レイヤ 2 トランスペアレント ファイアウォール

レイヤ2 トランスペアレント ファイアウォールは、ブリッジされたパケットに対して動作し、ローカル スイッチド イーサネット ポートのペアで有効になります。これらのポート経由で転送される埋め込み IP パケットは、ルーティング ネットワーク内の通常の IP パケットと同様に検査されます。トランスペアレント ファイアウォール設定では、ゾーンベース ファイアウォールまたはレイヤ 3 ファイアウォール設定をレイヤ 2 インターフェイスに適用できます。

このモジュールでは、レイヤ 2 トランスペアレント ファイアウォール機能の概要を紹介します。

レイヤ 2 トランスペアレント ファイアウォールのサポートに関する制約事項

- アドレス解決プロトコル（ARP）インスペクションはサポートされていません。
- ブリッジ ドメイン、ブリッジ ドメイン インターフェイス（BDI）、オーバーレイ トランスポート仮想化（OTV）、X-Connect、仮想プライベート LAN サービス（VPLS）、VxLAN、非 IP フローといったレイヤ 2 フォワーディング テクノロジーはサポートされません。
- イーサネット フレームでは、通常の IP または単純な VLAN のみがサポートされています。トランスペアレント ファイアウォールは TCP リセット（RST）パケットを生成し、これらのパケットをサポートされているイーサネット フレームで送信します。

- TCP RST はボックス内高可用性スイッチオーバーの後ではサポートされません。
- 仮想 TCP（vTCP）はサポートされません。
- ネットワーク アドレス変換（NAT）、ボックスツーボックス（B2B）高可用性、マルチプロトコル ラベル スイッチング（MPLS）、仮想ルーティングおよび転送（VRF）インスタンス、VRF 対応ソフトウェア インフラストラクチャ（VASI）、Locator-ID Separation Protocol（LISP）はレイヤ 2 スイッチ パスではサポートされません。
- イーサネット運用管理および保守（OAM）、接続障害管理（CFM）といった非 IP パケット フローはサポートされません。
- トランスペアレント ファイアウォール クラス マップでは、レイヤ 2 ベースのアクセス コントロール リスト（ACL）はサポートされません。

レイヤ 2 トランスペアレント ファイアウォールについて

レイヤ 2 トランスペアレント ファイアウォールのサポート

従来のゾーンベース ファイアウォールは、ネットワーク内でレイヤ3ノードのように機能し、ノードをパス スルーする IP トラフィックを検査します。従来の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。ただし、このレイヤ3ファイアウォールを既存のネットワークに配置するには、ネットワークを再びサブネット化しなければならないため、多くの時間とリソースが必要です。レイヤ2トランスペアレントファイアウォールはネットワークに対して透過的であり、セグメント間でレイヤ3の分離は必要ありません。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」のように動作し、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。トランスペアレント ファイアウォールはルーティング対象のホップではないので、既存のネットワークに容易に導入できます。IP再アドレッシングは不要です。トランスペアレントファイアウォールはブリッジされたパケットに対して動作し、レイヤ3ファイアウォールはルーティングされるパケットに対して動作します。

トランスペアレントファイアウォールは、ローカル スイッチド イーサネット ポートのペアで有効になります。これらのポート経由で転送される埋め込みIPパケットは、ルーティング ネットワーク内の通常の IP パケットと同様に検査されます。トランスペアレント ファイアウォールが検査するのは IP パケットのみです。

トランスペアレント ファイアウォール セッションは、5 タプル情報（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、プロトコル）が格納された IP レイヤ 3 およびレイヤ4ヘッダーを使用して作成されます。トランスペアレントファイアウォールはレイヤ2プロトコルとしてイーサネットのみをサポートし、IPv4アドレスとIPv6アドレスの両方をサポートします。

トランスペアレント ファイアウォール設定では、ゾーンベース ファイアウォールまたはレイヤ 3 ファイアウォール設定をレイヤ 2 インターフェイスに適用できます。レイヤ 3 ファイア

ウォールとレイヤ2トランスペアレントファイアウォールの両方を同じデバイスで共存させることができます。

トランスペアレントファイアウォールでは、次のトポロジでIP（Internet Control Message Protocol（ICMP）、TCP、UDP）インスペクションをサポートします。

- 2 つの GigabitEthernet インターフェイス間。
- GigabitEthernet インターフェイスと GigabitEthernet サブインターフェイス間。
- 2 つの GigabitEthernet サブインターフェイス間。

トランスペアレントファイアウォールは、ポリシーを関連付けずに次のパケットを渡します。

- アドレス解決プロトコル（ARP）
- マルチキャスト パケット：Routing Information Protocol（RIP）、Open Shortest Path First（OSPF）、OSPF バージョン 3（OSPFv3）、Enhanced Interior Gateway Routing Protocol（EIGRP）IPv4 および IPv6 パケット、Intermediate System-to-Intermediate System（ISIS）IPv4 および IPv6 パケット
- Protocol-Independent Multicast（PIM）IPv4 および IPv6 パケット
- Hot Standby Router Protocol（HSRP）、Virtual Router Redundancy Protocol（VRRP）、および Gateway Load Balancing Protocol（GLBP）
- Internet Group Management Protocol（IGMP）およびマルチキャスト リスナー検出（MLD）

レイヤ 2 トランスペアレント ファイアウォールの設定方法

ゾーンベース ファイアウォールと同じ設定を使用してレイヤ 2 トランスペアレント ファイアウォールを設定できます。詳細は、「ゾーンベース ファイアウォール」モジュールを参照してください。

レイヤ 2 トランスペアレント ファイアウォールの設定例

例：レイヤ 2 トランスペアレント ファイアウォールの設定

次に、TCP インスペクションと UDP インスペクションを使用してレイヤ 2 トランスペアレント ファイアウォールを設定する例を示します。

- クラス マップを定義します。
- ポリシー マップを定義します。

- ゾーンとゾーン ペアを定義します。
- インターフェイス GigabitEthernet 0/0/0 と GigabitEthernet 0/0/1 をファイアウォール ゾーンにアタッチします。
- GigabitEthernet 0/0/0 と GigabitEthernet 0/0/1 を接続することにより、ローカル スイッチングを有効にします。

```
!Class map configuration
Device# configure terminal
Device(config)# class-map typ inspect match-any lan-wan-inspect-tcp
Device(config-cmap)# match protocol tcp
Device(config-cmap)# match protocol udp
Device(config-cmap)# match protocol icmp
Device(config-cmap)# exit
Device(config-cmap)# exit
Device(config)# class-map type inspect match-any wan-lan-inspect-udp
Device(config-cmap)# match protocol tcp
Device(config-cmap)# match protocol udp
Device(config-cmap)# match protocol icmp
Device(config-cmap)# exit

Device(config-cmap)# exit

!Policy map configuration
Device(config)# policy-map type inspect policy-wan-lan
Device(config-pmap)# class type inspect lan-wan-inspect-tcp
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# class type inspect wan-lan-inspect-udp
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# exit
Device(config-pmap)# exit

!Zones and zone pair configuration
Device(config)# zone security lan
Device(config-sec-zone)# exit
Device(config)# zone security wan
Device(config-sec-zone)# exit
Device(config)# zone-pair security lan2wan source lan destination wan
Device(config-sec-zone-pair)# service-policy type inspect policy-lan-wan
Device(config-sec-zone-pair)# exit
Device(config)# zone-pair security wan2lan source wan destination lan
Device(config-sec-zone-pair)# service-policy type inspect policy-wan-lan
Device(config-sec-zone-pair)# exit

! Interface configuration
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# no ip address
Device(config-if)# zone-member security lan
Device(config-if)# exit
Device(config)# interface gigiabitethernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# zone-member security wan
Device(config-if)# exit

!Local switching configuration
Device(config)# connect l2fw-conn gigabitethernet 0/0/0 gigabitethernet 0/0/1
```

```
Device(config)# end
```

レイヤ 2 トランスペアレント ファイアウォールに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
ゾーンベースのファイアウォール	『*Zone-Based Policy Firewalls*, Configuration Guide』の「Zone-Based Policy Firewalls」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

レイヤ 2 トランスペアレント ファイアウォールに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1:* レイヤ *2* トランスペアレント ファイアウォールに関する機能情報

機能名	リリース	機能情報
レイヤ2トランスペアレント ファイアウォール	Cisco IOS XE 3.15S	レイヤ 2 トランスペアレント ファイアウォールは、ブリッジされたパケットに対して動作し、ローカル スイッチド イーサネット ポートのペアで有効になります。これらのポート経由で転送される埋め込みIPパケットは、ルーティング ネットワーク内の通常の IP パケットと同様に検査されます。トランスペアレント ファイアウォール設定では、ゾーンベース ファイアウォールまたはレイヤ3ファイアウォール設定をレイヤ 2 インターフェイスに適用できます。 この機能は、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータとシスコ クラウド サービス ルータ 1000V シリーズでサポートされます。 この機能のために導入または変更されたコマンドはありません。

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。