



Firepower Threat Defense 用のトランスペアレントまたはルーテッド ファイアウォールモード

この章では、ファイアウォールモードをルーテッドまたはトランスペアレントに設定する方法と、各ファイアウォールモードでファイアウォールがどのように機能するかについて説明します。



(注) ファイアウォールモードは通常のファイアウォールインターフェイスにのみ影響を与えます。インラインセットやパッシブインターフェイスなどの IPS 専用インターフェイスには影響を与えません。IPS 専用インターフェイスは両方のファイアウォールモードで使用可能です。IPS 専用インターフェイスの詳細については、[IPS のみ対応のインターフェイスの設定](#)を参照してください。インラインセットは「トランスペアレント インラインセット」と呼ばれることもありますが、インラインインターフェイスタイプはこの章で説明するトランスペアレントファイアウォールモードおよびファイアウォールタイプのインターフェイスとは無関係です。

- [ファイアウォールモードについて \(1 ページ\)](#)
- [デフォルト設定 \(11 ページ\)](#)
- [ファイアウォールモードのガイドライン \(11 ページ\)](#)
- [ファイアウォールモードの設定 \(12 ページ\)](#)

ファイアウォールモードについて

Firepower Threat Defense デバイスは、通常のファイアウォールインターフェイスでルーテッドファイアウォールモードとトランスペアレントファイアウォールモードの2つのファイアウォールモードをサポートします。

ルーテッドファイアウォールモードについて

ルーテッドモードでは、/Firepower Threat Defense デバイスはネットワーク内のルータホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。

統合ルーティングおよびブリッジングにより、ネットワーク上の複数のインターフェイスをまとめた「ブリッジグループ」を使用できます。また、/Firepower Threat Defense デバイスはブリッジング技術を使用してインターフェイス間のトラフィックを通すことができます。各ブリッジグループには、ネットワーク上でIPアドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。/Firepower Threat Defense デバイスはBVIと通常のルーテッドインターフェイス間でルーティングを行います。クラスターリング、EtherChannel、冗長またはメンバーインターフェイスが必要ない場合は、トランスペアレントモードではなくルーテッドモードの使用を検討してください。ルーテッドモードでは、トランスペアレントモードと同様に1つ以上の分離されたブリッジグループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッドインターフェイスも含めることができます。

トランスペアレントファイアウォールモードについて

従来、ファイアウォールはルーテッドホップであり、保護されたサブネットのいずれかに接続するホストのデフォルトゲートウェイとして機能します。一方、トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。ただし、他のファイアウォールのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

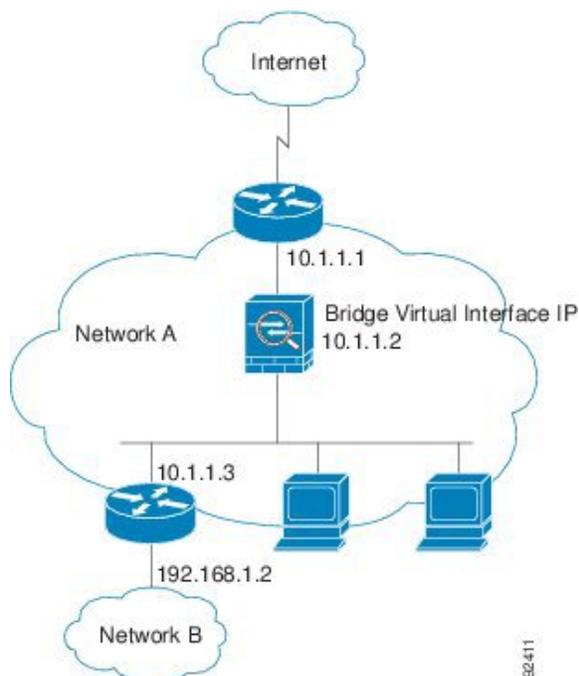
レイヤ2の接続は、ネットワーク上の内部、外部のインターフェイスをまとめた「ブリッジグループ」を使用して達成されます。また、/Firepower Threat Defense デバイスはブリッジング技術を使用してインターフェイス間のトラフィックを通します。各ブリッジグループには、ネットワーク上でIPアドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互通信できません。

ネットワークでのトランスペアレントファイアウォールの使用

/Firepower Threat Defense デバイスは、自身のインターフェイス間を同じネットワークで接続します。トランスペアレントファイアウォールはルーテッドホップではないので、既存のネットワークに簡単に導入できます。

次の図に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレントファイアウォールネットワークを示します。内部ルータと各ホストは、外部ルータに直接接続されているように見えます。

図 1: トランスペアレント ファイアウォール ネットワーク



/診断インターフェイス

各ブリッジ仮想インターフェイス（BVI）IPアドレスのほかに、別の /診断 スロット ポート インターフェイスを追加できます。このインターフェイスはどのブリッジグループにも属さず、/Firepower Threat Defense デバイス への管理トラフィックのみを許可します。

ルーテッド モード機能のためのトラフィックの通過

トランスペアレントファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、アクセスルールを使用することによって、（サポートされていない DHCP リレー機能の代わりに）DHCP トラフィックを許可したり、IP/TV で作成されるようなマルチキャストトラフィックを許可したりできます。また、トランスペアレントファイアウォールを通過するルーティングプロトコル隣接関係を確立することもできます。つまり、OSPF、RIP、EIGRP、または BGP トラフィックをアクセスルールに基づいて許可できます。同様に、HSRP や VRRP などのプロトコルは /Firepower Threat Defense デバイス を通過できます。

ブリッジグループについて

ブリッジグループは、/Firepower Threat Defense デバイス がルーティングではなくブリッジするインターフェイスのグループです。ブリッジグループはトランスペアレントファイアウォールモード、ルーテッドファイアウォールモードの両方でサポートされています。他のファイ

アウォールインターフェイスのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のチェックがすべて実施されます。

ブリッジ仮想インターフェイス (BVI)

各ブリッジグループには、ブリッジ仮想インターフェイス (BVI) が含まれます。/Firepower Threat Defense デバイスは、ブリッジグループから発信されるパケットの発信元アドレスとしてこの BVI IP アドレスを使用します。BVI IP アドレスはブリッジグループメンバーインターフェイスと同じサブネット上になければなりません。BVI では、セカンダリネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

トランスペアレントモード：インターフェイスベースの各機能はブリッジグループのメンバーインターフェイスだけを指定でき、これらについてのみ使用できます。

ルーテッドモード：BVI はブリッジグループと他のルーテッドインターフェイス間のゲートウェイとして機能します。ブリッジグループ/ルーテッドインターフェイス間でルーティングするには、BVI を指定する必要があります。一部のインターフェイスベース機能に代わり、BVI 自体が利用できます。

- DHCPv4 サーバ：BVI のみが DHCPv4 サーバの構成をサポートします。
- スタティックルート：BVI のスタティックルートを設定できます。メンバーインターフェイスのスタティックルートは設定できません。
- syslog サーバと /Firepower Threat Defense デバイス 由来の他のトラフィック：syslog サーバ（または SNMP サーバ、/Firepower Threat Defense デバイス からトラフィックが送信される他のサービス）を指定する際、BVI またはメンバーインターフェイスのいずれも指定できます。

ルーテッドモードで BVI を指定しない場合、/Firepower Threat Defense デバイスはブリッジグループのトラフィックをルーティングしません。この設定は、ブリッジグループのトランスペアレントファイアウォールモードを複製します。クラスタリング、EtherChannel、冗長またはメンバーインターフェイスが不要であれば、ルーテッドモードの使用を検討すべきです。ルーテッドモードでは、トランスペアレントモードと同様に1つ以上の分離されたブリッジグループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッドインターフェイスも含めることができます。

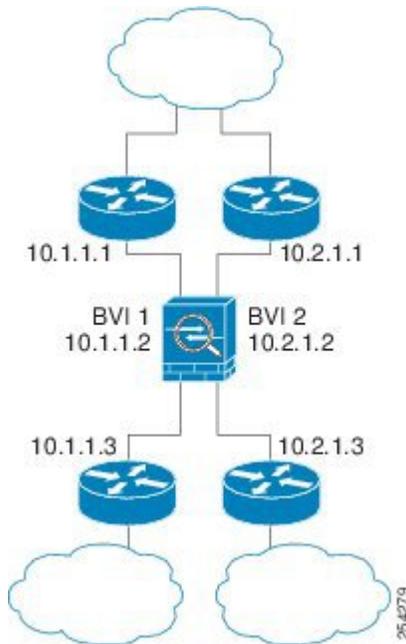
トランスペアレントファイアウォールモードのブリッジグループ

ブリッジグループのトラフィックは他のブリッジグループから隔離され、トラフィックは /Firepower Threat Defense デバイス 内の他のブリッジグループにはルーティングされません。また、トラフィックは外部ルータから /Firepower Threat Defense デバイス 内の別のブリッジグループにルーティングされる前に、/Firepower Threat Defense デバイス から出る必要があります。ブリッジング機能はブリッジグループごとに分かれています。その他の多くの機能はすべてのブリッジグループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジグループで共有されます。

1つのブリッジグループにつき複数のインターフェイスを入れることができます。サポートされるブリッジグループとインターフェイスの正確な数については、[ファイアウォールモードのガイドライン \(11 ページ\)](#) を参照してください。ブリッジグループごとに2つ以上のインターフェイスを使用する場合は、内部、外部への通信だけでなく、同一ネットワーク上の複数のセグメント間の通信を制御できます。たとえば、相互通信を希望しない内部セグメントが3つある場合、インターフェイスを別々のセグメントに置き、外部インターフェイスとのみ通信させることができます。または、インターフェイス間のアクセスルールをカスタマイズし、希望通りのアクセスを設定できます。

次の図に、2つのブリッジグループを持つ、Firepower Threat Defense デバイス に接続されている2つのネットワークを示します。

図 2: 2つのブリッジグループを持つトランスパレント ファイアウォール ネットワーク

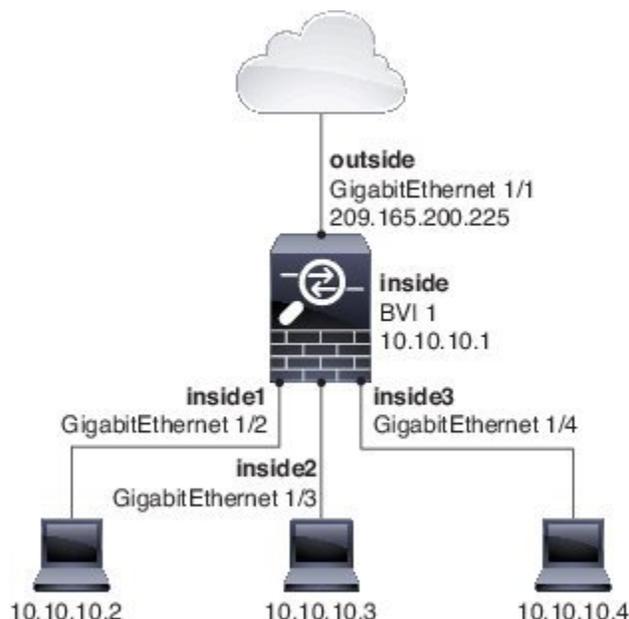


ルーテッド ファイアウォール モードのブリッジグループ

ブリッジグループトラフィックは他のブリッジグループまたはルーテッドインターフェイスにルーティングできます。ブリッジグループのBVIインターフェイスに名前を割り当てないことで、ブリッジグループのトラフィックを分離することもできます。BVIに名前を付けると、そのBVIはその他の通常のインターフェイスと同様にルーティングに参加します。

ルーテッドモードでブリッジグループを使用する方法として、外部スイッチの代わりにFirepower Threat Defense 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。たとえば、デバイスの中には、通常のインターフェイスとして外部インターフェイスを持ち、その他すべてのインターフェイスが内部ブリッジグループに割り当てられているというデフォルト設定のものがあります。このブリッジグループは外部スイッチを置き換えることを目的としているので、すべてのブリッジグループインターフェイスが自由に通信できるようにアクセスポリシーを設定する必要があります。

図 3: 内部ブリッジグループと外部ルーテッドインターフェイスを持つルーテッドファイアウォールネットワーク



レイヤ3トラフィックの許可

- ユニキャストのIPv4およびIPv6トラフィックがブリッジグループを通過するにはアクセスルールが必要です。
- ARPは、アクセスルールなしで両方向にブリッジグループを通過できます。ARPトラフィックは、ARPインスペクションによって制御できます。
- IPv6ネイバー探索およびルータ送信要求パケットは、アクセスルールを使用して通過させることができます。
- ブロードキャストおよびマルチキャストトラフィックは、アクセスルールを使用して通過させることができます。

許可されるMACアドレス

アクセスポリシーで許可されている場合、以下の宛先MACアドレスをブリッジグループで使用できます（[レイヤ3トラフィックの許可（6ページ）](#)を参照）。このリストにないMACアドレスはドロップされます。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ~ 0100.5EFE.FFFF までの IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ~ 3333.FFFF.FFFF までの IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD の BPDU マルチキャストアドレス

BPDU 処理

スパニング ツリー プロトコルの使用によるループを回避するため、BPDU はデフォルトで通過します。

MAC アドレスとルート ルックアップ

ブリッジ グループ内のトラフィックでは、パケットの発信インターフェイスは、ルート ルックアップではなく宛先 MAC アドレス ルックアップを実行することによって決定されます。

ただし、次の場合にはルート ルックアップが必要です。

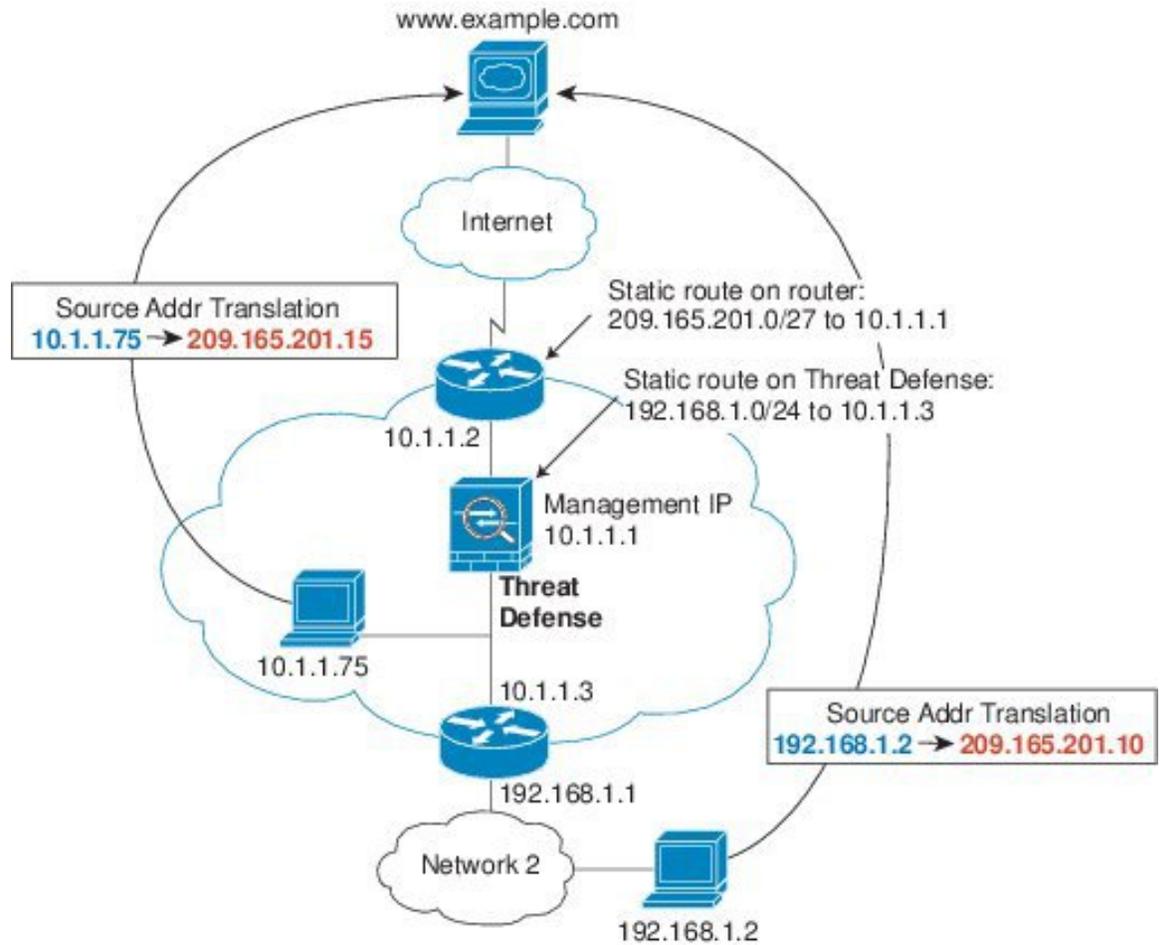
- トラフィックの発信元が /Firepower Threat Defense デバイス : syslog サーバなどがあるリモート ネットワーク宛てのトラフィック用に、/Firepower Threat Defense デバイス にデフォルト/スタティック ルートを追加します。
- Voice over IP (VoIP) および TFTP トラフィック、エンドポイントが 1 ホップ以上離れている : セカンダリ接続が成功するように、リモートエンドポイント宛てのトラフィック用に、/Firepower Threat Defense デバイス にスタティック ルートを追加します。/Firepower Threat Defense デバイスは、セカンダリ接続を許可するためにアクセス コントロール ポリシーに一時的な「ピンホール」を作成します。セカンダリ接続ではプライマリ接続とは異なる IP アドレスのセットが使用される可能性があるため、/Firepower Threat Defense デバイスは正しいインターフェイスにピンホールをインストールするために、ルート ルックアップを実行する必要があります。

影響を受けるアプリケーションは次のとおりです。

- H.323
- RTSP
- SIP
- Skinny (SCCP)
- SQL*Net
- SunRPC
- TFTP
- /Firepower Threat Defense デバイスが NAT を実行する 1 ホップ以上離れたトラフィック : リモート ネットワーク宛てのトラフィック用に、/Firepower Threat Defense デバイス にスタティック ルートを設定します。また、/Firepower Threat Defense デバイス に送信されるマッピングアドレス宛てのトラフィック用に、上流に位置するルータにもスタティック ルートが必要です。

このルーティング要件は、NAT が有効になっている VoIP と DNS の、1 ホップ以上離れている組み込み IP アドレスにも適用されます。/Firepower Threat Defense デバイスは、変換を実行できるように正しい出カインターフェイスを識別する必要があります。

図 4: NAT の例 : ブリッジグループ内の NAT



トランスパレントモードのブリッジグループのサポートされていない機能

次の表に、トランスパレントモードのブリッジグループでサポートされない機能を示します。

表 1: トランスパレントモードでサポートされない機能

機能	説明
ダイナミック DNS	-

機能	説明
DHCP リレー	トランスペアレント ファイアウォールは DHCPv4 サーバとして機能することができますが、DHCP リレーはサポートしません。2つのアクセスルール（1つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう1つはサーバからの応答を逆方向に許可します。）を使用して DHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。
ダイナミック ルーティング プロトコル	ただし、ブリッジグループメンバーインターフェイスの場合、/Firepower Threat Defense デバイスで発信されたトラフィックにスタティックルートを追加できます。アクセスルールを使用して、ダイナミックルーティングプロトコルが /Firepower Threat Defense デバイスを通過できるようにすることもできます。
マルチキャスト IP ルーティング	アクセスルールで許可することによって、マルチキャストトラフィックが /Firepower Threat Defense デバイスを通過できるようにすることができます。
QoS	□
通過トラフィック用の VPN 終端	トランスペアレント ファイアウォールは、ブリッジグループメンバーインターフェイスでのみ、管理接続用のサイト間 VPN トンネルをサポートします。これは、/Firepower Threat Defense デバイスを通過するトラフィックに対して VPN 接続を終端しません。アクセスルールを使用して VPN トラフィックに ASA を通過させることはできますが、非管理接続は終端されません。

ルーテッドモードのブリッジグループのサポートされていない機能

次の表に、ルーテッドモードのブリッジグループでサポートされない機能を示します。

表 2:ルーテッドモードでサポートされない機能

機能	説明
EtherChannel メンバー インターフェイス	物理インターフェイス、冗長インターフェイス、およびサブインターフェイスのみがブリッジグループメンバーインターフェイスとしてサポートされます。 診断インターフェイスもサポートされません。
クラスタリング	ブリッジグループはクラスタリングでサポートされません。
ダイナミック DNS	-
DHCP リレー	ルーテッドファイアウォールは DHCPv4 サーバとして機能することができますが、DHCP リレーを BVI またはブリッジグループメンバーインターフェイスでサポートしません。
ダイナミック ルーティング プロトコル	ただし、BVI のスタティック ルートを追加することはできます。アクセスルールを使用して、ダイナミックルーティングプロトコルが /Firepower Threat Defense デバイス を通過できるようにすることもできます。非ブリッジグループ インターフェイスは、ダイナミックルーティングをサポートします。
マルチキャスト IP ルーティング	アクセスルールで許可することによって、マルチキャストトラフィックが /Firepower Threat Defense デバイス を通過できるようにすることができます。非ブリッジグループ インターフェイスは、マルチキャストルーティングをサポートします。
QoS	非ブリッジグループ インターフェイスは、QoS をサポートします。

機能	説明
通過トラフィック用の VPN 終端	<p>VPN 接続を BVI で終端することはできません。非ブリッジ グループ インターフェイスは、VPN をサポートします。</p> <p>ブリッジグループメンバーインターフェイスは、管理接続専用のサイト間 VPN トンネルをサポートします。これは、/Firepower Threat Defense デバイス を通過するトラフィックに対して VPN 接続を終端しません。アクセスルールを使用して VPN トラフィックにブリッジグループを通過させることはできますが、非管理接続は終端されません。</p>

デフォルト設定

ブリッジグループのデフォルト

デフォルトでは、すべての ARP パケットはブリッジグループ内で渡されます。

ファイアウォール モードのガイドライン

モデルのガイドライン

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

ブリッジグループのガイドライン（トランスペアレントおよびルーテッドモード）

- 64 のインターフェイスをもつブリッジグループを 250 まで作成できます。
- 直接接続された各ネットワークは同じサブネット上に置かれている必要があります。
- /Firepower Threat Defense デバイス では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

- IPv4 の場合は、管理トラフィックと、/Firepower Threat Defense デバイス を通過するトラフィックの両方の各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv6 アドレスは BVI でサポートされますが必須ではありません。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホストサブネット (255.255.255.255) を設定することはできません。
- 管理インターフェイスはブリッジグループのメンバーとしてサポートされません。
- トランスペアレントモードでは、少なくとも1つのブリッジグループを使用し、データインターフェイスがブリッジグループに属している必要があります。
- トランスペアレントモードでは、接続されたデバイス用のデフォルトゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは /Firepower Threat Defense デバイスの反対側にあるルータをデフォルトゲートウェイとして指定する必要があります。
- トランスペアレントモードでは、管理トラフィックの戻りパスを指定するために必要なデフォルトルートは、1つのブリッジグループネットワークからの管理トラフィックにだけ適用されます。これは、デフォルトルートはブリッジグループのインターフェイスとブリッジグループネットワークのルータ IP アドレスを指定しますが、ユーザは1つのデフォルトルートしか定義できないためです。複数のブリッジグループネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティックルートを指定する必要があります。
- トランスペアレントモードでは、PPPoE は /診断インターフェイスとしてサポートされません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッドモードでは、EtherChannel インターフェイスがブリッジグループのメンバーとしてサポートされません。

ファイアウォールモードの設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Access Admin Administrator Network Admin

ファイアウォールモードは、最初のシステムセットアップの実行時に CLI で設定できます。セットアップ時にファイアウォールモードを設定することをお勧めします。これは、ファイアウォールモードを変更すると、非適合の設定が発生しないように設定が消去されるためです。

ファイアウォール モードの変更が後で必要になった場合は、CLI から変更する必要があります。

手順

ステップ 1 Management Center から Firepower Threat Defense デバイスの登録を解除します。

モードの変更は、デバイスの登録を解除するまで実行できません。

- [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
- 管理対象デバイスのリストから、デバイスを選択します。
- デバイスを削除 (ゴミ箱アイコンをクリック) して、確認してから、システムがデバイスを削除するまで待機します。

ステップ 2 Firepower Threat Defense デバイスの CLI にアクセスします。可能ならばコンソールポートからアクセスします。

診断インターフェイスへの SSH を使用している場合、モードを変更すると、インターフェイスの設定が消去され、切断されます。代わりに、管理インターフェイスに接続する必要があります。

ステップ 3 ファイアウォール モードを変更します。

configure firewall [routed | transparent]

例 :

```
> configure firewall transparent
This will destroy the current interface configurations, are you sure that you want to
proceed? [y/N] y
The firewall mode was changed successfully.
```

ステップ 4 Management Center に再登録します。

configure manager add {hostname | ip_address | DONTRESOLVE} reg_key [nat_id]

引数の説明

- {hostname | ip_address | DONTRESOLVE } は、Management Center の完全修飾ホスト名または IP アドレスのいずれかを指定します。Management Center を直接アドレス指定できない場合は、DONTRESOLVE を使用します。
- reg_key は、デバイスを Management Center に登録するために必要な一意の英数字による登録キーです。
- nat_id は、Management Center とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。これは、ホスト名が DONTRESOLVE に設定されている場合に必要です。

