Layer 2 Transparent Firewalls

A Layer 2 transparent firewall operates on bridged packets and is enabled on a pair of locally-switched Ethernet ports. Embedded IP packets forwarded through these ports are inspected similar to normal IP packets in a routing network. The zone-based firewall or Layer 3 firewall configuration can be applied to Layer 2 interfaces for the transparent firewall configuration.

This module provides an overview of the Layer 2 Transparent Firewalls feature.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Layer 2 Transparent Firewalls Support

- Address Resolution Protocol (ARP) inspection is not supported.
- Layer 2 forwarding technologies such as bridge domain, bridge domain interfaces (BDI), Overlay Transport Virtualization (OTV), X-Connect, Virtual Private LAN Services (VPLS), VxLAN, and non-IP flows, are not supported.
- Only normal IP or simple VLAN is supported on Ethernet frames. The transparent firewall generates TCP reset (RST) packets and sends these packets in supported Ethernet frame.
- TCP RST is not supported after intrabox high availability switchover.
- Virtual TCP (vTCP) is not supported.

- Network Address Translation (NAT), Box-to-Box (B2B) high availability, Multiprotocol Label Switching (MPLS), Virtual Routing and Forwarding (VRF) instances, VRF-Aware Software Infrastructure (VASI), Locator-ID Separation Protocol (LISP) are not supported in the Layer 2 switch path.
- Non IP packet flows like Ethernet Operation, Administration, and Maintenance (OAM), Connectivity Fault Management (CFM) is not supported.
- Layer 2-based access control lists (ACLs) are not supported in the transparent firewall class map.

Information About Layer 2 Transparent Firewalls

Layer 2 Transparent Firewall Support

A traditional zone-based firewall acts like a Layer 3 node in a network, and inspects the IP traffic that passes through the node. The traditional firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. However, to place this Layer 3 firewall in an existing network requires the network to be re-subnetted, which is time and resource-intensive. The Layer 2 transparent firewall is transparent to the network and does not require Layer 3 separation between segments. A transparent firewall acts like a "bump in the wire" or a "stealth firewall," and is not seen as a router hop to connected devices. Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network; IP readdressing is unnecessary. The transparent firewall operates on bridged packets and the Layer 3 firewall operates on routed packets.

A transparent firewall is enabled on a pair of locally-switched Ethernet ports. Embedded IP packets forwarded through these ports are inspected similar to normal IP packets in a routing network. The transparent firewall only inspects IP packets.

A transparent firewall session is created by using IP Layer 3 and Layer 4 headers that contain 5-tuple information (5-tuple information are source and destination IP addresses, source and destination ports, and the protocol). The transparent firewall supports only Ethernet as a Layer 2 protocol, and supports both IPv4 and IPv6 addresses.

The zone-based firewall or Layer 3 firewall configuration can be applied to Layer 2 interfaces for the transparent firewall configuration. Both Layer 3 firewall and Layer 2 transparent firewall can coexist on a device.

The transparent firewall supports IP (Internet Control Message Protocol [ICMP], TCP, and UDP) inspection with the following topologies:

- Between two GigabitEthernet interfaces.
- Between a GigabitEthernet interface and a GigabitEthernet subinterface.
- Between two GigabitEthernet subinterfaces

The transparent firewall passes the following packets without a policy attached to them:

- Address Resolution Protocol (ARP)
- Multicast packets: Routing Information Protocol (RIP), Open Shortest Path First (OSPF), OSPF Version 3 (OSPFv3), Enhanced Interior Gateway Routing Protocol (EIGRP) IPv4 and IPv6 packets, Intermediate System-to-Intermediate System (ISIS) IPv4 and IPv6 packets
- Protocol-Independent Multicast (PIM) IPv4 and IPv6 packets

- Hot Standby Router Protocol (HSRP), Virtual Router Redundancy Protocol (VRRP), and Gateway Load Balancing Protocol (GLBP)
- Internet Group Management Protocol (IGMP), and Multicast Listener Discovery (MLD)

How to Configure Layer 2 Transparent Firewalls

You can configure a Layer 2 transparent firewall using the same configuration as the zone-based firewalls. For more information, see the "Zone-Based Firewalls" module.

Configuration Examples for Layer 2 Transparent Firewalls

Example: Configuring a Layer 2 Transparent Firewall

The following example shows how to configure a Layer 2 transparent firewall with TCP and UDP inspection:

- Defines class maps.
- Defines policy maps.
- Defines zones and zone pairs.
- Attaches interfaces GigabitEthernet 0/0/0 and GigabitEthernet 0/0/1 to firewall zones.
- Enables local switching by connecting GigabitEthernet 0/0/0 with GigabitEthernet 0/0/1.

```
!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
```

Additional References for Layer 2 Transparent Firewalls

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security Commands	• 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
Zone-based firewalls	"Zone-Based Policy Firewalls" module in the *Zone-Based Policy Firewalls*, Configuration Guide.

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Layer 2 Transparent Firewalls

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Layer 2 Transparent Firewalls

Feature Name	Releases	Feature Information
Layer 2 Transparent Firewalls	Cisco IOS XE 3.15S	A Layer 2 transparent firewall operates on bridged packets and is enabled on a pair of locally-switched Ethernet ports. Embedded IP packets forwarded through these ports are inspected similar to normal IP packets in a routing network. The zone-based firewall or Layer 3 firewall configuration can be applied to Layer 2 interfaces for the transparent firewall configuration. This feature is supported on Cisco ASR 1000 Series Aggregation Services Routers, and Cisco Cloud Services Router 1000V Series. No commands were introduced or updated for this feature.