インターフェイス

ここでは、FTD 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。

- FTD 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限事項 （5 ページ）
- 物理インターフェイスの設定 （8 ページ）
- ブリッジ グループの設定 （12 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 （17 ページ）
- 高度なインターフェイス オプションの設定 （21 ページ）
- Firepower Threat Defense Virtual へのインターフェイスの追加 （24 ページ）
- モニタリング インターフェイス （26 ページ）
- インターフェイスの例 （27 ページ）

FTD インターフェイスについて

FTD には、データ インターフェイスや管理/診断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。

インターフェイス リストに、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、状態が示されます。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。また、ブリッジ グループ インターフェイスの開く/閉じる矢印を使用すると、メンバー インターフェイスが表示されます。これはリストにも個別に表示されます。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、Firepower 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。

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 モード

インターフェイスごとに、次のいずれかのモードを設定できます。

ルーテッド（Routed）

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。

BridgeGroupMember

ブリッジ グループは、FTD 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が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せん。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。

ブリッジ グループのルーテッド モードでの使い方の 1 つは、外部スイッチの代わりに Firepower Threat Defense デバイスで追加のインターフェイスを使用することです。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

管理ラベル付けされた物理ポート（または、Firepower Threat Defense Virtual の場合は Management0/0 仮想インターフェイス）には、2 つの別個のインターフェイスが実際に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 ライセンスに使用し、データベースの更新情報を取得するためのアドレスです。これに対して管理セッションを開くことができます（Firepower Device Manager および 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、実際には診断という名前が付けられています。外部 syslog サーバに syslog メッセージを送信するためにこのインターフェイスを使用できます。診断物理インターフェイスの IP アドレスの設定は任意です。syslog で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、トラフィックのスルーは許可しません。

（ハードウェア デバイス）管理/診断を設定する際、物理ポートをネットワークに接続しないことをお勧めします。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 Firepower Device Manager を開きます（管理アクセス リストの設定を参照）。

Firepower 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。診断用に別のアドレスを設定しないでください。

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、物理管理/診断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。

Firepower 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。

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、接続されたネットワークで IPv4 または IPv6 アドレス（または両方）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。

- インターフェイスを介して syslog サーバに syslog メッセージを送信しようとする場合にのみ、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）]**）。そうでない場合は、診断用のアドレスは設定しないでください。必要ありません。設定する IP アドレスは、管理 IP アドレスと同じサブネット上に存在する必要があります。DHCP サーバプールに設定することはできません。たとえば、デフォルト設定では 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ため、192.168.45.1 から 192.168.45.44 のアドレスを使用して診断アドレスを設定できます。

別の管理ネットワークのための管理/診断インターフェイス設定に関する制限事項

物理管理インターフェイスを配線する場合、またはFirepower Threat Defense Virtualの場合は、Management0/0を分離したネットワークに接続し、次の制限に従ってください。

- 管理ネットワークでDHCPサーバを設定する場合、管理インターフェイス（**[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）]**）で設定します。診断（物理）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。
- 管理ネットワークに別のDHCPサーバがある場合、それを無効にしないと管理インターフェイス上でそのDHCPサーバが実行されます。一般に、特定のサブネットで複数のDHCPサーバを設定することはできません。
- 管理および診断の両方にアドレスを設定する場合、それらが同じサブネット上にあることを確認します。
- （ハードウェア デバイスのみ）診断のIPアドレスを設定する場合であっても、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はデータ インターフェイスをゲートウェイとして使用することはありません。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な場合、管理ネットワーク上の別のルータが、診断IPアドレスから送信される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にスタティック 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。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。

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。

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限事項

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

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。
- パッシブ インターフェイスまたは ERSPAN インターフェイスを設定することはできません。
- インターフェイスをインライン（インラインセット内）またはインラインタップ（IPS オンリー処理用）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。
- EtherChannel や冗長インターフェイスは設定できません。
- 追加できるブリッジ グループは 1 つだけです。
- 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 と Firepower 2100 シリーズでは、オプションのネットワーク インターフェイス モジュールをインストールできます。モジュールはブートストラップ中（つまり、初期インストールまたは再イメージ化、ローカル/リモート管理間の切り替え時）にのみ検出されます。 Firepower Device Manager はこれらのインターフェイスの速度とデュプレックスに正しいデフォルトを設定します。利用可能なインターフェイスの合計数を変更することなく、オプションのモジュールを、インターフェイスの速度やデュプレックスのオプションが変わるモジュールと交換する場合、交換されたインターフェイスの正しい速度やデュプレックスの値をシステムが認識できるように、デバイスを再起動します。デバイスとの SSH セッションまたはコンソール セッションで、**reboot** コマンドを入力します。次に、Firepower Device Manager で、機能の変更を含む各物理インターフェイスを編集し、有効な速度とデュプレックスのオプションを選択します。システムは元の設定を自動的に修正しないためです。すぐに変更を展開して、システムが正しく動作していることを確認します。

（注） モジュールをインターフェイスの総数が変更されたモジュールと交換した場合や、他のオブジェクトによって参照されたインターフェイスを削除した場合は、予期しない問題が発生することがあります。このような変更が必要な場合は、まずセキュリティゾーンのメンバーシップ、VPN 接続など、削除するインターフェイスへのすべての参照を削除してください。また、変更を行う前にバックアップを実行することもお勧めします。

- Firepower Threat Defense Virtual へのインターフェイスの追加 （24 ページ）で説明しているように、Firepower Threat Defense Virtual デバイスでは、デバイスを再初期化せずに、インターフェイスを追加または削除することはできません。ただし、インターフェイスを異なる速度/デュプレックス能力を持っているインターフェイスと単純に交換する場合は、システムで新しい速度/デュプレックス値が認識されるようにデバイスを再起動してください。CLI コンソールから、**reboot** コマンドを入力します。次に、Firepower Device Manager で、能力の変更を含む各インターフェイスを編集し、有効な速度とデュプレックスのオプションを選択します。システムは元の設定を自動的に修正しないためです。すぐに変更を展開して、システムの正しい動作を確認します。

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 2100	1024
Firepower Threat Defense Virtual	50
ASA 5506-X ASA 5506W-X ASA 5506H-X	30
ASA 5508-X	50
ASA 5512-X	100
ASA 5515-X	100
ASA 5516-X	100
ASA 5525-X	200

モデル	VLAN サブインターフェイスの最大数
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	25

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、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。

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。

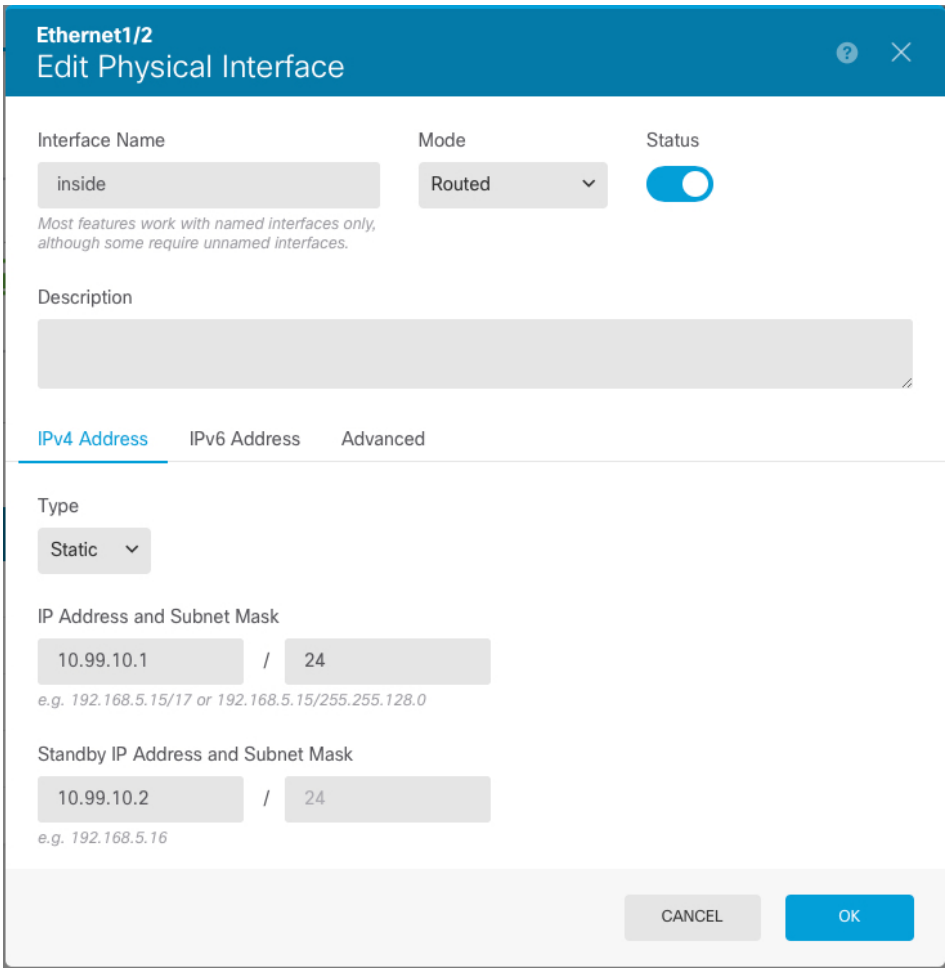
手順

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



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

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 （17 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。

c) （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。

- [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） 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。

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、FTD 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 （4 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。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、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。

  FTD 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 （22 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 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。

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。

注意事項と制約事項

- ブリッジ グループを 1 つ追加できます。
- Firepower 2100 シリーズ または Firepower 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。
- すべての ASA 5506-X モデル、新バージョンの 6.2+ システム、または再イメージ化された 6.2+ システムの場合、デバイスは、**inside** という名前のブリッジ グループ BVI1 が事前に設定されています。このブリッジ グループには、**outside** インターフェイスを除くすべてのデータ インターフェイスが含まれています。そのため、デバイスにはインターネットやその他のアップストリーム ネットワークへの接続に使用される 1 つのポートが事前に設定されています。また、その他のポートはすべて有効になっていて、エンドポイントへの直接接続に使用できます。ISA 3000 モデルは、このデフォルトの構成も付属します。新しい

サブネットで内部インターフェイスを使用する場合は、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。

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、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）] をクリックして、[インターフェイス（Interfaces）] サマリー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。ブリッジ グループがすでに存在している場合、それはフォルダです。開く/閉じる矢印をクリックして、メンバー インターフェイスを表示します。メンバー インターフェイスは、リストに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。

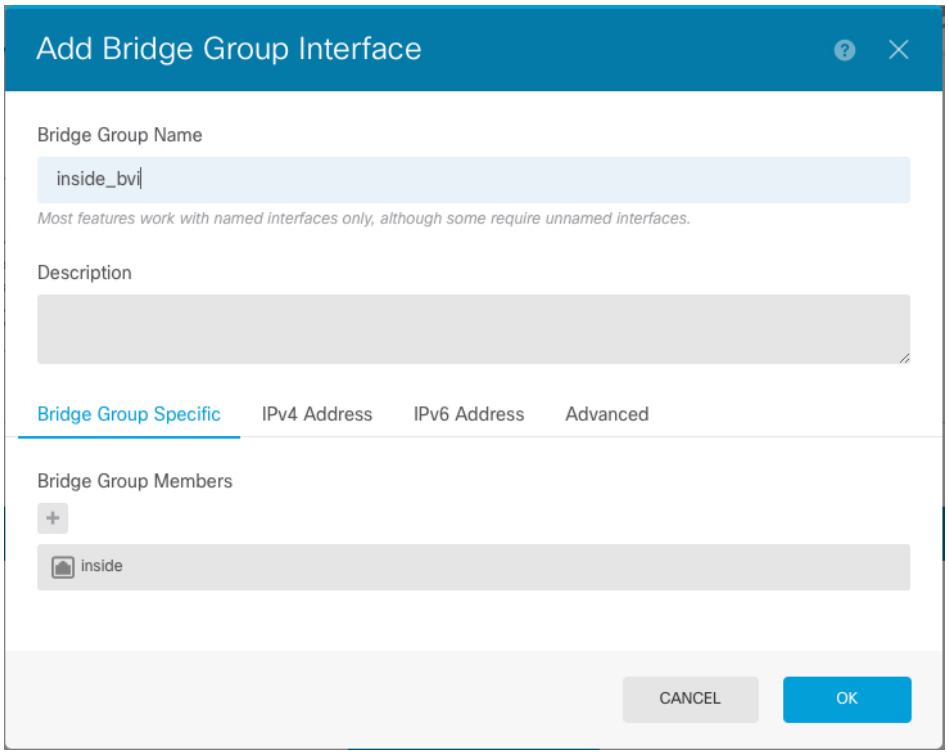
- BVI1 ブリッジ グループの編集アイコン（  ）をクリックします。
- 歯車のドロップダウン リストから [ブリッジグループインターフェイスの追加（Add Bridge Group Interface）] を選択して、新しいグループを作成します。

  （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 グループにそ

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 以下を設定します。



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との間における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 つまたは複数のインターフェイスをクリックして、[OK] をクリックします。

- インターフェイスの削除：インターフェイス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。ブリッジ グループが事前設定されたモデルでは、デフォルトの BVI1「inside」ネットワークは 192.168.1.1/24（例：255.255.255.0）です。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） 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）]：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 （4 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。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、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。

  FTD 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 （オプション）詳細オプションの設定 （22 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。

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。

注意事項と制約事項

- 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。
- 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。
- FTD 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バーンドイン MAC アドレスを使用するので、FTD で定義されたサブインターフェイスに一意の MAC アドレスを割り当てる必要の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、FTD 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。

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（Interface）] 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 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（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。

a) [親インターフェイス（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) [サブインターフェイス名（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) （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。

d) [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。

e) [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。

- [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） 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。

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、FTD 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 （4 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。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、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。

  FTD 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）詳細オプションの設定 （22 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。

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。

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。

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

Firepower 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） 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

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 FTD 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、9198 バイトまでの MTU を設定できます。Firepower Threat Defense Virtual の最大値は 9184 です。

（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 デバイスまたは Firepower Threat Defense Virtual 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。ジャンボ フレームのサポートが常に有効な場合、Firepower 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。ネットワーキングの問題を解決している場合にのみ、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。
- Firepower 2100 デバイス上の管理インターフェイスに、MTU、デュプレックス、または速度を設定することはできません。

手順

ステップ 1 [デバイス（Device）] をクリックしてから、[インターフェイス（Interface）] 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 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）] 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（Firepower Threat Defense Virtual の場合は 9184）の値を指定できます。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） ASA 5500-X シリーズ デバイス、ISA 3000 シリーズ デバイス、または Firepower 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。CLI にログインして **reboot** コマンドを使用します。ジャンボ フレームのサポートが常に有効な場合、Firepower モデルを再起動する必要はありません。

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。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るもののみです。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）] : [自動（Auto）]、[ハーフ（Half）]、[フル（Full）]、または [デフォルト（Default）] を選択します。 [自動（Auto）] は、インターフェイスによってサポートされる場合のみデフォルトとなります。たとえば、Firepower 2100 シリーズ デバイスの SFP インターフェイスでは [Auto] を選択できません。

  Firepower Device Manager が設定を試行できないことを示すために [Default] を選択します。既存の設定は、すべてそのまま変更されません。

- [速度（Speed）] : [自動（Auto）] を選択してインターフェイスに速度をネゴシエートさせるか（これがデフォルトです）、または特定の速度：[10]、[100]、[1000]、[10000] Mbps を選択します。 次の特別オプションも選択できます。

  - [ネゴシエートなし（No Negotiate）] : ファイバ インターフェイスの場合は、速度を 1000 Mbps に設定し、リンク パラメータをネゴシエートしません。これは、これらのインターフェイスのデフォルトの設定です。

  - [デフォルト（Default）] : Firepower Device Manager が設定を試行できないことを示します。いずれかが既存の設定のまま変更されていません。

  インターフェイスのタイプによって、選択可能なオプションが制限されます。たとえば、Firepower 2100 シリーズ デバイスの SFP+ インターフェイスは 1000（1 Gbps）および 10000

（10 Gpbs）のみをサポートし、SFP インターフェイスは 1000（1 Gbps）のみをサポートしますが、GigabitEthernet ポートは 10000（10 Gpbs）をサポートしません。その他のデバイス上の SPF インタ フェースでは [ネゴシエートなし（No Negotiate）] が必須の場合があります。インターフェイスのサポート対象については、ハードウェアのマニュアルを参照してください。

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

- [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 8 [OK] をクリックします。

Firepower Threat Defense Virtual へのインターフェイスの追加

FTDv を展開する際は、仮想マシンにインターフェイスを割り当てます。次に、FDM 内から、ハードウェア デバイスを設定する場合と同じ方法で、それらのインターフェイスを設定します。

ただし、仮想マシンにさらに仮想インターフェイスを追加して、FDM にそれらを自動的に認識させることはできません。FTDv と同等の物理インターフェイスを追加する必要がある場合は、基本的に初めからやり直す必要があります。新しい仮想マシンを導入することもできれば、次の手順を使用することもできます。

⚠

注意 仮想マシンにインターフェイスを追加する場合は、完全に FTDv 設定を消去する必要があります。設定でそのまま残しておける唯一の部分は、管理アドレスとゲートウェイ設定です。

始める前に

FDM で次の手順を実行します。

- FTDv 設定を調べ、新しい仮想マシンで複製する設定値を書き留めておきます。
- **[デバイス（Devices）] > [スマートライセンス（Smart License）] > [設定の表示（View Configuration）]** の順に選択し、すべての機能ライセンスを無効にします。

手順

ステップ 1 FTDvの電源を切ります。

ステップ 2 仮想マシン ソフトウェアを使用して、FTDv にインターフェイスを追加します。

VMware の場合、仮想アプライアンスはデフォルトで e1000（1 Gbit/s）インターフェイスを使用します。また、vmxnet3 または ixgbe（10 Gbit/s）インターフェイスを使用することもできます。

ステップ 3 FTDvの電源を入れます。

ステップ 4 FTDv コンソールを開いて、ローカルマネージャを削除し、その後、ローカルマネージャを有効にします。

ローカルマネージャを削除してから、それを有効にすると、デバイス設定がリセットされ、システムに新しいインターフェイスを認識させることができます。管理インターフェイス設定はリセットされません。次の SSH セッションはコマンドを表示します。

```
> show managers
Managed locally.

> configure manager delete

If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
DCHP Server Disabled

> show managers
No managers configured.

> configure manager local
>
```

ステップ 5 Firepower Device Manager へのブラウザ セッションを開き、デバイスのセットアップ ウィザードを完了して、デバイスを設定します。初期設定の完了を参照してください。

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 IP アドレス、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、メンバー情報と IP アドレスが含まれます。
- **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 サーバに関する情報が含まれます。

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。

- Firepower 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