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

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。

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。

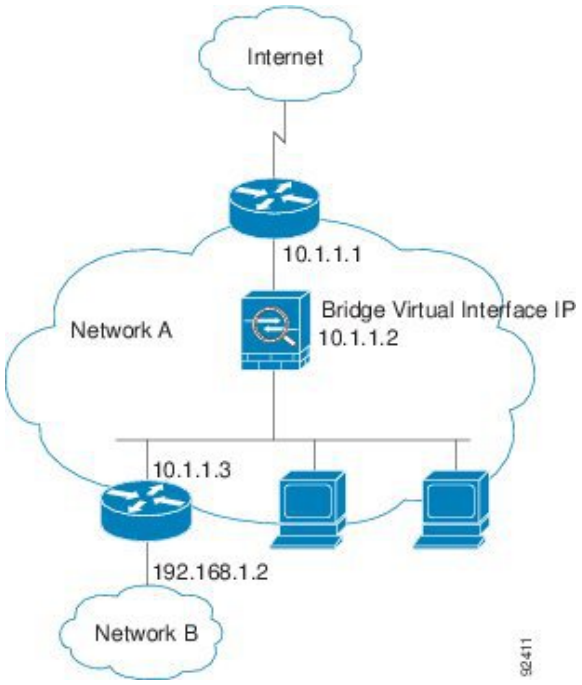
レイヤ2の接続は、ネットワーク上の内部、外部のインターフェイスをまとめた「ブリッジグループ」を使用して達成されます。また、Firepower Threat Defense デバイス はブリッジング技術を使用してインターフェイス間のトラフィックを通します。各ブリッジグループには、ネットワーク上でIPアドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレント モードでは、これらのブリッジグループは相互通信できません。

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



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 モードでのみ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。

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。

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

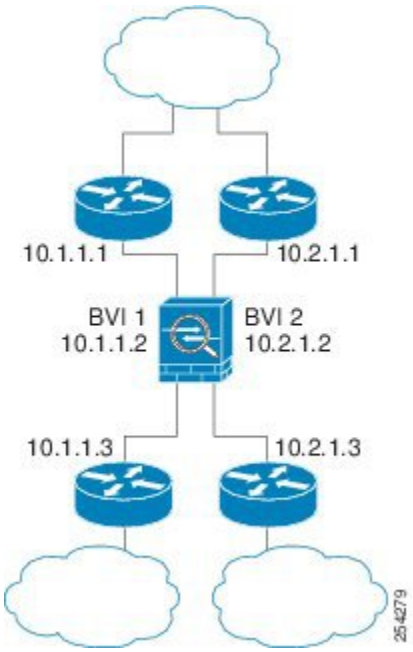
ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは Firepower Threat Defense デバイス 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから Firepower Threat Defense デバイス 内の別のブリッジ グループにルーティングされる前に、Firepower Threat Defense デバイス から出る必要があります。ブ

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が、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 （8 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。

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ル 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 （4 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。

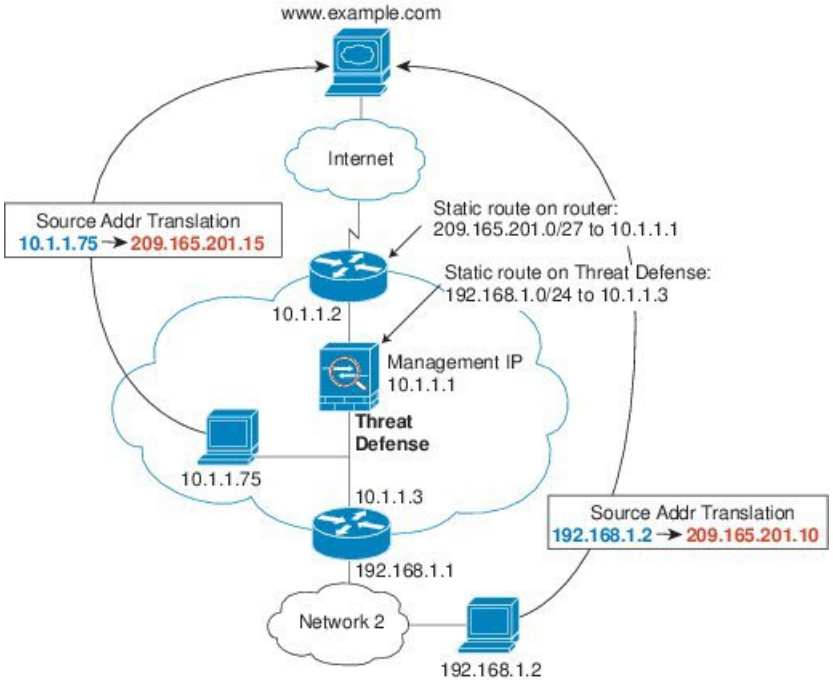
MAC アドレスとルート ルックアップ

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、次のトラフィック タイプにはルート ルックアップが必要です。

- Firepower Threat Defense デバイス で発信されたトラフィック：たとえば、syslog サーバがリモート ネットワークにある場合は、Firepower Threat Defense デバイス がそのサブネットに到達できるようにデフォルト/スタティック ルートを使用する必要があります。
- Firepower Threat Defense デバイス から少なくとも 1 ホップ離れており、Firepower Threat Defense デバイス が NAT を実行するトラフィック：Firepower Threat Defense デバイス がブリッジ グループ インターフェイスに入ったパケットに対して NAT を実行し、そのパケットがリモート ネットワークからのものだった場合、そのネットワークの Firepower Threat Defense デバイス のスタティック ルートを設定する必要があります。

図 *3 : NAT* の例：ブリッジ グループ内の *NAT*



1. 内部ホスト 10.1.1.75 が Web サーバにパケットを送信すると、パケットの実際の送信元アドレス 10.1.1.75 はマッピング アドレス 209.165.201.15 に変更されます。
2. サーバが応答すると、マッピング アドレス 209.165.201.15 に応答を送信し、Firepower Threat Defense デバイスがそのパケットを受信します。これは、アップストリーム ルータには、Firepower Threat Defense デバイス の管理 IP アドレスに転送されるスタティック ルートのこのマッピング ネットワークが含まれるためです。
3. その後、Firepower Threat Defense デバイス はマッピング アドレス 209.165.201.15 を変換して実際のアドレス 10.1.1.1.75 に戻します。実際のアドレスは直接接続されているため、Firepower Threat Defense デバイス はそのアドレスを直接ホストに送信します。
4. ホスト 192.168.1.2 の場合も、リターン トラフィックを除き、同じプロセスが発生します。Firepower Threat Defense デバイス はルーティング テーブルでルートを検索し、192.168.1.0/24 の Firepower Threat Defense デバイス スタティック ルートに基づいてパケットを 10.1.1.3 にあるダウンストリーム ルータに送信します。

- エンドポイントが Firepower Threat Defense デバイス から少なくとも 1 ホップ離れている Voice over IP（VoIP）と DNS トラフィック：たとえば、あるブリッジグループ メンバー インターフェイスに CCM があり、別のブリッジグループ メンバー インターフェイスにルータと H.323 ゲートウェイがある場合、H.323 ゲートウェイであるルータの正常なコール完了のために、Firepower Threat Defense デバイスにスタティック ルートを追加する必要があります。検査されるトラフィックに対して NAT を有効化すると、スタティック ルートは、パケットに埋め込まれている本当のホストアドレスの出力インターフェイスを決定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。

- DNS
- H.323
- RTSP
- SIP
- Skinny（SCCP）
- SunRPC
- TFTP

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	□

機能	説明
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。

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、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 モード）

- 4 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。

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。

a) **[デバイス（Devices）] > [デバイス管理（Device Management）]** を選択します。
b) 管理対象デバイスのリストから、デバイスを選択します。
c) 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。