



トランスペアレントファイアウォールモード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。オ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、[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。オンラインセットは「トランスペアレントオンラインセット」と呼ばれることがあります、オ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。

注意

- FTD CLI コマンドを使用して「ファイアウォールモード」を設定します。

- [ファイアウォールモードについて \(2 ページ\)](#)
- [デフォルト設定 \(10 ページ\)](#)
- [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

ファイアウォール モードについて

Firewall Threat Defense 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、Firewall 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、Firewall 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。Firewall 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、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。

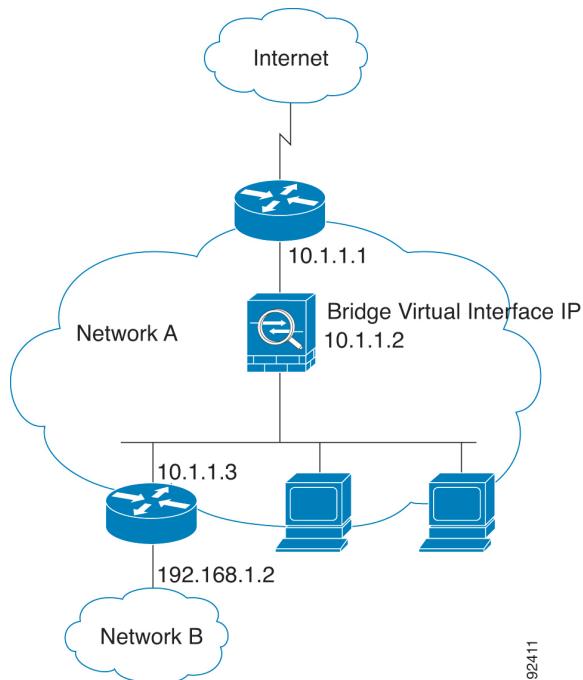
レイヤ2 の接続は、ネットワーク上の内部と外部のインターフェイスをまとめた「ブリッジグループ」を使用して確立されます。また、Firewall Threat Defense デバイスはブリッジング技術を使用してインターフェイス間のトラフィックを通します。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス (BVI) が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレント モードでは、これらのブリッジグループは相互通信できません。

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

Firewall 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



92411

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 Firewall 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、Firewall 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。Firewall 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。BVIIP 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 サーバーと Firewall Threat Defense デバイス 由来の他の他のトラフィック：syslog サーバー（または SNMP サーバー、Firewall 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、Firewall 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、または EtherChannel 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

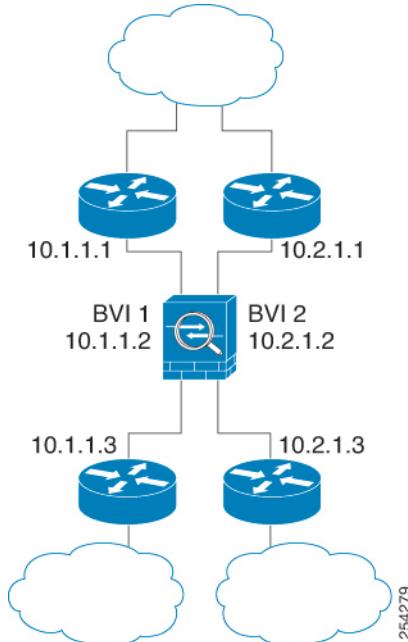
ブリッジグループのトラフィックは他のブリッジグループから隔離され、トラフィックは Firewall Threat Defense デバイス 内の他のブリッジグループにはルーティングされません。また、トラフィックは外部ルータから Firewall Threat Defense デバイス 内の他のブリッジグループにルーティングされる前に、Firewall Threat Defense デバイス から出る必要があります。ブリッジング機能はブリッジグループごとに分かれていますが、その他の多くの機能はすべてのブリッジグループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、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 \(11 ページ\)](#) 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、Firewall 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



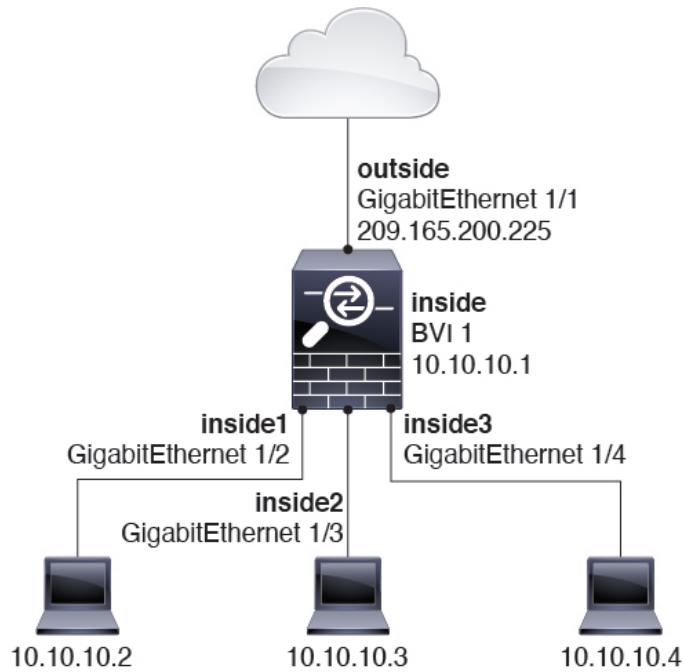
ルーテッド ファイアウォール モードのブリッジグループ

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Firewall Threat Defense 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、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。

レイヤ3 トラフィックの許可

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 の IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ~ 3333.FFFF.FFFF の IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD に等しい 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。

[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 Firewall Threat Defense デバイス：syslog サーバー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、Firewall 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、Firewall Threat Defense デバイスにスタティック ルートを追加します。Firewall 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、Firewall 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。

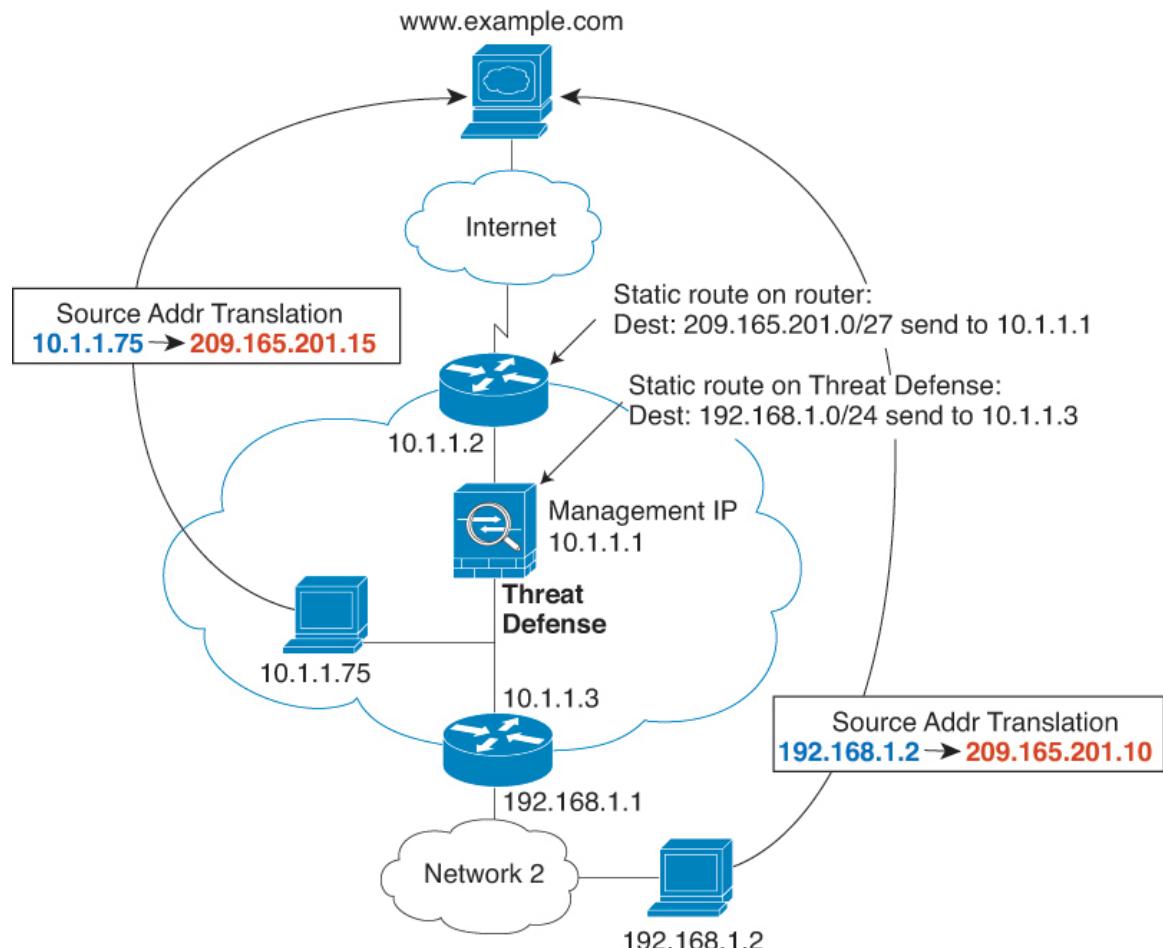
- H.323
- RTSP
- SIP
- Skinny (SCCP)
- SQL*Net

■ 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

- SunRPC
- TFTP
- Firewall 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、Firewall Threat Defense デバイスに static ルートを設定します。また、Firewall 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 static 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。Firewall 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

特長	説明
ダイナミック DNS	-
DHCPv6 ステートレス サーバ	ブリッジ グループ メンバー インターフェイスでは、DHCPv4 サーバのみがサポートされます。
DHCP リレー	トランスペアレント ファイアウォールは DHCPv4 サーバー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 つはサーバー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ますので、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、Firewall Threat Defense デバイスで発信されたトラフィックにスタイル 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 Firewall 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 Firewall 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、Firewall 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

特長	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。 Diagnostic インターフェイスもサポートされていません。

■ デフォルト設定

特長	説明
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	-
DHCPv6 ステートレス サーバ	DHCPv4 サーバーのみが BVI でサポートされます。
DHCP リレー	ルーテッド ファイアウォールは DHCPv4 サーバー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 のステティック 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 Firewall 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 Firewall 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。
通過 トラフィック用の VPN 終端	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。 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、Firewall 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。

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

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。
- Firewall 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。
- デバイスとデバイス間の管理トラフィック、および Firewall Threat Defense デバイス を通過するデータトラフィック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。IPv4 トラフィックの場合は、IPv4 アドレスを指定します。IPv6 トラフィックの場合は、IPv6 アドレスを指定します。
- 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。
- マルチインスタンスマードの場合、共有インターフェイスはブリッジグループ メンバーインターフェイス（トランスペアレントモードまたはルーテッドモード）ではサポートされません。
- ブリッジされた ixgbevf インターフェイスを備えた VMware の Firewall Threat Defense Virtual の場合、トランスペアレントモードはサポートされておらず、ブリッジグループはルーテッドモードではサポートされていません。
- 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 1010 では、同じブリッジグループ内に論理 VLAN インターフェイスと物理ファイアウォールインターフェイスを混在させることはできません。
- 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 Firewall Threat Defense 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

■ ファイアウォール モードの設定

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 Diagnostic インターフェイスでサポートされません。
- 透過モードは、Amazon Web Services、Microsoft Azure、Google Cloud Platform、および Oracle Cloud Infrastructure にデプロイされた脅威防御仮想インスタンスではサポートされていません。
- 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、Firewall Threat Defense 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 メンバを使用するときに、Firewall Threat Defense を介して許可されません。BFD を実行している Firewall Threat Defense の両側に 2 つのネイバーがある場合、Firewall Threat Defense 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

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 Firewall Management Center から Firewall Threat Defense デバイスを登録解除します。

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)] の順に選択します。
- b) 登録を解除するデバイスの横にある[その他 (More)] (⊕) をクリックし、[削除 (Delete)] をクリックします。

ステップ 2 Firewall 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 Firewall Management Center に再登録します。[CLI を使用した Firewall Threat Defense 初期設定の実行の完了](#)および[デバイスの追加](#)を参照してください。

■ ファイアウォール モードの設定

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。