます。この場合、BVI はメンバー インターフェイスとルーテッドインターフェイス間のゲートウェイとして機能します。BVI に名前を指定しない場合、ブリッジグループメンバーのインターフェイス上のトラフィックはブリッジグループを離れることができます。通常、インターネットにメンバーインターフェイスをルーティングするため、インターフェイスに名前を付けます。

ルーテッドモードでブリッジグループを使用する方法として、外部スイッチの代わりに脅威に対する防御 デバイスの予備インターフェイスを使用する方法があります。ブリッジグループのメンバーインターフェイスにエンドポイントを直接接続できます。また、BVI と同じネットワークにより多くのエンドポイントを追加するために、スイッチを接続できます。

管理/診断インターフェイス

管理インターフェイス

管理インターフェイスは、デバイスの他のインターフェイスとは分離されています。Device Manager 管理、スマートライセンス、およびデータベースの更新に使用されます。または、管理インターフェイスの代わりにデータインターフェイスを使用して Threat Defense デバイスを管理できます。管理インターフェイスでは、独自の Linux IP アドレスとスタティックルーティングが使用されます。管理インターフェイスは、**[デバイス (Device)] > [インターフェイス (Interfaces)]** ページで、または **configure network** コマンドを使用して CLI で設定できます。

ハードウェアデバイスの場合、管理インターフェイスを設定する一つの方法は、ポートをネットワークに接続しないことです。代わりに、管理 IP アドレスのみを設定し、インターネットからの更新情報を得るためのゲートウェイとして、データインターフェイスを使用するように設定します。次に、HTTPS/SSH トラフィック (デフォルトで HTTPS は有効) への内部インターフェイスを開き、内部 IP アドレスを使用して Device Manager を開きます ([管理アクセスリストの設定](#) を参照)。

Threat Defense Virtual の推奨設定は、Management0/0 を内部インターフェイスと同じネットワークに接続し、内部インターフェイスをゲートウェイとして使用することです。

診断インターフェイス（レガシー）

7.3 以降を使用している新しいデバイスの場合、レガシー診断インターフェイスは使用できません。マージされた管理インターフェイスのみを使用できます。

7.4 以降にアップグレードし、診断インターフェイスの設定がない場合は、インターフェイスが自動的にマージされます。

7.4 以降にアップグレードし、診断インターフェイスの設定がある場合は、インターフェイスを手動でマージするか、別の診断インターフェイスを引き続き使用できます。診断インターフェイスのサポートは今後のリリースで削除されるため、できるだけ早くインターフェイスをマージする必要があります。管理インターフェイスと診断インターフェイスを手動でマージするには、[管理インターフェイスと診断インターフェイスのマージ（83 ページ）](#) を参照してください。自動マージを防止する設定には、次のものが含まれます。

- 「管理」という名前のデータインターフェイス。この名前は、マージされた管理インターフェイスで使用するために予約されています。
- 診断の IP アドレス
- 診断で有効な DNS
- Syslog、または RADIUS（リモートアクセス VPN 用）送信元インターフェイスが診断
- 送信元インターフェイスが指定されておらず、管理専用（診断を含む）として設定されているインターフェイスが少なくとも 1 つある AD または RADIUS（リモートアクセス VPN 用）。これらのサービスのデフォルトルートルックアップは、管理専用ルーティングテーブルからデータルーティングテーブルに変更されていて、管理にフォールバックされません。したがって、管理専用インターフェイスを使用するには、ルートルックアップに依存する代わりに、その特定のインターフェイスを選択する必要があります。
- スタティックルートまたは診断の SLA モニタ
- 診断を使用した FlexConfig
- 診断用の DDNS

レガシー診断インターフェイスの動作の詳細については、このガイドの 7.3 バージョンを参照してください。

個別の管理ネットワークの設定に関する推奨事項

（ハードウェアデバイス）分離した管理ネットワークを使用する場合は、物理的管理インターフェイスをスイッチまたはルータに有線で接続します。

Threat Defense Virtual では、Management0/0 を任意のデータ インターフェイスから個別のネットワークに接続します。デフォルトの IP アドレスを使用している場合、管理 IP アドレスまた

は内部インターフェイス IP アドレスは同一サブネット上にあるため、いずれかを変更する必要があります。

次に、[デバイス (Device)] > [インターフェイス (Interfaces)] を選択し、管理インターフェイスを編集して、接続されたネットワークで IPv4 アドレスまたは IPv6 アドレス (あるいはその両方) を設定します。必要に応じて、ネットワーク上の他のエンドポイントに IPv4 アドレスを指定するように DHCP サーバーを設定できます。管理ネットワーク上にインターネットへのルートを持つルータがある場合、それをゲートウェイとして使用します。なければ、データインターフェイスをゲートウェイとして使用します。

セキュリティゾーン

各インターフェイスは単一のセキュリティゾーンに割り当てることができます。ゾーンに基づいてセキュリティポリシーを適用されます。たとえば、内部インターフェイスを内部ゾーンに割り当て、外部インターフェイスを外部ゾーンに割り当てることができます。また、たとえば、トラフィックが内部から外部に移動できるようにアクセスコントロールポリシーを設定することはできますが、外部から内部に向けては設定できません。

各ゾーンにはインターフェイスのモードに直接関係するモードがあります。インターフェイスは、同じモードのセキュリティゾーンにのみ追加できます。

ブリッジグループでは、メンバーインターフェイスをゾーンに追加できますが、ブリッジ仮想インターフェイス (BVI) を追加することはできません。

ゾーンに Management インターフェイスは含めないでください。ゾーンは、データインターフェイスにのみ適用されます。

セキュリティゾーンは [オブジェクト (Objects)] ページで作成できます。

IPv6 アドレス指定

次の 2 種類の IPv6 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、各メンバーインターフェイスではなくブリッジ仮想インターフェイス (BVI) 上でグローバルアドレスを設定します。次のいずれかをグローバルアドレスとして指定することはできません。
 - 内部で予約済みの IPv6 アドレス : `fd00::/56 (from=fd00:: to=fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)`
 - 未指定のアドレス (`::/128` など)
 - ループバックアドレス (`::1/128`)
 - マルチキャストアドレス (`ff00::/8`)
 - リンクローカルアドレス (`fe80::/10`)

- 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およびネイバー探索などのネットワーク検出機能に使用できます。ブリッジグループでは、BVI で IPv6 を有効にすると、自動的に各ブリッジグループのメンバー インターフェイスのリンクローカルアドレスが設定されます。リンクローカルアドレスがセグメントでのみ使用可能であり、インターフェイス MAC アドレスに接続されているため、各インターフェイスは独自のアドレスを持つ必要があります。

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。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。

Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、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 を有効にするには、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無効にされ、Auto-MDI/MDIX も無効になります。ギガビットイーサネットの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。

インターフェイスに関する注意事項と制約事項

ここでは、インターフェイスに関する制限事項について説明します。

インターフェイス設定の制限事項

Device Manager を使用してデバイスを設定する場合、インターフェイス設定に関するいくつかの制限があります。次の機能のいずれかが必要である場合、デバイスを設定するために Management Center を使用する必要があります。

- ルーテッドファイアウォールモードのみがサポートされます。トランスペアレントファイアウォールモードのインターフェイスは設定できません。
- パッシブインターフェイスの設定は可能ですが、ERSPAN インターフェイスを設定することはできません。
- 冗長インターフェイスは設定できません。

- Device Manager で EtherChannel を設定できるモデルは、Firepower 1000、Firepower 2100、Cisco Secure Firewall 3100、ISA 3000 です。Firepower 4100/9300 は EtherChannel をサポートしていますが、シャーシの FXOS で EtherChannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに Device Manager の [Interfaces] ページに表示されます。
- 追加できるブリッジグループは1つだけです。
- Threat Defense は、ルーテッドインターフェイスでのみ IPv4 PPPoE をサポートします。PPPoE は、ハイアベイラビリティユニットではサポートされません。

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
Threat Defense Virtual	50
ISA 3000	100

物理インターフェイスの設定

少なくとも、使用する物理インターフェイスは有効にする必要があります。通常は名前も付けて、IP アドレッシングを設定します。VLAN サブインターフェイスを設定する予定の場合、パッシブモードインターフェイスを設定している場合、またはインターフェイスをブリッジグループに追加する予定の場合は、IP アドレッシングを設定しません。Firepower 4100/9300 EtherChannel は、単一の物理インターフェイスとともに Device Manager の [インターフェイス (Interfaces)] ページに表示され、この手順はそれらの EtherChannel にも適用されます。シャー


シ上の FXOS で、Firepower 4100/9300 Etherchannel のすべてのハードウェア設定を実行する必要があります。



- (注) 物理インターフェイスを Firepower 1010 スイッチポートとして設定するには、[VLAN インターフェイスおよびスイッチポートの設定 \(Firepower 1010\) \(34 ページ\)](#) を参照してください。
- 物理インターフェイスをパッシブインターフェイスとして設定するには、[パッシブモードでの物理インターフェイスの設定 \(58 ページ\)](#) を参照してください。

接続されたネットワークでの送信を一時的に防ぐために、インターフェイスを無効にできません。インターフェイスの設定を削除する必要はありません。

手順

- ステップ 1** [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックします。
- [インターフェイス (Interfaces)] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。
- ステップ 2** 編集する物理インターフェイスの [編集 (edit)] アイコン () をクリックします。
- 高可用性設定でフェールオーバー リンクまたはステートフル フェールオーバー リンクとして使用しているインターフェイスを編集することはできません。
- ステップ 3** 次の設定を行います。

Ethernet1/2
Edit Physical Interface

Interface Name: inside Mode: Routed Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address IPv6 Address Advanced

Type: Static

IP Address and Subnet Mask: 10.99.10.1 / 24
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask: 10.99.10.2 / 24
e.g. 192.168.5.16

CANCEL OK

a) [インターフェイス名 (Interface Name)] を設定します。

インターフェイスの名前（最大 48 文字）を設定します。英字は小文字にする必要があります。例、[inside] または [outside]。名前を設定しないと、インターフェイスの残りの設定は無視されます。サブインターフェイスを設定する場合を除き、インターフェイスには名前が必要です。注：EtherChannel に追加するインターフェイスの名前は設定しないでください。


(注) 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティゾーン、syslog サーバオブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

b) [モード (Mode)] を選択します。

- [ルーテッド (Routed)] : ルーテッドモードインターフェイスでは、トラフィックはフローの維持、IP 層と TCP 層の両方でのフロー状態のトラッキング、IP の最適化、TCP の正規化、ファイアウォールポリシーなど、すべてのファイアウォール機能の管理下に置かれます。これが通常のインターフェイスモードです。

- [インライン (Inline)] : インターフェイスをインラインセットに追加すると、モードがインラインに変更されます。インラインをモードとして直接選択することはできません。インラインセットで使用するインターフェイスを編集する場合は、初期モードとしてルーテッドモードを選択し、どのタイプのIPアドレッシングも設定しないでください。
- [パッシブ (Passive)] : パッシブ インターフェイスは、スイッチ SPAN またはミラーポートを使用してネットワーク中のトラフィック フローをモニタします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワークトラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション (トラフィックのブロッキングやシェーピングなど) を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。このモードを選択する場合、残りの手順は実行しないでください。代わりに、[パッシブモードでの物理インターフェイスの設定 \(58 ページ\)](#) を参照してください。パッシブインターフェイスには IP アドレスを設定できません。
- [Switch Port] : (Firepower 1010) スイッチポートは、同じ VLAN 上のポート間でのハードウェアスイッチングを可能にします。スイッチングされたトラフィックはセキュリティポリシーの対象にはなりません。このモードを選択する場合、残りの手順は実行しないでください。代わりに、次を参照してください。[VLAN インターフェイスおよびスイッチポートの設定 \(Firepower 1010\) \(34 ページ\)](#)

後でこのインターフェイスをブリッジグループに追加すると、モードは自動的に「BridgeGroupMember」に変更されます。ブリッジグループのメンバーインターフェイスには IP アドレスを設定できません。

- c) [ステータス (Status)] スライダを [有効 (enabled)] 設定 () に設定します。

Firepower 4100/9300 デバイス上のインターフェイスの場合は、FXOS でもインターフェイスを有効にする必要があります。

この物理インターフェイスのサブインターフェイスを設定する予定の場合、すでに設定している可能性が高いです。[保存 (Save)] をクリックして、[VLAN サブインターフェイスと 802.1Q トランッキングの設定 \(48 ページ\)](#) に進みます。保存しない場合は、次に進みます。

- (注) サブインターフェイスを設定している場合でも、インターフェイスに名前を付けて、IP アドレスを指定できます。これは一般的な設定ではありませんが、必要だとわかっている場合は設定できます。

- d) (任意) [説明 (Description)] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

ステップ 4 [IPv4 アドレス (IPv4 Address)] タブをクリックして、IPv4 アドレスを設定します。

[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

- [DHCP] : ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
 - [ルートメトリック (Route Metric)] : DHCP サーバからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1~255 の間です。デフォルトは 1 です。
 - [デフォルトルートを取得 (Obtain Default Route)] : デフォルトルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。
- [スタティック (Static)] : 変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネットマスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

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

(注) インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレスプールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレスプールを構成する必要があります。[DHCP サーバの設定](#)を参照してください。

- [PPPoE] : イーサネット経由のポイントツーポイントプロトコル (PPPoE) を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。
 - [グループ名 (Group Name)] : この接続を表すために選択した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 (PPPoE Password)] : ISP によって提供されたパスワードを指定します。
 - [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の学習済みルートメトリック (PPPoE Learned Route Metric)] : アドミニストレーティブディスタンスを既知の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。
- [PPPoEからデフォルトルートを取得 (Obtain Default Route from PPPoE)] : PPPoEサーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。
- [IPアドレスタイプ (IP Address Type)] : PPPoEサーバからIPアドレスを取得するには、[動的 (Dynamic)]を選択します。ISPから静的IPアドレスが割り当てられている場合は、[静的 (Static)]を選択することもできます。

ステップ5 (オプション) [IPv6アドレス (IPv6 Address)] タブをクリックして、IPv6アドレスを設定します。

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

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

- [アドレスの自動設定 (Address Auto Configuration)] : アドレスを自動的に設定するには、このオプションを選択します。IPv6ステートレス自動設定では、デバイスが存在するリンクで使用するIPv6グローバルプレフィックスのアドバタイズメントなどの、IPv6サービスを提供するようにルータが設定されている場合に限り、グローバルなIPv6アドレスが生成されます。IPv6ルーティングサービスがリンクで使用できない場合、リンクローカルIPv6アドレスのみが取得され、そのデバイスが属するネットワークリンクの外部にはアクセスできません。リンクローカルアドレスはModified EUI-64インターフェイスIDに基づいています。

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、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。メッセージを抑制して、RFCに準拠するためには、[RAを抑制 (Suppress RA)]を選択します。

- [スタティックアドレスとプレフィックス (Static Address/Prefix)] : ステートレス自動設定を使用しない場合、完全なスタティックグローバルIPv6アドレスとネットワークプレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力しま

す。IPv6 アドレッシングの詳細については、[IPv6 アドレス指定 \(5 ページ\)](#) を参照してください。

アドレスをリンクローカル専用として使用する場合は、[リンクローカル (Link - Local)] オプションを選択します。リンクローカルアドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカルアドレスはブリッジグループ インターフェイスには設定できません。

(注) 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。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。

- [スタンバイ IP アドレス (Standby IP Address)]: 高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。
- [RA を抑制 (Suppress RA)]: ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、Threat Defense はルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ (ICMPv6 Type 134) は、設定済みの各 IPv6 インターフェイスに定期的送信されます。

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

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

ステップ 6 (任意) [詳細オプションの設定 \(64 ページ\)](#)。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 7 [OK] をクリックします。

次のタスク

- インターフェイスを適切なセキュリティゾーンに追加します。[セキュリティゾーンの設定](#) を参照してください。

- ダイナミック DNS サービスプロバイダーに完全修飾ドメイン名 (FQDN) を登録し、DNS サーバの IPv4 と IPv6 の両方のインターフェイスアドレスが更新されるように DDNS を設定します。 [ダイナミック DNS \(DDNS\) の設定](#) を参照してください。

管理インターフェイスの設定

管理インターフェイスは、[インターフェイス (Interface)] ページのデータインターフェイスとともに表示される特別なインターフェイスですが、データインターフェイスとしては動作しません。管理インターフェイスには次の使用方法があります。

- IP アドレスへの Web および SSH 接続を開き、インターフェイスからデバイスを設定できます。
- システムはこの IP アドレスを使用してスマート ライセンスおよびデータベースの更新情報を取得します。
- このインターフェイスは syslog にも使用できます。

CLI セットアップウィザードを使用すると、システムの初期設定時にデバイスの管理アドレスとゲートウェイを設定します。Device Manager のセットアップウィザードを使用すると、管理アドレスとゲートウェイはデフォルトのまま変更されません。

必要に応じて、Device Manager でこれらのアドレスを変更できます。**configure network ipv4 manual** および **configure network ipv6 manual** コマンドを使用して、CLI で管理アドレスおよびゲートウェイを変更することもできます。デフォルトの管理インターフェイス設定に戻すには、**configure network {ipv4 | ipv6} dhcp-dp-route** コマンドを使用します。

管理ネットワーク上の他のデバイスが DHCP サーバーとして機能している場合、スタティックアドレスを定義するか、または DHCP を介してアドレスを取得できます。ほとんどのプラットフォームでは、管理インターフェイスはデフォルトで DHCP から IP アドレスを取得します。



注意 現在接続されているアドレスを変更した場合は、その変更がすぐに適用されるため、変更の保存と同時に Device Manager (または CLI) にアクセスできなくなります。デバイスに接続し直す必要があります。新しいアドレスが管理ネットワークで使用できることを確認します。

始める前に

7.4以降にアップグレードしていて、管理インターフェイスと診断インターフェイスをまだマージしていない場合は、[管理インターフェイスと診断インターフェイスのマージ \(83 ページ\)](#) を参照してください。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[デバイス]>[インターフェイス] リンクをクリックします。 >

ステップ 2 管理インターフェイスを編集します。

ステップ 3 管理ゲートウェイの定義方法を選択します。

ゲートウェイは、システムがインターネット経由でスマートライセンスとデータベース更新 (VDB、ルール、地理位置情報、URL など) を取得し、管理 DNS サーバと NTP サーバに到達する方法を決定します。次のオプションから選択します。

静的 IP オプション :

- [データインターフェイスをゲートウェイとして使用 (Use the Data Interfaces as the Gateway)] : 管理インターフェイスに別の管理ネットワークが接続されていない場合、このオプションを選択します。トラフィックは、ルーティングテーブルに基づいてインターネットにルーティングされ、通常は、外部インターフェイスを通過します。このオプションは Threat Defense Virtual デバイスではサポートされません。
- [管理インターフェイスに固有のゲートウェイを使用 (Use Unique Gateways for the Management Interface)] : 管理インターフェイスに接続されている別の管理ネットワークがある場合、IPv4 および IPv6 に固有のゲートウェイ (以下) を指定します。

DHCP IP オプション :

- [データインターフェイスへのフォールバックが可能な管理インターフェイス用に一意のゲートウェイを使用 (Use Unique Gateways for the Management Interface with Fallback to Data Interfaces)] : DHCP サーバがゲートウェイを提供する場合、システムは管理インターフェイスを介してゲートウェイに管理トラフィックをルーティングします。DHCP サーバがゲートウェイを提供しない場合、システムはデータ インターフェイス ルーティング テーブルに基づいて管理トラフィックをルーティングし、通常は外部インターフェイスを介してトラフィックを送信します。このオプションは Threat Defense Virtual デバイスではサポートされません。
- [管理インターフェイス用に一意のゲートウェイを使用 (フォールバックなし) (Use Unique Gateways for the Management Interface (no Fallback))] : システムは、DHCP サーバの提供するゲートウェイに管理インターフェイスを介して管理トラフィックをルーティングします。DHCP サーバがゲートウェイを提供しない場合、システムが到達できるのは管理インターフェイスのローカルホストのみになります。データインターフェイスを介してルーティングするには、[フォールバック (Fallback)] オプションを選択します。

ステップ 4 IPv4 または IPv6 管理アドレス、サブネットマスクか IPv6 プレフィックス、および必要に応じてゲートウェイを設定します。

少なくとも 1 組のプロパティを設定する必要があります。1 組は空白にし、そのアドレッシング方式を無効にします。

- 静的 IP アドレスを設定するには、[タイプ (Type)]>[静的 (Static)] を選択します。 >

- **[タイプ (Type)] > [DHCP]** を選択し、DHCP または IPv6 自動設定によってアドレスおよびゲートウェイを取得します。

ステップ 5 (任意) スタティック **IPv4** アドレスを設定する場合は、インターフェイスで DHCP サーバーを設定します。

管理インターフェイスで DHCP サーバーを設定すると、管理ネットワークのクライアントは DHCP プールからアドレスを取得できます。このオプションは Threat Defense Virtual デバイスではサポートされません。

- a) **[DHCPサーバを有効化 (Enable DHCP Server)] > [オン (On)]** をクリックします。
- b) サーバーの **[アドレスプール (Address Pool)]** を入力します。

アドレスプールとは、アドレスを要求するクライアントに対してサーバーが提供できる、最小から最大までの IP アドレスの範囲です。IP アドレスの範囲は管理アドレスと同じサブネット上にある必要があり、次のものを含めることはできません：インターフェイス自体の IP アドレス、ブロードキャストアドレス、またはサブネットのネットワーク アドレス。プールに開始/終了アドレスをハイフンで区切って指定します。たとえば、192.168.45.46-192.168.45.254 などです。

ステップ 6 **[詳細設定 (Advanced)]** ページで、IPv4 の場合は 8-1500、IPv6 を有効にした場合は 1280-1500 の管理インターフェイスの **MTU** を設定します。

デフォルト値は 1500 バイトです。

ステップ 7 **[保存 (Save)]** をクリックして警告を読み、**[OK]** をクリックします。

ブリッジグループの設定

ブリッジグループは 1 つ以上のインターフェイスをグループ化する仮想インターフェイスです。インターフェイスをグループ化する主な理由は、スイッチドインターフェイスのグループを作成することにあります。そのため、ブリッジグループに含まれているインターフェイスにワークステーションやその他のエンドポイントデバイスを直接接続できます。それらは別の物理スイッチを介して接続する必要はありませんが、スイッチをブリッジグループメンバーに接続することもできます。

グループメンバーには IP アドレスはありません。代わりに、すべてのメンバーインターフェイスがブリッジ仮想インターフェイス (BVI) の IP アドレスを共有します。BVI で IPv6 を有効にすると、メンバーインターフェイスには一意のリンクローカルアドレスが自動的に割り当てられます。

メンバーインターフェイスは個別に有効または無効にします。そのため、未使用のインターフェイスはブリッジグループから削除することなく無効化できます。ブリッジグループ自体は常に有効になっています。

通常は、メンバーインターフェイス経由で接続されているエンドポイントの IP アドレスを提供するブリッジグループインターフェイス (BVI) に DHCP サーバーを設定します。ただし、

必要に応じて、メンバー インターフェイスに接続されているエンドポイントにスタティック アドレスを設定できます。ブリッジグループ内のすべてのエンドポイントには、ブリッジグループの IP アドレスと同じサブネットの IP アドレスが必要です。

ガイドラインと制約事項

- ブリッジグループを 1 つ追加できます。
- Device Manager 定義の EtherChannel はブリッジグループ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。
- Firepower 2100 シリーズ または Threat Defense Virtual デバイスにブリッジグループを設定することはできません。
- 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。
- ISA 3000 は、ブリッジグループ BV11 を使用して事前に設定されています（名前は付けられていません。これは、ルーティングに参加しないことを意味します）。BV11 にはすべてのデータインターフェイス（GigabitEthernet1/1 (outside1)、GigabitEthernet1/2 (inside1)、GigabitEthernet1/3 (outside2)、および GigabitEthernet1/4 (inside2)）が含まれます。ネットワークに合わせて BV11 IP アドレスを設定する必要があります。

始める前に

ブリッジグループのメンバーになるインターフェイスを設定します。具体的には、各メンバーインターフェイスは、次の要件を満たしている必要があります。

- インターフェイスには名前が必要です。
- 静的に、または DHCP を介してインターフェイス用に定義された IPv4 または IPv6 アドレスは設定できません。現在使用しているインターフェイスからアドレスを削除する必要がある場合、そのインターフェイスのその他の設定（アドレスを持つインターフェイスに依存するスタティック ルート、DHCP サーバー、NAT ルールなど）も削除する必要がある場合があります。
- インターフェイスをブリッジグループに追加する前に、セキュリティゾーン（ゾーン内にある場合）からそのインターフェイスを削除し、そのインターフェイスのすべての NAT ルールを削除する必要があります。

手順

ステップ 1 [デバイス (Device)] をクリックし、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックし、[ブリッジグループ (Bridge Groups)] をクリックします。

ブリッジグループのリストに、既存のブリッジグループが表示されます。各ブリッジグループのメンバーインターフェイスを表示するには、開/閉矢印をクリックします。また、メンバー

インターフェイスは[インターフェイス (Interfaces)]または[VLAN (VLANs)]ページでも個別に表示されます。

ステップ 2 次のいずれかを実行します。

- BV11 ブリッジグループの編集アイコン (🔗) をクリックします。
- [ブリッジグループの作成 (Create Bridge Group)] をクリックするか、プラス アイコン (+) をクリックして、新しいグループを作成します。

(注) ブリッジグループは1つ設定できます。ブリッジグループをすでに定義している場合は、新しいグループ作成するのではなく、そのグループを編集する必要があります。新しいブリッジグループを作成する必要がある場合は、まず既存のブリッジグループを削除する必要があります。
- 不要になったブリッジグループの [削除 (delete)] アイコン (🗑️) をクリックします。ブリッジグループを削除すると、そのメンバーは標準のルーテッドインターフェイスになり、NAT ルールまたはセキュリティ ゾーンのメンバーシップはすべて維持されます。インターフェイスを編集して、IP アドレスを付与できます。新しいブリッジグループにこれらのインターフェイスを追加する場合は、まず NAT ルールを削除し、インターフェイスをセキュリティ ゾーンから削除する必要があります。

ステップ 3 次を設定します。

- a) (任意) [インターフェイス名 (Interface Name)] を設定します。

ブリッジグループの名前（最大 48 文字）を設定します。英字は小文字にする必要があります。例、[inside] または [outside]。この BVI を他の名前付きインターフェイス間のルーティングに参加させる場合は、名前を設定します。

(注) 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティゾーン、syslog サーバオブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

b) (任意) [説明 (Description)] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

c) [ブリッジグループメンバー (Bridge Group Members)] のリストを編集します。

1 つのブリッジグループに最大 64 個のインターフェイスまたはサブインターフェイスを追加できます。

- インターフェイスの追加：プラスアイコン (+) をクリックし、1 つ以上のインターフェイスをクリックし、[OK] をクリックします。
- インターフェイスの削除：対象にカーソルを合わせ、右側に表示される [x] をクリックします。

ステップ 4 [IPv4 アドレス (IPv4 Address)] タブをクリックして、IPv4 アドレスを設定します。

[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

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

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

(注) インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレスプールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレスプールを構成する必要があります。DHCP サーバの設定を参照してください。

- [ダイナミック (Dynamic)] (DHCP) : ネットワーク上の DHCP サーバーからアドレスを取得する必要がある場合は、このオプションを選択します。これはブリッジグループの一

一般的なオプションではありませんが、必要に応じて設定できます。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。

- [ルートメトリック (Route Metric)]: DHCPサーバからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは1~255の間です。デフォルトは1です。
- [デフォルトルートを取得 (Obtain Default Route)]: デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。

ステップ5 (オプション) [IPv6アドレス (IPv6 Address)] タブをクリックして、IPv6 アドレスを設定します。

- [状態 (State)]: グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効 (Enabled)]を選択します。リンクローカルアドレスはインターフェイスのMACアドレス (Modified EUI-64形式) に基づいて生成されます。

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

- [スタティックアドレスとプレフィックス (Static Address/Prefix)]: ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワークプレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、[IPv6 アドレス指定 \(5 ページ\)](#) を参照してください。

アドレスをリンクローカル専用として使用する場合は、[リンクローカル (Link - Local)] オプションを選択します。リンクローカルアドレスでは、ローカルネットワークの外部にはアクセスできません。リンクローカルアドレスはブリッジグループインターフェイスには設定できません。

(注) 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。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。

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

- [RAを抑制 (Suppress RA)]: ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、Threat Defense デバイスはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ (ICMPv6 Type 134) は、設定済みの各 IPv6 インターフェイスに定期的に送信されます。

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

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

ステップ 6 (任意) [詳細オプションの設定 \(64 ページ\)](#)。

ブリッジグループメンバーインターフェイスに対して最も詳細なオプションを設定しますが、一部はブリッジグループ インターフェイスでも使用できます。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ 7 [OK] をクリックします。

次のタスク

- 使用する予定のすべてのメンバー インターフェイスが有効になっていることを確認します。
- ブリッジグループの DHCP サーバを設定します。[DHCP サーバの設定](#)を参照してください。
- メンバーインターフェイスを適切なセキュリティゾーンに追加します。[セキュリティゾーンの設定](#)を参照してください。
- アイデンティティ、NAT、アクセスなどのポリシーにより、ブリッジグループとメンバーインターフェイスに必要なサービスが提供されることを確認します。

EtherChannel の設定

ここでは、EtherChannel とそれらの設定方法について説明します。



(注) 次のモデルでは、Device Manager で EtherChannel を追加できます。

- Firepower 1000
- Firepower 2100
- Cisco Secure Firewall 3100
- ISA 3000

Firepower 4100/9300 は EtherChannel をサポートしていますが、シャーシの FXOS で EtherChannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の EtherChannel は、単一の物理インターフェイスとともに Device Manager の [Interfaces] ページに表示されません。また、Threat Defense Virtual などの他のモデルでは、Device Manager で EtherChannel を設定できません。

EtherChannel について

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネットリンク（チャンネルグループ）のバンドルで構成される論理インターフェイスです（ポートチャンネルインターフェイスと呼びます）。ポートチャンネルインターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

モデルでサポートされているインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。

チャンネルグループインターフェイス

各チャンネルグループは、最大 8 個のアクティブインターフェイスを設定できます。

チャンネルグループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャンネルグループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

EtherChannel によって、チャンネル内の使用可能なすべてのアクティブインターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュアルゴリズムを使用して選択されます。

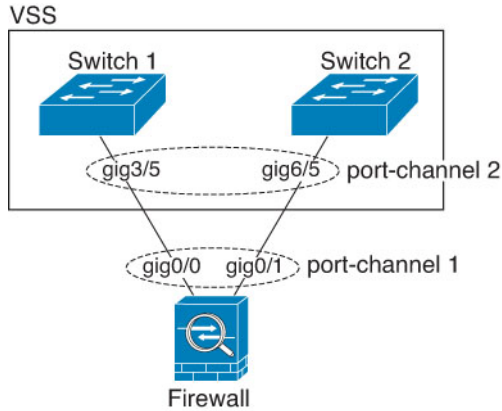
別のデバイスの EtherChannel への接続

Threat Defense EtherChannel の接続先のデバイスも 802.3ad EtherChannel をサポートしている必要があります。たとえば、Catalyst 6500 スイッチまたは Cisco Nexus 7000 に接続できます。

スイッチが仮想スイッチングシステム（VSS）または仮想ポートチャンネル（vPC）の一部である場合、同じ EtherChannel 内の Threat Defense インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。スイッチインターフェイスは同じ EtherChannel ポートチャンネルイン

ターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。

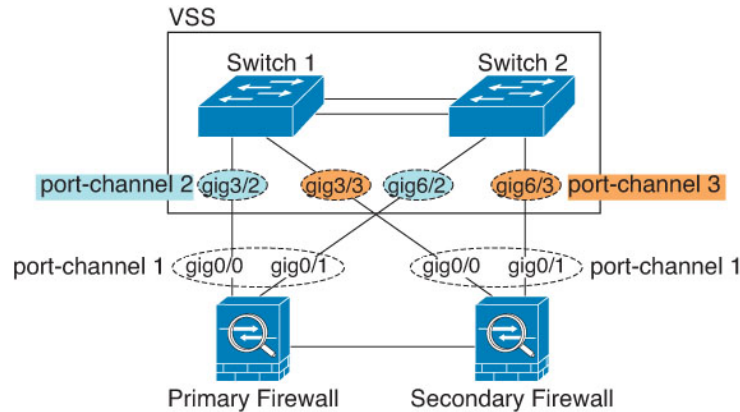
図 1: VSS/vPC への接続



(注) Threat Defense デバイスがトランスペアレント ファイアウォール モードになっており、2 組の VSS/vPC スイッチ間に Threat Defense デバイスを配置する場合は、EtherChannel 内で Threat Defense デバイスに接続されたすべてのスイッチポートで単方向リンク検出 (UDLD) を無効にしてください。スイッチポートで UDLD を有効にすると、他の VSS/vPC ペアの両方のスイッチから送信された UDLD パケットを受信する場合があります。受信側スイッチの受信インターフェイスは「UDLD Neighbor mismatch」という理由でダウン状態になります。

Threat Defense デバイスをアクティブ/スタンバイフェールオーバー展開で使用する場合、Threat Defense デバイスごとに 1 つ、VSS/vPC 内のスイッチで個別の EtherChannel を作成する必要があります。各 Threat Defense デバイスで、1 つの EtherChannel が両方のスイッチに接続します。すべてのスイッチインターフェイスを両方の Threat Defense デバイスに接続する単一の EtherChannel にグループ化できる場合でも（この場合、個別の Threat Defense システム ID のため、EtherChannel は確立されません）、単一の EtherChannel は望ましくありません。これは、トラフィックをスタンバイ Threat Defense デバイスに送信しないようにするためです。

図 2: アクティブ/スタンバイ フェールオーバーと VSS/vPC



リンク集約制御プロトコル

リンク集約制御プロトコル (LACP) では、2つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット (LACPDU) を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- **アクティブ** : LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- **オン** : EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャンネルグループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャンネルグループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ロード バランシング

Threat Defense デバイスは、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します (この基準は設定可能です)。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフローの割り当て先のインターフェイスが決まります。

$hash_value \bmod active_links$ の結果が 0 となるすべてのパケットは、EtherChannel 内の最初のインターフェイスに送信され、以降は結果が 1 となるものは 2 番目のインターフェイスに、結果が 2 となるものは 3 番目のインターフェイスに、というように送信されます。たとえば、15 個のアクティブリンクがある場合、モジュロ演算では 0~14 の値が得られます。6 個のアクティブリンクの場合、値は 0~5 となり、以降も同様になります。

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ2のスパニングツリーとレイヤ3のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

EtherChannel MAC アドレス

1つのチャンネル グループに含まれるすべてのインターフェイスは、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トランスペアレントになります。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。

Firepower および Secure Firewall ハードウェア

ポートチャンネル インターフェイスは、内部インターフェイスの内部データ 0/1 の MAC アドレスを使用します。または、ポートチャンネル インターフェイスの MAC アドレスを手動で設定することもできます。シャーシ上のすべての EtherChannel インターフェイスは同じ MAC アドレスを使用するため、たとえば、SNMP ポーリングを使用する場合、複数のインターフェイスが同じ MAC アドレスを持つことに注意してください。



- (注) メンバーインターフェイスは、再起動後に内部データ 0/1 MAC アドレスのみを使用します。再起動する前に、メンバーインターフェイスは独自の MAC アドレスを使用するが再起動後に新しいメンバーインターフェイスを追加する場合、MAC アドレスを更新するためにもう一度再起動する必要があります。

EtherChannel インターフェイスのガイドライン

ブリッジグループ

Device Manager 定義の EtherChannel はブリッジグループ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。

高可用性

- EtherChannel インターフェイスを高可用性 リンクとして使用する場合、高可用性 ペアの両方のユニットでその事前設定を行う必要があります。プライマリユニットで設定し、セカンダリユニットに複製されることは想定できません。これは、複製には高可用性 リンク自体が必要であるためです。
- EtherChannel インターフェイスをステートリンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリユニットから複製されます。Firepower 4100/9300 シャーシでは、EtherChannel を含むすべてのインターフェイスを、両方のユニットで事前に設定する必要があります。

- 高可用性の EtherChannel インターフェイスをモニターできます。アクティブなメンバーインターフェイスがスタンバイインターフェイスにフェールオーバーした場合、デバイスレベルの高可用性をモニタしているときには、EtherChannel インターフェイスで障害が発生しているようには見えません。すべての物理インターフェイスで障害が発生した場合にのみ、EtherChannel インターフェイスで障害が発生しているように見えます。
- EtherChannel インターフェイスを高可用性またはステートリンクに対して使用する場合、パケットが順不同にならないように、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。高可用性リンクとして使用中の EtherChannel の設定は変更できません。設定を変更するには、高可用性を一時的に無効にする必要があります。これにより、その期間中は高可用性が発生することはありません。

モデルのサポート

- 次のモデルでは、Device Manager で EtherChannel を追加できます。
 - Firepower 1000
 - Firepower 2100
 - Cisco Secure Firewall 3100
 - ISA 3000

Firepower 4100/9300 は EtherChannel をサポートしていますが、シャーシの FXOS で EtherChannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の Etherchannel は、単一の物理インターフェイスとともに Device Manager の [Interfaces] ページに表示されます。また、ASA 5500-X シリーズなどの他のモデルでは、Device Manager で EtherChannel を設定できません。

- EtherChannel で Firepower 1010 のスイッチポートまたは VLAN インターフェイスを使用することはできません。

EtherChannel の一般的なガイドライン

- モデルで利用可能なインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。
- 各チャンネルグループは、最大 8 個のアクティブインターフェイスを設定できます。
- チャンネルグループ内のすべてのインターフェイスは、メディアタイプと速度が同じでなければなりません。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GB と 10GB のインターフェイスなど）を混在させることはできません。ただし、Cisco Secure Firewall 3100 の場合は、速度が [SFP を検出 (Detect SFP)] に設定されている限り、異なるインターフェイス容量をサポートします。この場合、最も低い共通速度が使用されます。

- Threat Defense の EtherChannel の接続先デバイスも 802.3ad EtherChannel をサポートしている必要があります。
- Threat Defense デバイスは、VLAN タグ付きの LACPDU をサポートしていません。Cisco IOS `vlan dot1Q tag native` コマンドを使用して隣接スイッチのネイティブ VLAN タギングを有効にすると、Threat Defense デバイスはタグ付きの LACPDU をドロップします。隣接スイッチのネイティブ VLAN タギングは、必ずディセーブルにしてください。
- 次のデバイスモデルは、LACP レート高速機能をサポートしていません。LACP では常に通常のレートが使用されます。この値は設定不可能です。FXOS で EtherChannel を設定する Firepower 4100/9300 では、LACP レートがデフォルトで高速に設定されていることに注意してください。これらのプラットフォームでは、レートを設定できます。
 - Firepower 1000
 - Firepower 2100
 - Cisco Secure Firewall 3100
- 15.1(1)S2 以前の Cisco IOS ソフトウェアバージョンを実行する Threat Defense では、スイッチスタックへの EtherChannel の接続がサポートされていませんでした。デフォルトのスイッチ設定では、Threat Defense EtherChannel がクロススタックに接続されている場合、プライマリスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、`stack-mac persistent timer` コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0（無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- すべての Threat Defense コンフィギュレーションは、メンバー物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。

EtherChannel の追加

EtherChannel を追加して、メンバーインターフェイスを割り当てます。



(注) 次のモデルでは、Device Manager で EtherChannel を追加できます。

- Firepower 1000
- Firepower 2100
- Cisco Secure Firewall 3100
- ISA 3000

Firepower 4100/9300 は EtherChannel をサポートしていますが、シャーシの FXOS で EtherChannel のすべてのハードウェア設定を実行する必要があります。Firepower 4100/9300 の EtherChannel は、単一の物理インターフェイスとともに Device Manager の [Interfaces] ページに表示されます。また、ASA 5500-X シリーズなどの他のモデルでは、Device Manager で EtherChannel を設定できません。

始める前に

- チャネルグループ内のすべてのインターフェイスは、メディアタイプと速度が同じでなければなりません。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GB と 10GB のインターフェイスなど）を混在させることはできません。ただし、Cisco Secure Firewall 3100 の場合は、速度が [SFP 検出 (Detect SFP)] に設定されている限り、異なるインターフェイス容量をサポートします。この場合、最も低い共通速度が使用されます。
- メンバーインターフェイスに名前を付けることはできません。



注意 コンフィギュレーション内でインターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

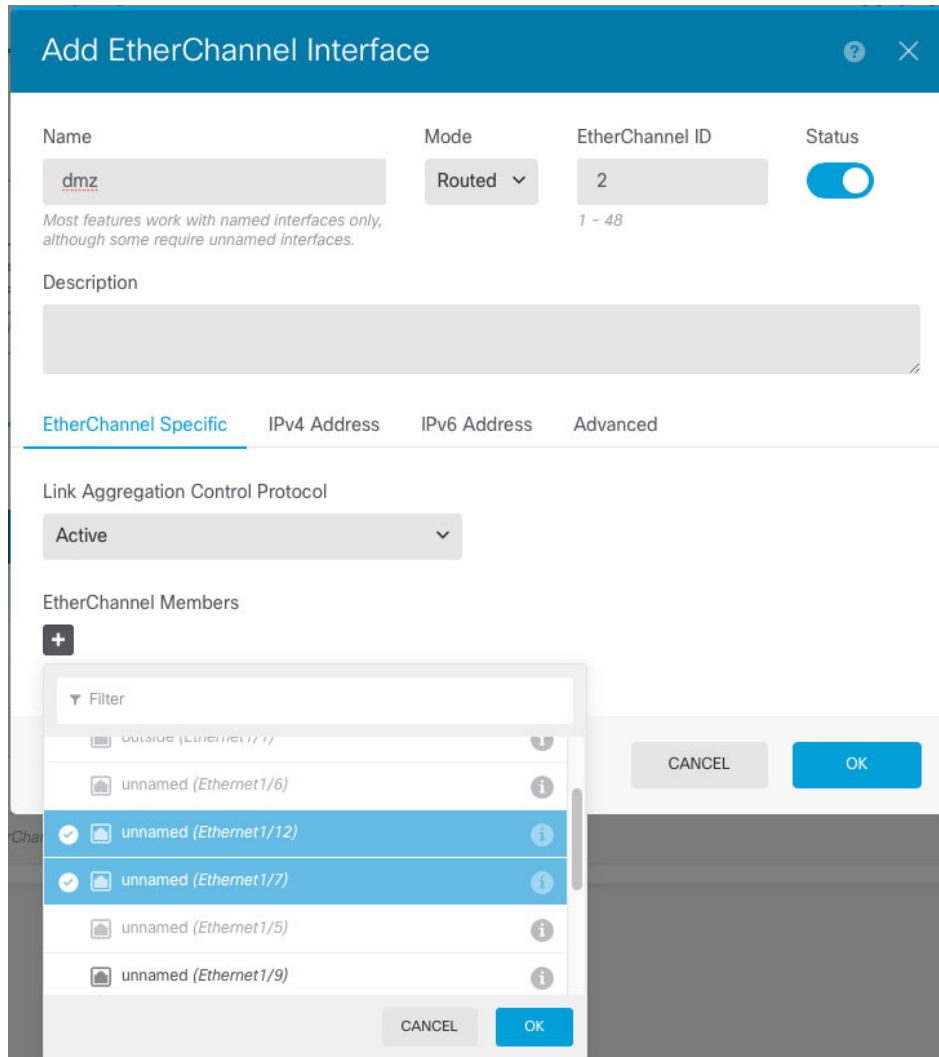
手順

ステップ 1 [デバイス (Device)] をクリックし、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックし、[EtherChannel (EtherChannels)] をクリックします。

[EtherChannel] リストには、既存の EtherChannel、それらの名前、アドレス、および状態が表示されます。各 EtherChannel のメンバーインターフェイスを表示するには、開/閉矢印をクリックします。メンバーインターフェイスは [インターフェイス (Interfaces)] ページにも個別に表示されます。

ステップ 2 [EtherChannelの作成 (Create EtherChannel)] をクリックするか (現在の EtherChannel がない場合)、またはプラスアイコン (+) をクリックして [EtherChannel] をクリックし、新しい EtherChannel を作成します。

ステップ 3 次を設定します。



a) [インターフェイス名 (Interface Name)] を設定します。


EtherChannel の名前を 48 文字以内で設定します。英字は小文字にする必要があります。例、[inside] または [outside]。

(注) 名前を変更すると、その変更は古い名前を使用しているすべての場所 (セキュリティゾーン、syslog サーバオブジェクト、DHCP サーバの定義を含む) に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

b) [モード (Mode)] を設定します。

- [ルーテッド (Routed)] : ルーテッドモードインターフェイスでは、トラフィックはフローの維持、IP 層と TCP 層の両方でのフロー状態のトラッキング、IP の最適化、TCP の正規化、ファイアウォールポリシーなど、すべてのファイアウォール機能の管理下に置かれます。トラフィックがインターフェイスを経由するようにする場合は、このモードを使用します。これが通常のインターフェイスモードです。
- [インライン (Inline)] : インターフェイスをインラインセットに追加すると、モードがインラインに変更されます。インラインをモードとして直接選択することはできません。インラインセットで使用するインターフェイスを編集する場合は、初期モードとしてルーテッドモードを選択し、どのタイプの IP アドレッシングも設定しないでください。
- [パッシブ (Passive)] : パッシブインターフェイスは、スイッチ SPAN またはミラーポートを使用してネットワーク中のトラフィックフローをモニタします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワークトラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。パッシブ展開で構成されたシステムでは、特定のアクション (トラフィックのブロッキングやシェーピングなど) を実行することができません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。このモードを選択する場合、残りの手順は実行しないでください。代わりに、[パッシブモードでの物理インターフェイスの設定 \(58 ページ\)](#) を参照してください。

c) [EtherChannel ID] を 1 ~ 48 の範囲で設定します (Firepower 1010 の場合は 1 ~ 8)。

d) [ステータス (Status)] スライダを [有効 (enabled)] 設定 () に設定します。

e) (任意) [説明 (Description)] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

f) [EtherChannelモード (EtherChannel Mode)] を指定します。

- [アクティブ (Active)] : LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブモードを使用する必要があります。
- [オン (On)] : EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

g) [EtherChannel メンバー (EtherChannel Members)] を追加します。

EtherChannel には、最大 8 つの (無名) インターフェイスを追加できます。

- インターフェイスの追加 : プラスアイコン (+) をクリックし、1 つ以上のインターフェイスをクリックし、[OK] をクリックします。
- インターフェイスの削除 : 対象にカーソルを合わせ、右側に表示される [x] をクリックします。

ステップ 4 [IPv4アドレス (IPv4 Address)] タブをクリックして、IPv4 アドレスを設定します。

[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

- [DHCP] : ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
 - [ルートメトリック (Route Metric)] : DHCP サーバからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1~255 の間です。デフォルトは 1 です。
 - [デフォルトルートを取得 (Obtain Default Route)] : デフォルト ルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。
- [スタティック (Static)] : 変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネットマスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

高可用性を設定し、このインターフェイスの HA をモニタしている場合は、同じサブネット上のスタンバイ IP アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットのネットワーク 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 ステートをトラックすることしかできません。

(注) インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレスプールを構成する必要があります。DHCP サーバの設定を参照してください。

- [PPPoE] : イーサネット経由のポイントツーポイント プロトコル (PPPoE) を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。
 - [グループ名 (Group Name)] : この接続を表すために選択した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 (PPPoE Password)] : ISP によって提供されたパスワードを指定します。

- [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 の学習済みルートメトリック (PPPoE Learned Route Metric)] : アドミニストレーティブディスタンスを既知の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。
- [PPPoE からデフォルトルートを取得 (Obtain Default Route from PPPoE)] : PPPoE サーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。
- [IP アドレスタイプ (IP Address Type)] : PPPoE サーバから IP アドレスを取得するには、[動的 (Dynamic)] を選択します。ISP から静的 IP アドレスが割り当てられている場合は、[静的 (Static)] を選択することもできます。

ステップ 5 (オプション) [IPv6 アドレス (IPv6 Address)] タブをクリックして、IPv6 アドレスを設定します。

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

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

- [アドレスの自動設定 (Address Auto Configuration)] : アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバルプレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティングサービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワークリンクの外部にはアクセスできません。リンクローカルアドレスは Modified EUI-64 インターフェイス ID に基づいています。

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、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。メッセージを抑制して、RFC に準拠するためには、[RA を抑制 (Suppress RA)] を選択します。

- [スタティックアドレスとプレフィックス (Static Address/Prefix)]: ステータス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、[IPv6 アドレス指定 \(5 ページ\)](#) を参照してください。

アドレスをリンクローカル専用として使用する場合は、[リンクローカル (Link - Local)] オプションを選択します。リンクローカルアドレスでは、ローカルネットワークの外部にはアクセスできません。リンクローカルアドレスはブリッジグループインターフェイスには設定できません。

(注) 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。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。

- [スタンバイ IP アドレス (Standby IP Address)]: 高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。
- [RA を抑制 (Suppress RA)]: ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるように、Threat Defense はルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメント メッセージ (ICMPv6 Type 134) は、設定済みの各 IPv6 インターフェイスに定期的送信されます。

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

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

ステップ 6 [詳細 (Advanced)] をクリックし、速度を設定して、メンバーインターフェイスの速度を設定します。

その他の高度なオプションを設定することもできます。[詳細オプションの設定 \(64 ページ\)](#) を参照してください。

ステップ 7 [OK] をクリックします。

次のタスク

- EtherChannel を適切なセキュリティゾーンに追加します。セキュリティゾーンの設定を参照してください。

VLAN インターフェイスおよびスイッチポートの設定 (Firepower 1010)

各 Firepower 1010 インターフェイスは、通常のファイアウォールインターフェイスとしてまたはレイヤ 2 ハードウェア スイッチ ポートとして実行するように設定できます。ここでは、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、VLAN へのスイッチ ポートの割り当てなど、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、この項では、サポート対象の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。

Firepower 1010 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

Firepower 1010 物理インターフェイスごとに、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その動作を設定できます。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。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 (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、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、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 VLAN 1 のアクセススイッチポートとして設定されています。Management 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、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 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

イーサネット 1/7 およびイーサネット 1/8 は Power on Ethernet+（PoE+）をサポートしていません。



(注) PoE は Firepower 1010E ではサポートされていません。

Firepower 1010 スイッチ ポートの注意事項と制約事項

高可用性

- 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ーできますが、スイッチポートはモニターできません。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

- 最大 60 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 :

- 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。[詳細オプションの設定 \(64 ページ\)](#) 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
- パッシブインターフェイス
- EtherChannel
- フェールオーバーおよびステートリンク

その他の注意事項と制約事項

- Firepower 1010 には、最大 60 の名前付きインターフェイスを設定できます。
- Management 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 は、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。

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。最初に、スイッチポートに割り当てられた VLAN ごとに VLAN インターフェイスを設定する必要があります。



- (注) 特定の VLAN 上でのスイッチポート間のスイッチングのみを有効にし、VLAN と他の VLAN またはファイアウォール インターフェイス間のルーティングを望まない場合は、VLAN インターフェイス名を空のままにします。この場合、IP アドレスを設定する必要もありません。IP 設定は無視されます。

手順

ステップ 1 [デバイス (Device)] をクリックし、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックしてから、[VLAN (VLANs)] をクリックします。

VLAN リストには、既存の VLAN インターフェイスが表示されます。各 VLAN に関連付けられているスイッチポートを表示するには、開/閉矢印をクリックします。また、スイッチポートは [インターフェイス (Interfaces)] ページでも個別に表示されます。

ステップ 2 [VLAN インターフェイスの作成 (Create VLAN Interface)] (現在の VLAN がない場合) またはプラスアイコン (+) をクリックして、新しい VLAN インターフェイスを作成します。

ステップ 3 次を設定します。

- a) [インターフェイス名 (Interface Name)] を設定します。


VLAN の名前を 48 文字以内で設定します。英字は小文字にする必要があります。例、[inside] または [outside]。

VLAN と他の VLAN またはファイアウォールインターフェイス間でルーティングしない場合は、VLAN インターフェイス名を空白のままにします。

(注) 名前を変更すると、その変更は古い名前を使用しているすべての場所（セキュリティゾーン、syslog サーバオブジェクト、DHCP サーバの定義を含む）に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

- b) [モード (Mode)] は [ルーテッド (Routed)] のままにします。

後でこの VLAN インターフェイスをブリッジグループに追加すると、モードは自動的に **BridgeGroupMember** に変更されます。ブリッジグループのメンバーインターフェイスには、IP アドレスを設定できません。

- c) [ステータス (Status)] スライダを [有効 (enabled)] 設定 () に設定します。
- d) [VLAN ID] を 1 ~ 4070 の間で設定します。

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。

- e) (任意) [このVLANに転送しない (Do not forward to this VLAN)] フィールドに、この VLAN インターフェイスがトラフィックを開始できない VLAN ID を入力します。

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。ホーム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、ホームVLANで [Block Traffic From this Interface to] オプションを使用できます。ビジネスネットワークはホーム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。

- f) (任意) [説明 (Description)] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

ステップ 4 [IPv4アドレス (IPv4 Address)] タブをクリックして、IPv4 アドレスを設定します。

[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

- [DHCP] : ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
 - [ルートメトリック (Route Metric)] : DHCPサーバからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1 ~ 255 の間です。デフォルトは 1 です。
 - [デフォルトルートを取得 (Obtain Default Route)] : デフォルトルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。
- [スタティック (Static)] : 変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネットマスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

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

(注) インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレスプールを構成する必要があります。DHCP サーバの設定を参照してください。

- [PPPoE] : イーサネット経由のポイントツーポイント プロトコル (PPPoE) を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。

- [グループ名 (Group Name)] : この接続を表すために選択した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 (PPPoE Password)] : ISP によって提供されたパスワードを指定します。
- [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 の学習済みルートメトリック (PPPoE Learned Route Metric)] : アドミニストレーティブディスタンスを既知の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。
- [PPPoE からデフォルトルートを取得 (Obtain Default Route from PPPoE)] : PPPoE サーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。
- [IP アドレスタイプ (IP Address Type)] : PPPoE サーバから IP アドレスを取得するには、[動的 (Dynamic)] を選択します。ISP から静的 IP アドレスが割り当てられている場合は、[静的 (Static)] を選択することもできます。

ステップ 5 (オプション) [IPv6 アドレス (IPv6 Address)] タブをクリックして、IPv6 アドレスを設定します。

- [状態 (State)] : グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効 (Enabled)] を選択します。リンクロー

カルアドレスはインターフェイスの MAC アドレス (*Modified EUI-64* 形式) に基づいて生成されます。

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

- [アドレスの自動設定 (Address Auto Configuration)]: アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバル プレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワーク リンクの外部にはアクセスできません。リンクローカルアドレスは Modified EUI-64 インターフェイス ID に基づいています。

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、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。メッセージを抑制して、RFC に準拠するためには、[RA を抑制 (Suppress RA)] を選択します。

- [スタティックアドレスとプレフィックス (Static Address/Prefix)]: ステートレス自動設定を使用しない場合、完全なスタティック グローバル IPv6 アドレスとネットワーク プレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、[IPv6 アドレス指定 \(5 ページ\)](#) を参照してください。

アドレスをリンクローカル専用として使用する場合は、[リンクローカル (Link - Local)] オプションを選択します。リンクローカルアドレスでは、ローカル ネットワークの外部にはアクセスできません。リンクローカルアドレスはブリッジグループ インターフェイスには設定できません。

(注) リンクローカルアドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。例、fe80::20d:88ff:feee:6a82。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。

- [スタンバイ IP アドレス (Standby IP Address)]: 高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイ アドレスは、スタンバイ デバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニタできず、リンク ステータスをトラッキングすることしかできません。
- [RA を抑制 (Suppress RA)]: ルータ アドバタイズメントを抑制するかどうかを指定します。ネイバー デバイスがデフォルトのルータ アドレスをダイナミックに把握できるよう

に、Threat Defenseはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメントメッセージ (ICMPv6 Type 134) は、設定済みの各 IPv6 インターフェイスに定期的送信されます。

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

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

ステップ6 (任意) [詳細オプションの設定 \(64 ページ\)](#)。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ7 [OK] をクリックします。

次のタスク

- VLAN を適切なセキュリティゾーンに追加します。[セキュリティゾーンの設定](#) を参照してください。

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。デフォルトでは、Ethernet1/2 ~ 1/8 のスイッチポートが有効になっていて、VLAN 1 に割り当てられています。



-
- (注) Firepower 1010 では、ネットワーク内のループ検出のためのスパニングツリープロトコルはサポートされません。したがって、Threat Defense デバイス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。
-

始める前に

アクセスポートを割り当てる VLAN ID に VLAN インターフェイスを追加します。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。「[VLAN インターフェイスの設定 \(36 ページ\)](#)」を参照してください。

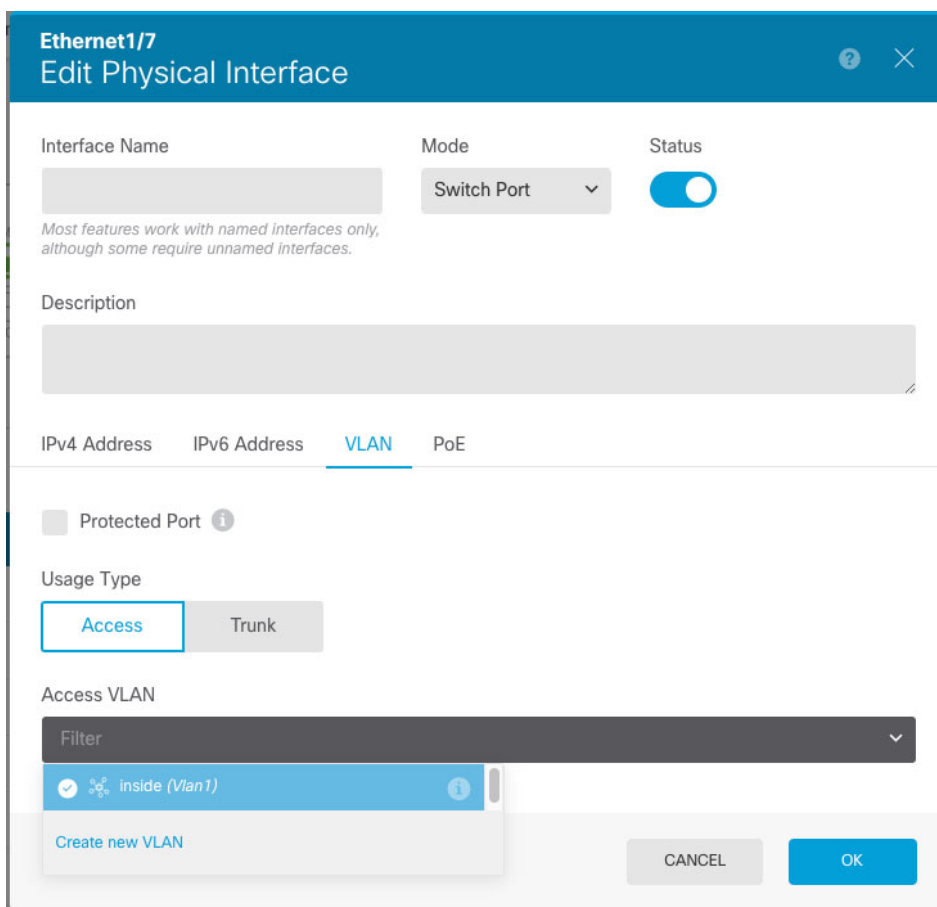
手順

ステップ1 [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックします。

[インターフェイス (Interfaces)] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ2 編集する物理インターフェイスの [編集 (edit)] アイコン (🔗) をクリックします。

ステップ3 次の設定を行います。



The screenshot shows the configuration page for Ethernet1/7. The 'Mode' is set to 'Switch Port' and the 'Status' is 'enabled'. The 'Usage Type' is set to 'Access'. The 'Access VLAN' dropdown menu is open, showing 'inside (Vlan1)' as the selected option. There are 'CANCEL' and 'OK' buttons at the bottom right.

- スイッチポートの [インターフェイス名 (Interface Name)] は設定しないでください。関連付けられている VLAN インターフェイスのみが名前付きインターフェイスです。
- [モード (Mode)] を [スイッチポート (Switch Port)] に設定します。
- [ステータス (Status)] スライダを [有効 (enabled)] 設定 (🔗) に設定します。
- (任意) [説明 (Description)] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

ステップ4 [VLAN] をクリックして、次のように設定します。

- a) (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、[保護ポート (Protected Port)] チェックボックスをオンにします。これにより、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぐことができます。
- スイッチポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチポートが相互に通信しないようにします。たとえば、3つの Web サーバーをホストする DMZ がある場合、各スイッチポートにこのオプションを適用すると、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。
- b) [使用タイプ (Usage Type)] で、[アクセス (Access)] をクリックします。
- c) [アクセスVLAN (Access VLAN)] の場合は、下矢印をクリックして既存の VLAN インターフェイスのいずれかを選択します。
- 新しいVLANインターフェイスを追加するには、[新しいVLANの作成 (Create new VLAN)] をクリックします。[VLAN インターフェイスの設定 \(36 ページ\)](#) を参照してください。

ステップ5 [OK] をクリックします。

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。

始める前に

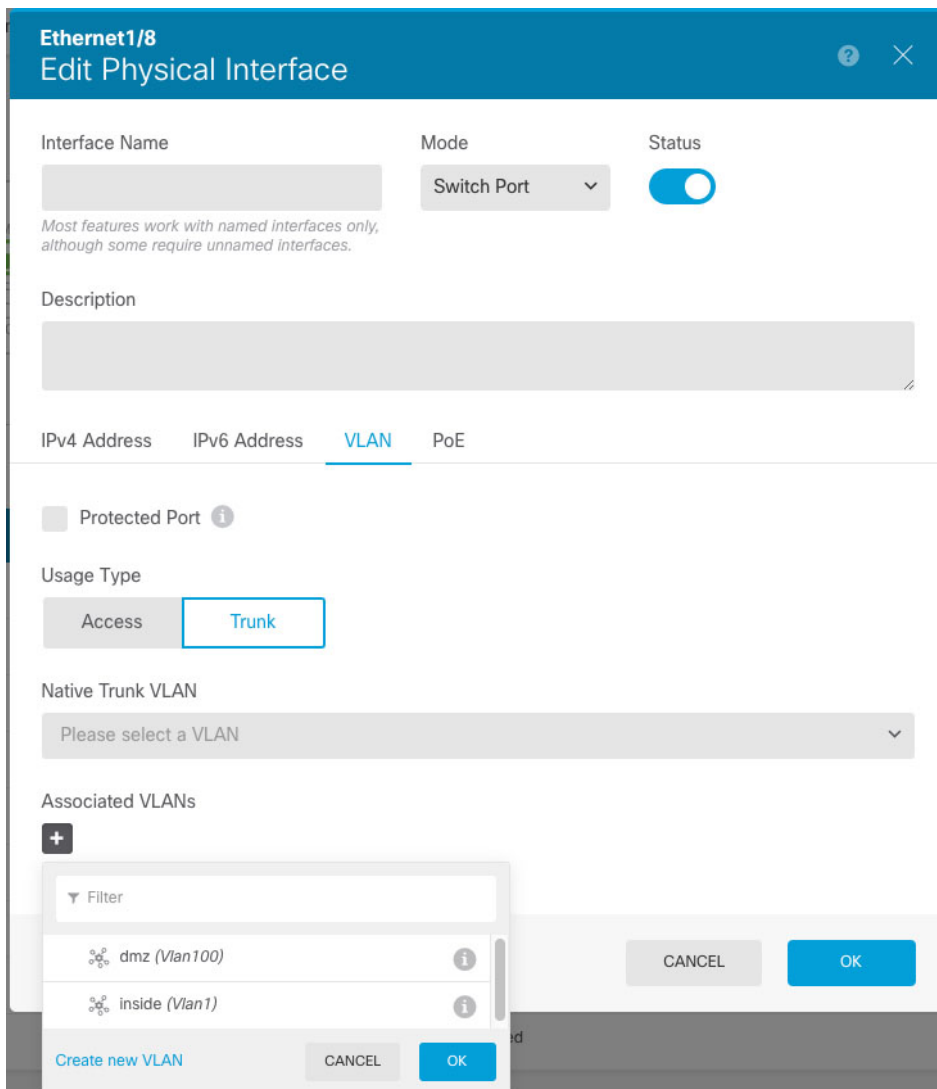
トランクポートを割り当てる VLAN ID ごとに VLAN インターフェイスを追加します。「[VLAN インターフェイスの設定 \(36 ページ\)](#)」を参照してください。

手順

ステップ1 [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックします。

[インターフェイス (Interfaces)] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

- ステップ 2** 編集する物理インターフェイスの [編集 (edit)] アイコン (🔗) をクリックします。
ステップ 3 次の設定を行います。



- スイッチポートの [インターフェイス名 (InterfaceName)] は設定しないでください。関連付けられている VLAN インターフェイスのみが名前付きインターフェイスです。
- [モード (Mode)] を [スイッチポート (Switch Port)] に設定します。
- [ステータス (Status)] スライダを [有効 (enabled)] 設定 (🔗) に設定します。
- (任意) [説明 (Description)] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

- ステップ 4** [VLAN] をクリックして、次のように設定します。

- a) (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、[保護ポート (Protected Port)] チェックボックスをオンにします。これにより、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぐことができます。
- スイッチポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチポートが相互に通信しないようにします。たとえば、3つの Web サーバーをホストする DMZ がある場合、各スイッチポートにこのオプションを適用すると、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。
- b) [使用タイプ (Usage Type)] で、[トランク (Trunk)] をクリックします。
- c) (任意) [ネイティブトランク VLAN (Native Trunk VLAN)] の場合は、下矢印をクリックしてネイティブ VLAN の既存の VLAN インターフェイスのいずれかを選択します。
- デフォルトのネイティブ VLAN ID 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。
- 新しい VLAN インターフェイスを追加するには、[新しい VLAN の作成 (Create new VLAN)] をクリックします。「[VLAN インターフェイスの設定 \(36 ページ\)](#)」を参照してください。
- d) [関連付けられている VLAN (Associated VLANs)] で、プラスアイコン (+) をクリックして、1 つまたは複数の既存の VLAN インターフェイスを選択します。
- このフィールドにネイティブ VLAN を含めても無視されます。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。また、まだネイティブ VLAN タグが付いているトラフィックを受信しません。
- 新しい VLAN インターフェイスを追加するには、[新しい VLAN の作成 (Create new VLAN)] をクリックします。[VLAN インターフェイスの設定 \(36 ページ\)](#) を参照してください。

ステップ 5 [OK] をクリックします。

Power over Ethernet の設定

Ethernet 1/7 および Ethernet 1/8 は、IP 電話や無線アクセスポイントなどのデバイス用に Power over Ethernet (PoE) をサポートしています。Firepower 1010 は、IEEE 802.3af (PoE) と 802.3at (PoE+) の両方をサポートしています。PoE+ は、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。PoE+ は、受電デバイスに最大 30 ワットの電力を提供できます。電力は必要なときのみ供給されます。

インターフェイスをシャットダウンすると、デバイスへの給電が無効になります。

PoE は、デフォルトで Ethernet 1/7 および Ethernet 1/8 で有効になっています。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。



(注) PoE は Firepower 1010E ではサポートされていません。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックします。

[インターフェイス (Interfaces)] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 Ethernet 1/7 または 1/8 の編集アイコン (🔍) をクリックします。

ステップ 3 [PoE] をクリックして、次のように設定します。

Ethernet1/8
Edit Physical Interface

Interface Name:

Mode: Switch Port

Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

IPv4 Address | IPv6 Address | VLAN | **PoE**

POWER OVER ETHERNET

Consumption Wattage:

4000 - 30000mW

CANCEL OK

- [Power Over Ethernet] を有効にするには、スライダ (🔍) をクリックして有効にします。PoE はデフォルトでイネーブルです。
- (任意) 必要なワット数を正確に把握している場合は、[消費ワット数 (Consumption Wattage)] を入力します。

デフォルトでは、PoE は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。Firepower 1010 は LLDP を使用して、適切なワット数をさらにネゴシエートします。特定のワット数が判明していて、LLDP ネゴシエーションを無効にする場合は、4000 ～ 3 万ミリワットの値を入力します。

ステップ 4 [OK] をクリックします。

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、物理インターフェイスを異なる VLAN ID が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。

物理インターフェイスをスイッチのトランクポートに接続する場合は、サブインターフェイスを作成します。スイッチ トランク ポートで表示できる各 VLAN のサブインターフェイスを作成します。物理インターフェイスをスイッチのアクセスポートに接続する場合は、サブインターフェイスを作成しても意味がありません。

ガイドラインと制約事項

- 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。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的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付け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にタグの付いていないパケットを通過させる場合には、通常のようにインターフェイスに名前を付けることができます。
- Firepower 1010：サブインターフェイスは、スイッチポートまたは VLAN インターフェイスではサポートされていません。
- 必要に応じて詳細設定を変更することはできますが、ブリッジグループメンバーインターフェイスの IP アドレスを設定することはできません。
- 同じ親インターフェイスのすべてのサブインターフェイスは、ブリッジグループメンバーかルーテッドインターフェイスのいずれかである必要があります。混在および一致はできません。
- Threat Defense はダイナミック トランキング プロトコル (DTP) をサポートしないため、接続されているスイッチポートを無条件に トランキングするように設定する必要があります。

- 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、脅威に対する防御デバイス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できません。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、脅威に対する防御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。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックします。

[インターフェイス (Interfaces)] タブがデフォルトで選択されます。EtherChannel にサブインターフェイスを追加するには、[EtherChannel] をクリックします。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ 2 次のいずれかを実行します。

- [Interfaces] ページで、プラスアイコン (+) をクリックして、新しいサブインターフェイスを作成します。
- [EtherChannel] ページで、プラスと下矢印のアイコン (+v) をクリックし、[Subinterface] を選択します。
- 編集するサブインターフェイスの編集アイコン (🔍) をクリックします。

サブインターフェイスが不要になった場合は、このサブインターフェイスの [削除 (delete)] アイコン (🗑️) をクリックして削除します。

ステップ 3 [ステータス (Status)] スライダを [有効 (enabled)] 設定 (🔘) に設定します。

ステップ 4 親インターフェイス、名前、および説明を設定します。

Add Subinterface ? ×

Parent Interface	Subinterface Name	Mode	Status
<input style="width: 90%;" type="text" value="Ethernet1/1"/>	<input style="width: 90%;" type="text" value="engineering"/>	<input style="width: 90%;" type="text" value="Routed"/>	<input checked="" type="checkbox"/>

Most features work with named interfaces only, although some require unnamed interfaces.

Description

VLAN ID	Subinterface ID
<input style="width: 90%;" type="text" value="200"/>	<input style="width: 90%;" type="text" value="200"/>

1 - 4094

IPv4 Address IPv6 Address Advanced

Type

IP Address and Subnet Mask

/

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

/

e.g. 192.168.5.16

- a) [Parent Interface] を選択します。

親インターフェイスは、サブインターフェイスの追加先となる物理インターフェイスです。いったん作成したサブインターフェイスの親インターフェイスは変更できません。

- b) [Subinterface Name] (最大 48 文字) を設定します。

英字は小文字にする必要があります。例、[inside] または [outside]。名前を設定しないと、インターフェイスの残りの設定は無視されます。

(注) 名前を変更すると、その変更は古い名前を使用しているすべての場所 (セキュリティゾーン、syslog サーバオブジェクト、DHCP サーバの定義を含む) に自動的に反映されます。ただし、通常、ポリシーや設定に名前のないインターフェイスは使用できないため、最初に古い名前を使用しているすべての設定を削除しないと、その名前は削除できません。

- c) [モード (Mode)] を [ルーテッド (Routed)] に設定します。

後でこのインターフェイスをブリッジグループに追加すると、モードは自動的に「BridgeGroupMember」に変更されます。ブリッジグループのメンバーインターフェイスには IP アドレスを設定できません。

- d) (任意) [Description] を設定します。

説明は 200 文字以内で、改行を入れずに 1 行で入力します。

- e) [VLAN ID] を設定します。

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する VLAN ID を 1～4094 の範囲で入力します。

- f) [サブインターフェイス ID (Subinterface ID)] を設定します。

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。この ID は、インターフェイス ID に追加されます。たとえば、Ethernet1/1.100 のようになります。便宜上 VLAN ID を一致させることもできますが、必須ではありません。いったん作成したサブインターフェイスの ID は変更できません。

ステップ 5 [IPv4 アドレス (IPv4 Address)] タブをクリックして、IPv4 アドレスを設定します。

[タイプ (Type)] フィールドから次のいずれかのオプションを選択します。

- [DHCP]: ネットワーク上の DHCP サーバからアドレスを取得する場合は、このオプションを選択します。高可用性を設定する場合、このオプションは使用できません。必要に応じて、次のオプションを変更します。
 - [ルートメトリック (Route Metric)]: DHCP サーバからデフォルトルートを取得する場合、学習済みルートまでのアドミニストレーティブ ディスタンスは 1～255 の間です。デフォルトは 1 です。
 - [デフォルトルートを取得 (Obtain Default Route)]: デフォルトルートを DHCP サーバから取得するかどうかを指定します。通常は、デフォルトのこのオプションを選択します。
- [スタティック (Static)]: 変更されない必要があるアドレスを割り当てる場合は、このオプションを選択します。インターフェイスに接続されたネットワークに対するインターフェイスの IP アドレスとサブネットマスクを入力します。たとえば、10.100.10.0/24 ネットワークを接続する場合は、「10.100.10.1/24」と入力します。このアドレスがネットワーク上ですでに使用されていないことを確認します。

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

(注) インターフェイスに対して設定されている DHCP サーバがある場合は、その設定が表示されます。DHCP アドレス プールを編集または削除できます。インターフェイスの IP アドレスを別のサブネットに変更する場合は、インターフェイスの変更を保存する前に、DHCP サーバを削除するか、新しいサブネット上にアドレスプールを構成する必要があります。DHCP サーバの設定を参照してください。

- [PPPoE] : イーサネット経由のポイントツーポイント プロトコル (PPPoE) を使用してアドレスを取得する必要がある場合は、このオプションを選択します。インターフェイスが DSL モデム、ケーブルモデム、または ISP への他の接続に接続されており、ISP が PPPoE を使用して IP アドレスを提供している場合は、PPPoE が必要になる場合があります。高可用性を設定する場合、このオプションは使用できません。次の値を設定します。

- [グループ名 (Group Name)] : この接続を表すために選択した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 (PPPoE Password)] : ISP によって提供されたパスワードを指定します。
- [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 の学習済みルートメトリック (PPPoE Learned Route Metric)] : アドミニストレーティブディスタンスを既知の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。
- [PPPoE からデフォルトルートを取得 (Obtain Default Route from PPPoE)] : PPPoE サーバからのデフォルトルートの取得を有効にするには、このチェックボックスをオンにします。
- [IP アドレスタイプ (IP Address Type)] : PPPoE サーバから IP アドレスを取得するには、[動的 (Dynamic)] を選択します。ISP から静的 IP アドレスが割り当てられている場合は、[静的 (Static)] を選択することもできます。

ステップ 6 (オプション) [IPv6 アドレス (IPv6 Address)] タブをクリックして、IPv6 アドレスを設定します。

- [状態 (State)] : グローバルアドレスを設定しない場合に IPv6 処理を有効にしてリンクローカルアドレスを自動的に設定するには、[有効 (Enabled)] を選択します。リンクロー

カルアドレスはインターフェイスの MAC アドレス (*Modified EUI-64* 形式) に基づいて生成されます。

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

- [アドレスの自動設定 (Address Auto Configuration)]: アドレスを自動的に設定するには、このオプションを選択します。IPv6 ステートレス自動設定では、デバイスが存在するリンクで使用する IPv6 グローバルプレフィックスのアドバタイズメントなどの、IPv6 サービスを提供するようにルータが設定されている場合に限り、グローバルな IPv6 アドレスが生成されます。IPv6 ルーティングサービスがリンクで使用できない場合、リンクローカル IPv6 アドレスのみが取得され、そのデバイスが属するネットワークリンクの外部にはアクセスできません。リンクローカルアドレスは Modified EUI-64 インターフェイス ID に基づいています。

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、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。メッセージを抑制して、RFC に準拠するためには、[RA を抑制 (Suppress RA)]を選択します。

- [スタティックアドレスとプレフィックス (Static Address/Prefix)]: ステートレス自動設定を使用しない場合、完全なスタティックグローバル IPv6 アドレスとネットワークプレフィックスを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、[IPv6 アドレス指定 \(5 ページ\)](#) を参照してください。

アドレスをリンクローカル専用として使用する場合は、[リンクローカル (Link - Local)]オプションを選択します。リンクローカルアドレスでは、ローカルネットワークの外部にはアクセスできません。リンクローカルアドレスはブリッジグループインターフェイスには設定できません。

(注) 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。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。

- [スタンバイ IP アドレス (Standby IP Address)]: 高可用性を設定し、このインターフェイスの HA をモニタリングしている場合は、同じサブネット上にスタンバイ IPv6 アドレスも設定します。スタンバイアドレスは、スタンバイデバイスでこのインターフェイスにより使用されます。スタンバイ IP アドレスを設定しない場合、アクティブユニットはネットワークテストを使用してスタンバイインターフェイスをモニタできず、リンクステータスをトラッキングすることしかできません。
- [RA を抑制 (Suppress RA)]: ルータアドバタイズメントを抑制するかどうかを指定します。ネイバーデバイスがデフォルトのルータアドレスをダイナミックに把握できるよう

に、Threat Defenseはルータ アドバタイズメントに参加できます。デフォルトでは、ルータ アドバタイズメントメッセージ (ICMPv6 Type 134) は、設定済みの各 IPv6 インターフェイスに定期的送信されます。

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

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

ステップ7 (任意) [詳細オプションの設定 \(64 ページ\)](#)。

詳細設定には、ほとんどのネットワークに適しているデフォルト設定があります。デフォルト設定はネットワークの問題を解決する場合のみ編集します。

ステップ8 [OK] をクリックします。

次のタスク

- サブインターフェイスを適切なセキュリティゾーンに追加します。[セキュリティゾーンの設定](#) を参照してください。
- ダイナミック DNS サービスプロバイダーに完全修飾ドメイン名 (FQDN) を登録し、DNS サーバの IPv4 と IPv6 の両方のインターフェイスアドレスが更新されるように DDNS を設定します。[ダイナミック DNS \(DDNS\) の設定](#) を参照してください。

パッシブインターフェイスの設定

パッシブインターフェイスは、スイッチ SPAN (スイッチドポートアナライザ) またはミラーポートを使用してネットワーク全体を流れるトラフィックをモニターします。SPAN またはミラーポートでは、スイッチ上の他のポートからトラフィックをコピーできます。この機能により、ネットワークトラフィックのフローに含まれなくても、ネットワークでのシステムの可視性が備わります。

パッシブ展開で設定されたシステムでは、特定のアクション (トラフィックのブロッキングなど) を実行できません。パッシブインターフェイスはすべてのトラフィックを無条件で受信します。このインターフェイスで受信されたトラフィックは再送されません。

パッシブインターフェイスを使用して、ネットワーク上のトラフィックをモニタし、トラフィックに関する情報を収集します。たとえば、侵入ポリシーを適用して、ネットワークを攻撃する脅威のタイプを特定したり、ユーザーが作成している Web 要求の URL カテゴリを確認できます。さまざまなセキュリティポリシーおよびルールを実装して、アクティブに展開されたシステムの動作を確認し、アクセス制御やその他のルールに基づいてトラフィックをドロップできます。

ただし、パッシブインターフェイスはトラフィックに影響を与えることができないため、多数の設定上の制限が存在します。これらのインターフェイスは、システムがトラフィックをピークすることを可能にするだけです。パッシブインターフェイスに入るパケットがデバイスを出ることはありません。

ここでは、パッシブインターフェイスとそれらの設定方法について説明します。

パッシブインターフェイスを使用する理由

パッシブインターフェイスの主な目的は、単純なデモンストレーションモードを提供することです。単一の送信元ポートをモニターするようにスイッチをセットアップし、ワークステーションを使用して、パッシブインターフェイスでモニターしたテストトラフィックを送信できます。これにより、脅威に対する防御システムが接続を評価したり脅威を特定したりする方法を確認できます。システムの実行方法に問題がなければ、その方法をネットワーク内にアクティブに展開して、パッシブインターフェイスの設定を削除できます。

ただし、次のサービスを提供するために実稼働環境でパッシブインターフェイスを使用することもできます。

- 純粋なIDS展開：システムをファイアウォールまたはIPS（侵入防御システム）として使用しない場合、IDS（侵入検知システム）としてパッシブに展開できます。この展開方法では、アクセス制御ルールを使用してすべてのトラフィックに侵入ポリシーを適用します。また、システムでスイッチ上の複数の送信元ポートもモニタします。さらに、ダッシュボードを使用してネットワークで見られる脅威をモニターできます。ただし、このモードでは、この脅威を防ぐためにできることはありません。
- 混合展開：アクティブルーテッドインターフェイスとパッシブインターフェイスを同じシステム上に混在させることができます。これにより、脅威に対する防御デバイスをいくつかのネットワークでファイアウォールとして展開すると同時に、複数のパッシブインターフェイスを他のネットワーク内のトラフィックをモニターするように設定することができます。

パッシブインターフェイスの制限

パッシブモードインターフェイスとして定義する物理インターフェイスには次の制限があります。

- パッシブインターフェイスのサブインターフェイスは設定できません。
- パッシブインターフェイスをブリッジグループに含めることはできません。
- パッシブインターフェイスでIPv4アドレスまたはIPv6アドレスを設定することはできません。
- パッシブインターフェイスに[管理専用 (Management Only)] オプションを選択することはできません。

- このインターフェイスはパッシブモードセキュリティゾーンにのみ含めることができます。ルーテッドセキュリティゾーンに含めることはできません。
- パッシブセキュリティゾーンをアクセス制御またはアイデンティティルールの送信元基準に含めることは可能です。パッシブゾーンを宛先基準で使用することはできません。パッシブゾーンとルーテッドゾーンを同じルールに混在させることもできません。
- パッシブインターフェイスの管理アクセスルール（HTTPS または SSH）を設定することはできません。
- パッシブインターフェイスを NAT ルールで使用することはできません。
- パッシブインターフェイスのスタティックルートを設定することはできません。パッシブインターフェイスをルーティングプロトコルの設定で使用することもできません。
- パッシブインターフェイスで DHCP サーバを設定することはできません。パッシブインターフェイスを使用して自動設定で DHCP 設定を取得することもできません。
- パッシブインターフェイスを syslog サーバ設定で使用することはできません。
- パッシブインターフェイスではどのタイプの VPN も設定することはできません。

ハードウェア Threat Defense パッシブインターフェイスのスイッチの設定

ハードウェア脅威に対する防御デバイス上のパッシブインターフェイスは、ネットワークスイッチを正しく設定している場合にのみ機能します。次の手順は、Cisco Nexus 5000 シリーズスイッチに基づいています。別のタイプのスイッチでは、コマンドが異なる可能性があります。

基本的な考え方としては、SPAN（スイッチドポートアナライザ）またはミラーポートを設定し、そのポートにパッシブインターフェイスを接続し、スイッチでモニタリングセッションを設定して、1つまたは複数の送信元ポートから SPAN またはミラーポートにトラフィックのコピーを送信します。

手順

ステップ1 スイッチ上のポートをモニタ（SPAN またはミラー）ポートとして設定します。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)#
```

ステップ2 モニタへのポートを特定するモニタリングセッションを定義します。

SPAN またはミラーポートを宛先ポートとして定義していることを確認します。次の例では、2つの送信元ポートがモニタされています。


```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

ステップ3 (任意) `show monitor session` コマンドを使用して、設定を確認します。

次の例に、セッション 1 の概要出力を示します。

```
switch# show monitor session 1 brief
  session 1
-----
type           : local
state          : up
source intf    :
  rx           : Eth1/7      Eth1/8
  tx           : Eth1/7      Eth1/8
  both         : Eth1/7      Eth1/8
source VSANs   :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

ステップ4 脅威に対する防御パッシブインターフェイスからスイッチ上の宛先ポートにケーブルを物理的に接続します。

物理接続を行う前後に、パッシブモードでインターフェイスを設定できます。[パッシブモードでの物理インターフェイスの設定 \(58 ページ\)](#) を参照してください。

Threat Defense Virtual パッシブインターフェイスの VLAN の設定

Threat Defense Virtual デバイスのパッシブインターフェイスは、仮想ネットワーク上で VLAN を正しく設定した場合にのみ機能します。次の手順を実行してください。

- Threat Defense Virtual インターフェイスを、無差別モードで設定した VLAN に接続します。その後、[パッシブモードでの物理インターフェイスの設定 \(58 ページ\)](#) での説明に従ってインターフェイスを設定します。パッシブインターフェイスでは、プロミスキャス VLAN 上のすべてのトラフィックのコピーが認識されます。
- 同じ VLAN に、1 つ以上のエンドポイント デバイス (仮想 Windows システムなど) を接続します。VLAN からインターネットへの接続がある場合は、単一のデバイスを使用できます。それ以外の場合は、トラフィックを通過させるために 2 つ以上のデバイスが必要です。URL カテゴリのデータを取得するには、インターネット接続が必要です。

パッシブモードでの物理インターフェイスの設定

インターフェイスはパッシブモードで設定できます。パッシブに機能する場合、インターフェイスは（ハードウェア デバイスの）スイッチそのものまたは（Threat Defense Virtual の）プロミスキャス VLAN に設定されたモニタリングセッションで送信元ポートからのトラフィックを単にモニターします。スイッチまたは仮想ネットワークで設定する必要がある内容の詳細については、次のトピックを参照してください。

- [ハードウェア Threat Defense パッシブインターフェイスのスイッチの設定（56 ページ）](#)
- [Threat Defense Virtual パッシブインターフェイスの VLAN の設定（57 ページ）](#)

トラフィックに影響を及ぼすことなくモニタ対象スイッチポートからのトラフィックを分析するには、パッシブモードを使用します。パッシブモードを使用するエンドツーエンドの例については、[ネットワーク上のトラフィックをパッシブにモニタする方法](#)を参照してください。

手順

ステップ 1 [Device] をクリックし、[Interfaces] サマリーにあるリンクをクリックし、[Interfaces] または [EtherChannel] をクリックします。

ステップ 2 編集する物理インターフェイスまたは EtherChannel の編集アイコン (🔧) をクリックします。

現在使用されていないインターフェイスを選択します。使用中のインターフェイスをパッシブインターフェイスに変換する場合は、最初にセキュリティゾーンからインターフェイスを削除し、そのインターフェイスを使用する他のすべての設定を削除する必要があります。

ステップ 3 [ステータス (Status)] スライダを [有効 (enabled)] 設定 (🔵) に設定します。

ステップ 4 次を設定します。

- [インターフェイス名 (Interface Name)] : 最大 48 文字のインターフェイスの名前。英字は小文字にする必要があります。たとえば、monitor などです。
- [モード (Mode)] : [パッシブ (Passive)] を選択します。
- (オプション) [説明 (Description)] : 説明は 200 文字以内で、改行を入れずに 1 行で入力します。

(注) IPv4 アドレスまたは IPv6 アドレスを設定することはできません。[詳細 (Advanced)] タブで変更できるのは、MTU、デュプレックス、速度設定のみです。

ステップ 5 [OK] をクリックします。

次のタスク

パッシブインターフェイスを作成するだけでは、インターフェイスで確認されるトラフィックの情報を十分にダッシュボードに示すことはできません、次の手順も実行する必要があります。

す。使用例で次の手順について説明します。ネットワーク上のトラフィックをパッシブにモニタする方法を参照してください。

- パッシブセキュリティゾーンを作成し、それにインターフェイスを追加します。セキュリティゾーンの設定を参照してください。
- パッシブセキュリティゾーンを送信元ゾーンとして使用するアクセス制御ルールを作成します。通常は、これらのルールに侵入ポリシーを適用して、IDS（侵入検知システム）モニタリングを実装します。アクセスコントロールポリシーを設定するを参照してください。
- 必要に応じて、パッシブセキュリティゾーン向けにSSL復号およびアイデンティティルールを作成し、セキュリティインテリジェンスポリシーを有効にします。

インラインセットの設定

インラインセットは、IPS専用インターフェイスを提供します。別のファイアウォールがこれらのインターフェイスを保護していて、ファイアウォール機能のオーバーヘッドを避けたい場合、IPS専用のインターフェイスを実装することがあります。

インラインセットはワイヤ上のバンプのように動作し、2つのインターフェイスを一緒にバンドルし、既存のネットワークに組み込みます。この機能によって、隣接するネットワークデバイスの設定がなくても、任意のネットワーク環境にデバイスをインストールすることができます。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インラインセットの外部に再送信されます。

ガイドラインと制約事項

- インラインセットは、Firepower 1000 シリーズ、Firepower 2100、Cisco Secure Firewall 3100 のデバイスモデルでのみ設定できます。
- インラインセットで許可されるインターフェイスタイプ：物理、EtherChannel。
- インラインセットに管理インターフェイスを含めることはできません。
- インラインセットで使用されるインターフェイスの属性（名前、モード、インターフェイス ID、MTU、IP アドレス）は変更できません。
- タップモードを有効にすると、Snort フェールオープンは無効になります。
- Bidirectional Forwarding Detection (BFD) エコーパケットは、インラインセットを使用するときに、デバイスを介して許可されません。BFDを実行しているデバイスの両側に2つのネイバーがある場合、デバイスは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。
- 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、デバイスではパケットで802.1Q ヘッダーが2つまでサポートされます（Q-in-Qサポートとも呼ばれます）。ファイアウォー

ルタイプのインターフェイスでは Q-in-Q はサポートされず、802.1Q ヘッダーは 1 つだけサポートされることに注意してください。

- インラインセット内のインターフェイスは、ルーティング、NAT、DHCP（サーバー、クライアント、またはリレー）、VPN、TCP インターセプト、アプリケーション インспекション、または NetFlow をサポートしません。

始める前に

- 脅威防御インライン ペア インターフェイスに接続する STP 対応スイッチに対して STP PortFast を設定することを推奨します。
- インラインセットのメンバーとなる物理インターフェイスまたは EtherChannel インターフェイスを設定します。名前、デュプレックス、速度、ルーテッドモード（パッシブを選択しないでください）の値のみを設定します。手動 IP アドレス、DHCP、または PPoE などのアドレッシングタイプは設定しないでください。



(注) インターフェイスをインラインセットに追加すると、モードがインラインに変更されます。インラインをモードとして直接選択することはできません。

手順

ステップ 1 [デバイス (Device)] をクリックして、[インターフェイス (Interfaces)] サマリーのリンクをクリックしてから、[インラインセット (Inline Sets)] をクリックします。

ステップ 2 次のいずれかを実行します。

- [+] をクリックして、新しいインラインセットを作成します。
- 既存のインラインセットを変更するには、そのインラインセットの編集アイコン (🔍) をクリックします。
- インラインセットが不要になった場合は、そのインラインセットの削除アイコン (🗑️) をクリックします。

ステップ 3 次のオプションを構成します

- インラインセットの [名前 (Name)] を設定します。
- (オプション) [MTU] を変更します。

デフォルトの MTU は 1500 です。より大きなパッケージを処理するには、より高い値に設定できます。

ステップ 4 [一般 (General)] タブで、インターフェイスペアを追加します。ペアごとに2つのインターフェイスを選択する必要があります。不要なペアは削除できます。

インラインセットにインターフェイスを追加すると、そのモードは[ルーテッド (Routed)] から[インライン (Inline)]に変更されます。インターフェイスの属性は、インラインセットから削除するまで編集できません。

ステップ 5 [詳細 (Advanced)] タブで、次のオプションパラメータを設定します。

- [モード (Mode)] : [インライン (Inline)] モードは標準モードであり、デバイスを通するトラフィックに影響を与えます。

[タップ (Tap)] モードでは、デバイスはインラインで展開されますが、ネットワークトラフィックフローは妨げられません。代わりに、デバイスは各パケットのコピーを作成して、パケットを分析できるようにします。それらのタイプのルールでは、ルールがトリガーされると侵入イベントが生成され、侵入イベントのテーブルビューにはトリガーの原因となったパケットがインライン展開でドロップされたことが示されることに注意してください。インライン展開されたデバイスでタップモードを使用することには、利点があります。たとえば、デバイスがインラインであるかのようにデバイスとネットワーク間の配線をセットアップし、デバイスで生成される侵入イベントのタイプを分析することができます。その結果に基づいて、効率性に影響を与えることなく最適なネットワーク保護を提供するように、侵入ポリシーを変更してドロップルールを追加できます。デバイスをインラインで展開する準備ができたなら、タップモードを無効にして、デバイスとネットワーク間の配線を再びセットアップせずに、不審なトラフィックのドロップを開始することができます。[タップ (Tap)] モードは、トラフィックによってはデバイスのパフォーマンスに大きく影響することに注意してください。

- [Snortフェールオープン (Snort Fail Open)] : Snort プロセスがビジーであるか、ダウンしている場合に、インスペクション (有効) またはドロップ (無効) されることなく、新規および既存のトラフィックを通させる場合は、[ビジー (Busy)] オプションおよび[ダウン (Down)] オプションのいずれかまたは両方を有効または無効にします。

デフォルトでは、Snort プロセスがダウンしている場合、トラフィックはインスペクションなしで通過し、Snort プロセスがビジーの場合、トラフィックはドロップされます。

Snort プロセスが次の場合。

- [ビジー (Busy)] : トラフィックバッファが満杯なため、トラフィックを高速処理できません。デバイスの処理量を超えるトラフィックが存在していること、またはその他のソフトウェアリソースの問題があることを示しています。
- [ダウン (Down)] : プロセスの再起動を必要とする設定を展開したため、プロセスが再起動中です。

Snort プロセスは、ダウンしてから再起動すると、新しい接続のインスペクションを実行します。Snort プロセスでは、誤検出と検出漏れを防ぐために、インラインインターフェイス、ルーテッドインターフェイス、またはトランスペアレントインターフェイスの既存の接続のインスペクションは実行されません。これは、プロセスがダウンしていた間に初期のセッション情報が失われている可能性があるためです。

(注) Snort フェールオープン時には、Snort プロセスに依存する機能は働きません。そのような機能には、アプリケーション制御とディープインスペクションが含まれます。システムでは、シンプルかつ容易に判断できるトランスポート層とネットワークの特性を使用して、基本的なアクセスコントロールのみ実行されます。

- [リンクステートの伝達 (Propagate Link State)] : リンクステートの伝達を設定します。

リンクステートの伝達によって、インラインセットのインターフェイスの1つが停止した場合、インラインインターフェイスペアの2番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2番目のインターフェイスも自動的に起動します。つまり、1つのインターフェイスのリンクステートが変化すると、デバイスはその変化を検知し、その変化に合わせて他のインターフェイスのリンクステートを更新します。ただし、デバイスからリンクステートの変更が伝達されるまで最大4秒かかります。障害状態のネットワークデバイスを自動的に避けてトラフィックを再ルーティングするようにルータが設定されている復元力の高いネットワーク環境では、リンクステートの伝達が特に有効です。

ステップ6 [OK] をクリックします。

高度なインターフェイス オプションの設定

[詳細 (Advanced)] オプションには、MTU、ハードウェア設定、管理専用、MAC アドレス、およびその他の設定が含まれています。

MAC アドレスについて

Media Access Control (MAC) アドレスを手動で設定してデフォルトをオーバーライドできません。

高可用性設定の場合は、インターフェイスのアクティブ MAC アドレスとスタンバイ MAC アドレスの両方を設定できます。アクティブユニットがフェールオーバーしてスタンバイユニットがアクティブになると、その新規アクティブユニットがアクティブな 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。

デフォルトの MAC アドレス

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は Burned-In MAC Address を使用します。
- VLAN インターフェイス (Firepower 1010) : 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。 [詳細オプションの設定 \(64 ページ\)](#) を参照してください。

- **EtherChannel** : EtherChannel の場合は、そのチャン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トランスペアレントになります。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ためです。ポートチャンネルインターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。
- **サブインターフェイス** : 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バインドイン MAC アドレスを使用します。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、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。

MTU について

MTU は、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 に設定した場合、想定されるフレームサイズはヘッダーを含めて 1518 バイト、VLAN を使用する場合は 1522 バイトです。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。

パス MTU ディスカバリ

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。

MTU およびフラグメンテーション

IPv4 では、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。フラグメントは宛先（場合によっては中間ホップ）で組み立て直されますが、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 では、通常、パケットをフラグメント化することはできません。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 サイズ以内に収める必要があります。

UDP または ICMP の場合、アプリケーションではフラグメント化を避けるために MTU を考慮する必要があります。



- (注) 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 が大きいほど、大きいパケットを送信できます。パケットが大きいほど、ネットワークの効率が良くなる可能性があります。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 Threat Defense インターフェイスとトラフィックパス内のその他のデバイスのインターフェイスでは、MTU が同じになるよう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**：ジャンボフレームとは、標準的な最大値 1522 バイト（レイヤ 2 ヘッダーおよび VLAN ヘッダーを含む）より大きく、9216 バイトまでのイーサネットパケットのことです。ジャンボフレームに対応するために、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。



- (注) MTU を増やすとジャンボフレームに割り当てるメモリが増え、他の機能（アクセスルールなど）の最大使用量が制限される場合があります。Threat Defense Virtual のデフォルト値の 1,500 よりも MTU のサイズを大きくする場合は、システムを再起動する必要があります。高可用性にデバイスが設定されている場合、スタンバイデバイスも再起動する必要があります。ジャンボフレームのサポートが常に有効な場合、その他のモデルを再起動する必要はありません。

詳細オプションの設定

高度なインターフェイスオプションには、ほとんどのネットワークに適合するデフォルト設定が用意されています。ネットワークの問題を解決している場合または高可用性を設定する場合にのみ、これを設定します。


次の手順では、インターフェイスが定義済みであることを前提としています。インターフェイスを最初に編集または作成するときに、これらの設定を編集することもできます。

制限事項

- ブリッジグループの場合は、このほとんどのオプションはメンバーインターフェイスに対して設定します。DAD 試行回数と HA モニタリングの有効化を除き、これらのオプションはブリッジ仮想インターフェイス（BVI）では使用できません。
- 管理インターフェイスに MTU、デプレックス、速度を設定することはできません。

- 拡張オプションは、Firepower 1010 スイッチポートでは使用できません。
- Firepower 4100/9300 のインターフェイスにデュプレックスおよび速度を設定することはできません。インターフェイスのこれらの機能を設定するには、FXOS を使用します。
- パッシブ インターフェイスでは、MTU、デュプレックス、速度のみ設定できます。インターフェイスの管理のみを行うことはできません。

手順

- ステップ 1** [デバイス (Device)] をクリックし、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックし、次にインターフェイスタイプをクリックして、インターフェイスのリストを表示します。
- ステップ 2** 編集するインターフェイスの編集アイコン () をクリックします。
- ステップ 3** [詳細オプション (Advanced Options)] をクリックします。
- ステップ 4** インターフェイスの状態を高可用性設定でピア装置にフェールオーバーするかどうか判断する際の要素にする場合は、[HA モニタリングの有効化 (Enable for HA Monitoring)] を選択します。
- このオプションは、高可用性を設定しない場合は無視されます。インターフェイスの名前を設定しない場合も、無視されます。
- ステップ 5** データ インターフェイスを管理専用指定する場合は、[管理専用 (Management Only)] を選択します。
- 管理専用インターフェイスはトラフィックの通過を許可しないため、データインターフェイスを管理専用で設定する意味はあまりありません。管理/診断インターフェイスは、常に管理専用であるため、この設定を変更することはできません。
- ステップ 6** Cisco Trustsec を有効にするには、[セキュリティグループタグの伝達 (Propagate Security Group Tag)] を選択します。
- 名前付きか名前なしにかかわらず、物理、サブインターフェイス、EtherChannel、VLAN、管理、または BVI インターフェイスで Cisco TrustSec を有効または無効にできます。デフォルトでは、インターフェイスに名前を付けると、Cisco TrustSec が自動的に有効になります。
- ステップ 7** [MTU] (最大伝送ユニット) を任意の値に設定します。
- デフォルトの MTU は 1500 バイトです。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。ジャンボフレームが頻繁にやり取りされるネットワークでは、大きな値に設定します。
- (注) ISA 3000 シリーズデバイス、Threat Defense Virtual で MTU を 1500 より大きい値に設定する場合は、デバイスを再起動する必要があります。高可用性にデバイスが設定されている場合、スタンバイデバイスも再起動する必要があります。ジャンボフレームのサポートが常に有効な場合、その他のモデルを再起動する必要はありません。
- ステップ 8** (物理インターフェイスのみ) 速度およびデュプレックスの設定を変更します。

デフォルトでは、インターフェイスは接続相手のインターフェイスに対し、互いに最適なデュプレックスおよび速度をネゴシエートしますが、必要に応じて、特定のデュプレックスおよび速度を強制的に適用することもできます。記載されているオプションは、インターフェイスでサポートされているものだけです。ネットワークモジュールのインターフェイスにこれらのオプションを設定する前に、[インターフェイス設定の制限事項 \(6 ページ\)](#) をお読みください。

- [二重 (Duplex)] : [ハーフ (Half)], または [フル (Full)] 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)] : 実際のオプションは、モデルとインターフェイスタイプによって異なります。速度、[自動 (Auto)]、[ネゴシエーションなし (No Negotiate)]、または[SFPを検出 (Detect SFP)] を選択してください。Firepower 1100 または 2100 SFP ファイバポートの場合、[ネゴシエーションなし (No Negotiate)] を指定すると速度が 1,000 Mbps に設定され、フロー制御パラメータとリモート障害情報のリンクネゴシエーションがディセーブルになります。(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。
- (Cisco Secure Firewall 3100 のみ) [自動ネゴシエーション (Auto Negotiation)] : インターフェイスのタイプに応じて、フロー制御パラメータとリモート障害情報のリンクステータス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 に追加する前に前方誤り訂正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 108 条 RS-FEC	第 108 条 RS-FEC
25G-LR	第 108 条 RS-FEC	第 108 条 RS-FEC
10/25G-CSR	第 108 条 RS-FEC	第 74 条 FC-FEC
25G-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 9 [IPv6設定 (IPv6 Configuration)] を変更します。

- [DHCPクライアントの有効化 (Enable DHCP Client)] : DHCPv6 を使用してアドレスを取得します。

ルータアドバタイズメントからデフォルトルートを取得するには、[DHCPを使用してデフォルトルートを取得 (Obtain default route using DHCP)] をオンにします。

- [Enable DHCP for IPv6 address configuration] : IPv6 ルータのアドバタイズメント パケットに、管理アクセス設定フラグを設定するかどうか。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。
- [Enable DHCP for IPv6 non-address configuration] : IPv6 ルータのアドバタイズメント パケットに、その他のアクセス設定フラグを設定するかどうか。このフラグは、DHCPv6 から DNS サーバ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。
- [DADの試行 (DAD Attempts)] : インターネット上で重複アドレス検出 (DAD) を実行する頻度 (0 ~ 600)。デフォルトは 1 です。ステートレス自動設定プロセスでは、DAD 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検証します。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。インターフェイスは、ネイバー送信要求メッセージを使用して、重複アドレス検出を実行します。重複アドレス検出 (DAD) プロセスを無効にするには、この値を 0 に設定します。

ステップ 10 (必要に応じて、サブインターフェイスおよび高可用性装置に推奨されます。) MAC アドレスを設定します。

デフォルトでは、システムはインターフェイスのネットワークインターフェイスカード (NIC) に焼き込まれた MAC アドレスを使用します。したがって、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 MAC アドレスを使用するため、サブインターフェイスごとに一意のアドレスを作成する必要がある場合があります。手動設定されたアクティブ/スタンバイ MAC アドレスも、高可用性を設定する場合に推奨されます。MAC アドレスを定義すると、フェールオーバー時にネットワークの一貫性を維持できます。

- [MACアドレス (MAC Address)] : H.H.H 形式の Media Access Control。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は 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。
- [スタンバイMACアドレス (Standby MAC Address)] : 高可用性で使用します。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 11 [OK] をクリックします。

インターフェイスの変更のスキャンとインターフェイスの移行

デバイスのインターフェイスを変更すると、デバイスは変更が発生したことを Device Manager に通知します。インターフェイスのスキャンを実行するまで、設定を展開することはできません。Device Manager では、セキュリティポリシー内のインターフェイスを別のインターフェイスに移行することができるため、インターフェイスの削除はほぼシームレスに実行できます。

インターフェイスのスキャンと移行について

Scanning

デバイスのインターフェイスを変更すると、デバイスは変更が発生したことを Device Manager に通知します。インターフェイスのスキャンを実行するまで、設定は展開できません。インターフェイスの追加、削除、または復元を検出するスキャンの後に設定を展開できますが、削除されたインターフェイスを参照している設定の部分は展開されません。

スキャンを必要とするインターフェイスの変更には、インターフェイスの追加や削除が含まれます。たとえば、ネットワークモジュールの変更、Firepower 4100/9300 シャーシ上に割り当てられたインターフェイスの変更、Threat Defense Virtual でのインターフェイスの変更などです。

次の変更は、スキャン後の展開をブロックしません。

- セキュリティゾーンのメンバーシップ
- EtherChannel インターフェイスのメンバーシップ
- Firepower 1010 VLAN インターフェイス スイッチ ポートのメンバーシップ
- BVI を参照するポリシーのブリッジ グループ インターフェイスのメンバーシップ



(注) syslog サーバーの出力インターフェイスの変更によって展開がブロックされることはありませんが、syslog サーバーの設定は、手動で、またはインターフェイス交換機能を使用して修正する必要があります。

Migrating

新しいインターフェイスの追加や未使用のインターフェイスの削除が、脅威に対する防御の設定に与える影響は最小限です。ただし、セキュリティポリシーで使用されているインターフェイスを削除すると、設定に影響を与えます。インターフェイスは、セキュリティゾーン、NAT、VPN、ルーティング、DHCP サーバーなど、脅威に対する防御設定内の多くの場所で直接参照できます。

DeviceManager では、セキュリティポリシー内のインターフェイスを別のインターフェイスに移行することができるため、インターフェイスの削除はほぼシームレスに実行できます。



- (注) 移行機能は、名前、IPアドレス、およびその他の設定をインターフェイス間でコピー「しません」。この機能は、古いインターフェイスではなく新しいインターフェイスを参照するようにセキュリティポリシーを変更します。移行する前に、新しいインターフェイスの設定を手動で設定する必要があります。

インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスを移行することをお勧めします。インターフェイスの追加と削除を同時に行っても移行プロセスは機能します。ただし、削除されたインターフェイスやそれらを参照するポリシーを「手動で」編集することはできません。そのため、移行を段階的に実行する方が簡単になる場合があります。

同じタイプのインターフェイスを交換する場合（たとえば、ネットワークモジュールを RMA する必要がある場合）は、次のことができます。1. シャーシからモジュールを取り外す。2. スキャンを実行する。3. 削除されたインターフェイスとは関係のない変更を展開する。4. モジュールを交換する。5. 新しいスキャンを実行する。6. インターフェイス関連の変更を含め、設定を展開します。新しいインターフェイスのインターフェイス ID と特性が古いインターフェイスと同じである場合は、移行を実行する必要はありません。

インターフェイスのスキャンと移行に関する注意事項と制限事項

サポートされていないインターフェイスの移行

- BVI への物理インターフェイス
- ファイアウォール インターフェイスへのパッシブインターフェイス
- ブリッジグループメンバー
- EtherChannel インターフェイスメンバー
- ISA 3000 ハードウェア バイパス メンバー
- Firepower 1010 VLAN インターフェイスまたはスイッチポート
- 診断インターフェイス
- HA フェールオーバーおよびステートリンク
- さまざまなタイプのインターフェイスの移行（たとえば、物理インターフェイスを必要とする機能へのブリッジグループ インターフェイスの移行）

その他のガイドライン

- インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスを移行することをお勧めします。

- Threat Defense Virtual では、インターフェイスリストの末尾でインターフェイスの追加や削除が行われるだけです。他の場所でインターフェイスを追加または削除した場合、ハイパーバイザによってインターフェイスの番号が再設定され、その結果、設定内のインターフェイス ID が誤ったインターフェイスと一致します。
- スキャン/移行が失敗した場合は、シャーシの元のインターフェイスを復元し、元の状態に戻すために再スキャンします。
- バックアップの場合は、新しいインターフェイスを使用して新しいバックアップを作成してください。古い設定で復元すると、古いインターフェイス情報が復元され、スキャン/置換を再度実行する必要があります。
- HA の場合は、アクティブユニットでインターフェイススキャンを実行する前に、両方の装置で同じインターフェイスの変更を行います。アクティブユニットでスキャン/移行を実行する必要があるだけです。設定の変更はスタンバイユニットに複製されます。

インターフェイスのスキャンと移行

Device Manager でインターフェイスの変更をスキャンし、削除されたインターフェイスからインターフェイス設定を移行します。インターフェイス設定の移行のみを必要とする場合は（スキャンは不要）、次の手順のうちスキャンに関連するステップを無視してください。



- (注) 移行機能は、名前、IPアドレス、およびその他の設定をインターフェイス間でコピー「しません」。この機能は、古いインターフェイスではなく新しいインターフェイスを参照するようにセキュリティポリシーを変更します。移行する前に、新しいインターフェイスの設定を手動で設定する必要があります。

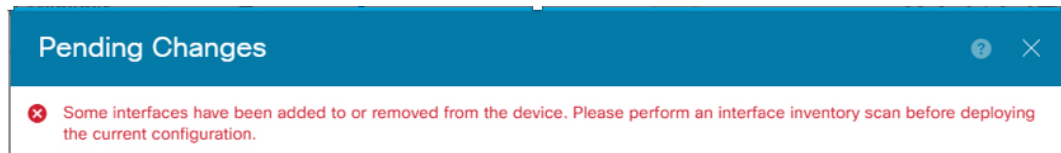
手順

ステップ1 シャーシでインターフェイスを追加または削除します。

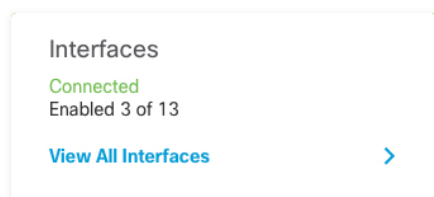
インターフェイスを削除する必要がある場合は、古いインターフェイスを削除する「前に」、新しいインターフェイスを追加し、古いインターフェイスの置き換えを実行することをお勧めします。


ステップ2 インターフェイスの変更をスキャンします。

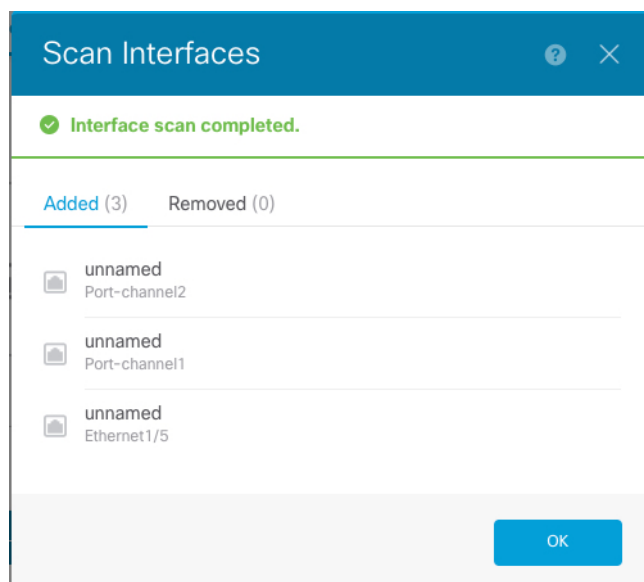
インターフェイスのスキャンを実行するまで、設定は展開できません。スキャンの前に展開しようとする、次のエラーが表示されます。



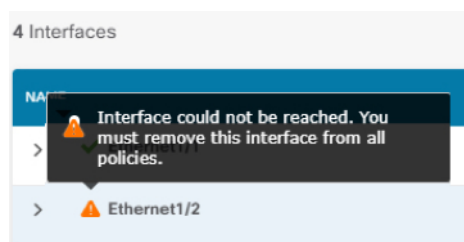
- a) [デバイス (Device)]をクリックしてから、[インターフェイス (Interfaces)]サマリーにある [すべてのインターフェイスを表示 (View All Interfaces)]リンクをクリックします。



- b) [インターフェイス (Interfaces)]アイコン () をクリックします。
 c) インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。



スキャン後、削除されたインターフェイスは、[インターフェイス (Interfaces)]ページに注意記号とともに表示されます。



ステップ3 既存のインターフェイスを新しいインターフェイスに移行するには、次の手順を実行します。

- a) 新しいインターフェイスに名前、IP アドレスなどを設定します。

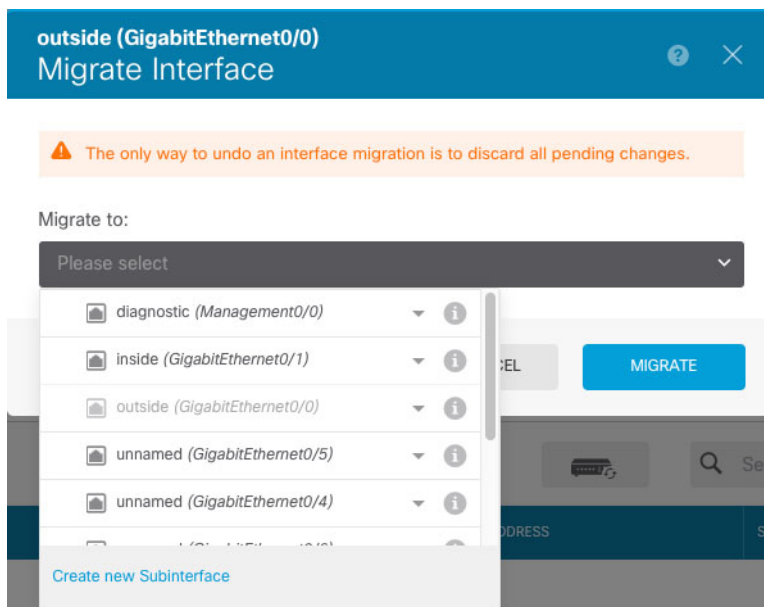
削除するインターフェイスの既存の IP アドレスと名前を使用する場合は、新しいインターフェイスでこれらの設定を使用できるように、まず古いインターフェイスをダミーの名前と IP アドレスで再設定する必要があります。

- b) 古いインターフェイスの [移行 (Migrate)]アイコンをクリックします。

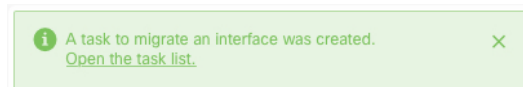


このプロセスによって、インターフェイスを参照しているすべての設定で、古いインターフェイスが新しいインターフェイスに移行されます。

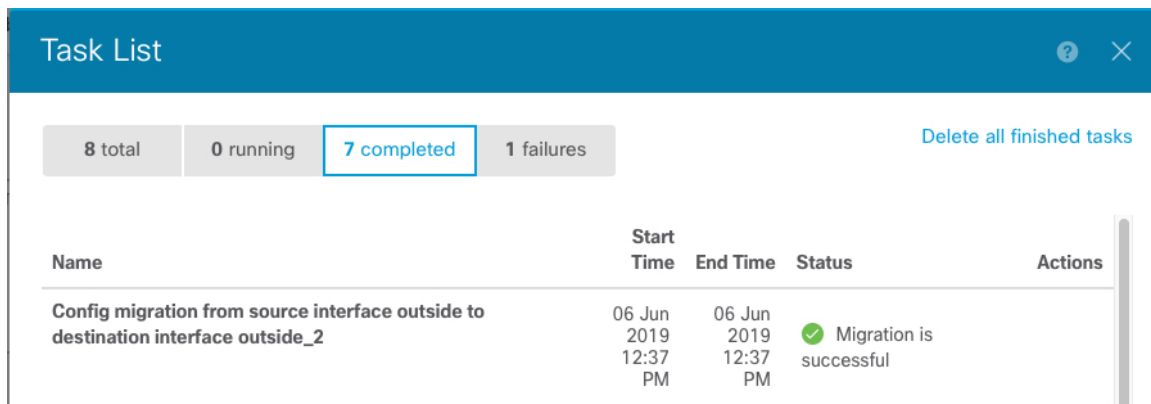
- c) [移行先： (Migrate to:)] ドロップダウンリストから新しいインターフェイスを選択します。



- d) [インターフェイス (Interfaces)] ページにメッセージが表示されます。メッセージ内のリンクをクリックします。



- e) [タスクリスト (Task List)] を調べて、移行が成功したことを確認します。

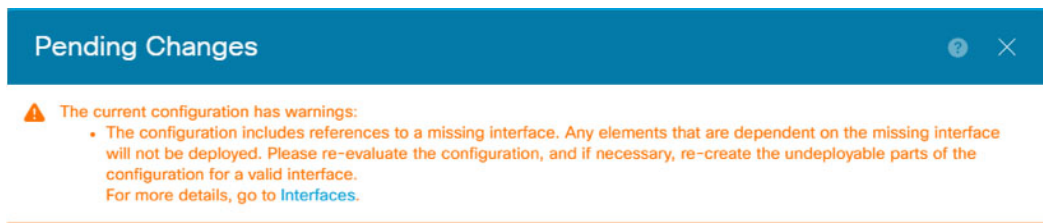


- f) 移行が失敗した場合は、API エクスプローラで理由を確認できます。

API エクスプローラを開くには、[詳細オプション (More options)] ボタン (☰) をクリックし、[APIエクスプローラ (API Explorer)] を選択します。[インターフェイス (Interface)] > [GET /jobs/interfacemigrations] を選択し、[試してみる (Try it Out!)] をクリックします。

ステップ 4 設定を展開します。

削除されたインターフェイスを参照する設定の部分は展開されません。その場合、次のメッセージが表示されます。



ステップ 5 シャーシの古いインターフェイスを取り外し、別のスキャンを実行します。

削除されたインターフェイスのうちポリシーで使用されなくなったものは、[インターフェイス (Interfaces)] ページから削除されます。

ステップ 6 設定を再度展開し、使用していないインターフェイスを設定から削除します。

Secure Firewall 3100 のネットワークモジュールの管理

最初にファイアウォールの電源をオンにする前にネットワークモジュールをインストールした場合、アクションは不要です。ネットワークモジュールは有効になり、使用できる状態になっています。

初回ブートアップ後にネットワークモジュールのインストールを変更する必要がある場合は、次の手順を参照してください。

ブレイクアウトポートの設定

40GB 以上のインターフェイスごとに 10GB のブレイクアウトポートを設定できます。この手順では、ポートの分割と再参加の方法について説明します。ブレイクアウトポートは、EtherChannel への追加を含め、他の物理イーサネットポートと同じように使用できます。

ハイアベイラビリティの場合は、アクティブユニットでこの手順を実行します。インターフェイスの変更は他のユニットに複製されます。

始める前に

- サポートされているブレイクアウトケーブルを使用する必要があります。詳細については、ハードウェア設置ガイドを参照してください。
- このインターフェイスは、ご使用の構成では使用できませんサブインターフェイスを持つことも、EtherChannelの一部にすることもできません。
- ハイアベイラビリティの場合、ハイアベイラビリティ用のインターフェイスの命名、有効化、またはモニタリングもできません。

手順

ステップ1 [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックします。

[インターフェイス (Interfaces)] タブがデフォルトで選択されます。インターフェイスリストに、物理インターフェイスとそれぞれの名前、アドレス、状態が表示されます。

ステップ2 40GB 以上のインターフェイスから 10GB ポートを分割するために、インターフェイスの右側にある [ブレイクアウト (Breakout)] アイコン (🔌) をクリックします。

確認ダイアログボックスで、[OK] をクリックします。インターフェイスが使用中の場合は、エラーメッセージが表示されます。分割を再試行する前に、ユースケースを解決する必要があります。たとえば、別のインターフェイスを使用するように設定を変更することができます。

たとえば、Ethernet2/1 40GB インターフェイスを分割する場合、分割後の子インターフェイスは、Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3、および Ethernet2/1/4 として識別されます。

インターフェイスのグラフィックでは、分割されたポートは🔌によって示されます。ブレイクアウトポートのステータスの詳細を示すページは、左右の矢印をクリックしてスクロールすることができます。

ステップ3 ブレイクアウトポートを再参加させるには、インターフェイスの右側にある [参加 (Join)] アイコン (🔌) をクリックします。

確認ダイアログボックスで、[OK] をクリックします。子ポートが使用中の場合は、エラーメッセージが表示されます。再参加を再試行する前に、ユースケースを解決する必要があります。たとえば、別のインターフェイスを使用するように設定を変更することができます。

インターフェイスのすべての子ポートを再参加させる必要があります。

ステップ4 設定を展開します。

ネットワークモジュールの追加

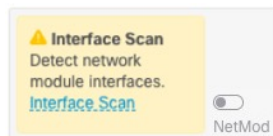
初回起動後にファイアウォールにネットワークモジュールを追加するには、次の手順を実行します。新しいモジュールを追加するには、再起動が必要です。

手順

- ステップ1** ハードウェア設置ガイドに従ってネットワークモジュールをインストールします。
ハイアベイラビリティの場合は、両方のユニットにネットワークモジュールをインストールします。
- ステップ2** ファイアウォールを再起動します。[システムの再起動またはシャットダウン](#)を参照してください。ハイアベイラビリティの場合は、スタンバイユニットを再起動してから、スタンバイユニットでこの手順の残りを実行します。
- ステップ3** [デバイス (Device)]をクリックしてから、[インターフェイス (Interfaces)]サマリーにある[すべてのインターフェイスを表示 (View All Interfaces)]リンクをクリックします。

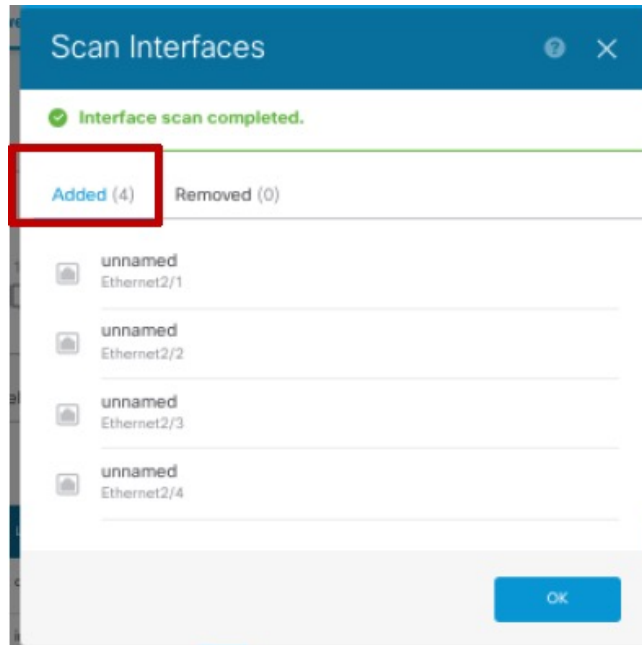
次のグラフィックは、インターフェイススキャンが必要であることを示しています。

図 3: インターフェイススキャンが必要



- ステップ4** [インターフェイススキャン (Interface Scan)]をクリックして、ネットワークモジュールの新しい詳細情報でページを更新します。
インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。

図 4: インターフェイスのスキャン




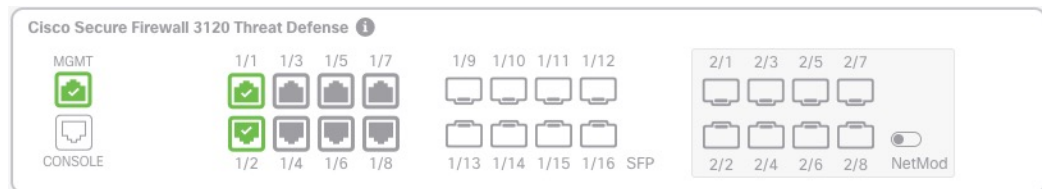
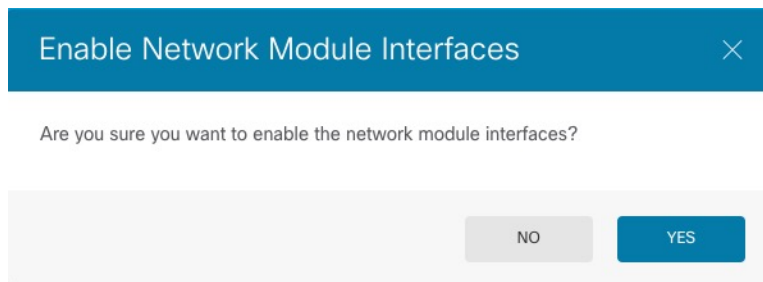
ステップ 5 インターフェイスのグラフィックで、スライダー () をクリックしてネットワークモジュールを有効にします。

図 5: ネットワークモジュールの有効化



ステップ 6 ネットワークモジュールを有効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 6: 有効化の確認



- ステップ7** ハイアベイラビリティの場合は、アクティブユニットを変更し（[アクティブピアとスタンバイピアの切り替え（強制フェールオーバー）](#)を参照）、新しいスタンバイユニットに対して上記の手順を実行します。

ネットワークモジュールの交換方法

再起動することなく、同じタイプの新しいモジュールのネットワークモジュールをホットスワップできます。ただし、現在のモジュールを安全に取り外すには、シャットダウンする必要があります。この手順では、古いモジュールをシャットダウンし、新しいモジュールをインストールして有効にする方法について説明します。

始める前に

ハイアベイラビリティの場合、フェールオーバーリンクがモジュール上にあると、ネットワークモジュールを無効化できません。ハイアベイラビリティを解除する必要があります（[ハイアベイラビリティの破棄](#)を参照）。モジュールをホットスワップした後、ハイアベイラビリティを再編成できます。

手順


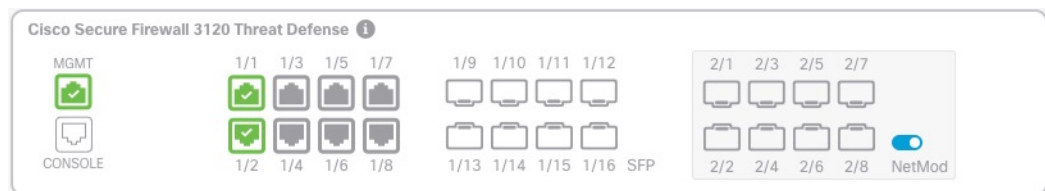
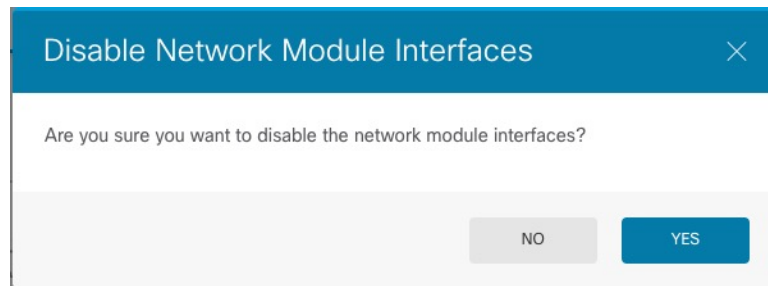
- ステップ1** ハイアベイラビリティの場合、ホットスワップを実行するユニットがスタンバイノードであることを確認します。[アクティブピアとスタンバイピアの切り替え（強制フェールオーバー）](#)を参照してください。
- ステップ2** [デバイス（Device）] をクリックしてから、[インターフェイス（Interfaces）] サマリーにある [すべてのインターフェイスを表示（View All Interfaces）] リンクをクリックします。
- ステップ3** インターフェイスのグラフィックで、スライダー（) をクリックしてネットワークモジュールを無効にします。

図 7: ネットワークモジュールの無効化



- ステップ4** ネットワークモジュールを無効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 8: 無効化の確認



ステップ 5 ハードウェア設置ガイドに従ってネットワークモジュールをインストールします。


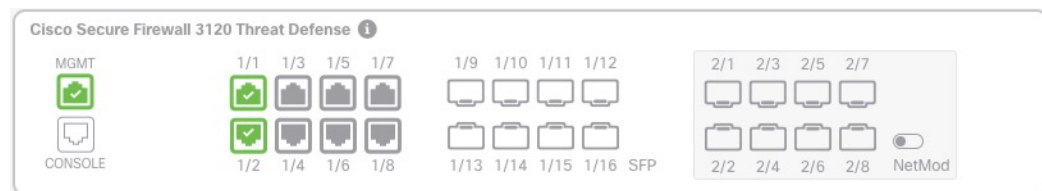
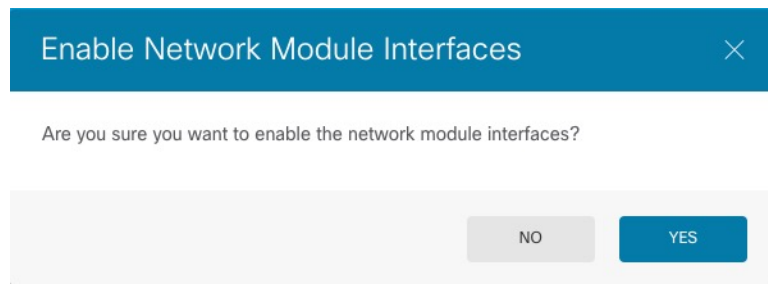
ステップ 6 インターフェイスのグラフィックで、スライダー () をクリックしてネットワークモジュールを有効にします。

図 9: ネットワークモジュールの有効化



ステップ 7 ネットワークモジュールを有効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 10: 有効化の確認



ネットワークモジュールを別のタイプに交換する

ネットワークモジュールを別のタイプに交換する場合は、再起動が必要です。新しいモジュールのインターフェイス数が古いモジュールよりも少ない場合は、存在しなくなるインターフェイスに関連する構成を手動で削除する必要があります。

始める前に

ハイアベイラビリティの場合、フェールオーバーリンクがモジュール上にあると、ネットワークモジュールを無効化できません。ハイアベイラビリティを解除する必要があります（[ハイアベイラビリティの破棄](#)を参照）。これにより、アクティブユニットの再起動時にダウンタイムが発生するようになります。ユニットの再起動が完了したら、ハイアベイラビリティを再編成できます。

手順


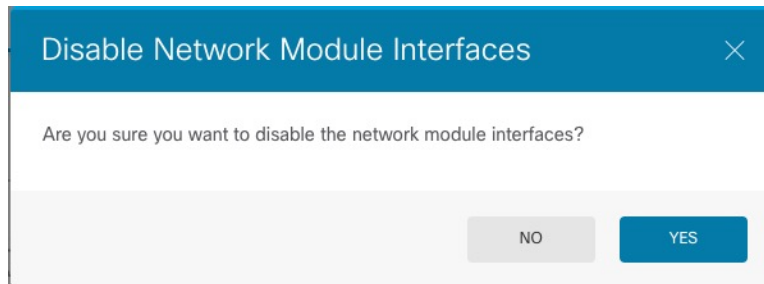
- ステップ 1** [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにある [すべてのインターフェイスを表示 (View All Interfaces)] リンクをクリックします。ハイアベイラビリティの場合は、最初にスタンバイユニットでこの手順を実行します。
- ステップ 2** インターフェイスのグラフィックで、スライダー () をクリックしてネットワークモジュールを無効にします。

図 11: ネットワークモジュールの無効化



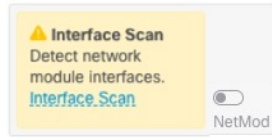
- ステップ 3** ネットワークモジュールを無効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 12: 無効化の確認



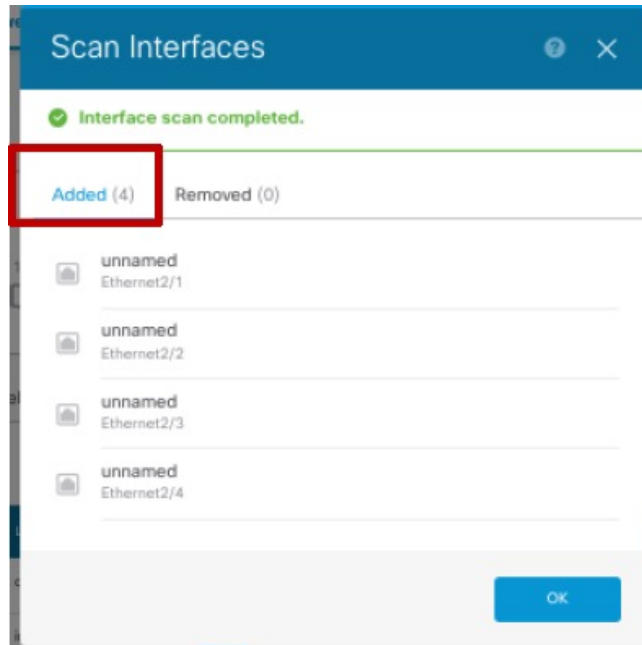
- ステップ 4** ハードウェア設置ガイドに従って、デバイスの古いネットワークモジュールを取り外し、新しいネットワークモジュールと交換します。
- ステップ 5** ファイアウォールを再起動します。 [システムの再起動またはシャットダウン](#) を参照してください。
- ステップ 6** [インターフェイス (Interfaces)] ページの次のグラフィックは、インターフェイススキャンが必要であることを示しています。[インターフェイススキャン (Interface Scan)] をクリックして、ネットワークモジュールの新しい詳細情報でページを更新します。

図 13: インターフェイススキャンが必要



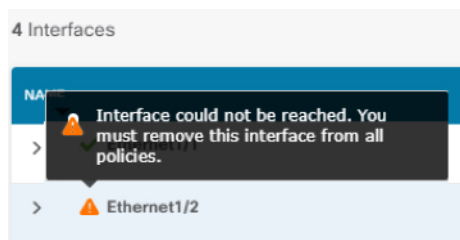
ステップ 7 インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。

図 14: インターフェイスのスキャン



スキャン後、削除されたインターフェイスは、[インターフェイス (Interfaces)] ページに注意記号とともに表示されます。

図 15: 削除されたインターフェイス



ステップ 8 ネットワークモジュールのインターフェイスの数が減少した場合は、削除されたインターフェイスを直接参照する設定を削除する必要があります。

セキュリティゾーンを参照するポリシーは影響を受けません。必要に応じて、設定を別のインターフェイスに移行させることができます。[インターフェイスのスキャンと移行 \(70ページ\)](#) を参照してください。


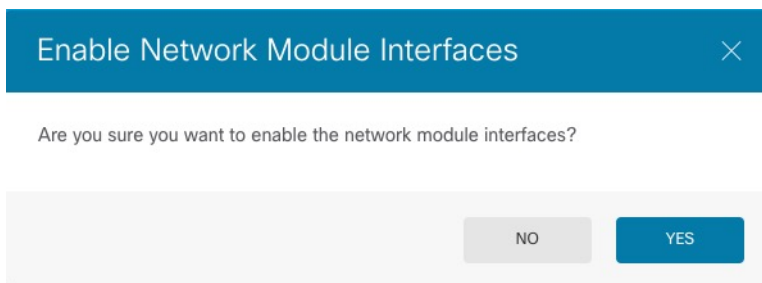
- ステップ 9** インターフェイスのグラフィックで、スライダー () をクリックしてネットワークモジュールを有効にします。

図 16: ネットワークモジュールの有効化



- ステップ 10** ネットワークモジュールを有効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 17: 有効化の確認



- ステップ 11** インターフェイス速度を変更するには、[詳細オプションの設定 \(64 ページ\)](#) を参照してください。
- デフォルトの速度は、[SFPを検出 (Detect SFP)] に設定されています。これにより、取り付けられている SFP から適切な速度が検出されます。速度を手動で特定の値に設定しており、その速度の変更が必要になった場合にのみ、速度を修正する必要があります。
- ステップ 12** 設定を変更する必要がある場合は、[展開 (Deployment)] アイコンをクリックします。
- ネットワークモジュールの変更を保存するためだけに展開する必要はありません。
- ステップ 13** ハイアベイラビリティの場合は、アクティブユニットを変更し ([アクティブピアとスタンバイピアの切り替え \(強制フェールオーバー\)](#) を参照)、新しいスタンバイユニットに対して上記の手順を実行します。

ネットワーク モジュールの取り外し

ネットワークモジュールを完全に削除する場合は、次の手順に従います。ネットワークモジュールを削除するには、再起動が必要です。

始める前に

ハイアベイラビリティの場合は、フェールオーバーリンクがネットワークモジュール上にないことを確認してください。

手順


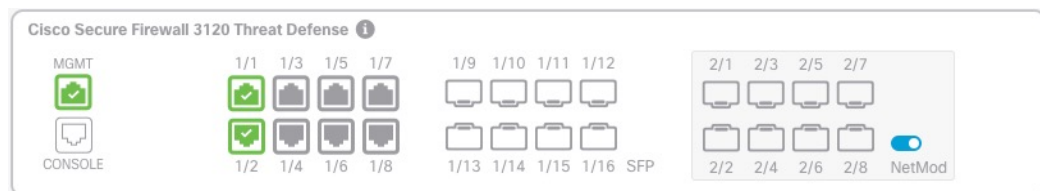
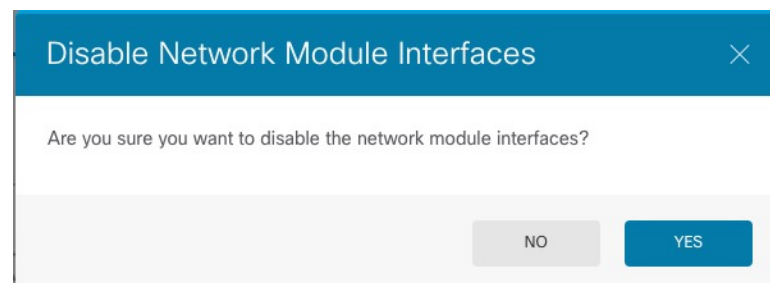
- ステップ 1** [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにある [すべてのインターフェイスを表示 (View All Interfaces)] リンクをクリックします。ハイアベイラビリティの場合は、最初にスタンバイユニットでこの手順を実行します。
- ステップ 2** インターフェイスのグラフィックで、スライダー () をクリックしてネットワークモジュールを無効にします。

図 18: ネットワークモジュールの無効化



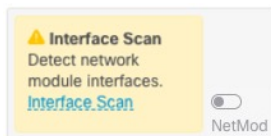
- ステップ 3** ネットワークモジュールを無効にするかどうかを確認するメッセージが表示されます。[Yes] をクリックします。

図 19: 無効化の確認



- ステップ 4** ファイアウォールで、ネットワークモジュールを削除します。
- ステップ 5** ファイアウォールを再起動します。 [システムの再起動またはシャットダウン](#) を参照してください。
- ステップ 6** [インターフェイス (Interfaces)] ページの次のグラフィックは、インターフェイススキャンが必要であることを示しています。[インターフェイススキャン (Interface Scan)] をクリックして、ネットワークモジュールの適切な詳細情報でページを更新します。

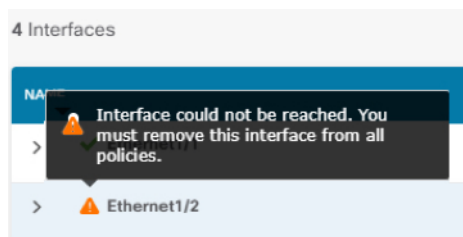
図 20: インターフェイススキャンが必要



ステップ 7 インターフェイスがスキャンされるのを待ってから、[OK] をクリックします。

スキャン後、削除されたインターフェイスは、[インターフェイス (Interfaces)] ページに注意記号とともに表示されます。

図 21: 削除されたインターフェイス



ステップ 8 削除されたインターフェイスを直接参照するすべての設定を削除する必要があります。

セキュリティゾーンを参照するポリシーは影響を受けません。必要に応じて、設定を別のインターフェイスに移行させることができます。[インターフェイスのスキャンと移行 \(70 ページ\)](#) を参照してください。

ステップ 9 設定を変更する必要がある場合は、[展開 (Deployment)] アイコンをクリックします。

ネットワークモジュールの変更を保存するためだけに展開する必要はありません。

ステップ 10 ハイアベイラビリティの場合は、アクティブユニットを変更し ([アクティブピアとスタンバイピアの切り替え \(強制フェールオーバー\)](#) を参照)、新しいスタンバイユニットに対して上記の手順を実行します。

管理インターフェイスと診断インターフェイスのマージ

Threat Defense 7.4 以降では、マージされた管理インターフェイスと診断インターフェイスがサポートされます。診断インターフェイスを使用する設定がある場合、インターフェイスは自動的にマージされないため、次の手順を実行する必要があります。この手順では、設定の変更を確認し、場合によっては手動で設定を修正する必要があります。

バックアップ/復元機能は、マージの状態 (マージされていないかマージされている) を保存および復元します。たとえば、インターフェイスをマージしてから、古いマージされていない設定を復元すると、復元された設定はマージされていない状態になります。

次の表に、レガシー診断インターフェイスで使用可能な設定と、マージの完了方法を示します。

表 2: *Device Manager* 統合管理インターフェイスのサポート

レガシー診断インターフェイスの設定	マージ動作	管理でサポートされるかどうか
インターフェイス		「管理」インターフェイスが [Interfaces] ページに表示され、設定できるようになりました。以前は、[System Settings] > [Management Interface] ページで設定が可能でした。
<ul style="list-style-type: none"> IP アドレス 	手動で削除する必要があります。	<p>代わりに現在の管理 IP アドレスが使用されます。</p> <p>高可用性の場合、管理インターフェイスはスタンバイ IP アドレスをサポートしません。各ユニットには、フェールオーバー後も維持される独自の IP アドレスがあります。そのため、現在のアクティブユニットとの通信に単一の管理 IP アドレスを使用することはできません。</p> <p>[Interfaces] ペインで設定するか、configure network ipv4 または configure network ipv6 コマンドを使用して CLI で設定します。</p>
<ul style="list-style-type: none"> 「診断」名 	<p>自動的に「管理」に変更されます。</p> <p>(注) 他のインターフェイスに「管理」という名前を付けることはできません。マージを続行するには、名前を変更する必要があります。</p>	「管理」に変更されます。

レガシー診断インターフェイスの設定	マージ動作	管理でサポートされるかどうか
スタティック ルート	手動で削除する必要があります。	<p>サポートしない</p> <p>管理インターフェイスには、データインターフェイスに基づく個別のLinux ルーティングテーブルがあります。脅威に対する防御には、実際のところ、データインターフェイス用と管理専用インターフェイス用の2つの「データ」ルーティングテーブルがあります（以前は診断インターフェイスが含まれていましたが、管理専用に変更されたすべてのインターフェイスも含まれています）。トラフィックタイプに応じて、脅威に対する防御は1つのルーティングテーブルをチェックし、次に他のルーティングテーブルにフォールバックします。このルートルックアップには、診断インターフェイスは含まれておらず、管理用のLinux ルーティングテーブルも含まれていません。詳細については、「管理トラフィック用ルーティングテーブル」を参照してください。</p> <p>configure network static-routes コマンドを使用して、CLIでLinux ルーティングテーブルのスタティックルートを追加できます。</p> <p>(注) デフォルトルートは、configure network ipv4 または configure network ipv6 コマンドで設定します。</p>
Syslog サーバー (Syslog Server)	自動的に管理インターフェイスに移動されました。	<p>はい。</p> <p>syslog サーバーの設定で、管理インターフェイスから syslog を送信するオプションを使用できるようになりました (6.3以降)。syslog に関して診断インターフェイスを明確に選択していた場合は、管理インターフェイスを使用するように変更されます。</p>
RADIUS サーバー	自動的に管理インターフェイスに移動されました。	<p>はい。</p> <p>診断インターフェイスを明確に選択していた場合は、管理インターフェイスを使用するように変更されます。</p> <p>(注) ルートルックアップを指定した場合、脅威に対する防御は管理専用インターフェイスからトラフィックを送信できなくなります。この場合、送信元インターフェイスとして管理専用インターフェイスを明示的に選択する必要があります。</p>

レガシー診断インターフェイスの設定	マージ動作	管理でサポートされるかどうか
AD サーバー	必要に応じて、管理インターフェイスを手動で指定します。	はい。 デフォルトでは、ADサーバー通信のルートルックアップが実行され、7.4 より前のインターフェイスは指定できませんでした。7.4 以降、脅威に対する防御は、ルートルックアップを使用して管理専用インターフェイスからトラフィックを送信できなくなります。この場合、送信元インターフェイスとして管理専用インターフェイスを明示的に選択できるようになりました。
DDNS	手動で削除する必要があります。	サポートしない
DHCP サーバー	手動で削除する必要があります。	サポートしない
DNS サーバー	自動的に管理インターフェイスに移動されました。	はい。 診断インターフェイスを明確に選択していた場合は、管理インターフェイスを使用するように変更されます。インターフェイス ([ANY]) を選択しなかった場合は、ルーティングルックアップも変更されません。ルーティングルックアップはデータルーティングテーブルを使用しますが、ルートが見つからない場合、管理専用ルーティングテーブルにフォールバックしません。 (注) 管理インターフェイスには、管理トラフィック専用の個別の DNS ルックアップ設定もあります。
SLA モニター	手動で削除する必要があります。	サポートしない
FlexConfig	手動で削除する必要があります。	サポートしない

始める前に

- デバイスの現在のモードを表示するには、脅威に対する防御 CLI で **show management-interface convergence** コマンドを入力します。次の出力は、管理インターフェイスがマージされていることを示しています。

```
> show management-interface convergence
management-interface convergence
>
```

次の出力は、管理インターフェイスがマージされていないことを示しています。

```
> show management-interface convergenc
```

```
no management-interface convergence
>
```

- 高可用性ペアの場合は、アクティブユニットでこのタスクを実行します。マージされた設定は、自動的にスタンバイユニットに複製されます。

手順

- ステップ 1** [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックします。

[Interfaces] テーブルの上部に、[Management Interface action needed] のメッセージとリンクが表示されます。
- ステップ 2** 診断インターフェイスを編集し、IP アドレスを削除します。

診断 IP アドレスを削除するまで、マージを完了できません。
- ステップ 3** [Management Interface action needed] エリアの [Merge Management Interface] をクリックします。

[Management Interface Merge] ダイアログボックスに、設定内の診断インターフェイスのオカレンスがすべて表示されます。手動で設定を削除または変更する必要があるオカレンスは、警告アイコン付きで表示されます。自動移行も表示されます。

❖ Management Interface Merge ? ×

i You must change the static route on the diagnostic interface before you can proceed; either delete the route or choose a new interface.

In this release you can merge the Management and Diagnostic interfaces to use a single IP address instead of two IP addresses. The merged interface will be called Management and use the current Management IP address. You will need to update all external services that communicate with the Diagnostic IP address. [Learn More](#)

The IP address for the merged Management Interface will be:
10.89.5.15 (current Management IP Address)
 The Diagnostic IP address is 10.99.5.60, and will be automatically replaced in the configuration with the current Management IP address

REVIEW 5 OCCURRENCES ↻ REFRESH

⚠ Items marked with a warning icon cannot be resolved automatically. You must resolve these uses manually by editing your configuration.

- 📄 **Current 10.99.5.60 will be auto-changed to 10.89.5.15**
- 📄 **Radius Identity Source**
 Current 10.99.5.60 will be auto-changed to 10.89.5.15
- ❖ **Static Routing**
 Manual resolution is needed
- 📄 **SLA Monitor**
 Manual resolution is needed

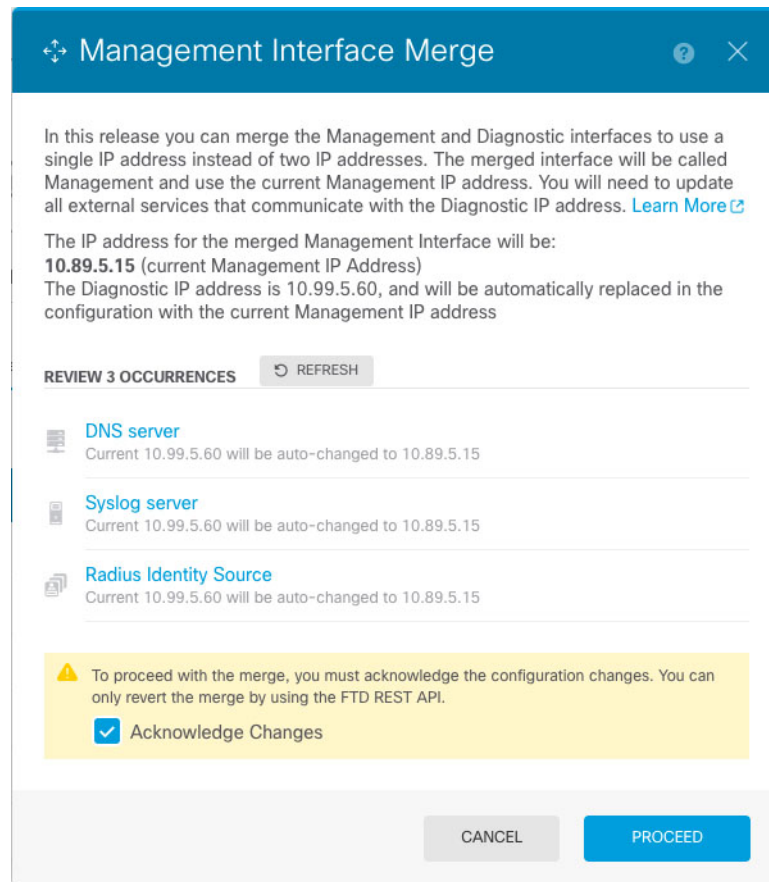
CANCEL
PROCEED

ステップ 4 リストされている設定を手動で削除または変更する必要がある場合は、次の手順を実行します。

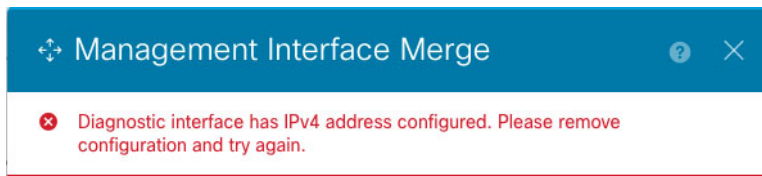
設定を変更している間、参考のために [Management Interface Merge] ダイアログボックスは開いたままにできます。

- a) 項目をクリックして設定ページを開きます。その後、項目を削除したり、データインターフェイスを選択したりできます。
- b) [Management Interface Merge] ダイアログボックスの内容を更新するには、[Refresh] をクリックします。

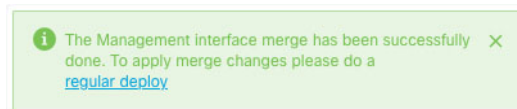
これで、警告は表示されなくなります。



ステップ 5 [Acknowledge Changes] をクリックしてから、[Proceed] をクリックします。
 診断 IP アドレスをまだ削除していない場合、次のエラーが表示されます。



この場合、診断 IP アドレスを削除してから、[Proceed] をもう一度クリックします。
 設定がマージされると、成功バナーが表示されます。



ステップ 6 マージされた新しい設定を展開します。

注意 マージを続行しない場合は、展開する前に [Discard All] を使用して変更を破棄し、マージを元に戻すことができます。マージされた設定を展開すると、Device Manager からインターフェイスのマージを解除できます。ただし、診断インターフェイスは手動で再設定する必要があります。「[管理インターフェイスのマージ解除 \(90 ページ\)](#)」を参照してください。また、マージされていない設定を復元すると、デバイスはマージされていない設定に戻ります。

マージ後、[Interfaces] ページに管理インターフェイスが表示され、設定可能になります。以前は、[System Settings] > [Management Interface] ページで設定が可能でした。

ステップ 7 マージ後は、診断インターフェイスと通信する外部サービスがある場合、管理インターフェイスの IP アドレスを使用するように設定を変更する必要があります。

次に例を示します。

- SNMP クライアント
- RADIUS サーバー : RADIUS サーバーでは多くの場合、着信トラフィックの IP アドレスが確認されるため、その IP アドレスを管理アドレスに変更する必要があります。さらに、高可用性ペアの場合、プライマリとセカンダリの両方の管理 IP アドレスを許可する必要があります。診断インターフェイスは、アクティブユニットに存在する単一の「フローティング」IP アドレスをサポートしていましたが、管理インターフェイスはサポートしていません。

管理インターフェイスのマージ解除

Threat Defense 7.4 以降では、マージされた管理インターフェイスと診断インターフェイスがサポートされます。インターフェイスのマージを解除する必要がある場合は、次の手順を実行します。ネットワークをマージモード展開に移行する際は、一時的にマージ解除モードを使用することを推奨します。個別の管理インターフェイスと診断インターフェイスは、将来のすべてのリリースでサポートされなくなる可能性があります。

インターフェイスのマージを解除しても、元の診断設定は復元されません（アップグレードしてからインターフェイスをマージした場合）。診断インターフェイスを手動で再設定する必要があります。また、管理インターフェイスは「管理」という名前になり、名前を「診断」に変更することはできません。

または、バックアップ機能を使用して古いマージされていない設定を保存した場合は、その設定を復元できます。その場合、診断設定は変わらず、デバイスがマージされていない状態になります。

始める前に

- デバイスの現在のモードを表示するには、脅威に対する防御 CLI で **show management-interface convergence** コマンドを入力します。次の出力は、管理インターフェイスがマージされていることを示しています。

```
> show management-interface convergence
management-interface convergence
>
```

次の出力は、管理インターフェイスがマーヅされていないことを示しています。

```
> show management-interface convergence
no management-interface convergence
>
```

- ・高可用性ペアの場合は、アクティブユニットでこのタスクを実行します。マーヅされていない設定は、自動的にスタンバイユニットに複製されます。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックします。


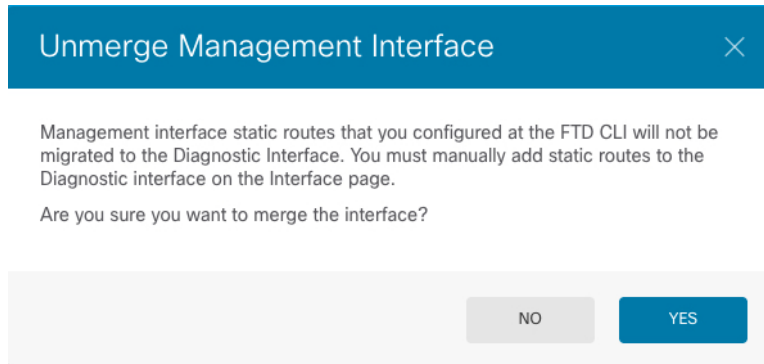
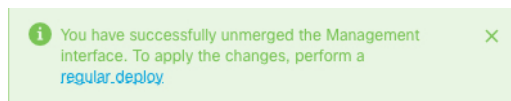
ステップ 2 [Management 1/1] インターフェイス行の右側にある [Unmerge] ([Unmerge]) をクリックし、[Unmerge Management Interface] ダイアログボックスで [Yes] をクリックします。 

図 22: 管理インターフェイスのマーヅ解除



[Interfaces] ページの上部に成功メッセージが表示されます。

図 23: マーヅ解除成功



ステップ 3 新しいマーヅされていない設定を展開します。

マーヅの解除を続行しない場合は、展開する前に [Discard All] を使用して変更を破棄し、マーヅされたインターフェイスを保持できます。また、マーヅされた設定を復元すると、デバイスはマーヅされた設定に戻ります。

マージ解除後、[System Settings]>[Management Interface] ページに管理インターフェイスが表示され、設定可能になります。

停電時のハードウェアバイパスの設定 (ISA 3000)

ハードウェアバイパスを有効にして、停電時でもトラフィックがインターフェイス ペア間を通過できるようにできます。サポートされているインターフェイスペアは銅線インターフェイスの GigabitEthernet 1/1 と 1/2、および GigabitEthernet 1/3 と 1/4 です。光ファイバーサネットモデルを保有している場合は、銅線イーサネット ペア (GigabitEthernet 1/1 と 1/2) でのみハードウェアバイパスがサポートされます。デフォルトでは、サポートされている場合、両方のインターフェイスペアに対してハードウェアバイパスが有効になります。

ハードウェアバイパスがアクティブの場合、トラフィックはレイヤ1でそれらのインターフェイス ペア間を通過します。Device Manager と Threat Defense CLI の両方に、インターフェイスがダウンしていることが表示されます。ファイアウォール機能はないため、トラフィックのデバイス通過を許可することのリスクを理解する必要があります。

(この手順で説明されている) TCP シーケンス番号のランダム化は無効にすることをお勧めします。デフォルトでは、ISA 3000 を通過する TCP 接続の最初のシーケンス番号 (ISN) が乱数に書き換えられます。ハードウェアバイパスがアクティブになると、ISA 3000 はデータパスには入らず、シーケンス番号は変換されません。受信側のクライアントが予期しないシーケンス番号を受信すると接続がドロップされるため、TCP セッションを再確立する必要があります。TCP シーケンス番号のランダム化が無効になっている場合でも、スイッチオーバー中に一時的にダウンするリンクがあるため、一部の TCP 接続は再確立する必要があります。

CLI コンソールまたは SSH セッションで、**show hardware-bypass** コマンドを使用して動作ステータスをモニターします。

始める前に

ハードウェアバイパスを機能させるための前提条件：

- インターフェイス ペアは同じブリッジグループに配置する必要があります。
- インターフェイスはスイッチのアクセスポートに接続する必要があります。トランクポートには接続しないでください。

手順

ステップ 1 [デバイス (Device)] をクリックしてから、[インターフェイス (Interfaces)] サマリーにあるリンクをクリックします。

ページの上にある [ハードウェアバイパス (Hardware Bypass)] セクションは、このデバイスに使用できるインターフェイスペアの現在の設定を示します。

ただし、ハードウェアバイパスを有効にする前に、ペアが同じブリッジグループで設定されていることを確認する必要があります。

ステップ 2 [編集 (Edit)] をクリックしてハードウェアバイパスを設定します。

[ハードウェアバイパスの設定 (Hardware Bypass Configuration)] ダイアログボックスが表示されます。

ステップ 3 自動ハードウェアバイパス動作を設定するには、インターフェイスペアごとに、[停電時のハードウェアバイパス (Hardware Bypass during Power Down)] エリアで次のいずれかのオプションを選択します。

- [無効化 (Disable)] : ハードウェアバイパスを無効にします。トラフィックは、停電時にデバイスを通しません。
- [有効化 (Enable)] : 停電時にハードウェアバイパスをアクティブにします。ハードウェアバイパスが、停電時にトラフィックが中断されないように確保します。バイパスされたトラフィックは検査されず、セキュリティポリシーは適用されないことに注意してください。電源が復旧したら、ハードウェアバイパスは自動的に無効になるため、トラフィックフローの通常の状態を維持することができ、検査も行われます。ハードウェアバイパスを無効にすると、トラフィックが一時的に中断する可能性があることに注意してください。
- [永続的に有効化 (Enable with Persistence)] : 停電時にハードウェアバイパスをアクティブにし、電源の復元後も有効な状態を維持します。電源が復旧したら、[手動ハードウェアバイパス (Manual Hardware Bypass)] スライダーを使用してハードウェアバイパスを無効にする必要があります。このオプションでは、トラフィックに一時的な中断が発生したときに制御することができます。

ステップ 4 (任意) ハードウェアバイパスを手動で有効または無効にするには、[手動ハードウェアバイパス (Manual Hardware Bypass)] スライダーをクリックします。

たとえば、システムをテストしたり、何らかの理由でデバイスを一時的にバイパスする必要がある場合があります。ハードウェアバイパスの状態を変更するには、設定を展開する必要があります。設定を変更するだけでは不十分です。

ハードウェアバイパスを手動で有効化または無効化すると、次の Syslog メッセージが表示されます。メッセージ内の *pair* は 1/1-1/2 または 1/3-1/4 です。

- %FTD-6-803002 : no protection will be provided by the system for traffic over GigabitEthernet *pair*
- %FTD-6-803003: User disabled bypass manually on GigabitEthernet *pair*

ステップ 5 [OK] をクリック

変更はすぐには適用されません。設定を展開する必要があります。

ステップ 6 (オプション) TCP シーケンス番号のランダム化を無効にするために必要な FlexConfig オブジェクトとポリシーを作成します。

- a) [デバイス (Device)] > [詳細設定 (Advanced Configuration)] で [設定の表示 (View Configuration)] をクリックします。

- b) 詳細設定の目次で **[FlexConfig] > [FlexConfigオブジェクト (FlexConfig Objects)]** をクリックします。
- c) 新しいオブジェクトを作成するには、**[+]** ボタンをクリックします。
- d) オブジェクトの名前を入力します。たとえば、**Disable_TCP_Randomization** と入力します。
- e) **[テンプレート (Template)]** エディタに、TCP シーケンス番号のランダム化を無効にするコマンドを入力します。

コマンドは **set connection random-sequence-number disable** ですが、ポリシーマップ内の特定のクラスに対して設定する必要があります。最も簡単なアプローチは、ランダムなシーケンス番号をグローバルに無効にする方法です。この場合、次のコマンドを入力する必要があります。

```
policy-map global_policy
  class default_class
    set connection random-sequence-number disable
```

- f) **[ネゲートテンプレート (Negate Template)]** エディタで、この設定を元に戻すために必要な行を入力します。

たとえば、TCP シーケンス番号のランダム化をグローバルに無効にしている場合、ネゲートテンプレートは次のようになります。

```
policy-map global_policy
  class default_class
    set connection random-sequence-number enable
```

- g) **[OK]** をクリックしてオブジェクトを保存します。
オブジェクトを FlexConfig ポリシーに追加する必要があります。オブジェクトを作成するだけでは十分ではありません。
- h) 目次で **[FlexConfigポリシー (FlexConfig Policy)]** をクリックします。
- i) **[グループリスト (Group List)]** で **[+]** をクリックします。
- j) **[Disable_TCP_Randomization]** オブジェクトを選択し、**[OK]** をクリックします。
プレビューはテンプレートのコマンドで更新されます。予想されるコマンドが表示されているか確認します。
- k) **[保存 (Save)]** をクリックします。
これでポリシーを展開できます。

モニタリングインターフェイス

次の領域に、インターフェイスに関する一部の基本情報を表示できます。

- [デバイス (Device)]。インターフェイスの現在の状態をモニターするには、ポートグラフィックを使用します。ポートにマウスポインタを合わせると、そのポートの IP アドレス、EtherChannel メンバーシップ、有効ステータス、リンクステータスが表示されます。IP アドレスは DHCP を使用して静的に割り当てたり取得したりできます。

インターフェイスポートは、次のカラーコーディングを使用します。

- 緑：インターフェイスは設定され、有効で、リンクは稼働中です。
 - グレー：インターフェイスは無効です。
 - オレンジ/赤：インターフェイスが設定され、有効ですが、リンクがダウンしています。インターフェイスが有線の場合、これは修正が必要なエラー状態です。インターフェイスが有線でない場合、これは予期されるステータスです。
- [モニタリング (Monitoring)] > [システム (System)]。[スループット (Throughput)] ダッシュボードには、システムを介して移動するトラフィックに関する情報が表示されます。すべてのインターフェイスに関する情報を表示できます。または、調査する特定のインターフェイスを選択できます。
 - [モニタリング (Monitoring)] > [ゾーン (Zones)]。これらのダッシュボードにはインターフェイスを設定するセキュリティゾーンに基づく統計情報が表示されます。詳細について、この情報を掘り下げることができます。

CLI でのインターフェイスのモニタリング

CLI コンソールを開くか、またはデバイスの CLI にログインして、次のコマンドを使用し、インターフェイス関連の動作と統計情報に関する詳細情報を取得することもできます。

- **show interface** はインターフェイスの統計情報と設定情報を表示します。このコマンドには多数のキーワードがあり、必要な情報を取得するために使用できます。使用可能なオプションを表示するには、「?」をキーワードとして使用します。
- **show ipv6 interface** はインターフェイスに関する IPv6 設定情報を表示します。
- **show bridge-group** は、メンバー情報や IP アドレスを含む、ブリッジ仮想インターフェイス (BVI) に関する情報を表示します。
- **show conn** は現在インターフェイスを通じて確立されている接続に関する情報を表示します。
- **show traffic** は各インターフェイスを介したトラフィックフローに関する統計情報を表示します。
- **show ipv6 traffic** はデバイスを介した IPv6 トラフィックフローに関する統計情報を表示します。
- **show dhcpd** はインターフェイスの DHCP 使用状況に関する統計とその他の情報を表示し、特にインターフェイスで設定されている DHCP サーバーに関する情報が含まれます。
- **show switch vlan** は VLAN とスイッチポートの関連付けを表示します。

- **show switch mac-address-table** はスタティックおよびダイナミック MAC アドレスエントリを表示します。
- **show arp** はダイナミック、スタティック、およびプロキシ ARP エントリを表示します。
- **show power inline PoE** ステータスを表示します。
- **show vpdn group** は PPPoE グループと、設定されているユーザー名と認証を表示します。
- **show vpdn username** は PPPoE のユーザー名とパスワードを表示します。
- **show vpdn session pppoe state** は PPPoE セッションのステータスを表示します。

インターフェイスの例

使用例の章には、次のインターフェイス関連の例が含まれています。

- [Device Manager でデバイスを設定する方法](#)
- [サブネットを追加する方法](#)
- [ネットワーク上のトラフィックをパッシブにモニタする方法](#)

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。