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。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、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。

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 （10 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

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、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、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。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。

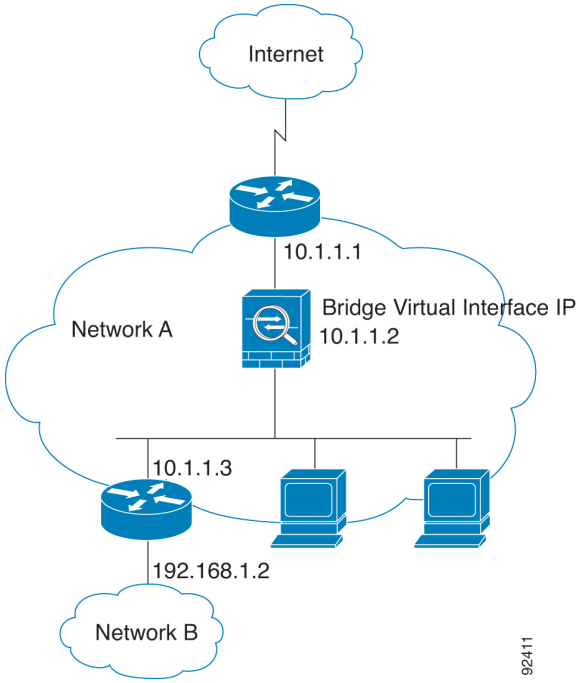
レイヤ2の接続は、ネットワーク上の内部と外部のインターフェイスをまとめた「ブリッジグループ」を使用して確立されます。また、Threat Defense デバイス はブリッジング技術を使用してインターフェイス間のトラフィックを通します。各ブリッジグループには、ネットワーク上でIPアドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互通信できません。

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

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



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

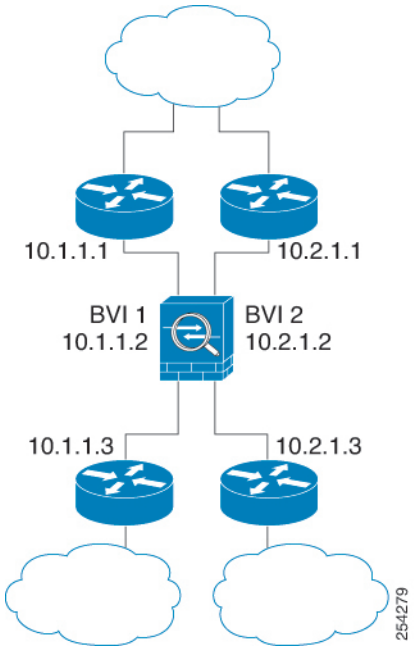
ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは Threat Defense デバイス 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから Threat Defense デバイス 内の他のブリッジ グループにルーティングされる前に、Threat Defense デバイス から出る必要があります。ブリッジング機能はブリッジグループごとに分かれていますが、その他の多くの機能はすべてのブリッジグループ間で共有されます。たとえば、syslog サーバーまたは AAA サーバーの設定は、すべてのブリッジグループで共有されます。

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（10 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、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

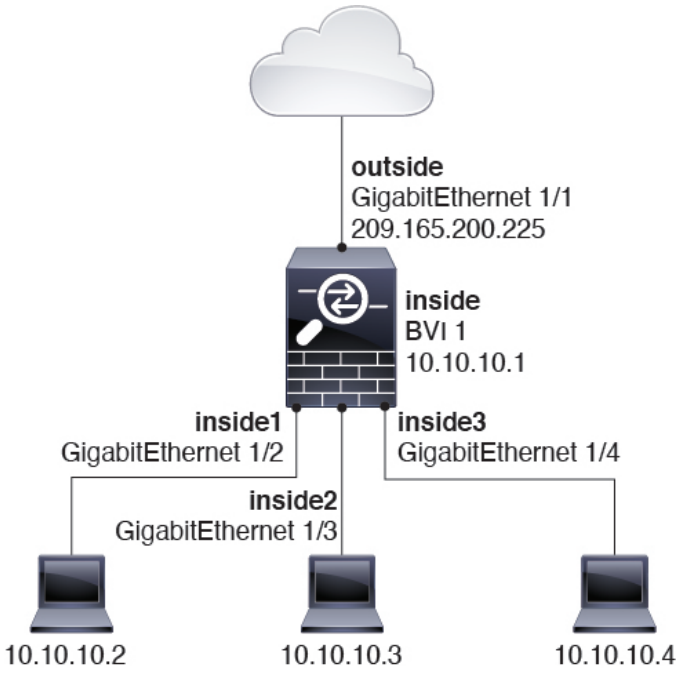


ルーテッド ファイアウォール モードのブリッジグループ

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 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。

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 ファイアウオール 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 （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。#unique_170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、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、Threat Defenseデバイス にスタティック ルートを追加します。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、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。

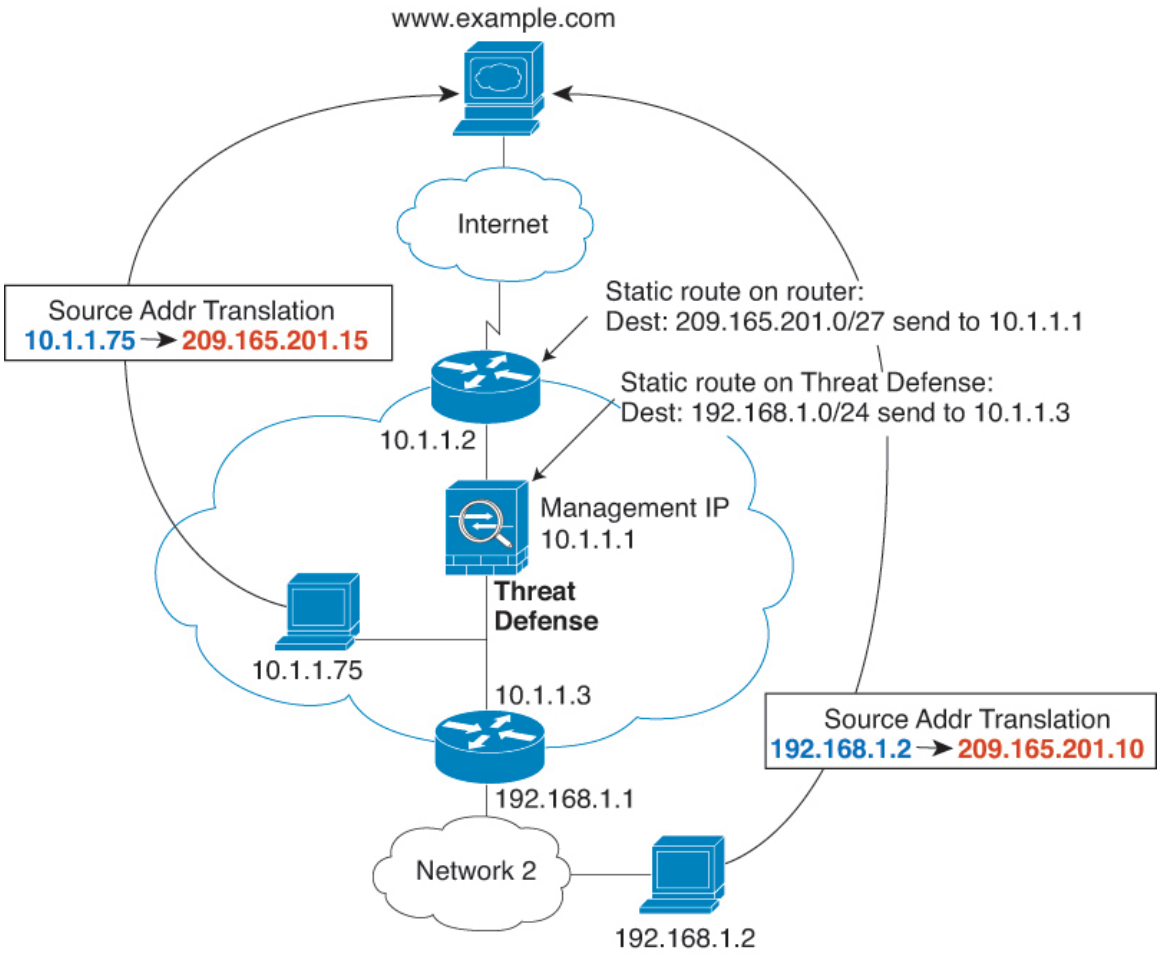
  - H.323
  - RTSP
  - SIP
  - Skinny（SCCP）
  - SQL*Net
  - SunRPC

- TFTP

- 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、Threat Defense デバイス にスタティック ルートを設定します。また、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。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、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 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 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、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。 Management インターフェイスもサポートされていません。
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。

機能	説明
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 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 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、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。

- 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 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モードの場合、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 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 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。
- 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、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、Threat Defense を介して許可されません。BFD を実行している Threat Defense の両側に 2 つのネイバーがある場合、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 Management Center から 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**（⋮） をクリックし、[削除（Delete）] をクリックします。

ステップ 2 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。

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。CLI を使用した Threat Defense 初期設定の実行の完了および登録キーを使用した Management Center へのデバイスの追加を参照してください。

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。