

Cisco Secure PIX Firewall Frequently Asked Questions

Document ID: 15247

Questions

Introduction
Hardware
Software – Installation and Upgrades
Software – Failover
Additional Software Questions
Related Information

Introduction

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

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

Hardware

Q. I want to install 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 does not boot to the command prompt.

A. The number of interfaces supported depends on the PIX model, software version, and licensing. Refer to the PIX documentation to find out about maximum physical interfaces, and maximum VLAN interfaces that can be configured on PIX 6.3 (latest version as of the writing of this document).

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 ships with two DB9 to RJ-45 adapters. If you have these adapters, connect one to the Cisco Secure PIX Firewall, and the other to the serial port of your PC. 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 still have trouble, check your PC COM port configuration and verify it is setup and works properly. If you are confident everything else is setup properly, test it on a router or switch and see if you get a prompt there. Refer to the PIX documentation for your PIX software version for more information. 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. Refer to Installing a PIX 520 or Earlier Model for more directions.

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

A. Make sure that you use a good crossover cable to connect the PIX directly to a router. If you connect 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 this 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 33 MHz and the i82543 represents 66 MHz.

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

A. No.

Q. When the PIX boots, the PIX reports the network interface card (NIC) interrupt request (IRQs) and some of them are used twice (duplicates). Does this cause a problem?

A. These messages are normal and can be ignored:

```
4: ethernet2: address is 00e0.0000.05cb, irq 11
5: ethernet3: address is 00e0.0000.05ca, irq 11
```

Q. When the PIX with Gigabit Ethernet network interface cards (NICs) boot, the PIX reports the NIC interrupt requests (IRQs) as being "irq 255." Does this cause a problem?

A. This message is normal and can be ignored:

```
0: gb-ethernet0: address is 0003.0000.1e75, irq 255
```

Q. What are the default hardware configurations for the PIX?

Platform	501	506	515 (R/UR)	515E (R/UR)	520	525 (R/UR)	535 (R/UR)
CPU	AMD 133	PI 200	PI 200	PII 433	PII 350	PIII 600	PIII 1GH
RAM (MB)	8	32	32/64	32/64	128	128/256	512/1024

Q. Can I upgrade the PIX bios?

A. No.

Software – Installation and Upgrades

Q. When I try to TFTP pixNNN.exe to my PIX, I receive errors that state "bad magic number." What am I doing wrong?

A. You need to load the .bin file, *not* the .exe file. The .exe file is a self-extracting archive that contains 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 and run the program to extract the files. Then copy the **pixNNN.bin** file over to your TFTP server.

Q. When I try to upgrade my software from a floppy, the Cisco Secure PIX Firewall keeps going in a loop every time it tries to read the disk. What is wrong?

A. Make sure the disk is properly formatted (use the DOS command **format A:**), then use **rawrite** to put the image on the floppy. If the process fails, try the operation from a different PC.

Note: Upgrade from a floppy disk 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. Issue the **clear arp-cache** command, or reboot your device in order to clear the ARP tables on Cisco equipment.
- ◆ 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 do not 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 that directs 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 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 successfully get to the Internet, but they cannot talk to this new, inside network. Users on the new network are unable to get past the inside router. What is wrong?

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

For example, if 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 route configuration of the PIX appears similar to 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
```

Work stations between the Cisco Secure PIX Firewall and router should have their gateway point to the router, not the PIX. Even though they are directly connected, they have problems accessing the new internal network if their gateway does not point to the router. The router should have a default gateway that directs all unknown traffic to the inside interface of the Cisco Secure PIX Firewall. The installation of a route for this new network in the PIX does not work either. The PIX does not route or redirect off the interface it received the packet. Unlike a router, the PIX cannot route packets back through the same interface where the packet was initially received. 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 this table 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, if your **show version** command output looks 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 is 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.

In order to request a non-56-bit activation key, send an email to licensing@cisco.com and provide this 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
- ◆ Your current PIX software version
- ◆ Type of License required (DES, 3DES, Restricted to Unrestricted).
- ◆ Either the Entitlement number, Purchase Order number, Sales Order number, or PAK number
- ◆ Your full company name and address

Go to the PIX 56-bit License Upgrade Key (registered customers only) page to request a 56-bit activation key.

Go to the Cisco ASA 3DES/AES License Registration (registered customers only) page to request a AES/3DES activation key.

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

Q. Can the PIX pass IPX or AppleTalk traffic?

A. No, the PIX is an IP-only Firewall.

Q. Does the PIX support secondary addressing on interfaces?

A. Unlike Cisco IOS®, the PIX does not support secondary addressing on interfaces.

Q. Does the PIX support 802.1Q on its interfaces?

A. Yes, in PIX 6.3 a new feature is added, where PIX can create logical interfaces. Each logical interface corresponds to a VLAN in the switch. Refer to Using VLANs with the Firewall for more information.

Q. Does the PIX support SSH?

A. Yes, refer to SSH – Inside or Outside which provides you with a step-by-step procedure to configure SSH. PIX uses SSH version 1.

Software – Failover

Q. I have two Cisco Secure PIX Firewalls configured in a Failover topology. The Cisco Secure PIX Firewall continues to fail over, back and forth throughout the day. Why does this happen?

A. For Failover to work correctly, it must be properly configured. Before version 5.1, 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 do not currently use. With version 5.1 and later, you can shutdown an unused interface. However, you need to shutdown the same interface number on both PIXes. Before version 5.1, Failover sends a Hello packet out each interface, even if they are shutdown. It expects to receive a reply back. If it receives no reply after several attempts, Failover activates. Also check if the primary PIX can ping the Failover interfaces, if not, check if the interfaces are up. Also, if they are

connected via a switch, check the switch interfaces.

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

A. The serial cable Cisco ships is six feet long. The pin-out is in the Cisco PIX Firewall 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. Refer to the PIX Firewall Version 6.2 documentation for more information.

Q. Can a VLAN interface be used in Failover?

A. Both the physical and logical VLAN are supported by Failover. The restriction is that the **failover lan interface** and **failover link** commands are unable to use a logical VLAN interface.

Q. Is the DHCP server feature supported with Failover?

A. No, the DHCP server is not supported with Failover, nor is a PIX configured to obtain an IP address via DHCP (since you need the **failover interface-name ip address** command for Failover to be configured).

Q. I have two Cisco Secure PIX Firewalls configured in a Failover topology. One has an Unrestricted license and the other has a Failover license. What happens if both PIX Firewalls lose power and only the Failover unit boots back up?

A. The PIX Firewall with the Failover license is intended to be used solely for failover and not in standalone mode. When both PIX Firewalls lose power and only the Failover unit boots back up, it is as if the Failover unit is used in standalone mode. If a Failover unit is used in standalone mode, the unit reboots at least once every 24 hours until the unit is returned to failover duty, when it senses the presence of the primary PIX Firewall.

Additional Software Questions

Q. Does the PIX forward IGMP traffic?

A. PIX Firewall software version 6.2 enables you to statically configure multicast routes or use an Internet Group Management Protocol (IGMP) helper address for forwarding IGMP reports and leave announcements.

This list summarizes multicast support in this release.

- ◆ Access list filters can be applied to multicast traffic to permit or deny specific protocols and ports.
- ◆ Network Address Translation (NAT) and Port Address Translation (PAT) can be performed on the multicast packet source addresses only.
- ◆ Multicast data packets with destination addresses in the 224.0.0.0/24 address range are not forwarded. However, everything else in the 224.0.0.0/8 address range is forwarded.
- ◆ IGMP packets for address groups within the 224.0.0.0 through 224.0.0.255 range are

not forwarded because these addresses are reserved for protocol use.

- ◆ NAT is not performed on IGMP packets. When IGMP forwarding is configured, the PIX forwards the IGMP packets (report and leave) with the IP address of the helper interface as the source IP address.

Q. Does the PIX have a troubleshooting feature that can grab the packet trace to see packet contents in detail?

A. PIX Firewall software version 6.2 supports packet capture to sniff or "see" any traffic accepted or blocked by the PIX. Once the packet information is captured, you can view the information on the console, transfer it to a file over the network using a TFTP server, or access it through a web browser using Secure HTTP. Note that the PIX does not capture traffic unrelated to itself on the same network segment. In addition, this packet capture feature does not include file system, DNS name resolution, or promiscuous mode support.

Q. Does the PIX support OSPF?

A. PIX Firewall implementation in version 6.3 code supports intra-area, inter-area, and external routes. This release also supports the distribution of static routes to Open Shortest Path First (OSPF) processes and route redistribution between OSPF processes.

Q. Does the PIX support PPPoE?

A. PIX Firewall software version 6.2 supports Point-to-Point Protocol over Ethernet (PPPoE). The support for L2TP/PPTP/PPPoE has been removed from the PIX Firewall software version 7.0 and later. (PPPoE provides a standard method for using PPP authentication over an Ethernet network and is used by many Internet service providers (ISPs) to grant client machines access to their networks, commonly through DSL.) PPPoE is supported on the outside interfaces of the Cisco PIX 500 Series Security Appliance.

Q. Is SFTP supported through the PIX?

A. No. In a typical FTP connection, either the client or the server must tell the other what port to use for data transfer. The PIX is able to inspect this conversation and open that port. However, with SFTP this conversation is encrypted and the PIX is unable to determine what ports to open and the SFTP connection ultimately fails.

One possible workaround in this situation is to use an SFTP client that supports the use of a "clear data channel." With this option enabled, the PIX should be able to determine what port needs to be opened.

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, it does not inspect the data portion of the TCP packet. Therefore, it cannot filter email content. Most modern-day mail servers can filter at the application layer.

Q. When I try to use Network Address Translation (NAT) on my Cisco Secure PIX Firewall using the NAT/GLOBAL statements, I have problems with outside users not being able to access internal hosts consistently. What is 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 when you apply 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, imagine that your web server's real IP address is 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 (for example, 10.10.10.25) attempts to go to www.mydomain.com, the browser resolves 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. It therefore assumes that packet is not intended for it but instead a directly connected host and drops this packet. In order 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 can 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 you make 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 does not work because the DNS lookup never transverses the PIX, so there is nothing to fix. In this case, configure you local DNS accordingly or use local 'hosts' files on your PCs to resolve this name. The other option

is better because it is more reliable. Take the 99.99.99.x subnet off the PIX and router. Choose an RFC 1918 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 receives this packet and routes 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.

PIX 6.2 introduces a new feature called Bidirectional NAT, which offers the functionality of the **alias** command and more.

Refer to Understanding the **alias** Command for the Cisco Secure PIX Firewall for more information on the **alias** command.

Refer to Using Outside NAT in the PIX command reference for more information on the Bidirectional NAT feature.

Note: If you run PIX/ASA software version 7.x it is recommended not to use the **alias** command. The outside NAT with DNS Switch is recommended instead. Refer to the DNS Inspection Section of Applying Application Layer Protocol Inspection.

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. When you connect two ISPs to a single PIX, it means that the Firewall needs 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. Alternatively, (if possible) you can use Open Shortest Path First (OSPF) which supports load balancing among a maximum of three peers on a single interface.

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

A. In PIX Software release 5.2 and later, 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. The Microsoft 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 that require 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 you use WINS, each and every host must have a static WINS entry for BOTH the local and translated addresses of the hosts that are accessed. The use of 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. You can also statically configure the IP addresses on the hosts that need 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 am on the console/Telnet of the PIX and I see an error like "201008: The PIX is disallowing new connections." My PIX does 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 does not respond to the syslog messages of the PIX. Try one of these options to correct this problem:

- ◆ Go to the NT server that runs PFSS and correct the problem that keeps the 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. Type **logging host ip_address**, then retype the command without the **protocol/port** portion. It defaults to the standard protocol/port of UDP/514.

Note: The "reliable TCP syslog" feature of PIX and PFSS is intended to create a security policy that states "If the PIX cannot log it, then do not do it." If this is not what you intended, then you should not run "reliable TCP syslog." Instead, use the standard syslog abilities that do 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 that states "The Flash device is in use by another task." What does this mean?

A. This output shows an example of this error:

```
pixfirewall#write memory
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#
```

This means that there is another session on the PIX where someone has used a **write terminal** or similar command that accesses 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, you see that a user from 14.36.1.66 is logged into the PIX via Telnet. You can use the **kill** command to forcefully log that user out.

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

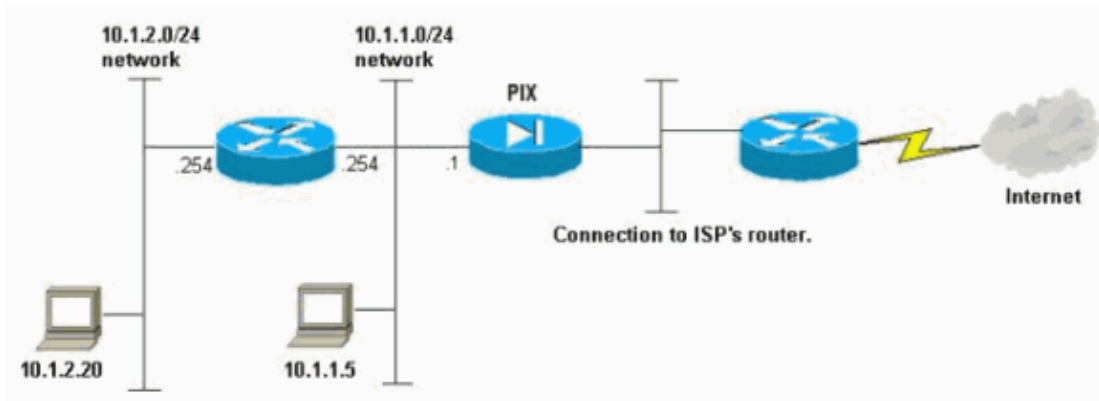
The user has been logged out and now you can perform your Flash operation. In the slight chance that this does not work, a reboot of the PIX also solves the problem.

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. Refer to Understanding PIX Firewall for more information.

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. Next, assume 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 IP address of the router. You might think that the 10.1.1.5 host can send a packet to 10.1.2.20 and this packet goes to the PIX, gets redirected to the router at 10.1.1.254, and goes on to the destination host. However, 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, with the assumption that the 10.1.1.5 host sent a packet with a destination address of 10.1.2.20 to the inside interface of the PIX, 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 interface of the router (10.1.1.254), and then have a default gateway on the router point to

the PIX (10.1.1.1).



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

A. Yes, however the PIX must be configured for 802.1Q encapsulation. This is addressed Does the PIX support 802.1Q on its interfaces?.

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

A. Yes, this is a new feature of version 6.3 . Refer to the **console timeout** command.

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. Refer to the PIX Firewall Version 6.2 documentation for more information.

Q. I cannot 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.

Q. Does the PIX do time-based access control lists (ACLs)?

A. Unlike Cisco IOS, the PIX does not do time-based ACLs. If you authenticate users who access the PIX and the authentication server supports limiting users to particular times of the day, then the PIX honors those user rejections.

Q. Can I customize the text of the syslog messages the PIX sends?

A. The syslog messages the PIX generates are hardcoded into the operating system, and it is not possible to customize them.

Q. Can the PIX do name resolution?

A. While a properly configured PIX does permit Domain Name System (DNS) traffic through to allow for inside and outside devices to do DNS, the PIX itself does not resolve names.

Q. I see "connection denied" messages in the PIX syslog, as well as denies for Telnets to the PIX interfaces. But I do not see denies for other traffic to the PIX interfaces. Is this normal?

A. Before version 6.2.2, the **deny** messages for traffic to the PIX interfaces are limited to denied Telnets or port TCP/23. In 6.2.3 and 6.3.1, new syslog messages are added of which syslog ID 710003 handles denied traffic to the PIX interface itself.

Q. I cannot ping from the network inside the PIX to the PIX outside interface, nor from the network outside the PIX to the PIX inside interface. Is this normal?

A. Yes, unlike Cisco IOS, the PIX does not respond to ICMP requests to the interfaces on the "far side" of the device that pings the PIX.

Q. Can the PIX act as an NTP server?

A. No.

Q. Is it possible to change the default ports used for IPsec on the PIX?

A. No.

Q. Does the PIX support Dynamic Domain Name Services (DDNS)?

A. No.

Q. A Cisco PIX Firewall is configured to communicate with a Cisco Works Auto-Update server and all traffic has stopped passing through it. Why does this happen and how do I fix this?

A. The Cisco PIX Firewall stops all new connections if it is configured to communicate with Auto Update server and it has not been contacted for a period of time. An administrator can change the value of the timeout period using the **auto-update timeout period** command.

The Auto Update specification provides the infrastructure necessary for remote management applications to download PIX Firewall configurations, software images, and to perform basic monitoring from a centralized location. Failure to communicate with the server causes the PIX to stop passing all traffic.

Q. I am unable to access the inside interface of the PIX when connected via a VPN tunnel. How can I do this?

A. The inside interface of the PIX cannot be accessed from the outside, and vice-versa, unless the **management-access** command is configured in global configuration mode. Once **management-access** is enabled, Telnet, SSH, or HTTP access must still be configured for the desired hosts.

```
pix(config)#management-access inside
pix(config)#show running-config management-access
management-access inside
```

Related Information

- [PIX Support Page](#)
 - [Documentation for PIX Firewall](#)
 - [PIX Command References](#)
 - [Requests for Comments \(RFCs\)](#)
 - [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: Sep 26, 2008

Document ID: 15247
