

Using nat, global, static, conduit, and access-list Commands and Port Redirection(Forwarding) on PIX

Document ID: 12496

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Network Diagram

Initial Configuration

Allow Outbound Access

- Allow Some of the Inside Hosts Access to Outside Networks
- Allow the Remaining Inside Hosts Access to Outside Networks
- Allow Inside Hosts Access to a DMZ without Translation
- Restrict Inside Hosts Access to Outside Networks

Allow Untrusted Hosts Access to Hosts on Your Trusted Network

- Use Conduits on PIX Versions 4.4.5 and Later
- Use ACLs on PIX Versions 5.0.1 and Later

Disable NAT

Port Redirection(Forwarding) with Statics

- Network Diagram – Port Redirection(Forwarding)
- Partial PIX Configuration – Port Redirection(Forwarding)

Outside NAT

- Network Diagram – Outside NAT
- Partial PIX Configuration – Outside NAT

Troubleshoot

Information to Collect if You Open a TAC Case

Related Information

Introduction

In order to maximize security when you implement a Cisco Secure PIX Firewall, it is important to understand how packets are passed from and to higher security interfaces from lower security interfaces by using the **nat**, **global**, **static**, and **conduit** commands, or **access-list** and **access-group** commands in PIX software versions 5.0 and later. This document explains the differences between these commands and how to configure port redirection(Forwarding) in PIX software version 6.0 and the outside Network Address Translation (NAT) feature added in PIX software version 6.2.

Refer to PIX/ASA 7.x NAT and PAT Statements in order to learn more about the basic NAT and Port Address Translation (PAT) configurations on the Cisco PIX 500 Series Security Appliances.

Refer to Using NAT and PAT Statements on the Cisco Secure PIX Firewall in order to learn more about the examples of basic NAT and PAT configurations on the Cisco Secure PIX Firewall.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software versions.

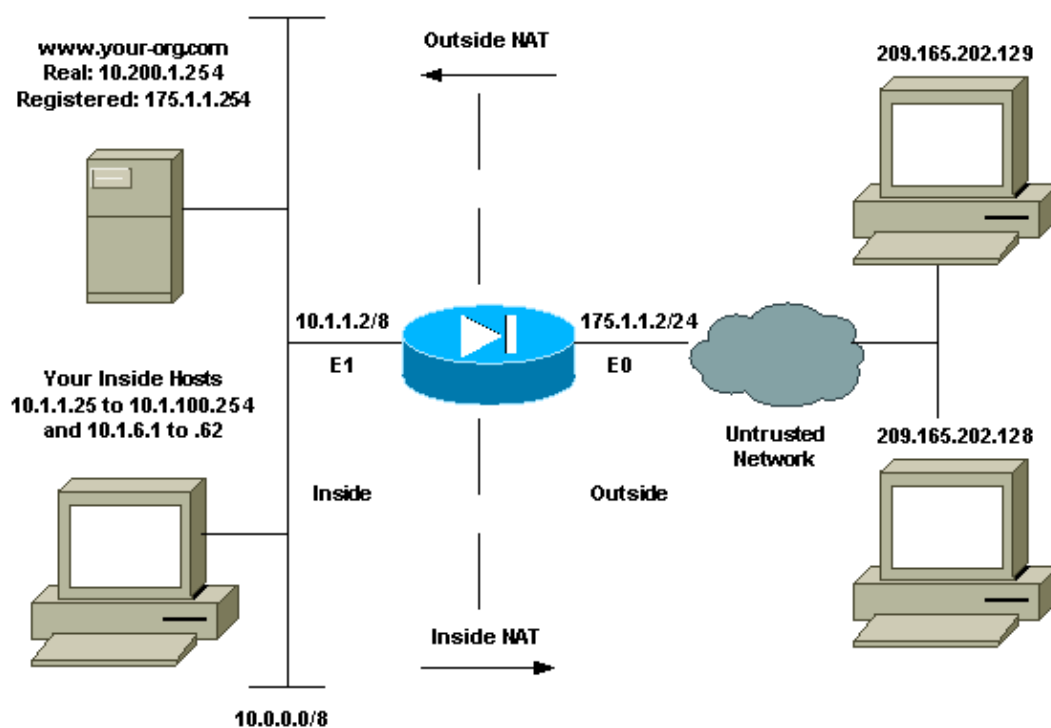
- Cisco Secure PIX Firewall Software versions 4.4.5 and later

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 Cisco Technical Tips Conventions for more information on document conventions.

Network Diagram



Initial Configuration

The names of the interfaces are:

- `nameif ethernet0 outside security0`
- `nameif ethernet1 inside security100`

Allow Outbound Access

Outbound access describes connections from a higher security level interface to a lower security level interface. This includes connections from inside to outside, inside to Demilitarized Zones (DMZs), and DMZs to outside. This can also include connections from one DMZ to another, provided the connection source interface has a higher security level than the destination. This can be confirmed by a review of the "nameif" configuration on the PIX.

There are two policies that are required to allow outbound access. The first one is a translation method. This can be a static translation using the **static** command, or a dynamic translation using a nat/global rule. The other requirement for outbound access is if there is an access control list (ACL) present, then it must allow the source host access to the destination host using the specific protocol and port. By default, there are no access restrictions on outbound connections through the PIX. This means that if there is no ACL configured for the source interface, then by default, the outbound connection are allowed if there is a translation method configured.

These sections provide examples in both the configuration of a translation method and the restriction of outbound access with the use of an ACL.

Allow Some of the Inside Hosts Access to Outside Networks

This configuration gives all of the hosts on the subnet 10.1.6.0/24 access to the outside. The **nat** and **global** commands are used to accomplish this.

1. Define the inside group to be included for NAT.

```
nat (inside) 1 10.1.6.0 255.255.255.0
```

2. Specify a pool of addresses on the outside interface to which the hosts defined in the NAT statement are translated.

```
global (outside) 1 175.1.1.3-175.1.1.64 netmask 255.255.255.0
```

Now the hosts on the inside can access outside networks. When hosts from the inside initiate a connection to the outside, they are translated to an address from the global pool. Note that the addresses are assigned from the global pool on a first-come, first-translated basis, and start with the lowest address in the pool. For example, if host 10.1.6.25 is the first to initiate a connection to the outside, it receives address 175.1.1.3. The next host out receives 175.1.1.4 and so on. This is not a static translation, and the translation times out after a period of inactivity as defined by the **timeout xlate hh:mm:ss** command.

Allow the Remaining Inside Hosts Access to Outside Networks

The problem is that there are more inside hosts than outside addresses. Use Port Address Translation (PAT) to allow all of the hosts access to the outside. If one address is specified in the **global** statement, that address is port translated. The PIX allows one port translation per interface and that translation supports up to 65,535 active xlate objects to the single global address. Complete these steps:

1. Define the inside group to be included for PAT. (By using 0 0 we select all inside hosts.)

```
nat (inside) 1 10.1.6.0 255.255.255.0
```

2. Specify the global address to be used for PAT.

```
global (outside) 1 175.1.1.65
```

There are a few things to consider when you use PAT.

- The IP addresses you specify for PAT cannot be in another global address pool.
- PAT does not work with H.323 applications, caching nameservers, and Point-to-Point Tunneling Protocol (PPTP). PAT works with Domain Name Service (DNS), FTP and passive FTP, HTTP, mail, remote-procedure call (RPC), rshell, Telnet, URL filtering, and outbound traceroute.
- Do not use PAT when multimedia applications need to be run through the firewall. Multimedia applications can conflict with port mappings provided by PAT.
- In PIX software release 4.2(2), the PAT feature does not work with IP data packets that arrive in reverse order. This problem is corrected in release 4.2(3).
- IP addresses in the pool of global addresses specified with the **global** command require reverse DNS entries to ensure that all external network addresses are accessible through the PIX. In order to create reverse DNS mappings, use a DNS Pointer (PTR) record in the address-to-name mapping file for each global address. Without the PTR entries, sites can experience slow or intermittent Internet connectivity and FTP requests fail consistently.

For example, if a global IP address is 175.1.1.3 and the domain name for the PIX Firewall is pix.caguana.com, the PTR record would be:

```
3.1.1.175.in-addr.arpa. IN PTR
pix3.caguana.com
4.1.1.175.in-addr.arpa. IN PTR
pix4.caguana.com & so on.
```

Allow Inside Hosts Access to a DMZ without Translation

While the configurations earlier in this document use the **nat** and **global** commands to allow hosts on the inside network to access hosts on a DMZ interface by translating the source addresses of the inside hosts, sometimes such a translation is not desired. But when a host on one PIX Firewall interface initiates a connection to a host on another interface, the PIX **must** have a way to translate that host's IP address across itself. **Even if it is not necessary for the IP address to be translated, a translation must still occur.** Therefore, in order to allow hosts on the inside access to hosts on the DMZ, a translation that does not actually translate must be configured.

Assume that hosts on the inside network of 10.1.6.0/24 need access to hosts on the DMZ network of 172.22.1.0/24:

1. Create a static translation between the entire inside network and the DMZ that does not actually translate inside addresses.

```
static (inside,dmz) 10.1.6.0 10.1.6.0 netmask 255.255.255.0
```

2. Create a static translation to allow one inside host access to the DMZ without actually translating the address of the host.

```
static (inside,dmz) 10.1.6.100 10.1.6.100
```

Note: The PIX automatically adds a netmask of 255.255.255.255.

Restrict Inside Hosts Access to Outside Networks

If there is a valid translation method defined for the source host, and no ACL defined for the source PIX interface, then the outbound connection is allowed by default. However, in some cases it might be necessary to restrict outbound access based on source, destination, protocol, and/or port. This can be accomplished when you configure an ACL with the **access-list** command and apply it to the connection source PIX interface with the **access-group** command. PIX ACLs are only applied in the inbound direction. ACLs are available in PIX version 5.0.1 code or later. Earlier code uses "outbound" and "apply" statements which are described in the PIX command reference.

This is an example that allows outbound HTTP access for one subnet, but denies all other hosts HTTP access to the outside, and allows all other IP traffic for everyone.

1. Define the ACL.

```
access-list acl_outbound permit tcp 10.1.6.0 255.255.255.0 any eq www
access-list acl_outbound deny tcp any any eq www
access-list acl_outbound permit ip any any
```

Note: PIX ACLs differ from ACLs on Cisco IOS routers in that the PIX does *not* use a wildcard mask like Cisco IOS. It uses a regular subnet mask in the ACL definition. As with Cisco IOS routers, the PIX ACL has an implicit "deny all" at the end of the ACL.

2. Apply the ACL to the inside interface.

```
access-group acl_outbound in interface inside
```

Allow Untrusted Hosts Access to Hosts on Your Trusted Network

Most organizations need to allow untrusted hosts onto resources in their trusted network, with a common example being an internal web server. By default, the PIX denies connections from outside hosts to inside hosts. Use the **static** and **conduit** commands to allow this connection. In PIX software versions 5.0.1 and later, **access-list** and **access-group** commands are available in addition to **conduit** commands.

Either conduits or ACLs make sense for a two-interface PIX. Conduits are direction-based. They have a concept of *inside* and *outside*. With a two-interface PIX, the conduit allows traffic from the *outside* to the *inside*. Unlike conduits, ACLs are applied to interfaces with an **access-group** command. This command associates the ACL with the interface to examine traffic that flows in a particular direction.

In contrast to the **nat** and **global** commands which allow inside hosts out, the **static** command creates a two-way translation that allows inside hosts out and outside hosts in if the proper conduits are created or ACLs/groups added (PIX software version 5.0.1 or later).

In the PAT configuration examples earlier in this document, if an outside host tried to connect to the global address, it could be used by thousands of inside hosts. The **static** command creates a one-to-one mapping. The **conduit** or **access-list** command defines what type of connection is allowed to an inside host and is always required when a lower security host connects to a higher security host. The **conduit** or **access-list** command is based on both port and protocol. It can be very permissive or very restrictive, depending on what the system administrator wants to achieve.

The network diagram in this document illustrates use of these commands to configure the PIX to allow any untrusted hosts to connect to the inside web server, and allows this untrusted host, 199.199.199.24, access to an FTP service on the same machine.

Use Conduits on PIX Versions 4.4.5 and Later

Complete these steps for PIX software versions 4.4.5 and later using conduits.

1. Define a static address translation for the inside web server to an outside/global address.

```
static (inside,outside) 175.1.1.254 10.200.1.254
```

2. Define which hosts can connect on which ports to your web/FTP server.

```
conduit permit tcp host 175.1.1.254 eq www any
```

```
conduit permit tcp host 175.1.1.254 eq ftp host 199.199.199.24
```

In PIX software versions 5.0.1 and later, ACLs with access groups can be used instead of conduits. Conduits are still available, but the decision should be made whether to use conduits or ACLs. It is not advisable to combine ACLs and conduits on the same configuration. If both are configured, ACLs take preference over the conduits.

Use ACLs on PIX Versions 5.0.1 and Later

Complete these steps for PIX software versions 5.0.1 and later using ACLs.

1. Define a static address translation for the inside web server to an outside/global address.

```
static (inside, outside) 175.1.1.254 10.200.1.254
```

2. Define which hosts can connect on which ports to your web/FTP server.

```
access-list 101 permit tcp any host 175.1.1.254 eq www
access-list 101 permit tcp host 199.199.199.24 host 175.1.1.254 eq ftp
```

3. Apply the ACL to the outside interface.

```
access-group 101 in interface outside
```

Note: Be careful when you implement these commands. If either the **conduit permit ip any any** or **access-list 101 permit ip any any** command is implemented, any host on the untrusted network can access any host on the trusted network using IP as long as there is an active translation.

Disable NAT

If you have a public address on the inside network, and you want the inside hosts to go out to the outside without translation, you can disable NAT. You also need to change the **static** command.

Using the example in this document, the **nat** command changes as this output shows:

```
nat (inside) 0 175.1.1.0 255.255.255.0
```

Use these commands if you use ACLs in PIX software versions 5.0.1 and later:

```
access-list 103 permit ip 175.1.1.0 255.255.255.0 any
nat (inside) 0 access-list 103
```

This command disables NAT for the 175.1.1.0 network. The **static** command for the web server changes as this output shows:

```
static (inside, outside) 175.1.1.254 175.1.1.254
```

This command defines the conduit for the web server.

```
conduit permit tcp host 175.1.1.254 eq www any
```

Use these commands if you use ACLs in PIX software versions 5.0.1 and later:

```
access-list 102 permit tcp any host 175.1.1.254 eq www
access-group 102 in interface outside
```

Note that the difference between using **nat 0** with specifying network/mask as opposed to using an ACL that

uses a network/mask that permits initiation of connections from inside only. The use of ACLs permits initiation of connections by inbound or outbound traffic. The PIX interfaces should be in different subnets to avoid reachability issues.

Port Redirection(Forwarding) with Statics

In PIX 6.0, the Port Redirection(Forwarding) feature was added to allow outside users to connect to a particular IP address/port and have the PIX redirect the traffic to the appropriate inside server; the **static** command was modified. The shared address can be a unique address, a shared outbound PAT address, or shared with the external interface.

Note: These commands are on two lines due to space limitations.

```
static [(internal_if_name, external_if_name)]
{global_ip/interface}
local_ip [netmask mask] [max_conns [emb_limit
[norandomseq]]]

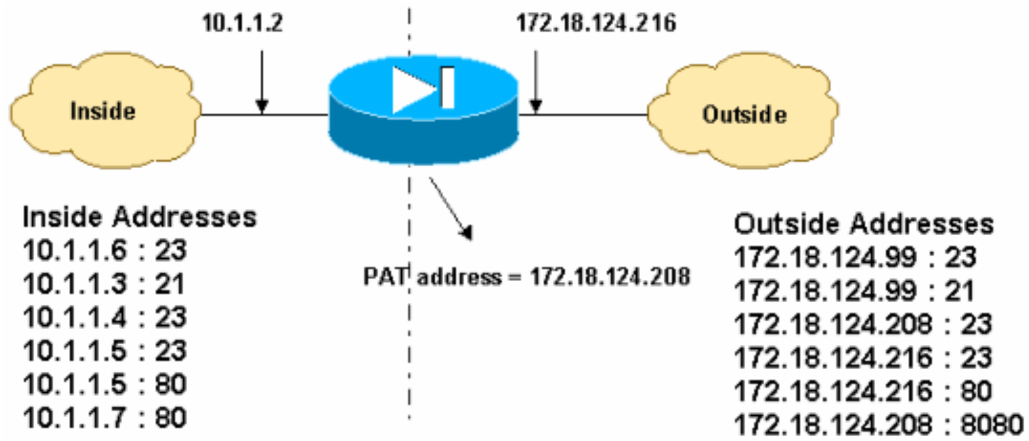
static [(internal_if_name, external_if_name)] {tcp|udp}
{global_ip/interface}
global_port local_ip local_port [netmask mask] [max_conns
[emb_limit [norandomseq]]]
```

These are the port redirections for the example network:

- External users direct Telnet requests to unique IP address 172.18.124.99, which the PIX redirects to 10.1.1.6.
- External users direct FTP requests to unique IP address 172.18.124.99, which the PIX redirects to 10.1.1.3.
- External users direct Telnet requests to PAT address 172.18.124.208, which the PIX redirects to 10.1.1.4.
- External users direct Telnet request to PIX outside IP address 172.18.124.216, which the PIX redirects to 10.1.1.5.
- External users direct HTTP request to PIX outside IP address 172.18.124.216, which the PIX redirects to 10.1.1.5.
- External users direct HTTP port 8080 requests to PAT address 172.18.124.208, which the PIX redirects to 10.1.1.7 port 80.

This example also blocks some users' access from inside to outside with ACL 100. This step is optional. All traffic is permitted outbound without the ACL in place.

Network Diagram – Port Redirection(Forwarding)



Partial PIX Configuration – Port Redirection(Forwarding)

This partial configuration illustrates the use of static port redirection.

```

Partial PIX Configuration – Port Redirection(Forwarding)

fixup protocol ftp 21

!--- Use of an outbound ACL is optional.

access-list 100 permit tcp 10.1.1.0 255.255.255.128 any eq www
access-list 100 deny tcp any any eq www
access-list 100 permit tcp 10.0.0.0 255.0.0.0 any
access-list 100 permit udp 10.0.0.0 255.0.0.0 host 172.18.124.100 eq domain

access-list 101 permit tcp any host 172.18.124.99 eq telnet
access-list 101 permit tcp any host 172.18.124.99 eq ftp
access-list 101 permit tcp any host 172.18.124.208 eq telnet
access-list 101 permit tcp any host 172.18.124.216 eq telnet
access-list 101 permit tcp any host 172.18.124.216 eq www
access-list 101 permit tcp any host 172.18.124.208 eq 8080

ip address outside 172.18.124.216 255.255.255.0
ip address inside 10.1.1.2 255.255.255.0

global (outside) 1 172.18.124.208
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

static (inside,outside) tcp 172.18.124.99 telnet 10.1.1.6
telnet netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.99 ftp 10.1.1.3
ftp netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 telnet 10.1.1.4
telnet netmask 255.255.255.255 0 0
static (inside,outside) tcp interface telnet 10.1.1.5
telnet netmask 255.255.255.255 0 0
static (inside,outside) tcp interface www 10.1.1.5
www netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 8080 10.1.1.7
www netmask 255.255.255.255 0 0

!--- Use of an outbound ACL is optional.

access-group 100 in interface inside
access-group 101 in interface outside

```

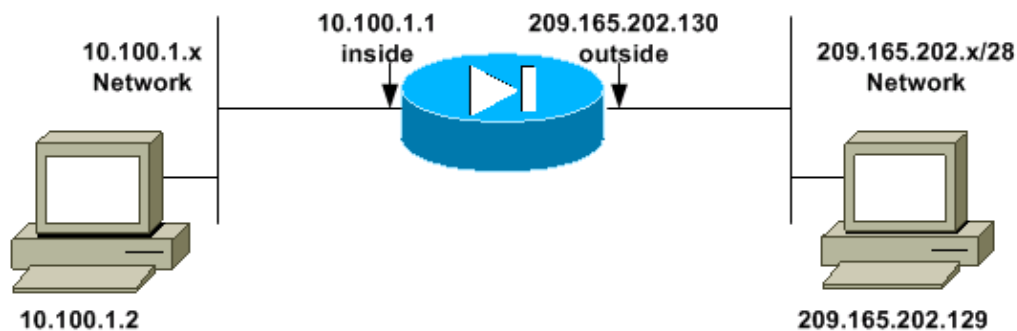
Outside NAT

In PIX 6.2 and later, NAT and PAT can be applied to traffic from an outside, or less secure, interface to an inside (more secure) interface. This is sometimes referred to as "bi-directional NAT."

Outside NAT/PAT is similar to inside NAT/PAT, but the address translation is applied to addresses of hosts that reside on the outer (less secure) interfaces of the PIX. In order to configure dynamic outside NAT, specify the addresses to be translated on the less secure interface and specify the global address or addresses on the inside (more secure) interface. Use the **static** command to specify the one-to-one mapping in order to configure static outside NAT.

After outside NAT is configured, when a packet arrives at the outer (less secure) interface of the PIX, the PIX attempts to locate an existing xlate (address translation entry) in the connections database. If no xlate exists, it searches the NAT policy from the running configuration. If a NAT policy is located, an xlate is created and inserted into the database. The PIX then rewrites the source address to the mapped or global address and transmits the packet on the inside interface. Once the xlate is established, the addresses of any subsequent packets can be quickly translated by consulting the entries in the connections database.

Network Diagram – Outside NAT



In the example:

- Device 10.100.1.2 to NAT to 209.165.202.135 when goes out
- Device 209.165.202.129 to NAT to 10.100.1.3 when comes in
- Other devices on the 10.100.1.x network to NAT to addresses in the 209.165.202.140–209.165.202.141 pool when goes out
- Connectivity from device 209.165.202.129 to device 10.100.1.2 with device 209.165.202.129 seeing the inside device as 209.165.202.135 and device 10.100.1.2 seeing traffic from 209.165.202.129 as coming from 10.100.1.3 (because of the outside NAT)

Access to all 209.165.202.x devices using ACLs or conduits is permitted.

Partial PIX Configuration – Outside NAT

```
Partial PIX Configuration – Outside NAT
ip address outside 209.165.202.130 255.255.255.224
ip address inside 10.100.1.1 255.255.255.0
global (outside) 5 209.165.202.140–209.165.202.141 netmask 255.255.255.224
nat (inside) 5 10.100.1.0 255.255.255.0 0 0
static (inside,outside) 209.165.202.135 10.100.1.2 netmask 255.255.255.255 0 0
static (outside,inside) 10.100.1.3 209.165.202.129 netmask 255.255.255.255 0 0
conduit permit ip 209.165.202.0 255.255.255.0 209.165.202.0 255.255.255.0
```

!--- Or in lieu of conduits, we leave the static statements but have the following.

```
access-list 101 permit ip 209.165.202.0 255.255.255.0 209.165.202.0 255.255.255.0
access-group 101 in interface outside
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

- If you use ICMP pings to test a configured translation, the pings are likely to fail and make it seem as though the translation is not working. By default, the PIX blocks ICMP messages from lower security interfaces to higher security interfaces. This occurs even if the echo-reply is in response to a ping initiated from the inside. As a result, be sure to use another method, like Telnet, to verify your configuration.
- After you make any changes to translation rules on the PIX it is strongly encouraged that the **clear xlate** command be issued. This ensures that any old translations do not interfere with newly configured ones and cause them to operate incorrectly.
- After you configure or change static translations between servers on the inside or DMZ and the outside, it might be necessary to clear the ARP cache of the gateway router or other next-hop device.

Information to Collect if You Open a TAC Case

If you still need assistance after following the troubleshooting steps above and want to open a case with the Cisco TAC, be sure to include the following information for troubleshooting your PIX Firewall.

- Problem description and relevant topology details
- Troubleshoot before you open the case
- Output from the **show tech-support** command
- Output from the **show log** command after running with the **logging buffered debugging** command, or console captures that demonstrate the problem (if available)

Attach the collected data to your case in non-zipped, plain text format (.txt). You can attach information to your case by uploading it using the Case Query Tool (registered customers only). If you cannot access the Case Query Tool, you can send the information in an email attachment to attach@cisco.com with your case number in the subject line of your message.

Related Information

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

