

PIX/ASA: Establish and Troubleshoot Connectivity through the Cisco Security Appliance

Document ID: 15245

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

How Connectivity Through the PIX Works

Configure Connectivity Through the PIX

Allow ARP Broadcast Traffic

- Allowed MAC Addresses

- Traffic not Allowed to Pass in Router Mode

Troubleshoot Connectivity Problems

- Error Message – %PIX|ASA-4-407001:

Access-list Command Syntax

- PIX Software Release 5.0.x and Later

Related Information

Introduction

When a PIX Firewall is configured initially, it has a default security policy where everyone on the inside can get out, and nobody from the outside can get in. If your site requires a different security policy, you can allow outside users to connect to your web server through the PIX.

Once you establish basic connectivity through the PIX Firewall, you can make configuration changes to the firewall. Make sure any configuration changes you make to the PIX Firewall are in compliance with your site security policy.

Refer to ASA 8.3: Establish and Troubleshoot Connectivity Through the Cisco Security Appliance for more information on the identical configuration on Cisco Adaptive Security Appliance (ASA) with version 8.3 and later.

Refer to Monitor and Troubleshoot PIX 500 Performance Issues in order to learn more about the various show commands that are useful for troubleshooting.

Refer to Troubleshoot Connections through the PIX and ASA in order to learn more about the security appliance connectivity troubleshooting.

Prerequisites

Requirements

This document assumes that some basic configurations have already been completed on the PIX. Refer to these documents for examples of an initial PIX configuration:

- Configuring the Cisco Secure PIX Firewall with a Single Internal Network

- Configuring the PPPoE Client on a Cisco Secure PIX Firewall

Components Used

The information in this document is based on PIX Firewall Software Releases 5.0.x and later.

Note: Earlier versions of the PIX software use the **conduit** command instead of the **access-list** command. Either command works in PIX Firewall Software Releases 5.0.x and later.

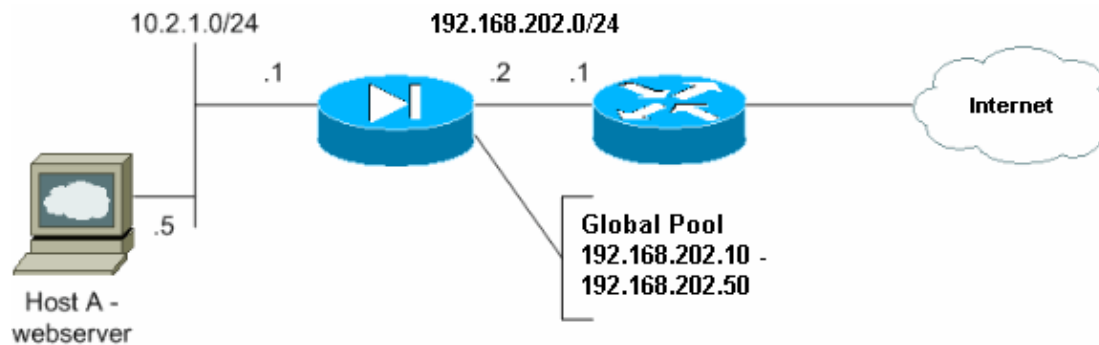
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

How Connectivity Through the PIX Works

In this network, Host A is the web server with an internal address of 10.2.1.5. The web server is assigned an external (translated) address of 192.168.202.5. Internet users must point to 192.168.202.5 in order to access the web server. The DNS entry for your web server needs to be that address. No other connections are allowed from the Internet.



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Configure Connectivity Through the PIX

Complete these steps in order to configure connectivity through the PIX.

1. Set up a global pool for the internal hosts to use when they access the Internet.

```
global (outside) 1 192.168.202.10-192.168.202.50 netmask 255.255.255.0
```

2. Direct internal addresses to select from the global 1 pool.

```
nat (inside) 1 0.0.0.0 0.0.0.0
```

3. Assign a static translated address for the internal host to which Internet users have access.

```
static (inside,outside) 192.168.202.5 10.2.1.5 0 0
```

4. Use the **access-list** command to allow outside users through the PIX Firewall. Always use the translated address in the **access-list** command.

```
access-list 101 permit tcp any host 192.168.202.5 eq www
access-group 101 in interface outside
```

For more information about command syntax, see the **conduit** and **access-list** Command Syntax section of this document.

Allow ARP Broadcast Traffic

The security appliance 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 re-addressing is not necessary. IPv4 traffic is allowed through the transparent firewall automatically from a higher security interface to a lower security interface, without an access list. Address Resolution Protocols (ARPs) are allowed through the transparent firewall in both directions without an access list. ARP traffic can be controlled by ARP inspection. For Layer 3 traffic that travels from a low to a high security interface, an extended access list is required.

Note: The transparent mode security appliance does not pass Cisco Discovery Protocol (CDP) packets or IPv6 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 bridge protocol data units (BPDUs), which are supported.

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

Traffic not Allowed to Pass in Router Mode

In router mode, some types of traffic cannot pass through the security appliance even if you allow it in an access list. The transparent firewall, however, can allow almost any traffic through using 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 Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), or Border Gateway Protocol (BGP) traffic through based on an extended access list. Likewise, protocols like Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) can pass through the security appliance.

Non-IP traffic (for example AppleTalk, IPX, BPDUs, and MPLS) can be configured to go through using 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, by using an extended access list, you can allow DHCP traffic (instead of the unsupported Dynamic Host Configuration Protocol [DHCP] relay feature) or multicast traffic such as that created by IP/TV.

Troubleshoot Connectivity Problems

If Internet users cannot access your web site, complete these steps:

1. Make sure you have entered configuration addresses correctly:
 - ◆ Valid external address
 - ◆ Correct internal address
 - ◆ External DNS has translated address
2. Check the outside interface for errors. Cisco Security Appliance is preconfigured to auto-detect the speed and duplex settings on an interface. However, several situations exist that can cause the auto-negotiation process to fail. This results in either speed or duplex mismatches (and performance issues). For mission-critical network infrastructure, Cisco manually hardcodes the speed and duplex on each interface so there is no chance for error. These devices generally do not move around, so if you configure them properly, you should not need to change them.

Example:

```
asa(config)#interface ethernet 0/0
asa(config-if)#duplex full
asa(config-if)#speed 100
asa(config-if)#exit
```

In some situations, hardcoding the speed and duplex settings leads to the generation of errors. So, you need to configure the interface to the default setting of autodetect mode as this example shows:

Example:

```
asa(config)#interface ethernet 0/0
asa(config-if)#duplex auto
asa(config-if)#speed auto
asa(config-if)#exit
```

Refer to the Speed and Duplex Settings section of Monitor and Troubleshoot PIX 500 Performance Issues for more information.

3. If the traffic does not send or receive through the interface of the PIX or the headend router, try to clear the ARP statistics.

```
asa#clear arp
```

4. Use the **show static** command in order to make sure that static translation is enabled.
5. Use the **interface** keyword instead of the interface IP address in the static NAT statements if the static mapping does not work after the upgrade to version 7.2(1).

Example:

```
static (inside,outside) tcp 192.168.202.2 80 10.2.1.5 1025 netmask 255.255.255.255
```

In this scenario, the outside IP address is used as the mapped IP address for the web server. So, this static mapping might not work for PIX/ASA version 7.2(1). In order to solve this issue, you can use this syntax.

```
static (inside,outside) tcp interface 80 10.2.1.5 1025 netmask 255.255.255.255
```

6. Check to see that the default route on the web server points to the inside interface of the PIX.
7. Check the translation table using the **show xlate** command in order to see if the translation was created.

8. Use the **logging buffer debug** command in order to check the log files to see if denies occur. (Look for the translated address and see if you see any denies.)
9. Use the **capture** command if you use version 6.2.2 or later with this command:

```
access-list webtraffic permit tcp any host 192.168.202.5  
  
capture capture1 access-list webtraffic interface outside
```

If you use a version earlier than 6.2.2 and if the network is not busy, you can capture the traffic with the **debug packet** command. This command captures packets that come from any external host toward the web server.

```
debug packet outside dst 192.168.202.5 proto tcp dport 80 bot
```

Note: This command generates a significant amount of output. It can cause a router to hang or reload under heavy traffic loads.

10. If packets make it to the PIX, make sure your route to the web server from the PIX is correct. (Check the **route** commands in your PIX configuration.)
11. Check to see if proxy ARP is disabled. Issue the command **show running-config sysopt** in PIX/ASA 7.x or **show sysopt** in PIX 6.x.

Here proxy ARP is disabled by the command **sysopt noproxyarp outside**:

```
ciscoasa#show running-config sysopt  
no sysopt connection timewait  
sysopt connection tcpmss 1380  
sysopt connection tcpmss minimum 0  
no sysopt nodnsalias inbound  
no sysopt nodnsalias outbound  
no sysopt radius ignore-secret  
sysopt noproxyarp outside  
sysopt connection permit-vpn
```

In order to re-enable proxy ARP, enter this command in global configuration mode:

```
ciscoasa(config)#no sysopt noproxyarp outside
```

When a host sends IP traffic to another device on the same Ethernet network, the host needs to know the MAC address of the device. ARP is a Layer 2 protocol that resolves an IP address to a MAC address. A host sends an ARP request and asks "Who is this IP address?". The device that owns the IP address replies, "I own that IP address; here is my MAC address."

Proxy ARP allows the security appliance to reply to an ARP request on behalf of hosts behind it. It does this by replying to ARP requests for the static mapped addresses of those hosts. The security appliance responds to the request with its own MAC address and then forwards the IP packets on to the appropriate inside host.

For example, in the diagram in this document, when an ARP request is made for the global IP address of the web server, 192.168.202.5, the security appliance responds with its own MAC address. If proxy ARP is not enabled in this situation, hosts on the outside network of the security appliance are not able to reach the web server by issuing an ARP request for the address 192.168.202.5. Refer to the command reference for more information about the **sysopt** command.

12. If everything appears to be correct, and users still cannot access the web server, open a case with Cisco Technical Support.

Error Message – %PIX|ASA-4-407001:

Few hosts are unable to connect to the internet and the Error Message – %PIX|ASA-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded error message is seen in the syslog. How can this error be resolved?

This error message is seen when the number of users exceeds the user limit of the license used. Upgrade the license to a higher number of users, which can be 50, 100 or unlimited user license as required, in order to resolve this error.

Access-list Command Syntax

PIX Software Release 5.0.x and Later

The **access-list** command was introduced in PIX Software Release 5.0. This example shows the syntax for the **access-list** command:

```
access-list acl_name [deny | permit] protocol source source_netmask destination destination_netmask
```

Example: **access-list 101 permit tcp any host 192.168.202.5 eq www**

In order to *apply* the access list, you must include this syntax in your configuration:

```
access-group acl_name in interface interface_name
```

The **access-group** command binds an access list to an interface. The access list is applied to traffic inbound to an interface. If you enter the **permit** option in an **access-list** command statement, the PIX Firewall continues to process the packet. If you enter the **deny** option in an **access-list** command statement, PIX Firewall discards the packet.

Note: Each Access Control Entry (ACE) that you enter for a given access list name is appended to the end of the access list unless you specify the line number in the ACE.

Note: The order of ACEs is important. When the security appliance decides whether to forward or drop a packet, the security appliance tests the packet against each ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked. For example, if you create an ACE at the beginning of an access list that explicitly permits all traffic, no further statements are checked.

Note: Access lists have an implicit deny at the end of the list. So unless you explicitly permit it, traffic cannot pass. For example, if you want to allow all users to access a network through the security appliance except for particular addresses, then you need to deny the particular addresses and then permit all others.

Related Information

- [PIX 500 Series Security Appliances Support Page](#)
 - [Cisco Adaptive Security Appliance Support Page](#)
 - [Documentation for PIX Firewall](#)
 - [Cisco Secure PIX Firewall Command References](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

