インターフェイス

ここでは、Firepower Threat Defense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。

Firepower Threat Defenseインターフェイスについて

Firepower Threat Defenseデバイスは、データ インターフェイスに加えて管理/診断インターフェイスが含まれています。次のトピックでは、Firepower Device Manager、および他のインターフェイス管理概念を通じたインターフェイス設定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

Firepower 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Firepower 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。
- IPS 専用モードはサポートされていません。IPS 専用処理では、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 専用モードのインターフェイスは、多数のファイアウォールの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。対照的に、ファイアウォール モードのインターフェイスでは、トラフィックが、フローの維持、IP レイヤおよび TCP レイヤの両方でのフロー状態の追跡、TCP の標準化などのファイアウォール機能の対象となります。また、任意で、セキュリティ ポリシーに従ってファイアウォール モードのトラフィックに IPS 機能を設定することもできます。

- 冗長インターフェイスでは EtherChannel を設定できません。
- IPv4 の PPPoE を設定することはできません。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 ISP へのその他の接続に接続されていて、ISP が PPPoE を使用して IP アドレスを提供している場合、これらの構成を設定するには、Firepower Management Center を使用する必要があります。
- ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X では、オプションのネットワーク インターフェイス カード（EPM）を設置できます。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、インストールの間にローカルまたはリモート管理を切り替えるとき、およびメジャー/マイナー リリース アップグレードの間）。SFP インターフェイスを含むカードでは、Firepower Device Manager が速度とデュプレックスを「自動」に設定しますが、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は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 に設定し、デュプレックスを [フル（Full）] に設定してから設定を展開します。リンクが機能しない場合、異なる速度を試行します。

ルーテッド インターフェイス

ルーテッド ファイアウォール モードでは、各インターフェイスは、一意のサブネットで IP アドレスを設定する必要があるレイヤ 3 ルーテッド インターフェイスになります。

1 つのインターフェイスに IPv6 アドレスと IPv4 アドレスの両方を設定できます。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

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。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。

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。

管理/診断インターフェイスとネットワーク配置

物理的な管理インターフェイスは、診断論理インターフェイスと管理論理インターフェイスの間で共有できます。

管理インターフェイス

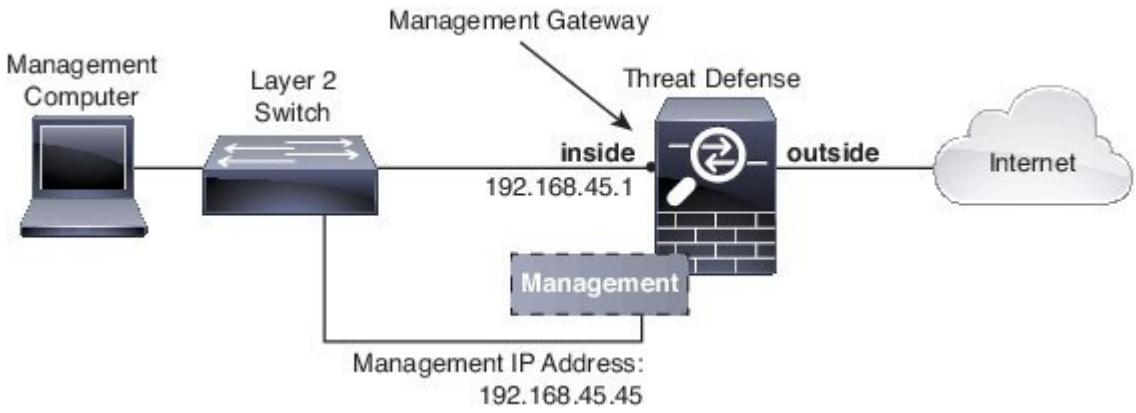
管理論理インターフェイスはデバイスの他のインターフェイスから切り離されています。これはコンフィギュレーション インターフェイス を実行し、デバイスのコマンドライン インターフェイス（CLI）にアクセスしてさまざまな機能の更新情報を取得するために使用されます。アドレスは [システム設定（System Settings）] > [デバイス管理 IP（Device Management IP）] ページで設定します。**configure network** コマンドを使用して、CLIに追加の設定を構成できます。

診断インターフェイス

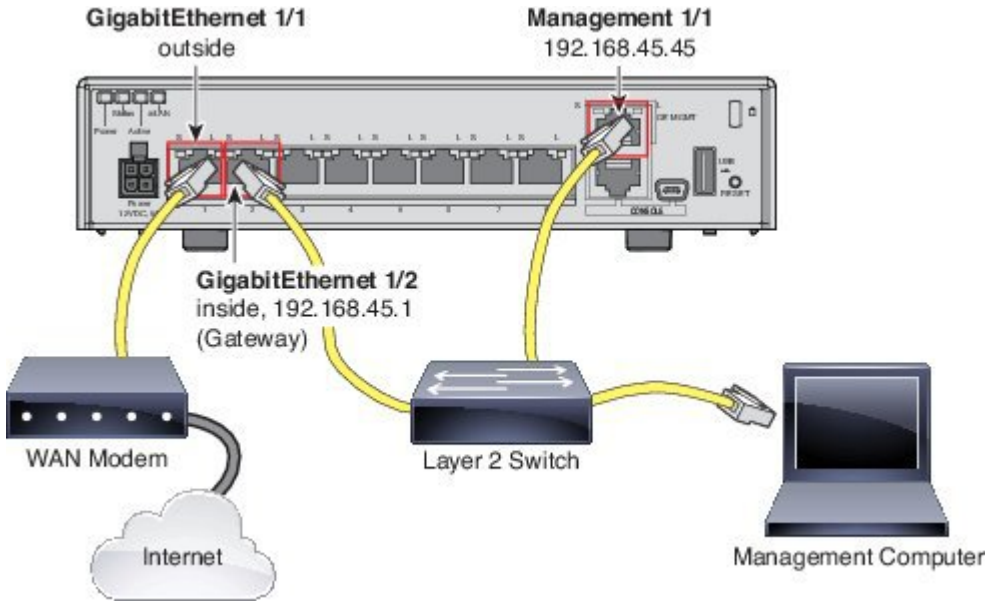
診断論理インターフェイスは、他のデータ インターフェイスと一緒に設定できます。診断インターフェイスの使用はオプションです。たとえば、データ インターフェイスを介してリモート syslog サーバにログ メッセージを送信する必要がない場合は、IP アドレスを設定します。診断インターフェイスは管理トラフィックのみを許可し、トラフィックのスルーは許可しません。

ルーテッド モードの導入

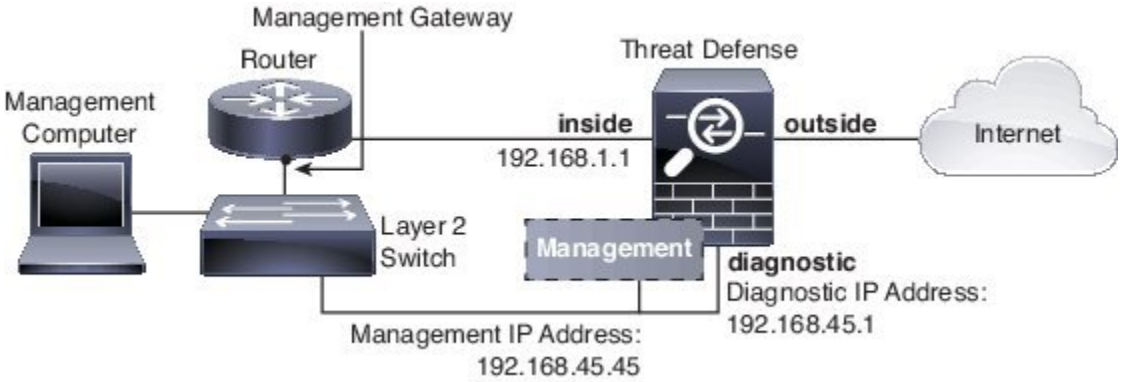
内部ルータがない場合は診断インターフェイスのIPアドレスを設定しないことをお勧めします。診断インターフェイスのIPアドレスを設定しなければ、他のデータインターフェイスと同じネットワーク上に管理インターフェイスを配置できます。診断インターフェイスを設定すると、一般的にその IP アドレスは管理 IP アドレスと同じネットワークになり、他のデータ インターフェイスと同じネットワーク上に存在できない標準インターフェイスと見なされます。管理インターフェイスは更新のためにインターネットにアクセスする必要があるため、管理インターフェイスを内部インターフェイスと同じネットワーク上に置くと、内部にスイッチのみを持つFirepower Threat Defenseデバイスを導入して、そのゲートウェイとして内部インターフェイスを指定することができます。内部スイッチを使用する次の導入を参照してください。



ASA 5506-X、ASA 5508-X、または ASA 5516-X で上記のシナリオをケーブル接続するには、次を参照してください。



診断 IP アドレスを設定する場合は、内部ルータが必要です。



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。その後、ゾーンに基づいてセキュリティ ポリシーを適用します。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。

診断/管理インターフェイスはゾーンに含まれません。ゾーンは、データインターフェイスにのみ適用されます。

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

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 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。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 は常にイネーブルになり、ディセーブルにできません。

MTU について

MTU は、Firepower 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する最大フレーム 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

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 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） 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できます。

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 Firepower Threat Defense デバイス 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お勧めします。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、9198 バイトまでの MTU を設定できます。

（注） MTU を増やすとジャンボ フレームに割り当てられるメモリが増加し、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 デバイスで、MTU をデフォルトの 1500 以上に増やす場合、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

インターフェイス接続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、物理インターフェイスを有効にし、この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 リストは、利用可能なインターフェイス、その名前、アドレスおよびステータスを表示します。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。

インターフェイスの現在の状態をモニタするには、ポート グラフィックを使用します。マウスオーバーでそのIPアドレス、有効なステータスとリンク ステータスを確認します。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：インターフェイスが設定され、イネーブルであり、リンクが稼働中です。
- グレー：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されている場合、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されていない場合、これは予想される状態です。

次に、インターフェイスの設定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、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作成する予定の場合、、IPアドレッシングを設定する必要はありません。

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（Device）]メニューのデバイス名クリックして、[インターフェイス（Interfaces）]サマリのリンクをクリックします。
インターフェイス リストに、使用可能なインターフェイス、インターフェイス名、アドレス、および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有効にするには、[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 トランキングの設定, （10 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 アドレスを指定することができます。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。

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） 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。

- （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。

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。

- [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、デフォルトである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。

（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に対して DHCP サーバを設定していると、アドレスの変更機能は制限されます。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存在する必要があり、そのプールの一部にすることはできません。別のサブネットの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。

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、Firepower 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, （2 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。

- [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。Firepower Threat Defense デバイス は、ネイバー デバイスがデフォルトのルータ アドレスを動的に学習できるように、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）詳細インターフェイス オプションの設定，（13 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 [保存（Save）]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、1 つの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やデバイスを追加しなくても、ネットワーク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。

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、通常は、物理インターフェイスをトラフィックが通過しないようにします。これは、物理インターフェイスはタグなしパケットを通過させるためです。トラフィックがサブインターフェイスを通過するためには物理インターフェイスを有効にする必要があるため、物理インターフェイスに名前を付けないことで、物理インターフェイスをトラフィックが通過しないようにします。物理インターフェイスにタグなしパケットを通過させる場合は、通常どおり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（Device）]メニューのデバイス名クリックして、[インターフェイス（Interfaces）]サマリのリンクをクリックします。

インターフェイス リストに、使用可能なインターフェイス、インターフェイス名、アドレス、および状態が表示されます。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。

- [+]ボタンをクリックして、新しいサブインターフェイスを作成します。
- 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、削除するサブインターフェイスの削除アイコン（）をクリックします。

ステップ 3 インターフェイスを有効にするには、[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、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。サブインターフェイスを作成後に、親インターフェイスを変更することはできません。
- [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。

- （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。

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]：このサブインターフェイス上のパケットにタグ付けするために使用される VLAN ID（1 ～ 4094）を入力します。
- [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数は、プラットフォームによって異なります。サブインターフェイスを作成後に、ID を変更することはできません。

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。

- [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、デフォルトである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。

  （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に対して DHCP サーバを設定していると、アドレスの変更機能は制限されます。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存在する必要があり、そのプールの一部にすることはできません。別のサブネットの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。

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、Firepower 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, （2 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。

- [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。Firepower Threat Defense デバイス は、ネイバー デバイスがデフォルトのルータ アドレスを動的に学習できるように、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）詳細インターフェイス オプションの設定, （13 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 9 [保存（Save）]をクリックします。

詳細インターフェイス オプションの設定

詳細インターフェイス オプションには、ほとんどのネットワークに適しているデフォルト設定があります。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。

次の手順は、インターフェイスがすでに定義されていることを前提としています。これらの設定は、インターフェイスの初期編集時または作成時にも編集できます。

手順

ステップ 1 [デバイス（Device）]メニューのデバイス名クリックして、[インターフェイス（Interfaces）] サマリのリンクをクリックします。

インターフェイス リストに、使用可能なインターフェイス、インターフェイス名、アドレス、および状態が表示されます。

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 インターフェイスの管理のみを行うには、[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として設定する価値はあまりありません。常に管理専用の管理/診断インターフェイスの場合、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）を目的の値に変更します。
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 9000）。ネットワーク上にジャンボ フレームが多い場合は、高い値を設定します。

（注） ASA 5500-X シリーズ デバイスの MTU を 1500 より上の値にする場合、デバイスを再起動する必要があります。CLI にログインして、**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）速度とデュプレックスの設定を変更します。
デフォルトでは、インターフェイスがネットワークの反対側にあるインターフェイスと最適なデュプレックスと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または速度を強制することができます。

- [デュプレックス（Duplex）] : [全（Full）]、[半（Half）]、または [自動（Auto）]を選択します。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）]の設定を変更します。

- [IPv6 アドレス設定での DHCP の有効化（Enable DHCP for IPv6 address configuration）] : IPv6 ルータ アドバタイズメント パケットに管理対象アドレス設定フラグを設定するかどうかを指定します。このフラグは、取得されるステートレス自動設定アドレス以外のアドレスを取得するために 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 以外のアドレス設定での DHCP の有効化（Enable DHCP for IPv6 non-address configuration）] : IPv6 ルータ アドバタイズメント パケットにその他のアドレス設定フラグを設定するかどうかを指定します。このフラグは、DNS サーバ アドレスなどの追加情報を DHCPv6 から取得するために 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 試行（DAD Attempts）] : インターフェイスが重複アドレス検出（DAD）を実行する頻度（0 ～ 600）を指定します。デフォルトは 1 です。ステートレス自動設定プロセスの間、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る場合、インターフェイス上での 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る場合、そのアドレスは使用されません。インターフェイスは、ネ

イバー要請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）処理を無効にするには、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。

- [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）] > [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には、インターフェイスで構成されるゾーンに基づいた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。
- [デバイス（Device）]。接続図にインターフェイスのステータスが表示されます。ポートの上にマウスを移動すると、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、起動している必要がある場合にダウンしているインターフェイスを特定できます。

CLI でのインターフェイスのモニタリング

デバイス CLI にログインして次のコマンドを使用すると、インターフェイス関連の動作および統計情報に関するより詳細な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および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、インターフェイスを介し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介して移動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、デバイスを介して移動する IPv6 トラフィックに関する統計情報を表示します。

- **show dhcpd** は、インターフェイスでの DHCP の使用状況、特にインターフェイスで設定されている 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。