



# 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、ファイアウォールが各ファイアウォールモードで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のみに影響し、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しません。IPS専用インターフェイスはどちらのファイアウォールモードでも使用できます。IPS専用インターフェイスの詳細については、[Firepower Threat Defense のインラインセットとパッシブインターフェイス](#)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 \(13 ページ\)](#)

## 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。そして、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。これに対し、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」のように動作するレイヤ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。

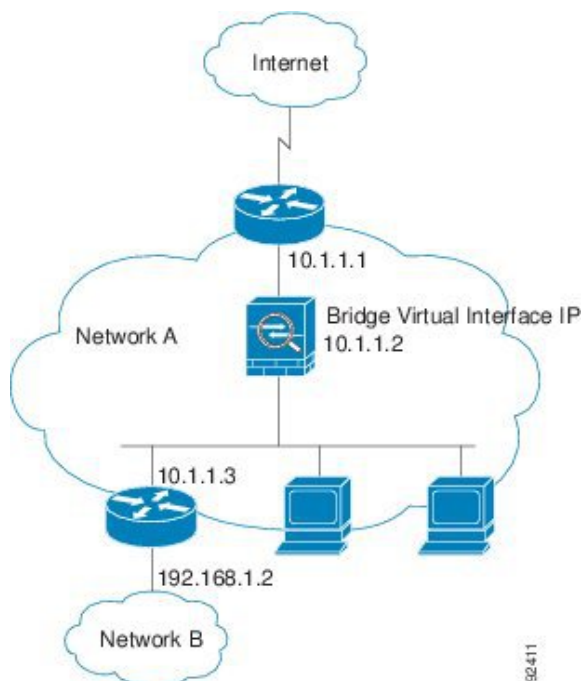
レイヤ2の接続は、ネットワークの内部と外部のインターフェイスをまとめた「ブリッジグループ」を使用して実現されます。また、Firepower Threat Defense デバイスはブリッジング技術を使用してインターフェイス間のトラフィックを通すことができます。各ブリッジグループには、ネットワーク上でIPアドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互通信できません。

## ネットワーク内で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ィングされたホップではないため、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 (Interface)]

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すべてのチェックが実施されます。

## 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送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かも指定できます。

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。

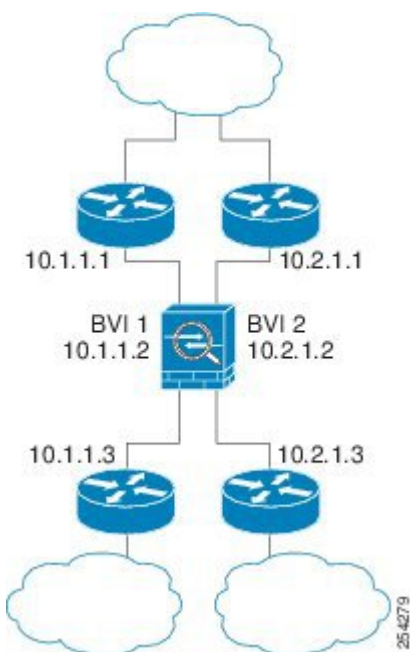
## トランスペアレントファイアウォールモードのブリッジグループ

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 デバイス内の他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

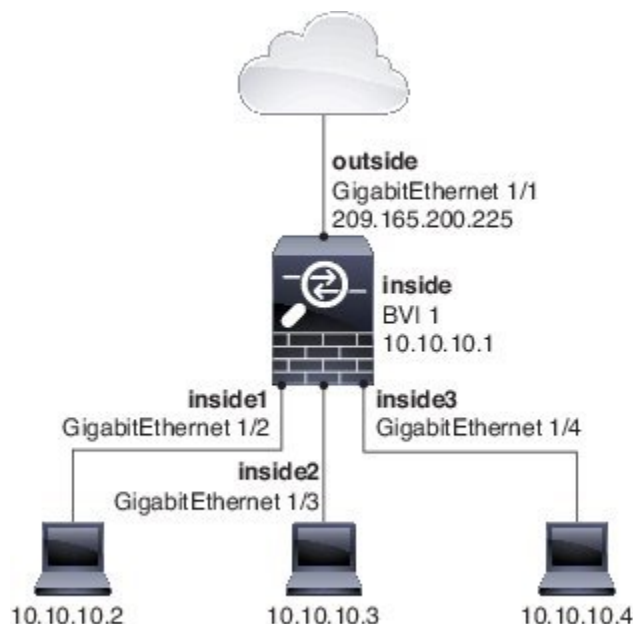


## ルーテッド ファイアウォール モードのブリッジグループ

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でおくことで、ブリッジグループトラフィックを分離できます。BVIの名前を指定すると、このBVIは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 追加のインターフェイスを使用する方法があります。たとえば、一部のデバイスのデフォルト設定では、外部インターフェイスが通常のインターフェイスとして含まれており、その他の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ため、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からなる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 の処理

スパニングツリープロトコルを使用するときのループを防止するために、デフォルトでBPDUが渡されます。

デフォルトでは、BPDUは高度なインスペクションにも転送されます。このインスペクションは、このタイプのパケットには必要なく、インスペクションの再起動によってブロックされた場合など、問題を引き起こす可能性があります。BPDUは高度なインスペクションから常に除外することをお勧めします。これを行うには、FlexConfigを使用してBPDUを信頼するEtherType ACLを設定し、各メンバーインターフェイス上の高度な検査からBPDUを除外します。[Firepower Threat Defense の FlexConfig ポリシー](#)を参照してください。

FlexConfig オブジェクトは次のコマンドを展開する必要があります。ここで、<if-name> はインターフェイス名に置き換えます。必要な数の `access-group` コマンドを追加して、デバイス上の各ブリッジグループのメンバー インターフェイスをカバーします。また、ACL に別の名前を選択することもできます。

```
access-list permit-bpdu ethertype trust bpdu
access-group permit-bpdu in interface <if-name>
```

## 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。

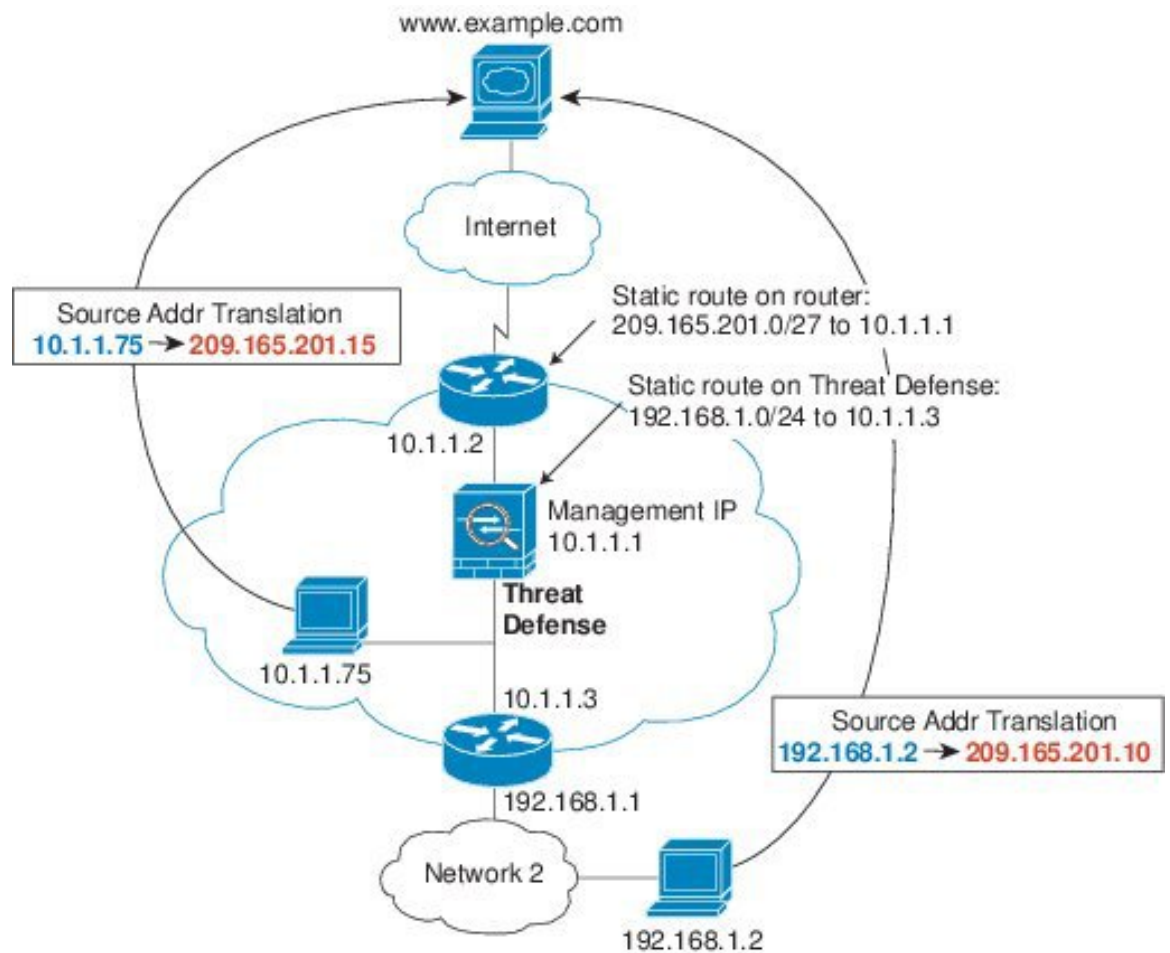
影響を受けるアプリケーションは次のとおりです。

- 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스에 스태ティックルートを設定します。また、Firepower Threat Defense デバイ스에 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 스태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力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



## トランスペア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、トランスペア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: トランスペアレント 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	-
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 コマンドはサポートしません。2つのアクセスルールを使用して 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。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。
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 ターミネーション	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てい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ていない機能

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ていません。
クラスタ	クラスタリングではブリッジグループは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 サーバとして機能しますが、BVI またはブリッジグループメンバーインターフェイス上でのDHCP リレーはサポートしません。
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ターミネーション	<p>BVI で VPN 接続を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、管理接続についてのみ、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一のサブネット上にある必要があります。
- 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。
- Firepower 4100/9300 では、データ共有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 デバイスの他方側の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 *default* 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で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、FTD 定義の 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。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。
- Bidirectional Forwarding Detection (BFD) エコーパケットは、ブリッジグループメンバーを使用するときに、FTD を介して許可されません。BFD を実行している FTD の両側に2つのネイバーがある場合、FTD 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。

## 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数	サポートされるドメイン数	アクセス
いずれか (Any)	該当なし	FTD	いずれか (Any)	Admin Access Admin 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。

**ステップ 1** FMC から FTD 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** FTD 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** FMC 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、FMC 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。FMC 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 FMC へ登録するのに必要な英数字の一意の登録キーです。

- *nat\_id* は、FMC 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。
-