

Cisco Secure PIX Firewall Frequently Asked Questions

Table of Contents

<u>Cisco Secure PIX Firewall Frequently Asked Questions</u>	1
<u>Questions</u>	1
<u>Hardware</u>	1
<u>Software</u>	1
<u>Hardware</u>	2
<u>Software</u>	4
<u>Tools Information</u>	11
<u>Related Information</u>	11

Cisco Secure PIX Firewall Frequently Asked Questions

This document contains frequently asked questions (FAQs) about the Cisco Secure PIX Firewall.

Questions

Hardware

- I am installing a new interface card in my Cisco Secure PIX Firewall. Which slot should I install it in?
- I am trying to install a new interface card in my Cisco Secure PIX Firewall. The card appears to be too big for any of the slots. Do I have the wrong part?
- My Cisco Secure PIX Firewall shipped with two Ethernet cards. I am adding additional interfaces and now it won't boot to the command prompt.
- I need to establish a console connection with my Cisco Secure PIX Firewall. What kind of cable should I use?
- Where is the floppy drive on the PIX 520 model?
- My Cisco Secure PIX Firewall is directly connected to a router, but the link lights won't come on and neither device can ping the other. What's wrong?
- How can I tell the processor speed difference on Gigabit Ethernet cards in the PIX? For example, how can I tell the difference between the PIX-1GE-66 and the PIX-1GE cards?
- If I purchase network cards from a source other than Cisco and use them in the PIX, will they be supported?

Software

Installation and Upgrades

- I'm trying to TFTP pixNNN.exe to my PIX. I keep getting errors saying "bad magic number." What am I doing wrong?
- I am trying to upgrade my software from a floppy and the Cisco Secure PIX Firewall keeps going in a loop every time it tries to read the disk.
- I am installing a new Cisco Secure PIX Firewall that appears to be configured correctly. My LAN used to be connected directly to my Internet router. Now with the PIX in place, my users on the LAN cannot get out. What is wrong?
- I recently added an inside router to connect a second inside network to my Cisco Secure PIX Firewall. Users between the Cisco Secure PIX Firewall and inside router can get to the Internet just fine, but they cannot talk to this new, inside network. Users on the new network can't get past the inside router. What's wrong?
- How do I determine how much flash memory my PIX has?
- When do I need to use a new activation key for the PIX?

Failover

- I have two Cisco Secure PIX Firewalls configured in a failover topology. The Cisco Secure PIX Firewalls keep failing over, back and forth throughout the day. Why is this happening?
- How long is the PIX failover cable and can I use a longer cable?

Other Software Questions

- Is there a way to filter email packets on the Cisco Secure PIX Firewall? For instance, can I have the Cisco Secure PIX Firewall filter the "I luv you" virus?
- I am trying to use Network Address Translation (NAT) on my Cisco Secure PIX Firewall using the NAT/GLOBAL statements and I'm having problems with outside users not being able to access internal hosts consistently. What's wrong?
- I have my web server on the inside statically translated to the outside. Outside users cannot get in. What causes this?
- I have a web server on the inside interface of the Cisco Secure PIX Firewall. It is mapped to an outside public address. I want my inside users to be able to access this server by its DNS name or outside address. How can this be done?
- Does the Cisco Secure PIX Firewall support port mapping?
- Can I map a single, inside address to more than one outside address?
- Can I connect two different ISPs to my Cisco Secure PIX Firewall (for load-balancing)?
- How many PAT addresses can I have on my Cisco Secure PIX Firewall?
- Is there a way to tell the Cisco Secure PIX Firewall to grant more bandwidth to certain users?
- I need to allow my users access to shared folders on my NT Domain from remote locations. How do I do this?
- I'm on the console/Telnet of the PIX and I see an error like "201008: The PIX is disallowing new connections." My PIX will not pass any inbound or outbound traffic. What is wrong?
- When I execute certain commands on the PIX that access the configuration in flash (show config command), I get an error stating "The flash device is in use by another task." What does this mean?
- Can I operate the PIX in a "one armed" configuration?
- Will a PIX operate correctly if plugged into a trunk port on a switch?
- Can I set a timeout on the console port of the PIX?
- I know the PIX can do NAT based on the source address, but can the PIX do NAT based on destination?
- I can't get Network File System (NFS) mounts to work across the PIX. What am I doing wrong?

Tools Information

Related Information

Hardware

Q. I am installing a new interface card in my Cisco Secure PIX Firewall. Which slot should I install it in?

A. Each PIX model is different. Go to the PIX documentation and select your software version. From that page, select **Installation Guide**, and then select **Installing a Circuit Board** for detailed diagrams and instructions.

Q. I am trying to install a new interface card in my Cisco Secure PIX Firewall. The card appears to be too big for any of the slots. Do I have the wrong part?

A. It is normal for some of the gold teeth on the card to extend past the edge of the socket.

Q. My Cisco Secure PIX Firewall shipped with two Ethernet cards. I am adding additional interfaces and now it won't boot to the command prompt.

A. The number of interfaces supported depends on the PIX model, software version, and licensing. The following chart shows the maximum number of interfaces supported in PIX Software version 6.0:

Platform	Interfaces
506	2 (embedded)
515 R	3
515 UR	6
520 conn	6 (connection-based license 128, 1K, UR)
520 UR	6 (feature-based license)
525 R	6
525 UR	8
535 R	8
535 UR	10

Issue a **show version** command to determine the R (restricted) or UR (unrestricted) licensing status.

Q. I need to establish a console connection with my Cisco Secure PIX Firewall. What kind of cable should I use?

A. Use a DB9 to DB9 null modem cable, available from most computer shops. Sometimes the Cisco Secure PIX Firewall will ship with two DB9 to RJ-45 adapters. If you have these adapters, connect one to the Cisco Secure PIX Firewall, and the other to your PC's serial port. Use a *rollover* cable (*not* a crossover cable) to connect between the two RJ-45 adapters. Set your HyperTerminal settings to N81, no flow control, 9600 baud. If you are still having trouble, check your PC COM port configuration and verify it is setup and working properly. If you're confident everything else is setup properly, test it on a router or switch and see if you get a prompt there. For more information, go to the PIX documentation for your PIX software version. From that page, select **Installation Guide**, and then select **Installing Interface Cables** for detailed diagrams and instructions.

Q. Where is the floppy drive on the PIX 520 model?

A. It is located behind a small metal plate on the front in the upper left corner. Remove the two finger tight screws to gain access. For more directions, see Installing a PIX Firewall and click the link to **Installing a PIX 520 or Earlier Model**.

Q. My Cisco Secure PIX Firewall is directly connected to a router, but the link lights won't come on and neither device can ping the other. What's wrong?

A. Make sure you are using a good crossover cable to connect the PIX directly to a router. If you are connecting the PIX to a hub or switch, use a straight through Ethernet cable.

Q. How can I tell the processor speed difference on Gigabit Ethernet cards in the PIX? For example, how can I tell the difference between the PIX-1GE-66 and the PIX-1GE cards?

A. Type **show interface** and look at the following line:

```
Hardware is i82542 rev03 gigabit ethernet, address is XXXX.XXXX.XXXX
```

or

Hardware is i82543 rev02 gigabit ethernet, address is XXXX.XXXX.XXXX
The i82542 represents 33MHz; the i82543 represents 66MHz.

Q. If I purchase network cards from a source other than Cisco and use them in the PIX, will they be supported?

A. No.

Software

Installation and Upgrades

Q. I'm trying to TFTP pixNNN.exe to my PIX. I keep getting errors saying "bad magic number." What am I doing wrong?

A. You should be loading the .bin file, *not* the .exe. The .exe is a self-extracting archive containing the bin file (among other things). **Note:** The bin file is used only for PIX Software versions 5.0.x and earlier. Copy the .exe file to a temporary directory on your PC hard drive, then run the program to extract the files. Then copy the **pixNNN.bin** file over to your TFTP server.

Q. I am trying to upgrade my software from a floppy and the Cisco Secure PIX Firewall keeps going in a loop every time it tries to read the disk.

A. Make sure the disk has been properly formatted with "format A:" and then rawrite used to put the image on the floppy. Try the operation from another PC. **Note:** Upgrade from floppy is valid only for PIX Software versions 5.0.x and earlier.

Q. I am installing a new Cisco Secure PIX Firewall that appears to be configured correctly. My LAN used to be connected directly to my Internet router. Now with the PIX in place, my users on the LAN cannot get out. What is wrong?

A. There are a few different possibilities.

- ◆ Most commonly, this is caused by corrupt Address Resolution Protocol (ARP) tables in the outside or surrounding routers. Remember that routers route to physical MAC addresses, not IP addresses, and they usually cache these layer 2 addresses for several hours. To clear the ARP tables on Cisco equipment, issue the **clear arp-cache** command, or reboot your device.

- ◆ You might also be using the same network IP addresses around your network, the PIX's interfaces and the outside router. While this is acceptable if you never need to directly access your outside router, (that is, you don't need to Telnet to it from inside) it is not practical. If you are unable to use Network Address Translation (NAT) and renumber your network right away, then use an RFC 1918

network scheme on the OUTSIDE segment and set up the routing between the two devices accordingly.

- ◆ You could have inadvertently set up the PIX with an IP address already in use on your network. Check by disconnecting the PIX and ping the addresses you used. You should not get a response since the PIX is out of the network. Check your configuration as well.

- ◆ Make sure the Cisco Secure PIX Firewall has a route outside statement directing all unknown

traffic to the directly-connected Ethernet port of your outside router.

- ◆ Also make sure all inside workstations have the correct gateway (usually the inside interface of the Cisco Secure PIX Firewall, unless there is an inside router involved).
- ◆ If your network is routed on the inside, make sure you have a static gateway route pointed at the PIX. Finally, make sure the PIX has only one default route set. Multiple default routes are no longer supported and will cause inconsistent and undesirable results.

Q. I recently added an inside router to connect a second inside network to my Cisco Secure PIX Firewall. Users between the Cisco Secure PIX Firewall and inside router can get to the Internet just fine, but they cannot talk to this new, inside network. Users on the new network can't get past the inside router. What's wrong?

A. You must either enter a specific route inside statement into the PIX for this new network through the new router, or better yet, enter a specific **route inside** statement for the major network through this router, which allows for future growth.

Let's say your existing network is 192.168.1.0/24 and your new network is 192.168.2.0/24. The Ethernet port of your internal router is 192.168.1.2. The PIX's route configuration would look like this:

```
route inside 192.168.2.0 255.255.255.0 192.168.1.2 1
```

or (the major network):

```
route inside 192.168.0.0 255.255.0.0 192.168.1.2 1
```

Workstations between the Cisco Secure PIX Firewall and router should have their gateway pointing to the router, *not the PIX*. Even though they are directly connected, they will have problems accessing the new internal network if their gateway does not point to the router. The router should have a default gateway directing all unknown traffic to the inside interface of the Cisco Secure PIX Firewall. Installing a route for this new network in the PIX will not work either. The PIX does not route or redirect off the interface it received the packet. Also, make sure your **nat** statement includes the new network or the major net you are adding.

Q. How do I determine how much flash memory my PIX has?

A. If you perform a **show version** command on your PIX, and the flash size is not given in MB, then use the table below to see how much flash your PIX has.

i28F020	512 KB
AT29C040A	2 MB
atmel	2 MB
i28F640J5	8 MB – PIX 506 16 MB – all other PIXes
strata	16 MB

For example, suppose your **show version** command output looked like this:

```
Cisco Secure PIX Firewall Version 5.1(1)
Compiled on Fri 01-Oct-99 13:56 by pixbuild

pix515 up 4 days 22 hours 10 mins 42 secs

Hardware: PIX-515, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300
BIOS Flash AT29C257 @ 0xffffd8000

0: ethernet0: address is 00aa.0000.0037, irq 11
1: ethernet1: address is 00aa.0000.0038, irq 10
2: ethernet2: address is 00a0.c92a.f029, irq 9
3: ethernet3: address is 00a0.c948.45f9, irq 7

Licensed Features:
Failover: Enabled
VPN-DES: Enabled
VPN-3DES: Disabled
Maximum Interfaces: 6

Serial Number: 123 (0x7b)
Activation Key: 0xc5233151 0xb429f6d0 0xda93739a 0xe15cdf51
```

The amount of flash memory would be 16 MB.

Q. When do I need to use a new activation key for the PIX?

A. You need a new activation key when you upgrade a PIX from a restricted software bundle to a bundle which supports additional features, such as more connections, failover, IPSec, or additional interfaces. Also, a new activation key is sometimes necessary after a flash upgrade on a PIX. To request a non-56-bit activation key, send an email to licensing@cisco.com and provide the following information:

- ◆ The PIX serial number (or, if you are doing a flash upgrade, the serial number on the flash card)
- ◆ The result of a **show version** command issued on the PIX

To request a 56-bit activation key, if you are a registered CCO user and you have logged in, you can request a new activation key for 56-bit encryption by completing the form at the following location.

Note: A 56-bit activation key is required for encryption using IPSec.

Failover

Q. I have two Cisco Secure PIX Firewalls configured in a failover topology. The Cisco Secure PIX Firewalls keep failing over, back and forth throughout the day. Why is this happening?

A. For failover to work correctly, it must be properly configured. All interfaces must be configured with an IP address that is unique on each respective subnet, and all interfaces must be physically connected. This includes interfaces you are not currently using. Failover sends a "Hello" packet out each interface, even if they are "shutdown." It expects to get a reply back. If it receives no reply after so many tries, failover activates. You may use crossover cables between the active and standby ports that are not going to be used. Do not use the "shutdown" option when using failover.

Q. How long is the PIX failover cable and can I use a longer cable?

The serial cable Cisco ships is 6 feet long. The pin-out is in the PIX documentation for your PIX software version. Longer cables have not been tested; use of a longer cable is not unsupported. In PIX 6.2 there is a new feature called "LAN failover" that allows the use of a dedicated interface on the PIX as the failover cable. See the PIX 6.2 documentation for more information.

Other Software Questions

Q. Is there a way to filter email packets on the Cisco Secure PIX Firewall? For instance, can I have the Cisco Secure PIX Firewall filter the "I luv you" virus?

A. The Cisco Secure PIX Firewall does not perform content filtering at the Application layer. In other words, we don't inspect the data portion of the TCP packet. Therefore, we cannot filter email content. Most modern-day mail servers can filter at the application layer.

Q. I am trying to use Network Address Translation (NAT) on my Cisco Secure PIX Firewall using the NAT/GLOBAL statements and I'm having problems with outside users not being able to access internal hosts consistently. What's wrong?

A. Dynamic NAT using the **nat** and **global** commands creates a temporary connection/translation state that is ALWAYS built from a higher security level interface to a lower security level interface (inside to outside). The conduits on these dynamically built translations only apply when the connection state is built. Any inside host that the outside needs to initiate a connection into without the inside host first establishing a connection out, must be translated using the **static** command. By statically translating the host, this connection state is permanently mapped and all conduits applied to this static translation remain open at all times. With this in place, IP connections can be initiated from the Internet without fail. With PIX Software versions 5.0.x and later, you can use access lists instead of conduits.

Q. I have my web server on the inside statically translated to the outside. Outside users cannot get in. What causes this?

A. Static mapping makes the translation/connection possible, but by default, the Cisco Secure PIX Firewall denies ALL inbound connection attempts unless explicitly permitted. This "permission" is granted by applying a conduit to the static translation. Conduit statements tell the Cisco Secure PIX Firewall whom on the Internet you want to permit where and on what protocol and port. With PIX Software versions 5.0.x and later, you can use access lists instead of conduits.

Q. I have a web server on the inside interface of the Cisco Secure PIX Firewall. It is mapped to an outside public address. I want my inside users to be able to access this server by its DNS name or outside address. How can this be done?

A. The rules of TCP do not allow you to do this, but there are good workarounds. For example, let's imagine that your web server's real IP address is 10.10.10.10 and public address is 99.99.99.99. DNS resolves 99.99.99.99 to www.mydomain.com. If your inside host (say 10.10.10.25) attempts to go to www.mydomain.com, the browser will resolve that to 99.99.99.99. Then the browser sends that packet off to the PIX, which in turn sends it off to the Internet router. The Internet router already has a directly connected subnet of 99.99.99.x, so it assumes that packet is not intended for it but instead a directly connected host and drops this packet. To get around this issue your inside host either must resolve www.mydomain.com to its real 10.10.10.10 address or you must take the outside segment off the 99.99.99.x network so the router can be configured to route this packet back to the PIX. If your DNS resides outside the PIX (or across one of its DMZs) you may use the **alias** command on

the Cisco Secure PIX Firewall to fix the DNS packet to make it resolve to the 10.10.10.10 address. Make sure you reboot your PCs to flush the DNS cache after making this change. (Test by pinging `www.mydomain.com` before and after the `alias` command is applied to make sure the resolution changes from the 99.99.99.99 to 10.10.10.10 address.)

If you have your own DNS server inside your network, this obviously won't work because the DNS lookup never transverses the PIX, so there's nothing to fix. In this case, configure you local DNS accordingly or use local 'hosts' files on your PC's to resolve this name. The other option is actually better because it is more reliable. Take the 99.99.99.x subnet off the PIX and router. Choose an RFC1918 numbering scheme not being used internally (or on any perimeter PIX interface). Then put a route statement back to the PIX for this network and remember to change your PIX default route outside to the new IP address on the router. The outside router will receive this packet and route it back to the PIX based on its routing table. The router will no longer ignore this packet, because it has no interfaces configured on that network.

For more information on the `alias` command, see Understanding the `alias` Command for the Cisco Secure PIX Firewall.

Q. Does the Cisco Secure PIX Firewall support port mapping?

A. The PIX supports inbound port redirection with PIX Software version 6.0. Earlier PIX Software versions do not support port mapping.

Q. Can I map a single, inside address to more than one outside address?

A. The Cisco Secure PIX Firewall only allows a single one-to-one translation for a local (inside) host. If you have more than two interfaces on the Cisco Secure PIX Firewall, you can translate a local address to different addresses on each respective interface but only one translation per interface is allowed for each address. Likewise, you cannot do a static mapping of a single outside address to multiple local addresses.

Q. Can I connect two different ISPs to my Cisco Secure PIX Firewall (for load-balancing)?

A. No, you cannot load-balance on the PIX. The Cisco Secure PIX Firewall is designed to handle only one default route. Connecting two ISPs to a single PIX means that the the firewall would need to make routing decisions at a much more intelligent level. Instead, use a gateway router outside the PIX so that the PIX continues to send all of its traffic to one router. That router can then route/load-balance between the two ISPs. An alternative is to have two routers outside the PIX using Hot Standby Router Protocol (HSRP) and set the default gateway of the PIX to be the virtual HSRP address.

Q. How many PAT addresses can I have on my Cisco Secure PIX Firewall?

A. Beginning with PIX Software release 5.2, you can have multiple PAT addresses per interface. Earlier PIX Software releases do not support multiple PAT addresses per interface.

Q. Is there a way to tell the Cisco Secure PIX Firewall to grant more bandwidth to certain users?

A. No.

Q. I need to allow my users access to shared folders on my NT Domain from remote locations. How do I do this?

A. Microsoft's NetBios protocol allows file and printer sharing. Enabling NetBios across the Internet does not meet the security requirements of most networks. Further, NetBios is difficult to configure using NAT. While Microsoft makes this more secure using encrypted technologies, which work seamlessly with the PIX, it is possible to open the necessary ports.

In brief, you will need to set static translations for ALL hosts requiring access and conduits (or access lists in PIX Software 5.0.x and later) for TCP ports 135 and 139 and UDP ports 137 and 138. You must either use a WINS server to resolve the translated addresses to NetBios names or local properly configured LMHOSTS file on all your remote client machines. If using WINS, each and every host must have a static WINS entry for BOTH the local and translated addresses of the hosts being accessed. Using LMHOSTS should have both as well, unless your remote users are never connected to your inside network (for example, laptop computers). Your WINS server must be accessible to the Internet with the **static** and **conduit** commands and your remote hosts must be configured to point at this WINS server. Finally, Dynamic Host Configuration Protocol (DHCP) leases must be set to never expire, or better yet, statically configure the IP addresses on the hosts needing to be accessed from the Internet.

A safer and more secure way to do this is to configure either Point-to-Point Tunneling Protocol (PPTP) or IPsec encryption. Consult with your network security and design specialists for further details on the security ramifications.

Q. I'm on the console/Telnet of the PIX and I see an error like "201008: The PIX is disallowing new connections." My PIX will not pass any inbound or outbound traffic. What is wrong?

A. This error means that you are doing "reliable TCP syslog" to a PIX Firewall Syslog Server (PFSS) software on a Windows NT system and that the system is not responding to PIX's syslog messages. To correct this problem, try one of the following options:

- ◆ Go to the NT server running PFSS and correct the problem that is keeping that server from accepting TCP syslog data from the PIX. The problem is usually a full hard drive or an issue with the syslog service not running.
- ◆ Disable the TCP syslog feature and return to the standard syslog utility udp. This can be done on the command line of the PIX with the **logging host [in_if_name] ip_address [protocol/port]** command. Simply type **logging host ip_address**, then retype the command without the **protocol/port** portion. It will default to the standard protocol/port of UDP/514.

Note: The "reliable TCP syslog" feature of PIX and PFSS was intended to create a security policy that basically says: "If the PIX can't log it, then don't do it." If this is *not* what you intended, then you should not run "reliable TCP syslog." Instead, use the standard syslog abilities that will not block inbound/outbound traffic if the syslog server is unavailable.

Q. When I execute certain commands on the PIX that access the configuration in flash (show config command), I get an error stating "The flash device is in use by another task." What does this mean?

A. An example of this error is the following.

```
pixfirewall# write mem
Building configuration...
Cryptochecksum: 386bb809 e4d28698 91990edb 8483760c
The flash device is in use by another task.
[FAILED]
Type help or '?' for a list of available commands.
pixfirewall#
```

What this means is that there is another session on the PIX where someone has used a **write terminal** or similar command that will access the flash and it is sitting at a "--more--" prompt.

In order to verify this, execute the **who** command while logged onto the console of the PIX.

```
PIX# who
0: 14.36.1.66
PIX#
```

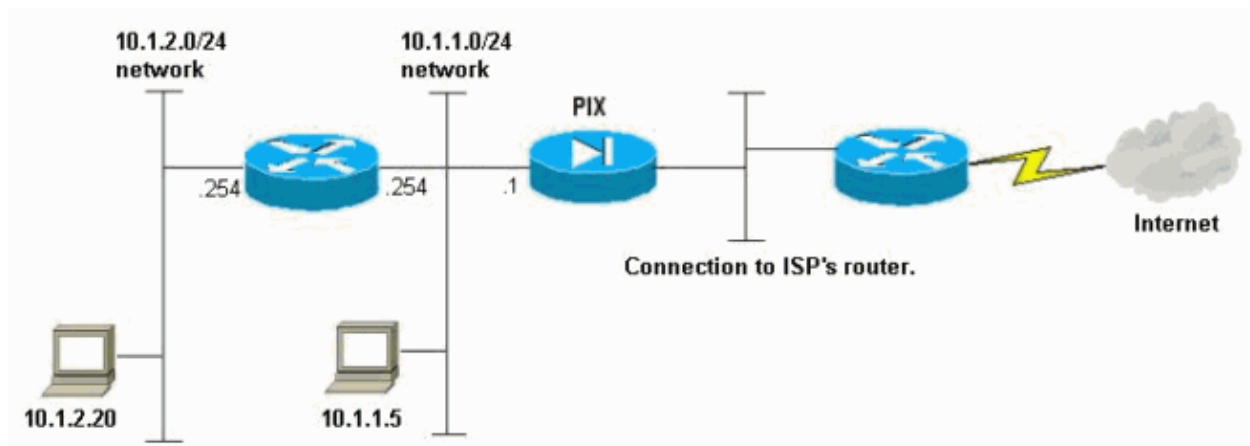
In this example, we see that a user from 14.36.1.66 is logged into the PIX via Telnet. We can use the **kill** command to forcefully log that user out.

```
PIX# kill ?
usage: kill <telnet_id>
PIX# kill 0
PIX# who
PIX#
```

The user has been logged out and now you can perform your flash operation. In the slight chance that this does not work, a reboot of the PIX will also solve the problem.

Q. Can I operate the PIX in a "one armed" configuration?

A. No, the PIX cannot operate in a "one-armed" configuration because of the Adaptive Security Algorithm under which the PIX operates. For more information, see Understanding PIX Firewall. For example, if you have a PIX with two interfaces (inside and outside) and on the inside interface there is a 10.1.1.0/24 network. Off this network there is a router with the 10.1.2.0/24 network connected to it. Then suppose there is a server on the inside interface which is 10.1.1.5. This host has a default gateway of the inside interface of the PIX (10.1.1.1). In this scenario, assume that the PIX has the correct routing information, such as route inside 10.1.2.0 255.255.255.0 10.1.1.254 where 10.1.1.254 is the router's IP address. You might think that the 10.1.1.5 host could send a packet to 10.1.2.20 and this packet would go to the PIX, get redirected to the router at 10.1.1.254, and go on to the destination host, but this is not the case. The PIX does not send ICMP redirects like a router. Also, the PIX does not allow a packet to leave an interface from which it came. So assuming the 10.1.1.5 host sent a packet with a destination address of 10.1.2.20 to the PIX's inside interface, the PIX would drop that packet because it was destined to go out the same interface (inside interface) on which it came. This is true for any PIX interface, not just the inside interface. In this scenario, the solution is for the 10.1.1.5 host to set its default gateway to be the router's interface (10.1.1.254), and then have a default gateway on the router point to the PIX (10.1.1.1).



Q. Will a PIX operate correctly if plugged into a trunk port on a switch?

A. No, the PIX does not understand ISL or 802.1Q encapsulation.

Q. Can I set a timeout on the console port of the PIX?

A. No, this cannot be done on the PIX.

Q. I know the PIX can do NAT based on the source address, but can the PIX do NAT based on destination?

A. Only in PIX version 6.2 and later can you NAT based on destination. See the PIX 6.2 documentation for more information.

Q. I can't get Network File System (NFS) mounts to work across the PIX. What am I doing wrong?

A. The PIX does not support portmapper (port 111) over TCP. You should configure your NFS to use UDP instead.

Tools Information

For additional resources, refer to Cisco TAC Tools for Security Technologies.

Related Information

- **PIX Top Issues**
 - **Documentation for PIX Firewall**
 - **More PIX Firewall Technical Tips**
 - **PIX Command Reference**
 - **Security Product Field Notices (including PIX)**
 - **PIX Product Support Page**
 - **Requests for Comments (RFCs)**
-

All contents are Copyright © 1992—2002 Cisco Systems Inc. All rights reserved. Important Notices and Privacy Statement.