PIX/ASA: Transparent Firewall Configuration Example

Document ID: 97853

Contents

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 security appliance connects the same network on its inside and outside ports. Because the firewall is not a routed hop, you can easily introduce a transparent firewall into an existing network; it is unnecessary to re−address IP.

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

Even though the transparent mode acts as a bridge, Layer 3 traffic, such as IP traffic, cannot pass through the security appliance 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 security appliance 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 security appliance.

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 security appliance 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 security appliance−originated traffic. For example, if your syslog server is located on a remote network, you must use a static route, so the security appliance can reach that subnet.

You can set the adaptive security appliance to run in the default routed firewall mode or transparent firewall mode. When you change modes, the adaptive security appliance clears the configuration because many commands are not supported in both modes. If you already have a populated configuration, be sure to back up this configuration before you change the mode; you can use this backup configuration for reference when you create a new configuration.

For multiple context mode, you can use only one firewall mode for all contexts. You must set the mode in the system execution space. For multiple context mode, the system configuration is erased, which removes any contexts. If you again add a context that has an existing configuration that was created for the wrong mode, the context configuration does not work correctly.

Note: Be sure to create your context configurations for the correct mode before you add them again, or add new contexts with new paths for new configurations.

Note: If you download a text configuration to the security appliance that changes the mode with the **firewall transparent** command, be sure to put the command at the top of the configuration; the adaptive security appliance changes the mode as soon as the command is executed and then continues to read the configuration that you downloaded. If the command occurs later in the configuration, the adaptive security appliance clears all previous lines in the configuration.

In order to configure Multiple Context Mode in Transparent Firewall, refer to Multiple Mode, Transparent Firewall with Outside Access

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- ASA with version 7.x and later

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.

Related Products

This configuration can also be used with these hardware and software versions:

- PIX Security Appliance with 7.x and later

Conventions

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

Transparent Firewall

Guidelines

Follow these guidelines when you plan your transparent firewall network:

- A management IP address is required; for multiple context mode, an IP address is required for each context.

  Unlike routed mode, which requires an IP address for each interface, a transparent firewall has an IP address assigned to the entire device. The security appliance uses this IP address as the source address for packets that originate on the security appliance, 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 transparent security appliance uses an inside interface and an outside interface only. If your platform includes a dedicated management interface, you can also configure the management interface or subinterface for management traffic only.

  In single mode, you can only use two data interfaces (and the dedicated management interface, if available) even if your security appliance includes more than two interfaces.
- Each directly connected network must be on the same subnet.
- Do not specify the security appliance management IP address as the default gateway for connected devices; devices need to specify the router on the other side of the security appliance as the default gateway.
- 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 a different subnet. You can use subnets that overlap, 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 security appliance.

  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.

  Note: Starting with ASA/PIX 8.0(2), NAT/PAT is supported in the transparent firewall. Refer to NAT in Transparent Mode for more information.
- Dynamic routing protocols (such as RIP, EIGRP, OSPF)

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

  Note: IS−IS is IP protocol 124 (is−is over ipv4). IS−IS transient packets can be allowed through the transparent mode by the form of an ACL that permits protocol 124. The transparent mode supports all 255 IP protocols.
- IPv6
- 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 security appliance if you allow it in an extended access list. In a transparent firewall, access−lists are required to pass the multicast traffic from higher to lower, as well as from lower to higher security zones. In normal firewalls, higher to lower security zones are not required. For more information, refer to the Pass Through Traffic section in the Firewall Service Module Transparent Firewall Configuration Example.
- 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 security appliance. You can pass VPN traffic through the security appliance with an extended access list, but it does not terminate non−management connections.

Note: The transparent mode security appliance does not pass CDP packets or any packets that do not have a valid EtherType greater than or equal to 0x600.

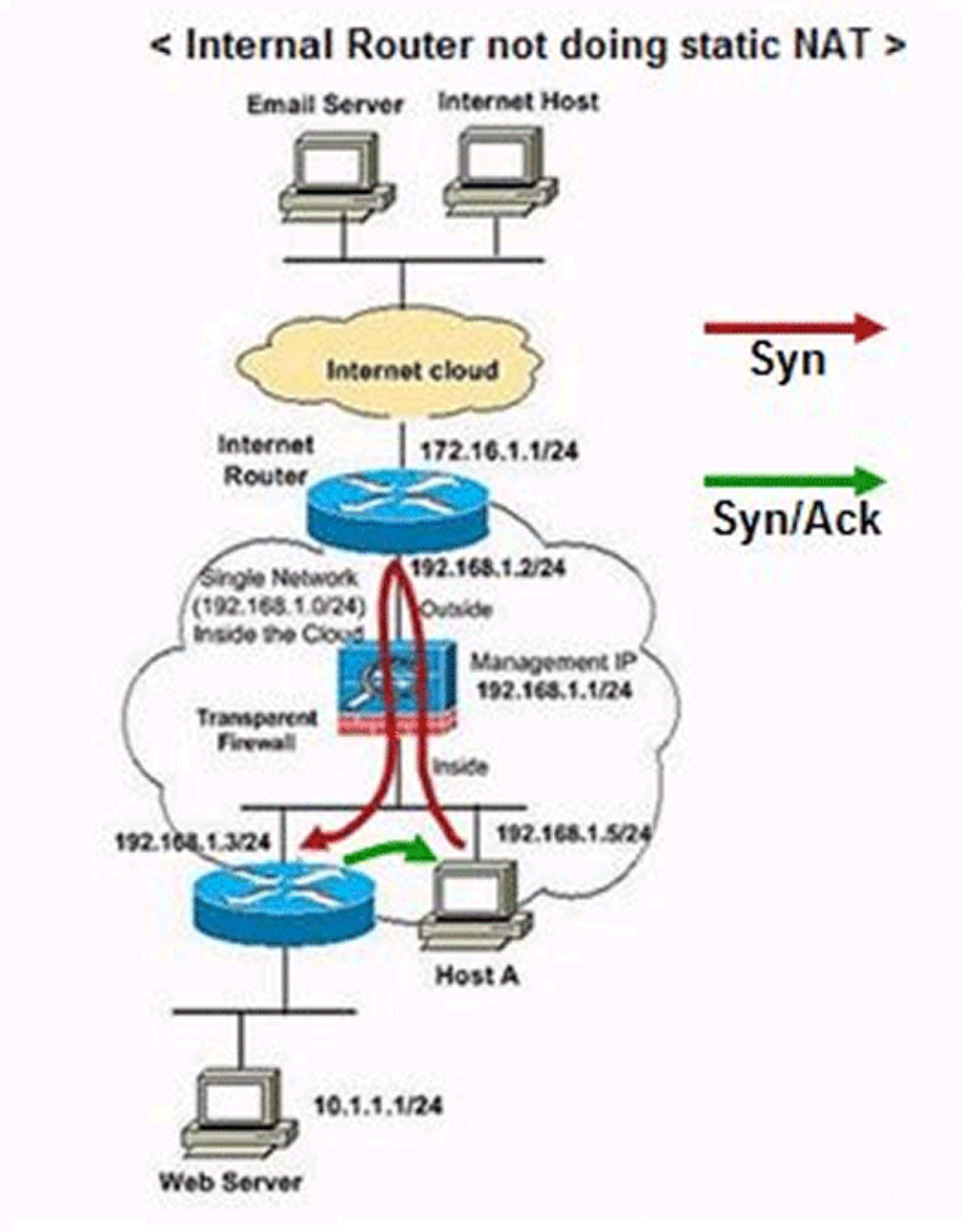
Configure

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

ASA 8.x
ciscoasa#**show running-config** : Saved : ASA Version 8.0(2) ! *!--- In order to set the firewall mode to transparent mode*

```
firewall transparent
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
!
interface Ethernet0/1
 nameif inside
 security-level 100
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
pager lines 24
mtu outside 1500
mtu inside 1500


!--- IP Address for the Management.
!---  Avoid using this IP Address as a default gateway.
!---  The security appliance uses this address as the source address
!---  for traffic originating on the security appliance, such as system
!---  messages or communications with AAA servers. You can also use this
!---  address for remote management access.


ip address 192.168.1.1 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1



!--- Output Suppressed



service-policy global_policy global
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
ciscoasa(config)#
```

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 security appliance 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 security appliance first classifies the packet in accordance with a unique interface.

The security appliance records that a session is established. If the destination MAC address is in its table, the security appliance 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 security appliance table, the security appliance 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 security appliance 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 security appliance 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 security appliance first classifies the packet in accordance with a unique interface.

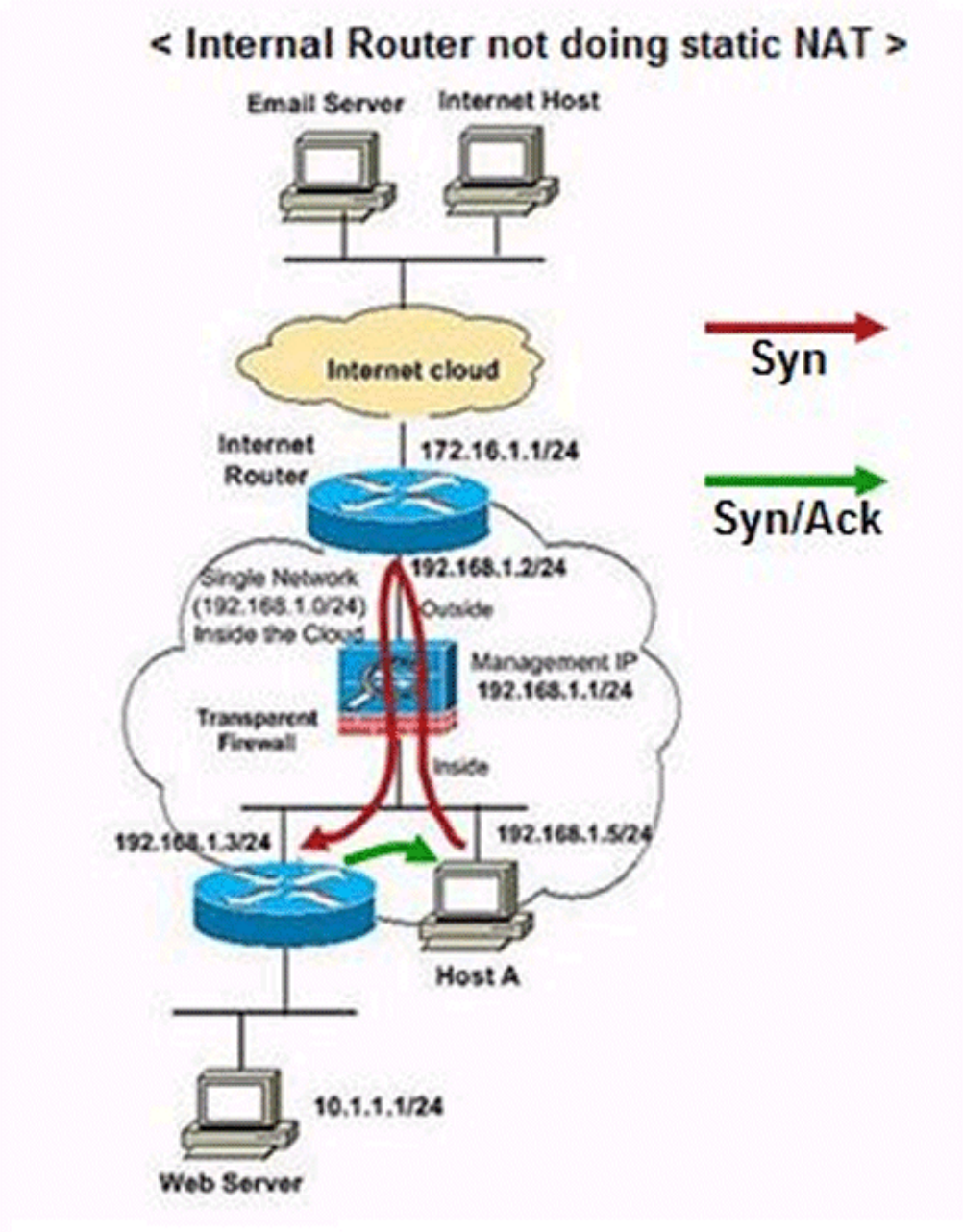
The Internet router translates the real address of Host A (192.168.1.5) to the mapped address of the Internet router (172.16.1.1). Because the mapped address is not on the same network as the outside interface, make sure that upstream router has a static route to the mapped network that points to the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

The security appliance records that a session is established and forwards the packet from the outside interface. If the destination MAC address is in its table, the security appliance 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 security appliance table, the security appliance 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 security appliance 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, 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 security appliance:

A user on the outside network requests a web page from the inside web server. The security appliance 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 security appliance first classifies the packet in accordance with a unique interface.

The security appliance 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.

If the destination MAC address is in its table, the security appliance forwards the packet out of the inside interface. The destination MAC address is that of the downstream router, 192.168.1.3.

If the destination MAC address is not in the security appliance table, the security appliance attempts to discover the MAC address when it sends an ARP request and a ping. The first packet is dropped.

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 security appliance 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 security appliance 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 security appliance first classifies the packet in accordance with a unique interface.

The packet is denied, and the security appliance 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 security appliance 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)# sh firewall
Firewall mode: Transparent
```

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **FWSM : Transparent Firewall Configuration**
- **Cisco PIX 500 Series Security Appliances**

- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Technical Support & Documentation − Cisco Systems**

Updated: Sep 26, 2008 Document ID: 97853