

Firewall Service Module Transparent Firewall Configuration Example

Document ID: 100773

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Transparent Firewall

- Bridge Groups
- Guidelines
- Allowed MAC Addresses
- Unsupported Features

Configure

- Network Diagram
- Configurations

Data Moves Across the Transparent Firewall in Different Scenarios

- An Inside User Accesses the Outside Email Server
- An Inside User Visits a Web Server with NAT
- An Inside User Visits an Inside Web Server
- An Outside User Visits a Web Server on the Inside Network
- An Outside User Attempts to Access an Inside Host

Verify

Troubleshoot

- Pass Through Traffic
- MSFC VLAN vs FWSM VLAN

Related Information

Introduction

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a *bump in the wire* or a *stealth firewall* and is not seen as a router hop to connected devices. The Firewall Service Module (FWSM) connects the same network on its inside and outside interfaces. Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network. IP readdressing is unnecessary.

Maintenance is facilitated because there are no complicated routing patterns to troubleshoot and no NAT configuration.

Even though transparent mode acts as a bridge, Layer 3 traffic (such as IP traffic) cannot pass through the FWSM unless you explicitly permit it with an extended access list. The only traffic allowed through the transparent firewall without an access list is ARP traffic. ARP traffic can be controlled by ARP inspection.

In routed mode, some types of traffic cannot pass through the FWSM even if you allow it in an access list. Alternatively, the transparent firewall can allow any traffic through with either an extended access list (for IP traffic) or an EtherType access list (for non-IP traffic).

For example, you can establish routing protocol adjacencies through a transparent firewall. You can allow VPN (IPSec), OSPF, RIP, EIGRP, or BGP traffic through based on an extended access list. Likewise,

protocols such as HSRP or VRRP can pass through the FWSM.

Non-IP traffic (for example, AppleTalk, IPX, BPDUs, and MPLS) can be configured to go through with an EtherType access list.

For features that are not directly supported on the transparent firewall, you can allow traffic to pass through so that upstream and downstream routers can support the functionality. For example, with an extended access list, you can allow DHCP traffic (instead of the unsupported DHCP relay feature) or multicast traffic, such as that created by IP/TV.

When the FWSM runs in transparent mode, the outbound interface of a packet is determined by a MAC address lookup instead of a route lookup. Route statements can still be configured, but they only apply to FWSM-originated traffic. For example, if your syslog server is located on a remote network, you must use a static route, so the FWSM can reach that subnet.

An exception to this rule is when you use voice inspections and the endpoint is at least one hop away from the FWSM. For example, if you use the transparent firewall between a CCM and an H.323 gateway, and there is a router between the transparent firewall and the H.323 gateway, then you need to add a static route on the FWSM for the H.323 gateway for successful call completion.

Note: The transparent mode FWSM does not pass CDP packets or any packets that do not have a valid EtherType greater than or equal to 0x600. For example, you cannot pass IS-IS packets. An exception is made for BPDUs, which are supported.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on FWSM with version 3.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Transparent Firewall

Bridge Groups

If you do not want the overhead of security contexts, or want to maximize your use of security contexts, you can configure up to eight pairs of interfaces, called bridge groups. Each bridge group connects to a separate network. Bridge group traffic is isolated from other bridge groups. Traffic is not routed to another bridge group within the FWSM, and traffic must exit the FWSM before it is routed by an external router back to another bridge group in the FWSM. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a system log server

or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context.

Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network. IP readdressing is unnecessary. Maintenance is facilitated because there are no complicated routing patterns to troubleshoot and no NAT configuration.

Note: Each bridge group requires a management IP address. The FWSM uses this IP address as the source address for packets that originate from the bridge group. The management IP address must be on the same subnet as the connected network.

Guidelines

Follow these guidelines when you plan your transparent firewall network:

- A management IP address is required for each bridge group.

Unlike routed mode, which requires an IP address for each interface, a transparent firewall has an IP address assigned to the entire bridge group. The FWSM uses this IP address as the source address for packets that originate on the FWSM, such as system messages or AAA communications.

The management IP address must be on the same subnet as the connected network. You cannot set the subnet to a host subnet (255.255.255.255). The FWSM does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported. Refer to *Assigning an IP Address to a Bridge Group* for more information about management IP subnets.

- Each bridge group uses an inside interface and an outside interface only.
- Each directly connected network must be on the same subnet.
- Do not specify the bridge group management IP address as the default gateway for connected devices. Devices need to specify the router on the other side of the FWSM as the default gateway.
- The default route for the transparent firewall, which is required to provide a return path for management traffic, is only applied to management traffic from one bridge group network. This is because the default route specifies an interface in the bridge group as well as the router IP address on the bridge group network, and you can only define one default route. If you have management traffic from more than one bridge group network, you need to specify a static route that identifies the network from which you expect management traffic.
- For multiple context mode, each context must use different interfaces. You cannot share an interface across contexts.
- For multiple context mode, each context typically uses different subnets. You can use overlapping subnets, but your network topology requires router and NAT configuration to make it possible from a routing standpoint.

You must use an extended access list to allow Layer 3 traffic, such as IP traffic, through the FWSM. You can also optionally use an EtherType access list to allow non-IP traffic through.

Allowed MAC Addresses

These destination MAC addresses are allowed through the transparent firewall. Any MAC address not on this list is dropped.

- TRUE broadcast destination MAC address equal to FFFF.FFFF.FFFF
- IPv4 multicast MAC addresses from 0100.5E00.0000 to 0100.5EFE.FFFF
- IPv6 multicast MAC addresses from 3333.0000.0000 to 3333.FFFF.FFFF
- BPDU multicast address equal to 0100.0CCC.CCCD

- AppleTalk multicast MAC addresses from 0900.0700.0000 to 0900.07FF.FFFF

Unsupported Features

These features are not supported in transparent mode:

- NAT /PAT

NAT is performed on the upstream router.

- Dynamic routing protocols (such as RIP, EIGRP, OSPF)

You can add static routes for traffic that originates on the FWSM. You can also allow dynamic routing protocols through the FWSM with an extended access list.

- IPv6 for the bridge group IP address.

However, you can pass the IPv6 EtherType using an EtherType access list.

- DHCP relay

The transparent firewall can act as a DHCP server, but it does not support the DHCP relay commands. DHCP relay is not required because you can allow DHCP traffic to pass through with an extended access list.

- Quality of Service (QoS)
- Multicast

You can allow multicast traffic through the FWSM if you allow it in an extended access list. Refer to the Pass Through Traffic section for more information.

- VPN termination for through traffic

The transparent firewall supports site-to-site VPN tunnels for management connections only. It does not terminate VPN connections for traffic through the FWSM. You can pass VPN traffic through the FWSM with an extended access list, but it does not terminate non-management connections.

- LoopGuard on the switch

Do not enable LoopGuard globally on the switch if the FWSM is in transparent mode. LoopGuard is automatically applied to the internal EtherChannel between the switch and the FWSM, so after a failover and a failback, LoopGuard causes the secondary unit to be disconnected because the EtherChannel goes into the err-disable state.

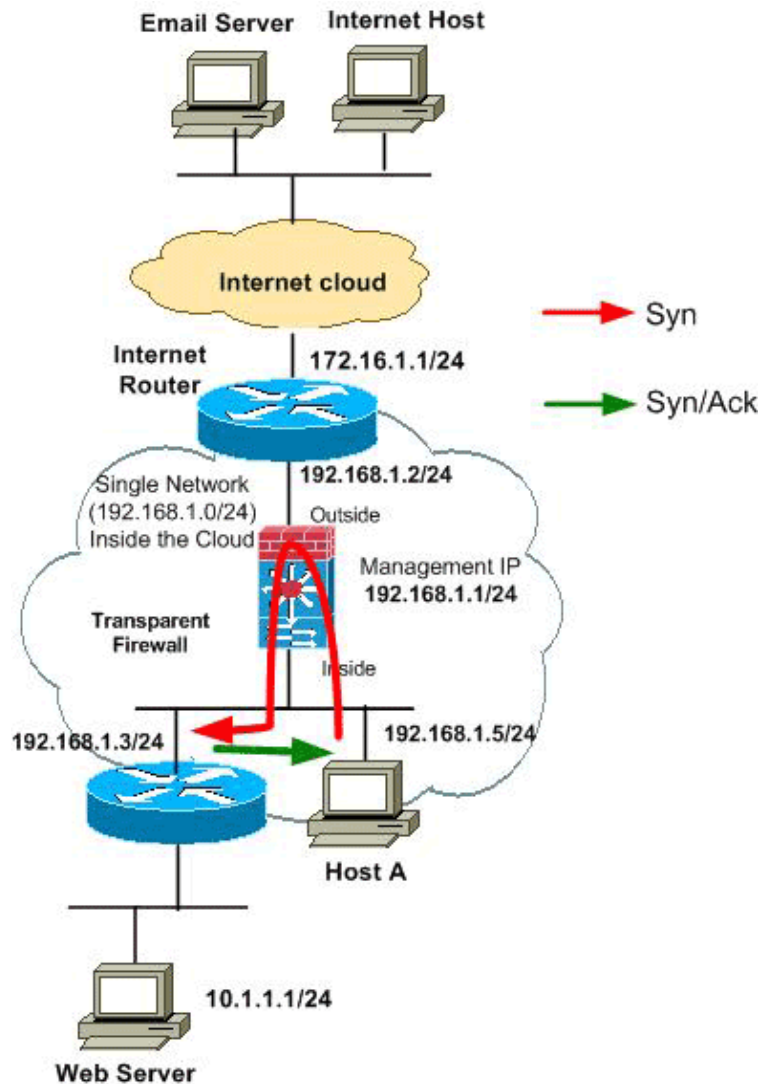
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

The network diagram shows a typical transparent firewall network where the outside devices are on the same subnet as the inside devices. The inside router and hosts appear to be directly connected to the outside router.



Configurations

You can set each context to run in routed firewall mode (the default) or transparent firewall mode.

When you change modes, the FWSM clears the configuration because many commands are not supported for both modes. If you already have a populated configuration, be sure to back up your configuration before you change the mode. You can use this backup for reference when creating your new configuration.

If you download a text configuration to the FWSM that changes the mode with the `firewall transparent` command, be sure to put the command at the top of the configuration. The FWSM changes the mode as soon as it reads the command and then continues reading the configuration that you downloaded. If the command is later in the configuration, the FWSM clears all the preceding lines in the configuration.

In order to set the mode to transparent, enter this command in each context:

```
hostname(config)#firewall transparent
```

In order to set the mode to routed, enter this command in each context:

```
hostname(config)#no firewall transparent
```

Data Moves Across the Transparent Firewall in Different Scenarios

An Inside User Accesses the Outside Email Server

The user on the inside network accesses the email server placed in the Internet (outside). The FWSM receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed in accordance with the terms of the security policy (access lists, filters, or AAA).

Note: For multiple context mode, the FWSM first classifies the packet in accordance with a unique interface.

The FWSM records that a session is established. If the destination MAC address is in its table, the FWSM forwards the packet out of the outside interface. The destination MAC address is that of the upstream router, 192.168.1.2. If the destination MAC address is not in the FWSM table, the FWSM attempts to discover the MAC address when it sends an ARP request and a ping. The first packet is dropped.

The email server responds to the request. Because the session is already established, the packet bypasses the many lookups associated with a new connection. The FWSM forwards the packet to the inside user.

An Inside User Visits a Web Server with NAT

If you enable NAT in the Internet router, the flow of the packet across the Internet router is slightly changed.

The user on the inside network accesses the email server placed in the Internet (outside). The FWSM receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed in accordance with the terms of the security policy (access lists, filters, or AAA).

Note: For multiple context mode, the FWSM first classifies the packet in accordance with a unique interface.

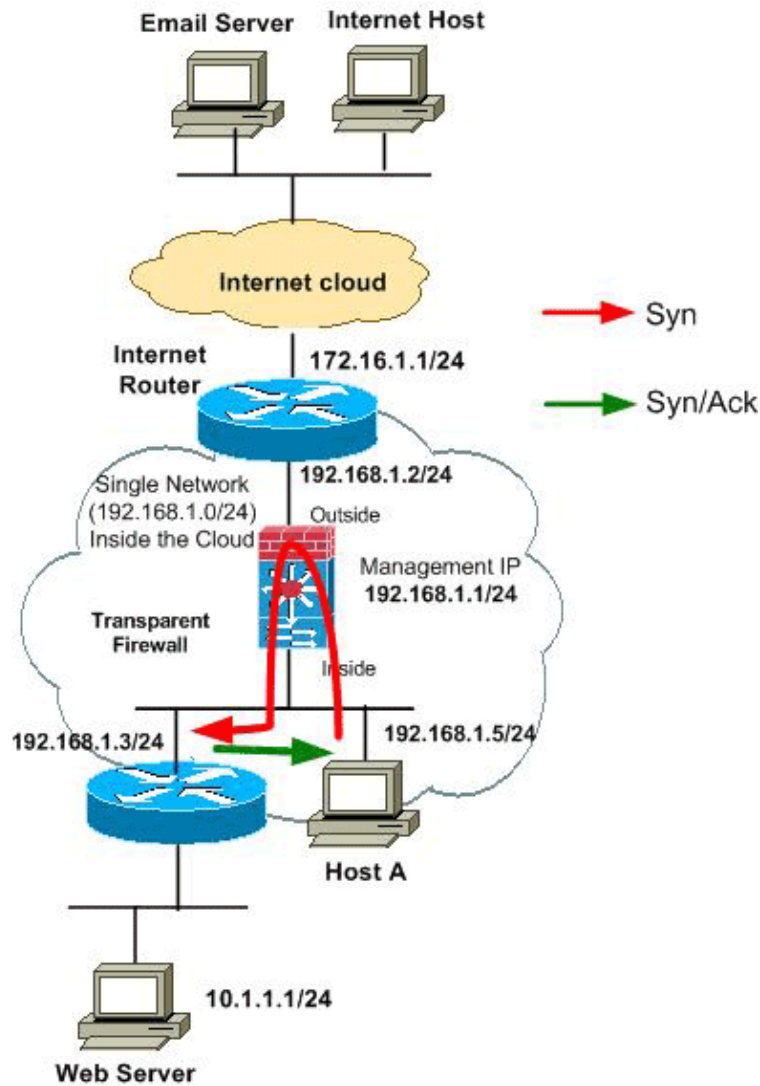
The Internet router translates the real address of Host A (192.168.1.5) to the mapped address of the Internet router (172.16.1.1). Because the mapped address is not on the same network as the outside interface, make sure that upstream router has a static route to the mapped network that points to the FWSM.

The FWSM records that a session is established and forwards the packet from the outside interface. If the destination MAC address is in its table, the FWSM forwards the packet out of the outside interface. The destination MAC address is that of the upstream router, 172.16.1.1. If the destination MAC address is not in the FWSM table, the FWSM attempts to discover the MAC address when it sends an ARP request and a ping. The first packet is dropped.

The email server responds to the request. Because the session is already established, the packet bypasses the many lookups associated with a new connection. The FWSM performs NAT when it translates the mapped address to the real address, 192.168.1.5.

An Inside User Visits an Inside Web Server

If Host A tries to access the inside web server (10.1.1.1), Host A (192.168.1.5) sends the request packet to the Internet router (since it is a default gateway) through the ASA from the inside to the outside. Then the packet is redirected to the web server (10.1.1.1) through ASA (outside to inside) and the internal router.



Note: The request packet returns to the web server only if the ASA has an access list to allow the traffic from the outside to the inside.

In order to resolve this issue, change the default gateway for Host A (10.1.1.1) to be the internal router (192.168.1.3) instead of the Internet router (192.168.1.2). This avoids any unnecessary traffic sent to the outside gateway and redirects occurrences on the outside router (Internet router). It also resolves in the reverse way, that is, when the web server or any host (10.1.1.0/24) present on the inside of the internal router tries to access Host A (192.168.1.5).

An Outside User Visits a Web Server on the Inside Network

These steps describe how data moves through the FWSM:

1. A user on the outside network requests a web page from the inside web server. The FWSM receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies that the packet is allowed in accordance with the terms of the security policy (access lists, filters, or AAA).

Note: For multiple context mode, the FWSM first classifies the packet in accordance with a unique interface.

2. The FWSM records that a session is established only if the outside user has the valid access to the internal web server. The access list must be configured to allow the outside user to get the access for

the web server.

3. If the destination MAC address is in its table, the FWSM forwards the packet out of the inside interface. The destination MAC address is that of the downstream router, 192.168.1.3.
4. If the destination MAC address is not in the FWSM table, the FWSM attempts to discover the MAC address when it sends an ARP request and a ping. The first packet is dropped.
5. The web server responds to the request. Because the session is already established, the packet bypasses the many lookups associated with a new connection. The FWSM forwards the packet to the outside user.

An Outside User Attempts to Access an Inside Host

A user on the outside network attempts to reach an inside host. The FWSM receives the packet and adds the source MAC address to the MAC address table, if required. Because it is a new session, it verifies whether the packet is allowed in accordance with the terms of the security policy (access lists, filters, or AAA).

Note: For multiple context mode, the FWSM first classifies the packet in accordance with a unique interface.

The packet is denied, and the FWSM drops the packet because the outside user does not have the access to the inside host. If the outside user attempts to attack the inside network, the FWSM employs many technologies to determine whether a packet is valid for an already established session.

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

```
ciscoasa(config)#show firewall
Firewall mode: Transparent
```

Troubleshoot

Pass Through Traffic

In transparent firewall, to pass multicast traffic from high to low and low to high access-lists are required. In normal firewalls from high to low is not required.

Note: Multicast address (224.0.0.9) can never be source address for return traffic, so it won't be allowed to come back in, that's why we need ACL's from in to out and out to in.

For example, in order to pass through Rip traffic, the transparent firewall access list would be similar to this example:

RIP

Outside ACL (from out to in):

```
access-list outside permit udp host (outside source router) host 224.0.0.9 eq 520
access-group outside in interface outside
```

Inside ACL (from inside to outside):

```
access-list inside permit udp host (inside source router) host 224.0.0.9 eq 520
access-group inside in interface inside
```

EIGRP to run:

```
access-list inside permit eigrp host (inside source) host 224.0.0.10
access-group inside in interface inside
access-list outside permit eigrp host (outside source) host 224.0.0.10
access-group outside in interface outside
```

For OSPF:

```
access-list inside permit ospf host ( inside source ) host 224.0.0.5
( this access-list is for hello packets )
access-list inside permit ospf host ( inside source ) host 224.0.0.6
( dr send update on this port )
access-list inside permit ospf host ( inside source ) host ( outside source )
access-group inside in interface inside
access-list outside permit ospf host ( outside source ) host 224.0.0.5
access-list outside permit ospf host ( outside source ) host 224.0.0.6
access-list outside permit ospf host ( outside source ) host ( inside source )
access-group outside in interface outside
```

MSFC VLAN vs FWSM VLAN

In transparent mode, it is not necessary to have the same VLANs in MSFC interface and FWSM, since it is a type of bridging.

Related Information

- [Cisco PIX Firewall Software](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Security Product Field Notices \(including PIX\)](#)
 - [Cisco Secure PIX Firewall Command References](#)
 - [PIX/ASA: Transparent Firewall Configuration Example](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 05, 2008

Document ID: 100773
