インターフェイス

ここでは、Firepower Threat Defenseのインターフェイスを設定する方法について説明します。

- Firepower Threat Defenseインターフェイスについて，1 ページ
- インターフェイスの設定，7 ページ
- モニタリング インターフェイス，20 ページ

Firepower Threat Defenseインターフェイスについて

Firepower Threat Defenseデバイスには、データ インターフェイスの他、管理インターフェイスと診断インターフェイスが含まれます。以下の各トピックでは、Firepower 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。

インターフェイス設定の制約

Firepowerデバイス マネージャを使用してデバイスを設定する場合は、インターフェイスの設定に関するいくつかの制約があります。次の機能のいずれかが必要な場合は、Firepower Management Centerを使用してデバイスを設定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ています。トランスペアレントファイアウォール モード インターフェイスは設定できません。
- IPS 専用モードはサポートされていません。IPS 専用処理向けにインターフェイスをインライン、インライン タップ、パッシブまたは ERSPAN に設定することはできません。IPS 専用モードインターフェイスは、多数のファイアウォール チェックをバイパスし、IPS セキュリティ ポリシーのみをサポートします。比較すると、ファイアウォール モード インターフェイスは、フローの維持、IP 層と TCP 層の両方でのフロー状態の追跡、IP の最適化、TCP の正規化などのファイアウォール機能の対象となるトラフィックを処理します。オプションで、このファイアウォール モード トラフィックの IPS 機能をセキュリティ ポリシーに従って設定できます。

- EtherChannel または冗長インターフェイスは設定できません。
- IPv4 対応の PPPoE は設定できません。インターネット インターフェイスが DSL、ケーブル モデム、または その他の接続を介して ISP 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、Firepower Management Centerを使用してこれらの設定を行う必要があります。
- ASA 5512-X、5515-X、5525-X、5545-X および 5555-X の場合は、オプションのネットワーク インターフェイス カード（EPM）を装着できます。カードはブートストラップの間にのみ検出されます（つまり、インストール中、ローカル/リモート管理の切り替え時、およびメジャー/マイナー リリース アップグレード中）。SFP インターフェイスが組み込まれたカードの場合、Firepower デバイス マネージャは、速度とデュプレックスを自動（auto）に設定します。ただし、SFP インターフェイスは自動に設定された速度とデュプレックスをサポートしていません。速度とデュプレックスは、手動で設定する必要があります。速度を 1000、デュプレックスを Full に設定してから、設定を展開します。リンクが起動しない場合は、別の速度を試行します。

データ インターフェイス

以下のタイプのインターフェイスを設定できます。

ルーテッド

個々のレイヤ 3 ルーテッド インターフェイス（またはサブインターフェイス）には、一意のサブネットの IP アドレスが必要です。通常、このタイプのインターフェイスはスイッチ、別のルータのポート、または ISP/WAN ゲートウェイに接続します。

スタティック アドレスを割り当てることも、DHCP サーバからアドレスを取得することもできます。しかし、デバイス上で静的に定義されたインターフェイスと同じサブネットのアドレスが DHCP サーバによって提供された場合は、DHCP インターフェイスが無効になります。DHCP を使用してアドレスを取得しているインターフェイスがトラフィックの通過を停止している場合は、アドレスがデバイス上の別のインターフェイスのサブネットと重複していないかどうかを確認してください。

ブリッジド

ブリッジ グループは、ルータではなく Firepower Threat Defense デバイスによってブリッジされるインターフェイス グループです。ブリッジされる各インターフェイスは1つのブリッジ グループに属し、すべてのインターフェイスは同一ネットワークに属します。ブリッジ グループは、ブリッジ ネットワーク上の単一の 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 を指定して、ルーテッド インターフェイスと BVI 間をルーティングできます。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 を指定しないと、ブリッジ グループのメンバー インターフェイス上のトラフィックは、ブリッジ グループの外に出ることができません。通常、メンバー インターフェイスをインターネットにルーティングすることのできるインターフェイスを指定します。

ルーテッドモードでブリッジグループを使用する例として、外部スイッチではなく、Firepower Threat Defense デバイスの予備のインターフェイスを使用できます。エンドポイントは、ブリッジ グループのメンバー インターフェイスに直接接続できます。また、スイッチを接続して、BVI と同じネットワークにさらに多くのエンドポイントを追加することもできます。

ルーテッド インターフェイスと BVI のどちらにも、IPv6 および IPv4 アドレスを設定できます。IPv6 と IPv4 の両方で、デフォルト ルートを設定してください。ブリッジ グループのメンバー インターフェイスには、アドレスを設定しません。

IPv6 アドレッシング

IPv6 では、2 タイプのユニキャスト 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できるパブリック アドレスです。ブリッジ グループの場合は、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）にグローバルアドレスを設定します。グローバルアドレスとして次のいずれかを指定することはできません。
  - 内部的に予約された 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でのみ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しません。これらのアドレスは、特定の物理ネットワーク セグメントでの通信専用です。アドレス設定、またはアドレス解決やネイバー探索などネットワーク検出機能で使用できます。ブリッジ グループでは、BVI で IPv6 を有効にすると、各ブリッジ グループ メンバーの

インターフェイスのリンクローカル アドレスが自動的に設定されます。リンクローカル アドレスはセグメントでのみ使用可能であり、インターフェイス MAC アドレスに結合されているため、各インターフェイスは専用のアドレスを保持する必要があります。

IPv6 を動作させるには、少なくとも 1 つのリンクローカル 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は自動的にインターフェイスに設定されます。そのため、特に、リンクローカル アドレスを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 アドレスを自動または手動のいずれかで設定する必要があります。

管理/診断インターフェイス

Management とラベル付けされた物理ポートには、実際は 2 つの個別のインターフェイスが関連付けられています。

- 管理仮想インターフェイス：このIPアドレスは、システムの通信に使用されます。これは、システムがスマートライセンス用に使用したり、データベース更新を取得するために使用したりするアドレスです。このアドレスへの管理セッションを開くことができます（Firepower デバイス マネージャまたは CLI）。[システム設定（System Settings）] > [管理インターフェイス（Management Interface）] で定義されている管理アドレスを設定する必要があります。
- 診断物理インターフェイス：物理管理ポートは実際には、Diagnostic という名前が付けられています。このインターフェイスは、外部 syslog サーバへの syslog メッセージを送信するために使用できます。診断物理インターフェイスの IP アドレスの設定はオプションです。このインターフェイスを syslog 用に使用する場合にのみ、インターフェイスを設定します。このインターフェイスは、[デバイス（Device）] > [インターフェイス（Interfaces）] ページに表示され、そこで設定できます。診断物理インターフェイスは、管理トラフィックのみを許可し、トラフィックの通過は許可しません。

管理/診断を設定するための推奨方法は、物理ポートをネットワークに配線しないことです。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を取得す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。その後、HTTPS/SSH トラフィックへの内部インターフェイス（デフォルトでは、HTTPS は有効）を開き、内部 IP アドレスを使用して Firepower デバイス マネージャを開きます（管理アクセス リストの設定を参照）。

個別の管理ネットワークを設定するための推奨事項

個別の管理ネットワークを使用する場合は、管理/診断用物理インターフェイスをスイッチまたはルータに有線接続します。

その後、次の設定を行います。

- [デバイス（Device）] > [システム設定（System Settings）] > [管理インターフェイス（Management Interface）] を選択して、接続されているネットワークに IPv4 または IPv6 アドレス（あるいは両方）を設定します。必要に応じて、ネットワーク上のその他のエンドポイントに IPv4 アドレスを提供するように DHCP サーバを設定できます。管理ネットワーク上

のインターネットへのルートがあるルータが存在する場合、そのルータをゲートウェイとして使用します。それ以外の場合は、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。

- インターフェイス経由で syslog サーバに syslog メッセージを送信する場合のみ、診断インターフェイスのアドレスを設定します（[デバイス（Device）] > [インターフェイス（Interface）]）。それ以外の場合は、不要なので診断インターフェイスのアドレスは設定しないでください。設定する IP アドレスはすべて、管理 IP アドレスと同じサブネット上のアドレスである必要があり、DHCP サーバ プールのアドレスは指定できません。たとえば、デフォルト設定で 192.168.45.45 を管理アドレスとして使用し、192.168.45.46 ～ 192.168.45.254 を DHCP プールとして使用している場合、192.168.45.1 ～ 192.168.45.44 の任意のアドレスを使用して診断インターフェイスを設定できます。

個別管理ネットワークの管理/診断インターフェイス設定の制限事項

物理的な管理インターフェイスを配線する場合、以下の制限事項に注意してください。

- 管理ネットワークで DHCP サーバを使用する場合は、DHCP サーバを管理インターフェイスに設定します（[デバイス（Device）] > [システム設定（System Settings）] > [管理インターフェイス（Management Interface）]）。DHCP サーバを診断（物理）インターフェイスに設定することはできません。
- 管理ネットワークに別の DHCP サーバが存在する場合は、この DHCP サーバ、または管理インターフェイス上で実行されている DHCP サーバを無効にします。規則として、1 つのサブネットでは 1 つの DHCP サーバしか使用できません。
- 管理インターフェイスおよび診断インターフェイスの両方にアドレスを設定する場合は、どちらも同じサブネット上にあることを確認します。
- 診断インターフェイスの IP アドレスを設定した場合であっても、データ インターフェイスを管理ゲートウェイとして使用できます。しかし、診断インターフェイスでは、データ インターフェイスはゲートウェイとして使用されません。診断インターフェイスから他のネットワークへのパスが必要となる場合は、管理ネットワーク上の別のルータによって、診断 IP アドレスから送信されたトラフィックをルーティングする必要があります。必要に応じて、診断インターフェイスのスタティック ルートを設定します（[デバイス（Device）] > [ルーティング（Routing）] を選択）。

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。たとえば、内部から外部へのトラフィックは有効にして、外部から内部へは有効にしないアクセス コントロール ポリシーを設定できます。

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。

ゾーンには診断/管理インターフェイスを含めません。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。

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 機能も含まれます。Auto-MDI/MDIX 機能は、自動ネゴシエーション フェーズでストレート ケーブルが検出された場合に、内部クロスオーバーを実行します。したがって、クロスオーバー配線が不要になります。インターフェイスに対して Auto-MDI/MDIX 機能を有効にするには、速度またはデュプレックスのいずれかを自動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設定して、両方の設定の自動ネゴシエーションを無効にすると、Auto-MDI/MDIX も無効になります。ギガビット イーサネットの場合は、速度を 1000 に、デュプレックスを全二重に設定すると、インターフェイスでは常に自動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、無効にすることができなくなります。

MTU について

MTU は、Firepower Threat Defense デバイス がイーサネット インターフェイス上で送信可能な最大のフレーム ペイロード サイズを指定します。MTU 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む 1518 バイト、または VLAN を使用する場合は1522バイトとなります。これらのヘッダーも収容できるように、過度に大きな値を MTU に設定しないでください。

パス MTU ディスカバリ

Firepower Threat Defense デバイス は、パス MTU ディスカバリ（RFC 1191 に規定）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 とフラグメンテーション

IPv4 の場合、出力 IP パケットが指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは送信先（場合によっては中継先）で組立て直されますが、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 の場合、通常、パケットのフラグメント化は許可されません。したがってフラグメント化を避けるために、IP パケットを MTU サイズ以内に収める必要があります。

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

（注） Firepower 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

大きな MTU はより大きなパケットを送信できます。パケットが大きくなると、ネットワークの効率性が向上することがあります。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：トラフィック パス内のすべての Firepower Threat Defense デバイス インターフェイスとその他のデバイスのインターフェイスの MTU を同じサイズ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 ヘッダーと 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 は最大で 9198 バイトに設定できます。

（注） MTU のサイズを増やすと、ジャンボ フレームに割り当てるメモリが増え、その他の機能（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。ASA 5500-X シリーズ デバイスのデフォルト値の 1500 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。

インターフェイスの設定

インターフェイスにケーブルを接続する場合は、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。このインターフェイスがブリッジ グループのメンバーであれば、設定はこれで十分です。ブリッジグループのメンバーでない場合は、インターフェイスにIPアドレスも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を特定のポートに設定するのではなく、VLAN サブインターフェイスを作成する場合は、通常は物理インターフェイスではなくサブインターフェイスに 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、それぞれ異なる 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。

インターフェイス リストには、使用可能なインターフェイスと、その名前、アドレス、およびステータスが表示されます。インターフェイスの状態（オンまたはオフ）は、インターフェイス リスト内で直接変更できます。リストには、設定に基づいたインターフェイス特性が表示されます。ブリッジ グループ インターフェイスのオープン/クローズ矢印を使用すると、メンバー インターフェイスを表示できます。メンバー インターフェイスは、リスト内に単独でも表示されます。

ポート図を使用して、インターフェイスの現在の状態をモニタします。ポートの上にマウスを合わせると、そのIPアドレス、およびイネーブル ステータスやリンク ステータスが表示されます。IP アドレスは DHCP を使用してスタティックに割り当てたり、取得できます。

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：インターフェイスが設定され、イネーブルで、リンクが稼働中です。
- 灰色：インターフェイスがイネーブルではありません。
- オレンジ/赤：インターフェイスが設定され、イネーブルですが、リンクがダウンしています。インターフェイスが有線接続である場合、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接続でない場合、これは予想される状態です。

以下の各トピックでは、インターフェイスを設定する方法について説明します。

物理インターフェイスの設定

少なくとも、物理インターフェイスをイネーブルにし、使用できるようにする必要があります。また、通常は物理インターフェイスの名前を指定し、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作成する場合、またはブリッジ グループにインターフェイスを追加する場合は、IP アドレッシングを設定しません。

（注） ブリッジ グループのメンバー インターフェイスには IP アドレスは設定できませんが、必要に応じて、詳細設定を変更できます。

インターフェイスをディセーブルにして、接続されたネットワークへの伝送を一時的に禁止することができます。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 デバイスをクリックし、[インターフェイス（Interfaces）]概要ページのリンクをクリックします。インターフェイス リストには、使用可能なインターフェイスと、その名前、アドレス、およびステータスが表示されます。

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

ステップ 3 インターフェイスをイネーブルにするには、[ステータス（Status）]>[オン（On）]をクリックします。
この物理インターフェイスにサブインターフェイスを設定しようとする段階では、多くの場合、設定は完了です。[保存（Save）]をクリックし、VLAN サブインターフェイスと 802.1Q トランキングの設定，（11 ページ）に進みます。それ以外の場合は、続行します。

（注） サブインターフェイスを設定する場合でも、インターフェイスに名前を付け、IPアドレスを割り当てることは有効です。これは一般的な設定ではありませんが、必要に応じて設定できます。

ステップ 4　以下を設定します。

- [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。英字は小文字である必要があります。たとえば、「inside」や「outside」などの名前を使用します。名前を設定しない場合は、残りのインターフェイス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を設定する必要があります。

  （注）　名前を変更すると、セキュリティ ゾーン、syslog サーバ オブジェクト、および DHCP サーバの定義を含む、古い名前を使用したすべての場所にその変更が自動的に反映されます。ただし、一般に名前の付いていないインターフェイスをポリシーや設定に使用できないため、名前を削除するには、まず、その使用するすべての設定を削除する必要があります。

- （オプション）[説明（Description）]：説明は200文字以内で入力できます。改行を入れずに1行で入力します。

ステップ 5　[IPv4 アドレス（IPv4 Address）] タブをクリックし、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。

- [ダイナミック（Dynamic）]（DHCP）：ネットワーク上の DHCP サーバ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。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、学習された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ー255です。デフォルトは1です。
  - [デフォルト ルートの取得（Obtain Default Route）]：DHCP サーバからデフォルト ルートを取得するかどうか。通常、このオプションをオン（デフォルト）にします。
- [スタティック（Static）]：変更しないアドレスを割り当てる場合は、このオプションをオンにします。インターフェイスの IP アドレスと、インターフェイスに接続されるネットワークのサブネット 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。そのアドレスがまだネットワークで使用されていないことを確認してください。

  （注）　既存のインターフェイスの場合、そのインターフェイス用に DHCP サーバが設定されているときは、アドレスを変更する機能が制限されます。新しい IP アドレスは、DHCP アドレス プールと同じサブネット上にある必要があります。また、このアドレスをそのプールに含めることはできません。異なるサブネット上にアドレスを設定する必要がある場合は、最初に DHCP サーバの設定を削除します。DHCP サーバの設定 を参照してください。

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、IPv6 アドレスを設定します。

- [状態（State）]：IPv6 処理を有効にして、グローバル アドレスを設定しないときにリンクローカル アドレスを自動設定するには、[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 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、IPv6 アドレスが明示的に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での IPv6 処理は無効になりません。

- [アドレス自動設定（Address Auto Configuration）]：アドレスを自動的に設定させるには、このオプションをオンにします。IPv6 ステートレス自動設定は、デバイスが存在するリンクで使用するグローバルな IPv6 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 アドレスを生成します。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカルな IPv6 アドレスのみが取得され、そのデバイスが属すネットワーク リンクの外部に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に基づきます。

  RFC 4862 では、ステートレスな自動設定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していますが、Firepower Threat Defense デバイスはこの場合、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、RFC に準拠させるには、[RA の抑制（Suppress RA）] を選択します。

- [スタティック アドレス/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は、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 と指定します。IPv6 アドレッシングの詳細については、IPv6 アドレッシング，（3 ページ）を参照してください。

  アドレスをリンクローカルとしてのみ使用する場合は、[リンクローカル（Link - Local）] オプションをオンにします。リンクローカル アドレスはローカル ネットワークの外部にはアクセスできません。ブリッジ グループ インターフェイスではリンクローカル アドレスを設定できません。

  （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。たとえば fe80::20d:88ff:feee:6a82 のようになります。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカルアドレスのパケットはドロップされる可能性があります。

- [RA の抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうか。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、Firepower 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、各 IPv6 対応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送信要求メッセージに応答して送信されます（ICMPv6 Type 133）。ルータ送信要求メッセージは、ホストからシステムの起動時に送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

  Firepower 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 （オプション）高度なインターフェイス オプションの設定，（18 ページ）.

詳細設定には、ほとんどのネットワークで最適となるデフォルトが用意されています。ネットワーク問題を解決する場合に限り、これらを編集します。

ステップ 8 [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、それぞれ異なる 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。

（注） ブリッジ グループのメンバー インターフェイスには IP アドレスは設定できませんが、必要に応じて、詳細設定を変更できます。

はじめる前に

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イネーブル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。

手順

ステップ 1 デバイスをクリックし、[インターフェイス（Interfaces）]概要ページのリンクをクリックします。インターフェイス リストには、使用可能なインターフェイスと、その名前、アドレス、およびステータスが表示されます。サブインターフェイスは、それぞれの物理インターフェイスの下位にグループ化されます。

ステップ 2 次のいずれかを実行します。

- 歯車のドロップダウン リストから [サブインターフェイスの追加（Add Subinterface）]を選択し、サブインターフェイスを新規作成します。
- 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アイコン（）をクリックして削除します。

ステップ 3 インターフェイスをイネーブルにするには、[ステータス（Status）] > [オン（On）] をクリックします。

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。

- [親インターフェイス（Parent Interface）]：サブインターフェイスを追加する物理インターフェイスを選択します。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。
- [名前（Name）]：最大 48 文字のサブインターフェイスの名前。英字は小文字である必要があります。たとえば、「inside」や「outside」などの名前を使用します。名前を設定しない場合は、残りのインターフェイス設定は無視されます。

  （注） 名前を変更すると、セキュリティ ゾーン、syslog サーバ オブジェクト、および DHCP サーバの定義を含む、古い名前を使用したすべての場所にその変更が自動的に反映されます。ただし、一般に名前の付いていないインターフェイスをポリシーや設定に使用できないため、名前を削除するには、まず、その使用するすべての設定を削除する必要があります。
- （オプション）[説明（Description）]：説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 5 サブインターフェイスの一般的な特性を設定します。

- [VLAN ID]：VLAN ID を 1 ～ 4094 の範囲で入力します。これは、このサブインターフェイス上のパケットにタグを付けるために使用されます。
- [サブインターフェイス ID（Subinterface ID）]：サブインターフェイス ID を 1 ～ 4294967295 の範囲の整数で入力します。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。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 6 [IPv4 アドレス（IPv4 Address）] タブをクリックし、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。

- [ダイナミック（Dynamic）]（DHCP）：ネットワーク上の DHCP サーバ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。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、学習された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 ー 255 です。デフォルトは 1 です。
  - [デフォルト ルートの取得（Obtain Default Route）]：DHCP サーバからデフォルト ルートを取得するかどうか。通常、このオプションをオン（デフォルト）にします。
- [スタティック（Static）]：変更しないアドレスを割り当てる場合は、このオプションをオンにします。インターフェイスの IP アドレスと、インターフェイスに接続されるネットワークのサブネット 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。そのアドレスがまだネットワークで使用されていないことを確認してください。

（注） 既存のインターフェイスの場合、そのインターフェイス用に DHCP サーバが設定されているときは、アドレスを変更する機能が制限されます。新しい IP アドレスは、DHCP アドレス プールと同じサブネット上にある必要があります。また、このアドレスをそのプールに含めることはできません。異なるサブネット上にアドレスを設定する必要がある場合は、最初に DHCP サーバの設定を削除します。DHCP サーバの設定 を参照してください。

ステップ 7 （オプション）[IPv6 アドレス（IPv6 Address）] タブをクリックし、IPv6 アドレスを設定します。

- [状態（State）]：IPv6 処理を有効にして、グローバル アドレスを設定しないときにリンクローカル アドレスを自動設定するには、[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 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、IPv6 アドレスが明示的に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での IPv6 処理は無効になりません。

- [アドレス自動設定（Address Auto Configuration）]：アドレスを自動的に設定させるには、このオプションをオンにします。IPv6 ステートレス自動設定は、デバイスが存在するリンクで使用するグローバルな IPv6 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 アドレスを生成します。IPv6 ルーティング サービスがリンクで使用できない場合、リンクローカルな IPv6 アドレスのみが取得され、そのデバイスが属すネットワーク リンクの外部に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に基づきます。

  RFC 4862 では、ステートレスな自動設定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していますが、Firepower Threat Defense デバイスはこの場合、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、RFC に準拠させるには、[RA の抑制（Suppress RA）] を選択します。

- [スタティック アドレス/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は、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 と指定します。IPv6 アドレッシングの詳細については、IPv6 アドレッシング，（3 ページ）を参照してください。

  アドレスをリンクローカルとしてのみ使用する場合は、[リンクローカル（Link - Local）] オプションをオンにします。リンクローカル アドレスはローカル ネットワークの外部にはアクセスできません。ブリッジ グループ インターフェイスではリンクローカル アドレスを設定できません。

  （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。たとえば fe80::20d:88ff:feee:6a82 のようになります。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカルアドレスのパケットはドロップされる可能性があります。

- [RA の抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうか。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、Firepower 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、各 IPv6 対応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送信要求メッセージに応答して送信されます（ICMPv6 Type 133）。ルータ送信要求メッセージは、ホストからシステムの起動時に送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

  Firepower 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 8 （オプション）高度なインターフェイス オプションの設定，（18 ページ）.
詳細設定には、ほとんどのネットワークで最適となるデフォルトが用意されています。ネットワーク問題を解決する場合に限り、これらを編集します。

ステップ 9 [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した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です。これにより、ワークステーションまたは他のエンドポイント デバイスを、ブリッジ グループ内のインターフェイスに直接接続できます。個別の物理スイッチを経由して接続する必要はありません。ただし、ブリッジグループ メンバーにスイッチを接続することも可能です。

各グループ メンバーは、IP アドレスを持ちません。代わりに、すべてのメンバーインターフェイスは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、各メンバーインターフェイスには自動的に、一意のリンクローカルアドレスが割り当てられます。

通常は、□ブリッジ グループ インターフェイス（BVI）には DHCP サーバを設定します。これにより、メンバー インターフェイスを介して接続されたすべてのエンドポイントに、IP アドレスが提供されます。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たエンドポイントにスタティック アドレスを設定することもできます。ブリッジグループ内のすべてのエンドポイントは、ブリッジ グループの IP アドレスと同じサブネット上の IP アドレスを持つ必要があります。

（注） すべての ASA 5506-X モデルでは、新バージョンの 6.2+ システム、またはイメージを再作成した 6.2+ システムにおいて、デバイスにはあらかじめBVI1「inside」と名前の付いたブリッジ グループが設定されています。これには、「outside」 インターフェイス以外のすべてのデータ インターフェイスが含まれます。したがって、デバイスにはインターネット、またはその他のアップストリーム ネットワークへのリンクに使用される 1 つのポートが事前に設定されています。また、他のすべてのポートも有効であり、エンドポイントを直接接続できます。新しいサブネットで内部インターフェイスを使用するには、まず、必要なインターフェイスを BVI1 から削除する必要があります。

はじめる前に

ブリッジグループのメンバーと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す必要があります。

- インターフェイスには名前が必要です。
- スタティック アドレスであっても、DHCP 経由であっても、インターフェイスに何らかの IPv4 または IPv6 アドレスを定義することはできません。現在使用中の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、アドレスを保持するインターフェイスの種類に応じて、スタティック ルート、DHCP サーバ、NAT ルールなど、インターフェイスの他の設定も削除しなければならない可能性があります。
- インターフェイスをブリッジ グループに追加するには、このインターフェイスをセキュリティ ゾーンから削除し（ゾーンに属している場合）、インターフェイスに設定されていたすべての NAT ルールを削除しておく必要があります。

また、各メンバー インターフェイスは個別に有効化および無効化します。これにより、未使用のインターフェイスを、ブリッジグループから削除することなく無効にできます。ブリッジグループ自体は常に有効です。

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）] 概要ページのリンクをクリックします。
インターフェイス リストには、使用可能なインターフェイスと、その名前、アドレス、およびステータスが表示されます。ブリッジ グループがすでに存在する場合は、フォルダとして表示されます。オープン/クローズ矢印をクリックすると、メンバー インターフェイスを表示できます。また、リストには個別のメンバー インターフェイスも表示されます。

ステップ 2 次のいずれかを実行します。

- BVI1ブリッジ グループの編集アイコン（）をクリックします。
- 歯車のドロップダウン リストから [ブリッジ グループ インターフェイスの追加（Add Bridge Group Interface）]を選択し、新規グループを作成します。

（注） 使用できるのは 1 つのブリッジ グループのみです。すでにブリッジ グループを定義している場合は、新たなグループを新規作成するのではなく、既存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、既存のブリッジ グループを事前に削除しておく必要があります。

- 不要になったブリッジグループを削除する場合は、削除アイコン（）をクリックします。ブリッジグループを削除すると、このグループの各メンバーは標準的なルーテッドインターフェイスとなり、すべての NAT ルールまたはセキュリティ ゾーン メンバーシップは維持されます。各インターフェイスを編集して、それぞれの IP アドレスを指定できます。新しいブリッジ グループにインターフェイスを追加するには、まず、NAT ルールを削除し、セキュリティゾーンからこのインターフェイスを削除する必要があります。

ステップ 3 以下を設定します。

- [インターフェイス名（Interface Name）]：最大 48 文字のブリッジ グループの名前。英字は小文字である必要があります。たとえば、「inside」や「outside」などの名前を使用します。名前を設定しない場合は、残りのインターフェイス設定は無視されます。

  （注） 名前を変更すると、セキュリティ ゾーン、syslog サーバ オブジェクト、および DHCP サーバの定義を含む、古い名前を使用したすべての場所にその変更が自動的に反映されます。ただし、一般に名前の付いていないインターフェイスをポリシーや設定に使用できないため、名前を削除するには、まず、その使用するすべての設定を削除する必要があります。

- （オプション）[説明（Description）]：説明は 200 文字以内で入力できます。改行を入れずに 1 行で入力します。

ステップ 4 ブリッジ グループのメンバー リストを編集します。
1 つのブリッジ グループには、最大 64 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。

- [+]をクリックして、インターフェイスを追加します。
- インターフェイスを削除するには、インターフェイス上にマウス オーバーし、右側の [x]をクリックします。

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、次のオプションのいずれかを選択します。

- [スタティック（Static）]：変更されることのないアドレスを割り当てるには、このオプションを選択します。ブリッジ グループの IP アドレスおよびサブネット マスクを入力します。接続されるすべてのエンドポイントは、このネットワークに接続されます。ASA 5506-X モデルでは、BVI1 の inside ネットワークはデフォルトで 192.168.1.1/24（つまり 255.255.255.0）となります。このアドレスが、ネットワーク上でまだ未使用であることを確認します。

（注） 既存のブリッジ グループでは、グループに DHCP サーバを設定している場合、アドレスの変更に制限が生じます。新しい IP アドレスは、DHCP アドレス プールと同じサブネット上でなければならず、このプールの一部にすることはできません。別のサブネットにアドレスを設定する必要がある場合は、まず、DHCP サーバの設定を削除します。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。これはブリッジ グループの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。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）]：デフォルト ルートを DHCP サーバから取得する場合の、学習したルートまでのアドミニストレーティブ ディスタンス（1 ～ 255）。デフォルトは 1 です。
  - [デフォルト ルートを取得（Obtain Default Route）]：DHCP サーバからデフォルト ルートを取得するかどうか。デフォルトではオンであり、通常はこのオプションを選択します。

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、IPv6 アドレスを設定します。

- [状態（State）]：IPv6 処理を有効にして、グローバル アドレスを設定しないときにリンクローカル アドレスを自動設定するには、[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 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、IPv6 アドレスが明示的に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での IPv6 処理は無効になりません。

- [スタティック アドレス/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は、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 と指定します。IPv6 アドレッシングの詳細については、IPv6 アドレッシング，（3 ページ）を参照してください。

  アドレスをリンクローカルとしてのみ使用する場合は、[リンクローカル（Link - Local）] オプションをオンにします。リンクローカル アドレスはローカル ネットワークの外部にはアクセスできません。ブリッジ グループ インターフェイスではリンクローカル アドレスを設定できません。

  （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。たとえば fe80::20d:88ff:feee:6a82 のようになります。Modified EUI-64 形式に基づくリンクローカル アドレスを自動的に割り当てることを推奨します。たとえば、他のデバイスが Modified EUI-64 形式の使用を必要とする場合、手動で割り当てたリンクローカル アドレスのパケットはドロップされる可能性があります。

- [RA の抑制（Suppress RA）]：ルータ アドバタイズメントを抑制するかどうか。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、Firepower 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、各 IPv6 対応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送信要求メッセージに応答して送信されます（ICMPv6 Type 133）。ルータ送信要求メッセージは、ホストからシステムの起動時に送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

Firepower 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 （オプション）高度なインターフェイス オプションの設定, （18 ページ）.

□ブリッジ グループのメンバー インターフェイスにはほとんどの詳細オプションを設定できますが、いくつかの詳細オプションは□ブリッジ グループ インターフェイスにも設定できます。

詳細設定には、ほとんどのネットワークで最適となるデフォルトが用意されています。ネットワーク問題を解決する場合に限り、これらを編集します。

ステップ 8 [OK]をクリックします。

次の作業

- 使用するすべてのメンバー インターフェイスが有効化され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 ポリシー、NAT ポリシー、アクセス ポリシーなどのポリシーが、ブリッジ グループおよびメンバー インターフェイスに必要なサービスを供給することを確認してください。

高度なインターフェイス 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する場合のみ設定を行います。

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。

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 の試行を除き、これらのオプションをブリッジ仮想インターフェイス（BVI）に設定することはできません。

手順

ステップ 1 デバイスをクリックし、[インターフェイス（Interfaces）]概要ページのリンクをクリックします。インターフェイス リストには、使用可能なインターフェイスと、その名前、アドレス、およびステータスが表示されます。

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）]タブをクリックします。

ステップ 4 データ インターフェイスを管理専用に指定する場合は、[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に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 5 [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。64 ～ 9198 の値を指定できます（Firepower Threat Defense Virtualの場合は最大値が 9000）。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） ASA 5500-X シリーズ デバイス に対して MTU を 1500 以上に設定した場合は、デバイスをリブートする必要があります。CLI にログインし、**reboot** コマンドを使用します。

ステップ 6 （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。

- [デュプレックス（Duplex）] : [全二重（Full）]、[半二重（Half）]、または [自動（Auto）]のいずれかを選択します。デフォルトは [自動（Auto）] です。
- [速度（Speed）] : [10]、[100]、[1000]、[10000] Mbps、または [自動（Auto）]を選択します。デフォルトは [自動（Auto）] です。

ステップ 7 [IPv6 設定（IPv6 Configuration）]を変更します。

- [IPv6 アドレス設定で DHCP を有効化する（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。
- [IPv6 のアドレス以外の設定で DHCP を有効化する（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パケットの処理はディセーブルになります。重複アドレスがグローバルアドレスであれば、そのアドレスは使用されません。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）プロセスをディセーブルにするには、この値を 0 に設定します。

ステップ 8 [OK]をクリックします。

モニタリング インターフェイス

次のエリアで、インターフェイスに関する基本情報を表示できます。

- [モニタリング（Monitoring）] > [システム（System）]。[スループット（Throughput）]ダッシュボードはシステムを経由するトラフィックに関する情報を表示します。すべてのインターフェイスに関する情報を表示することもできれば、特定のインターフェイスを選択して調べることもできます。
- [モニタリング（Monitoring）] > [入力ゾーン（Ingress Zones）] および [出力ゾーン（Egress Zones）]。これらのダッシュボードは、インターフェイスで構成されたゾーンに基づく統計情報を表示します。この情報はさらに詳細な情報へ堀り下げることができます。
- [デバイス（Device）]。[接続図（Connection Diagram）] には、インターフェイスのステータスが表示されます。ポートをマウス オーバーすると、インターフェイスの IP アドレス、インターフェイスの状態およびリンク ステートが表示されます。この情報を使用すると、稼働している必要があるときにダウンしているインターフェイスを識別するために役立ちます。

CLI でのインターフェイスのモニタリング

デバイス CLI にログインし、次のコマンドを使用して、インターフェイス関連の動作と統計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、必要な情報を取得するために使用できる多数のキーワードがあります。使用可能なオプションを確認するには、? 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、メンバー情報と 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、インターフェイスを通じて現在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経由するトラフィックに関する統計情報を表示します。
- **show ipv6 traffic** は、デバイスを経由する IPv6 トラフィック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、特に、インターフェイスに設定された DHCP サーバに関する統計情報とその他の情報を表示します。