



D through F Commands

debug

Debug packets or ICMP tracings through the PIX Firewall. The **debug** command provides information which helps troubleshoot protocols operating with and through the PIX Firewall. (Configuration mode.)

debug crypto ca [*level*]

no debug crypto ca [*level*]

debug crypto ipsec [*level*]

no debug crypto ipsec [*level*]

debug crypto isakmp [*level*]

no debug crypto isakmp [*level*]

debug dhcpc detail | error | packet

no debug dhcpc detail | error | packet

debug dhcpd event | packet

no debug dhcpd event | packet

debug fover *option*

no debug fover *option*

debug h323 h225 [*asn* | *event*]

no debug h323 h225 [*asn* | *event*]

debug h323 h245 [asn | event]

no debug h323 h245 [asn | event]

debug h323 ras [asn | event]

no debug h323 ras [asn | event]

debug icmp trace

no debug icmp trace

**debug packet *if_name* [src *source_ip* [netmask *mask*]] [dst *dest_ip* [netmask *mask*]]
[[proto icmp] | [proto tcp [sport *src_port*] [dport *dest_port*]] |
[proto udp [sport *src_port*] [dport *dest_port*]] [rx | tx | both]**

**no debug packet *if_name* [src *source_ip* [netmask *mask*]] [dst *dest_ip* [netmask *mask*]]
[[proto icmp] | [proto tcp [sport *src_port*] [dport *dest_port*]] |
[proto udp [sport *src_port*] [dport *dest_port*]] [rx | tx | both]**

debug pdm history

[no] debug pdm history

debug ppp error | io | uauth | upap | chap | negotiation

no debug ppp error | io | uauth | upap | chap | negotiation

debug rip

no debug rip

debug rtsp

no debug rtsp

debug sip

no debug sip

debug sqlnet

no debug sqlnet

debug ssh

no debug ssh

debug ssl [cypher | device]

no debug ssl [cypher | device]

debug vpdn event | error | packet

no debug vpdn event | error | packet

show debug

Syntax Description

crypto ca	Display information about certification authority (CA) traffic.
<i>level</i>	The level of debugging feedback. The higher the level number, the more information is displayed. The default <i>level</i> is 1. The levels correspond to the following events: <ul style="list-style-type: none"> • Level 1: Interesting events • Level 2: Normative and interesting events • Level 3: Diminutive, normative, and interesting events Refer to the “Examples” section at the end of this command page for an example of how the debugging level appears within the show debug command.
crypto ipsec	Display information about IPSec traffic.
crypto isakmp	Display information about IKE traffic.
dhcpc detail	Display detailed information about the DHCP client packets.
dhcpc error	Display error messages associated with the DHCP client.
dhcpc packet	Display packet information associated with the DHCP client.
dhcpcd event	Display event information associated with the DHCP server.
dhcpcd packet	Display packet information associated with the DHCP server.
fover <i>option</i>	Display failover information. Refer to Table 5-1 for the <i>options</i> .
h323	Display information about the packet-based multimedia communications systems standard.
h225 asn	Display the output of the decoded PDUs.
h225 events	Display the events of the H.225 signalling, or turn both traces on.

h245 asn	Display the output of the decoded PDUs.
h245 events	Display the events of the H.245 signalling, or turn both traces on.
ras asn	Display the output of the decoded PDUs.
ras events	Display the events of the RAS signalling, or turn both traces on.
icmp	Display information about ICMP traffic.
packet	Display packet information.
<i>if_name</i>	Interface name from which the packets are arriving; for example, to monitor packets coming into the PIX Firewall from the outside, set <i>if_name</i> to outside .
src source_ip	Source IP address.
netmask mask	Network mask.
dst dest_ip	Destination IP address.
proto icmp	Display ICMP packets only.
proto tcp	Display TCP packets only.
sport src_port	Source port. See the “Ports” section in “Chapter 1, “Using PIX Firewall Commands” for a list of valid port literal names.
dport dest_port	Destination port.
debug pdm history	Turns on the PDM history metrics debugging information. The no version of this command disables PDM history metrics debugging.
proto udp	Display UDP packets only.
rx	Display only packets received at the PIX Firewall.
tx	Display only packets that were transmitted from the PIX Firewall.
both	Display both received and transmitted packets.
sqlnet	Debug SQL*Net traffic.
ppp	Debug L2TP or PPTP traffic, which is configured with the vpdn command.
ppp error	Display L2TP or PPTP PPP virtual interface error messages.
ppp io	Display the packet information for L2TP or PPTP PPP virtual interface.
ppp uauth	Display the L2TP or PPTP PPP virtual interface AAA user authentication debugging messages.
upap	Display PAP authentication.
chap	Display CHAP/MS-CHAP authentication.
negotiation	Equivalent of the error , uauth , upap and chap debug command options.
sip	Debug the fixup Session Initiation Protocol (SIP) module.
ssh	Debug information and error messages associated with the ssh command.
ssl	Debug information and error messages associated with the ssl command.
cypher	Display information about the cipher negotiation between the HTTP server and the client.
device	Display information about the SSL device including session initiation and ongoing status.
vpdn event	Display L2TP or PPTP tunnel event change information.
vpdn error	Display L2TP or PPTP protocol error messages.
vpdn packet	Display L2TP or PPTP packet information about PPTP traffic.

Usage Guidelines

The **debug** command lets you view debug information. The **show debug** command displays the current state of tracing. You can debug the contents of network layer protocol packets with the **debug packet** command.

When creating your digital certificates, use the **debug crypto ca** command to ensure that the certificate is created correctly. Important error messages only display when the **debug crypto ca** command is enabled. For example, if you enter an Entrust fingerprint value incorrectly, the only warning message that indicates the value is incorrect appears in the **debug crypto ca** command output.

Output from the **debug crypto ipsec** and **debug crypto isakmp** commands does not display in a Telnet console session.

The **debug dhcpc detail** command displays detailed packet information about the DHCP client. The **debug dhcpc error** command displays DHCP client error messages. The **debug dhcpc packet** command displays packet information about the DHCP client. Use the **no** form of the **debug dhcpc** command to disable debugging.

The **debug dhcpcd event** command displays event information about the DHCP server. The **debug dhcpcd packet** command displays packet information about the DHCP server. Use the **no** form of the **debug dhcpcd** commands to disable debugging.

The **debug h323** command allows you to debug H.323 connections. Use the **no** form of the command to disable debugging. This command works when the **fixup protocol h323** command is enabled.

**Note**

The **debug h323** command, particularly the **debug h323 h225 asn**, **debug h323 h245 asn**, and **debug h323 ras asn** commands, might delay the sending of messages and cause slower performance in a real-time environment.

The **debug icmp trace** command shows ICMP packet information, the source IP address, and the destination address of packets arriving, departing, and traversing the PIX Firewall including pings to the PIX Firewall unit's own interfaces.

The **debug sqlnet** command reports on traffic between Oracle SQL*Net clients and servers through the PIX Firewall.

The **debug ssh** command reports on information and error messages associated with the **ssh** command.

The **debug ppp** and **debug vpdn** commands provide information about PPTP traffic. PPTP is configured with the **vpdn** command.

Use of the **debug** commands can slow down busy networks.

[Table 5-1](#) lists the options for the **debug fover** command.

Table 5-1 *debug fover command Options*

Option	Description
cable	Failover cable status
fail	Failover internal exception
fmsg	Failover message
get	IP network packet received
ifc	Network interface status trace
open	Failover device open
put	IP network packet transmitted

Table 5-1 *debug fover command Options (continued)*

Option	Description
rx	Failover cable receive
rxdump	Cable rcv message dump (serial console only)
rxip	IP network failover packet received
tx	Failover cable transmit
txdump	Cable xmit message dump (serial console only)
txip	IP network failover packet transmit
verify	Failover message verify
switch	Failover Switching status

Trace Channel Feature

The **debug packet** command sends its output to the Trace Channel. All other **debug** commands do not. Use of Trace Channel changes the way you can view output on your screen during a PIX Firewall console or Telnet session.

If a **debug** command does not use Trace Channel, each session operates independently, which means any commands started in the session only appear in the session. By default, a session not using Trace Channel has output disabled by default.

The location of the Trace Channel depends on whether you have a simultaneous Telnet console session running at the same time as the console session, or if you are using only the PIX Firewall serial console:

- If you are only using the PIX Firewall serial console, all **debug** commands display on the serial console.
- If you have both a serial console session and a Telnet console session accessing the console, then no matter where you enter the **debug** commands, the output displays on the Telnet console session.
- If you have two or more Telnet console sessions, the first session is the Trace Channel. If that session closes, the serial console session becomes the Trace Channel. The next Telnet console session that accesses the console will then become the Trace Channel.

The **debug** commands, except the debug crypto commands, are shared between all Telnet and serial console sessions.

**Note**

The downside of the Trace Channel feature is that if one administrator is using the serial console and another administrator starts a Telnet console session, the serial console **debug** command output will suddenly stop without warning. In addition, the administrator on the Telnet console session will suddenly be viewing **debug** command output, which may be unexpected. If you are using the serial console and **debug** command output is not appearing, use the **who** command to see if a Telnet console session is running.

Additional debug Command Information**Note**

Use of the **debug packet** command on a PIX Firewall experiencing a heavy load may result in the output displaying so fast that it may be impossible to stop the output by entering the **no debug packet** command from the console. You can enter the **no debug packet** command from a Telnet session.

**Note**

To let users ping through the PIX Firewall, add the **access-list** *acl_grp* **permit icmp any any** command statement to the configuration and bind it to each interface you want to test with the **access-group** command. This lets pings go outbound and inbound.

To stop a **debug packet trace** command, enter the following command:

```
no debug packet if_name
```

Replace *if_name* with the name of the interface; for example, **inside**, **outside**, or a perimeter interface name.

To stop a **debug icmp trace** command, enter the following command:

```
no debug icmp trace
```

Examples

The following is partial sample output from the **debug dhcpc packet** and the **debug dhcpc detail** commands. The **ip address dhcp setroute** command was configured after entering the **debug dhcpc** commands to obtain debugging information.

```
debug dhcpc packet
debug dhcpc detail
ip address outside dhcp setroute

DHCP:allocate request
DHCP:new entry. add to queue
DHCP:new ip lease str = 0x80ce8a28
DHCP:SDiscover attempt # 1 for entry:
Temp IP addr:0.0.0.0 for peer on Interface:outside
Temp sub net mask:0.0.0.0
    DHCP Lease server:0.0.0.0, state:1 Selecting
    DHCP transaction id:0x8931
    Lease:0 secs, Renewal:0 secs, Rebind:0 secs
    Next timer fires after:2 seconds
    Retry count:1   Client-ID:cisco-0000.0000.0000-outside

DHCP:SDiscover:sending 265 byte length DHCP packet
DHCP:SDiscover 265 bytes
DHCP Broadcast to 255.255.255.255 from 0.0.0.0
DHCP client msg received, fip=10.3.2.2, fport=67
DHCP:Received a BOOTREP pkt
DHCP:Scan:Message type:DHCP Offer
DHCP:Scan:Server ID Option:10.1.1.69 = 450A44AB
DHCP:Scan:Server ID Option:10.1.1.69 = 450A44AB
DHCP:Scan:Lease Time:259200
DHCP:Scan:Subnet Address Option:255.255.254.0
DHCP:Scan:DNS Name Server Option:10.1.1.70, 10.1.1.140
DHCP:Scan:Domain Name:example.com
DHCP:Scan:NBNS Name Server Option:10.1.2.228, 10.1.2.87
DHCP:Scan:Router Address Option:10.3.2.1
DHCP:rcvd pkt source:10.3.2.2, destination: 255.255.255.255
...
```

The following example executes the **debug icmp trace** command:

```
debug icmp trace
```

When you ping a host through the PIX Firewall from any interface, trace output displays on the console. The following example shows a successful ping from an external host (209.165.201.2) to the PIX Firewall unit's outside interface (209.165.201.1).

```
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
NO DEBUG ICMP TRACE
ICMP trace off
```

This example shows that the ICMP packet length is 32 bytes, the ICMP packet identifier is 1, and the ICMP sequence number. The ICMP sequence number starts at 0 and is incremented each time a request is sent.

The following is sample output from the **show debug** command output:

```
show debug
debug ppp error
debug vpdn event
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto ca 1
debug icmp trace
debug packet outside both
debug sqlnet
```

The preceding sample output includes the **debug crypto** commands.

You can debug the contents of packets with the **debug packet** command:

```
debug packet inside
----- PACKET -----
-- IP --
4.3.2.1 ==> 255.3.2.1
  ver = 0x4      hlen = 0x5      tos = 0x0      tlen = 0x60
  id = 0x3902   flags = 0x0      frag off=0x0
  ttl = 0x20    proto=0x11     chksum = 0x5885
-- UDP --
      source port = 0x89      dest port = 0x89
      len = 0x4c      checksum = 0xa6a0
-- DATA --
00000014:                                00 01 00 00 |
....
00000024: 00 00 00 01 20 45 49 45 50 45 47 45 47 45 46 46 | ..
.. EIEPEGEGEFF
00000034: 43 43 4e 46 41 45 44 43 41 43 41 43 41 43 41 43 | CC
NFAEDCACACACAC
00000044: 41 43 41 41 41 00 00 20 00 01 c0 0c 00 20 00 01 | AC
AAA.. .....
00000054: 00 04 93 e0 00 06 60 00 01 02 03 04 00          | ..
....\.....
----- END OF PACKET -----
```

This display lists the information as it appears in a packet.

The following is sample output from the **show debug** command:

```
show debug
debug icmp trace off
debug packet off
debug sqlnet off
```

dhcpd

The **dhcpd** command controls the DHCP server feature. (Configuration mode.)

dhcpd address *ip1*[-*ip2*] [*if_name*]

no dhcpd address *ip1*[-*ip2*] [*if_name*]

dhcpd auto_config [*client_ifx_name*]

no dhcpd auto_config [*client_ifx_name*]

dhcpd dns *dns1* [*dns2*]

no dhcpd dns *dns1* [*dns2*]

dhcpd wins *wins1* [*wins2*]

no dhcpd wins *wins1* [*wins2*]

dhcpd lease *lease_length*

no dhcpd lease *lease_length*

dhcpd domain *domain_name*

no dhcpd domain *domain_name*

dhcpd enable [*if_name*]

no dhcpd enable [*if_name*]

show dhcpd [*binding*|*statistics*]

clear dhcpd [*binding*|*statistics*]

debug dhcpd event

no debug dhcpd event

debug dhcpd packet

no debug dhcpd packet

dhcpd ping_timeout *timeout*

no dhcpd ping_timeout *timeout*

Syntax Description

address <i>ip1</i> [<i>ip2</i>]	The IP pool address range. The size of the pool is limited to 32 addresses for the PIX 506 platform and 256 addresses for other platforms. Note that if the address pool range is larger than 253 addresses, the netmask of the PIX Firewall interface cannot be a Class C (for example 255.255.255.0) and hence needs to be something larger, for example, 255.255.254.0.
<i>if_name</i>	Name of the PIX Firewall interface. The default is the inside interface. Currently, the PIX Firewall DHCP server daemon can only be enabled on the inside interface.
dns <i>dns1</i> [<i>dns2</i>]	The IP addresses of the DNS servers for the DHCP client. The second server address is optional.
auto_config	Enable PIX Firewall to automatically configure DNS, WINS and domain name values from the DHCP client to the DHCP server. If the user also specifies dns , wins , and domain parameters, then the CLI parameters overwrite the auto_config parameters.
<i>client_ifx_name</i>	This optional argument supports only the outside interface at this time. When more interfaces are supported, this argument will specify which interface supports the DHCP auto_config feature.
wins <i>wins1</i> [<i>wins2</i>]	The IP addresses of the Microsoft NetBios name servers (WINS server). The second server address is optional.
lease <i>lease_length</i>	The length of the lease, in seconds, granted to DHCP client from the DHCP server. The lease indicates how long the client can use the assigned IP address. The default is 3600 seconds. The minimum lease length is 300 seconds, and the maximum lease length is 2,147,483,647 seconds.
domain <i>domain_name</i>	The DNS domain name. For example, example.com .
binding	The binding information for a given server IP address and its associated client hardware address and lease length.
statistics	Statistical information, such as address pool, number of bindings, malformed messages, sent messages, and received messages.
<i>ping_timeout</i>	Allows the configuration of the timeout value of a ping, in milliseconds, before assigning an IP address to a DHCP client.

Usage Guidelines

A DHCP server provides network configuration parameters to a DHCP client. Support for the DHCP server within the PIX Firewall means the PIX Firewall can use the DHCP to configure connected PC clients. This DHCP feature is designed for the remote home or branch office that will establish a connection to an enterprise or corporate network. See the *Cisco PIX Firewall and VPN Configuration Guide* for information on how to implement the DHCP server feature into the PIX Firewall.

**Note**

The PIX Firewall DHCP server does not support **BOOTP** requests and **failover** configurations.

The **dhcpd address** command specifies the DHCP server address pool. The address pool of a PIX Firewall DHCP server must be within the same subnet of the PIX Firewall interface that is enabled. In other words, the client must be physically connected to the subnet of a PIX Firewall interface. The size of the pool is currently limited to 32 addresses for the PIX 506 platform, and 256 addresses for other

platforms. The default for the PIX Firewall interface name is the **inside** interface, which is the only interface currently supported. The **no dhcpd address** command removes the DHCP server address pool you configured.

The **dhcpd dns** command specifies the IP address(es) of the DNS server(s) for DHCP client. You have the option to specify two DNS servers. The **no dhcpd dns** command removes the DNS IP address(es) from your configuration.

The **dhcpd wins** command specifies the addresses of the WINS server for the DHCP client. The **no dhcpd dns** command removes the WINS server IP address(es) from your configuration.

The **dhcpd lease** command specifies the length of the lease in seconds granted to the DHCP client. This lease indicates how long the DHCP client can use the assigned IP address the DHCP granted. The **no dhcpd lease** command removes the lease length that you specified from your configuration and replaces this value with the default value of 3600 seconds.

The **dhcpd domain** command specifies the DNS domain name for the DHCP client. For example, **example.com**. The **no dhcpd domain** command removes the DNS domain server from your configuration.

The **dhcpd enable** command enables the DHCP daemon to begin to listen for the DHCP client requests on the DHCP-enabled interface. The **no dhcpd enable** command disables the DHCP server feature on the specified interface.

DHCP must be enabled to use this command. Use the **dhcpd enable** command to turn on DHCP.


Note

With version 5.2 or higher, the PIX Firewall DHCP server daemon can only be enabled on the **inside** interface, and does not support clients that are not directly connected to the **inside** interface.

The **show dhcpd** command displays **dhcpd** commands, binding and statistics information associated with all of the **dhcpd** commands.

The **clear dhcpd** command clears all of the **dhcpd** commands, binding, and statistics information.

The **debug dhcpd event** command displays event information about the DHCP server. The **debug dhcpd packet** command displays packet information about the DHCP server. Use the **no** form of the **debug dhcpd** commands to disable debugging.

Examples

The following partial configuration example shows use of the **dhcpd address**, **dhcpd dns**, and **dhcpd enable** commands. In this example, an address pool for the DHCP clients is defined, a DNS server address is specified for the DHCP client, and the inside interface of the PIX Firewall is enabled for the DHCP server function.

```
dhcpd address 10.0.1.100-10.0.1.108
dhcpd dns 209.165.200.226
dhcpd enable
```

The following partial configuration example shows how to define a DHCP pool of 256 addresses and use the **auto_config** command to configure the DNS, WINS and DOMAIN parameters. Note the netmask of the inside interface is 255.255.254.0.

```
ip address inside 10.0.1.1 255.255.254.0
dhcpd address 10.0.1.2-10.0.1.257
dhcpd auto_config
dhcpd enable
```

The following partial configuration example shows how to use three new features that are associated with each other: DHCP server, DHCP client, and PAT using interface IP to configure a PIX Firewall in a small office, home office (SOHO) environment:

```
! use dhcp to configure the outside interface and default route
ip address outside dhcp setroute
! enable dhcp server daemon on the inside interface
ip address inside 10.0.1.2 255.255.255.0
dhcpd address 10.0.1.101-10.0.1.110
dhcpd dns 209.165.201.2 209.165.202.129
dhcpd wins 209.165.201.5
dhcpd lease 3000
dhcpd domain example.com
dhcpd enable
! use outside interface IP as PAT global address
nat (inside) 1 0 0
global (outside) 1 interface
```

The following is sample output for the **show dhcpd** command:

```
show dhcpd
dhcpd address 10.0.1.100-10.0.1.108 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd dns 192.23.21.23
dhcpd enable inside
```

The following is sample output for the **show dhcpd binding** command:

```
show dhcpd binding
IP Address Hardware Address Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

The following is sample output for the **show dhcpd statistics** command:

```
show dhcpd statistics
Address Pools 1
Automatic Bindings 1
Expired Bindings 1
Malformed messages 0

Message Received
BOOTREQUEST 0
DHCPDISCOVER 1
DHCPREQUEST 2
DHCPDECLINE 0
DHCPRELEASE 0
DHCPINFORM 0

Message Sent
BOOTREPLY 0
DHCPOFFER 1
DHCPACK 1
DHCPNAK 1
```

Related Commands

- [ip address](#)

disable

Exit privileged mode and return to unprivileged mode. (Privileged mode.)

disable

Usage Guidelines

The **disable** command exits privileged mode and returns you to unprivileged mode. Use the **enable** command to return to privileged mode.

Examples

The following example shows how to exit privileged mode:

```
pixfirewall# disable
pixfirewall>
```

domain-name

Change the IPSec domain name. (Configuration mode.)

domain-name *name*

Syntax Description

name A domain name.

Usage Guidelines

The **domain-name** command lets you change the IPSec domain name.



Note

The change of the domain name causes the change of the fully qualified domain name. Once the fully qualified domain name is changed, delete the RSA key pairs using the **ca zeroize rsa** command, and delete related certificates using the **no ca identity ca_nickname** command.

Examples

The following example shows use of the **domain-name** command:

```
domain-name example.com
```

dynamic-map

Create, view, or delete a dynamic crypto map entry. (Configuration mode.)

clear dynamic-map

show dynamic-map

Usage Guidelines

The **clear dynamic-map** command removes **dynamic-map** commands from the configuration. The **show dynamic-map** command lists the **dynamic-map** commands in the configuration.



Note

The **dynamic-map** command is the same as the **crypto dynamic-map** command. Refer to the [crypto dynamic-map](#) command page for more information such as examples and other command options.

eeprom

The **eeprom** command displays and updates the contents of the EEPROM non-volatile storage devices used for low level Ethernet interface configuration information for certain PIX 535 units.

show eeprom

eeprom update



Note

This command applies only to PIX 525 models with serial numbers 44480380055 through 44480480044.

Syntax Description

show eeprom	Displays the current EEPROM register settings. See the Examples section for more information.
eeprom update	Modifies the EEPROM register settings if necessary after checking the contents of EEPROM registers 6 and 10 to ensure they contain the hexadecimal values 0x4701 and 0x40c0, respectively. If these registers contain different values, then all EEPROM register settings, except the MAC address registers, which were not affected by the problem, are reset to the correct values.

Usage Guidelines

The **eeprom** commands added in version 5.2(4) and later fixes a caveat (CSCds76768) involving corruption of the eeprom on the onboard Ethernet interfaces. For additional information, see the December 20, 2000 Field Notice, "Cisco Secure PIX Firewall: PIX-525 Ethernet EEPROM Programming Issue." This field notice is available at the following website:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_field_notice09186a00800949c4.shtml

The problem is summarized as follows:

If you configure the onboard Ethernet interfaces (ethernet0 and ethernet1) on a PIX 525 with a serial number of 44480380055 through 44480480044 to full duplex, interface errors and throughput reductions may occur. If you configure the interfaces to half duplex or to auto-sense, the speed and duplex function normally without error.

The **eeprom** command is designed to fix the problem and performs the same function as the "eedisk" utility without requiring access to the ROM monitor mode. The two variants of the **eeprom** command are the **show eeprom** command and **eeprom update** command.

The **eeprom update** command performs the same function as the "eedisk" utility without requiring access to the ROM monitor mode, whereas the **show eeprom** command indicates whether the Ethernet EEPROM programming is correct or not.

The **show eeprom** command displays the current EEPROM setting, and the **eeprom update** command modifies the settings if necessary. If the **eeprom** command does update the EEPROM settings, a reboot of the PIX Firewall is recommended.

The **eeprom** command verifies the EEPROM register settings and updates them if they are not set to the recommended values. The **eeprom** command does not update the settings if they are correct and does not recommend a reboot unless the settings are changed.

The **eeprom update** command checks the contents of EEPROM registers 6 and 10 to ensure they contain the hexadecimal values 0x4701 and 0x40c0, respectively. If these registers contain different values, then all EEPROM register settings except the MAC address registers, which were not affected by the problem causing CSCds76768, are reset to the correct values.

Each register is 16 bits. The correct register values are as follows:

Register	Name	Value
Register 0 to 2	MAC address	Differs on each system (unique)
Register 3	Compatibility Bits	0x3
Register 5	Controller and connector type	0x201
Register 6	Onboard PHY type	0x4701
Register 10	Onboard Prom ID	0x40C0
Register 12	Vendor ID, where 8086 is Intel	0x8086

Examples

The **show eeprom** command will display the current EEPROM register settings:

```
pix525# show eeprom
eeprom settings for ifc0:
 reg0: 0x5000
 reg1: 0xfe54
 reg2: 0x65f6
 reg3: 0x3
 reg5: 0x201
 reg6: 0x4702
 reg10: 0x40c0
 reg12: 0x8086
eeprom settings for ifc1:
 reg0: 0x5000
 reg1: 0xfe54
 reg2: 0x66f6
 reg3: 0x3
 reg5: 0x201
 reg6: 0x4702
 reg10: 0x40c0
 reg12: 0x8086reg12: 0x8086
```

If the command is run on a unit that is not a PIX 525, the following will be seen:

```
pix515# show eeprom
This unit is not a PIX-525.
Type help or '?' for a list of available commands.
```

If the update needs to be run on the PIX 525, the **eeprom update** command returns the following:

```

pix525# eeprom update
eeprom settings on ifc0 are being reset to defaults:
  reg0: 0x5000
  reg1: 0xfe54
  reg2: 0x65f6
  reg3: 0x3
  reg5: 0x201
  reg6: 0x4701
  reg10: 0x40c0
  reg12: 0x8086
eeprom settings on ifc1 are being reset to defaults:
  reg0: 0x5000
  reg1: 0xfe54
  reg2: 0x66f6
  reg3: 0x3
  reg5: 0x201
  reg6: 0x4701
  reg10: 0x40c0
  reg12: 0x8086
*** WARNING! *** WARNING! *** WARNING! *** WARNING! ***
The system should be restarted as soon as possible.
*** WARNING! *** WARNING! *** WARNING! *** WARNING! ***

```

If the update has been run successfully, the **eeprom** command output will appear as follows:

```

pix525# eeprom update
eeprom settings on ifc0 are already up to date:
  reg0: 0x5000
  reg1: 0xfe54
  reg2: 0x65f6
  reg3: 0x3
  reg5: 0x201
  reg6: 0x4701
  reg10: 0x40c0
  reg12: 0x808
eeprom settings on ifc1 are already up to date:
  reg0: 0x5000
  reg1: 0xfe54
  reg2: 0x66f6
  reg3: 0x3
  reg5: 0x201
  reg6: 0x4701
  reg10: 0x40c0
  reg12: 0x80866

```

enable

Start privileged mode. (Unprivileged mode.)

enable

Usage Guidelines

The **enable** command starts privileged mode. The PIX Firewall prompts you for your privileged mode password. By default, a password is not required—press the **Enter** key at the Password prompt to start privileged mode. Use the **disable** command to exit privileged mode. Use the **enable password** command to change the password.

Examples

The following example shows how to start privileged mode with the **enable** command and then configuration mode with the **configure terminal** command.

```
pixfirewall> enable
Password:
pixfirewall# configure terminal
pixfirewall(config)#
```

enable password

Set the privileged mode password. (Privileged mode.)

enable password *password* [**encrypted**]

show enable password

Syntax Description

<i>password</i>	A case-sensitive password of up to 16 alphanumeric characters.
encrypted	Specifies that the password you entered is already encrypted. The <i>password</i> must be 16 characters in length.

Usage Guidelines

The **enable password** command changes the privileged mode password, for which you are prompted after you enter the **enable** command. When the PIX Firewall starts and you enter privileged mode, the password prompt appears. There is not a default password (press the **Enter** key at the Password prompt). The **show enable password** command lists the encrypted form of the password.

You can return the enable password to its original value (press the **Enter** key at prompt) by entering the following command:

```
pixfirewall# enable password
pixfirewall#
```



Note

If you change the password, write it down and store it in a manner consistent with your site's security policy. Once you change this password, you cannot view it again. Also, ensure that all who access the PIX Firewall console are given this password.

Use the **passwd** command to set the password for Telnet access to the PIX Firewall console. The default **passwd** value is **cisco**.

See the **passwd** command page for more information.

Examples

The following examples show how to start privileged mode with the **enable** command, change the enable password with the **enable password** command, enter configuration mode with the **configure terminal** command, and display the contents of the current configuration with the **write terminal** command:

```
pixfirewall> enable
Password:
pixfirewall# enable password w0ttal1fe
pixfirewall# configure terminal
pixfirewall(config)# write terminal
Building configuration...
...
enable password 2oifudsaoid.9ff encrypted
...
```

The following example shows the use of the **encrypted** option:

```
enable password 1234567890123456 encrypted
show enable password
enable password 1234567890123456 encrypted
```

```
enable password 1234567890123456
show enable password
enable password feCkwUGktTCAgIbD encrypted
```

established

Permit return connections on ports other than those used for the originating connection based on an established connection. (Configuration mode.)

established *dest_protocol dest_port [src_port] [permitto protocol dport [-dport]] [permitfrom protocol sport[-sport]]*

no established *dest_protocol dest_port [src_port] [permitto protocol dport [-dport]] [permitfrom protocol sport[-sport]]*

clear established

show established

Syntax Description

<i>dest_protocol</i>	The destination protocol (TCP or UDP only).
<i>dest_port</i>	The destination port used for the established connection lookup. This is the originating traffic's destination port and may be specified as 0 if the protocol does not specify which destination port(s) will be used. Use wildcard ports (0) only when necessary.
<i>src_port</i>	The source port used for the established connection lookup. This is the originating traffic's source port and may be specified as 0 if the protocol does not specify which source port(s) will be used. Use wildcard ports (0) only when necessary.
permitto	Used to specify the return traffic's protocol and to which destination port(s) the traffic will be permitted.
<i>dport</i>	The destination port(s) to which the return traffic is permitted.
permitfrom	Used to specify the return traffic's protocol and from which source port(s) the traffic will be permitted.
<i>sport</i>	The source port(s) from which the return traffic is permitted.
<i>protocol</i>	Specifies the protocol, TCP or UDP only.

Usage Guidelines

The **established** command allows outbound connections return access through the PIX Firewall. This command works with two connections, an original connection outbound from a network protected by the PIX Firewall and a return connection inbound between the same two devices on an external host.

The first protocol, destination port, and optional source port specified are for the initial outbound connection. The **permitto** and **permitfrom** options refine the return inbound connection.



Note

We recommend that you always specify the **established** command with the **permitto** and **permitfrom** options. Without these options, the use of the **established** command opens a security hole that can be exploited for attack of your internal systems. See the “Security Problem” section that follows for more information.

The **permitto** option allows you to specify a new protocol or port for the return connection at the PIX Firewall.

The **permitfrom** option allows you to specify a new protocol or port at the remote server.

The **no established** command disables the **established** feature.

The **show established** command shows the **established** commands in the configuration.

The **clear established** command removes all **establish** command statements from your configuration.

**Note**

For the **established** command to work properly, the client must listen on the port specified with the **permitto** option.

You can use the **established** command with the **nat 0** command statement (where there are no **global** command statements).

**Note**

The **established** command cannot be used with Port Address Translation (PAT).

The **established** command works as shown in the following format:

```
established A B C permitto D E permitfrom D F
```

This command works as though it were written “If there exists a connection between two hosts using protocol A from src port B destined for port C, permit return connections through the PIX Firewall via protocol D (D can be different from A), if the source port(s) correspond to F and the destination port(s) correspond to E.”

For example:

```
established tcp 6060 0 permitto tcp 6061 permitfrom tcp 6059
```

In this case, if a connection is started by an internal host to an external host using TCP source port 6060 and any destination port, the PIX Firewall permits return traffic between the hosts via TCP destination port 6061 and TCP source port 6059.

For example:

```
established udp 0 6060 permitto tcp 6061 permitfrom tcp 1024-65535
```

In this case, if a connection is started by an internal host to an external host using UDP destination port 6060 and any source port, the PIX Firewall permits return traffic between the hosts via TCP destination port 6061 and TCP source port 1024-65535.

Security Problem

The **established** command has been enhanced to optionally specify the destination port used for connection lookups. Only the source port could be specified previously with the destination port being 0 (a wildcard). This addition allows more control over the command and provides support for protocols where the destination port is known, but the source port is not.

The **established** command can potentially open a large security hole in the PIX Firewall if not used with discretion. Whenever you use this command, if possible, also use the **permitto** and **permitfrom** options to indicate ports to which and from which access is permitted. Without these options, external systems to which connections are made could make unrestricted connections to the internal host involved in the connection. The following are examples of potentially serious security violations that could be allowed when using the **established** command.

For example:

```
established tcp 0 4000
```

In this example, if an internal system makes a TCP connection to an external host on port 4000, then the external host could come back in on any port using any protocol:

```
established tcp 0 0 (Same as previous releases established tcp 0 command.)
```

Examples

The following example occurs when a local host 10.1.1.1 starts a TCP connection on port 9999 to a foreign host 209.165.201.1. The example allows packets from the foreign host 209.165.201.1 on port 4242 back to local host 10.1.1.1 on port 5454.

```
established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

The next example allows packets from foreign host 209.165.201.1 on any port back to local host 10.1.1.1 on port 5454:

```
established tcp 9999 permitto tcp 5454
```

XDMCP Support

PIX Firewall now provides support for XDMCP (X Display Manager Control Protocol) with assistance from the **established** command.



Note

XDMCP is on by default, but will not complete the session unless the **established** command is used.

Example:

```
established tcp 0 6000 to tcp 6000 from tcp 1024-65535
```

Will allow internal XDMCP equipped (UNIX or ReflectionX) hosts to access external XDMCP equipped XWindows servers. UDP/177 based XDMCP negotiates a TCP based XWindows session and subsequent TCP back connections will be permitted. Because the source port(s) of the return traffic is unknown, the *src_port* field should be specified as 0 (wildcard). The destination port, *dest_port*, will typically be 6000; the well-known XServer port. The *dest_port* should be 6000 + *n*; where *n* represents the local display number. Use the following UNIX command to change this value.

```
setenv DISPLAY hostname:displaynumber.screennumber
```

The **established** command is needed because many TCP connections are generated (based on user interaction) and the source port for these connection is unknown. Only the destination port will be static. The PIX Firewall does XDMCP fixups transparently. No configuration is required, but the **established** command is necessary to accommodate the TCP session. Be advised that using applications like this through the PIX Firewall may open up security holes. The XWindows system has been exploited in the past and newly introduced exploits are likely to be discovered.

exit

Exit an access mode. (All modes.)

exit

Usage Guidelines

Use the **exit** command to exit from an access mode. This command is the same as **quit**.

Examples

The following example shows how to exit configuration mode and then privileged mode:

```
pixfirewall(config)# exit  
pixfirewall# exit  
pixfirewall>
```

failover

Change or view access to the optional failover feature. (Configuration mode.)

```

failover [active]

no failover

failover ip address if_name ip_address

failover link [stateful_if_name]

no failover link

failover poll seconds

failover replicate http

no failover replicate http

failover reset

no failover active

show failover

```

Syntax Description

active	Make a PIX Firewall the active unit. Use this command when you need to force control of the connection back to the unit you are accessing, such as when you want to switch control back from a unit after you have fixed a problem and want to restore service to the primary unit. Either enter no failover active on the secondary unit to switch service to the primary or failover active on the primary unit.
<i>if_name</i>	Interface on which the standby unit resides.
<i>ip_address</i>	The IP address used by the standby unit to communicate with the active unit. Use this IP address with the ping command to check the status of the standby unit. This address must be on the same network as the system IP address. For example, if the system IP address is 192.159.1.3, set the failover IP address to 192.159.1.4.
link	Specify the interface where a fast LAN link is available for Stateful Failover.
<i>stateful_if_name</i>	In addition to the failover cable, a dedicated fast LAN link is required to support Stateful Failover. Do not use FDDI because of its blocksize or Token Ring because Token Ring requires additional time to insert into the ring. The default interface is the highest LAN port with failover configured.
poll <i>seconds</i>	Specify how long failover waits before sending special failover “hello” packets between the primary and standby units over all network interfaces and the failover cable. The default is 15 seconds. The minimum value is 3 seconds and the maximum is 15 seconds. Set to a lower value for Stateful Failover. With a faster poll time, PIX Firewall can detect failure and trigger failover faster. However, faster detection may cause unnecessary switchovers when the network is temporarily congested or a network card starts slowly.

reset	Force both units back to an unfailed state. Use this command once the fault has been corrected. The failover reset command can be entered from either unit, but it is best to always enter commands at the active unit. Entering the failover reset command at the active unit will “unfail” the standby unit.
replicate http	The [no] failover replicate http command allows the stateful replication of HTTP sessions in a Stateful Failover environment. The no form of this command disables HTTP replication in a Stateful Failover configuration. When HTTP replication is enabled, the show failover command displays the failover replicate http configuration.

Usage Guidelines

Use the **failover** command without an argument after you connect the optional failover cable between your primary PIX Firewall and a secondary PIX Firewall. The default configuration has failover enabled. Enter **no failover** in the configuration file for the PIX Firewall if you will not be using the failover feature. Use the **show failover** command to verify the status of the connection and to determine which unit is active.



Note

See Chapter 8, “Using PIX Firewall Failover,” in the *Cisco PIX Firewall and VPN Configuration Guide* for configuration information.

For Failover, PIX Firewall requires any unused interfaces be given IP addresses and connected to the standby unit for use in receiving failover checkup messages.

Set the Stateful Failover dedicated interface to 100 Mbps full duplex using the **100full** option to the **interface** command.

Use the **failover active** command to initiate a failover switch from the standby unit, or the **no failover active** command from the active unit to initiate a failover switch. You can use this feature to return a failed unit to service, or to force an active unit off line for maintenance. Because the standby unit does not keep state information on each connection, all active connections will be dropped and must be re-established by the clients.

Use the **failover link** command to enable Stateful Failover. The Stateful Failover interface can be either Ethernet or Token Ring interfaces. FDDI interfaces are supported for non-Stateful Failover interfaces. Enter the **no failover link** command to disable the Stateful Failover feature.

If a failover IP address has not been entered, **show failover** will display 0.0.0.0 for the IP address, and monitoring of the interfaces will remain in “waiting” state. A failover IP address must be set for failover to work.

The **failover poll seconds** command allows you to determine how long failover waits before sending special failover “hello” packets between the primary and standby units over all network interfaces and the failover cable. The default is 15 seconds. The minimum value is 3 seconds and the maximum is 15 seconds. Set to a lower value for Stateful Failover. With a faster poll time, PIX Firewall can detect failure and trigger failover faster. However, faster detection may cause unnecessary switchovers when the network is temporarily congested or a network card starts slowly.

When a failover cable connects two PIX Firewall units, the **no failover** command now disables failover until you enter the **failover** command to explicitly enable failover. Previously, when the failover cable connected two PIX Firewall units and you entered the **no failover** command, failover would automatically re-enable after 15 seconds.

If you reboot the PIX Firewall without entering the **write memory** command and the failover cable is connected, failover mode automatically enables.

You can also view the information from the **show failover** command using SNMP. Refer to “Using the Firewall and Memory Pool MIBs” in Chapter 7, “PIX Firewall System Management” of the *Cisco PIX Firewall and VPN Configuration Guide* for more information.

A failover configuration example is provided in Chapter 8, “Using PIX Firewall Failover” of the *Cisco PIX Firewall and VPN Configuration Guide*.

Examples

The following sample output shows that failover is enabled, and that the primary unit state is active:

```

show failover
pixfirewall (config)# show failover
  Failover On
  Cable status:Normal
  Reconnect timeout 0:00:00
  Poll frequency 15 seconds
  failover replication http
    This host:Secondary - Standby
      Active time:0 (sec)
      Interface FailLink (172.16.31.2):Normal
      Interface 4th (172.16.16.1):Normal
      Interface int5 (192.168.168.1):Normal
      Interface intf2 (192.168.1.1):Normal
      Interface outside (209.165.200.225):Normal
      Interface inside (10.1.1.4):Normal
    Other host:Primary - Active
      Active time:242145 (sec)
      Interface FailLink (172.16.31.1):Normal

```

The rest of command output is omitted.

The “Cable status” has these values:

- Normal—Indicates that the active unit is working and that the standby unit is ready.
- Waiting—Indicates that monitoring of the other unit’s network interfaces has not yet started.
- Failed—Indicates that the PIX Firewall has failed.

The “Stateful Obj” has these values:

- Xmit—Indicates the number of packets transmitted.
- Xerr—Indicates the number of transmit errors.
- Rcv—Indicates the number of packets received.
- Rcv—Indicates the number of receive errors.

Each row is for a particular object static count:

- General—The sum of all stateful objects.
- Sys cmd—Refers to logical update system commands, such as **login** or **stay alive**.
- Up time—The value for PIX Firewall up time which the active PIX Firewall unit will pass on to the standby unit.
- Xlate—The PIX Firewall translation information.
- Tcp conn—The PIX Firewall dynamic TCP connection information.
- Udp conn—The PIX Firewall dynamic UDP connection information.
- ARP tbl—The PIX Firewall dynamic ARP table information.

- RIF tbl—The dynamic router table information.

You can view the IP addresses of the standby unit with the **show ip address** command:

show ip address

System IP Addresses:

```
ip address outside 209.165.201.2 255.255.255.224
ip address inside 192.168.2.1 255.255.255.0
ip address perimeter 192.168.70.3 255.255.255.0
```

Current IP Addresses:

```
ip address outside 209.165.201.2 255.255.255.224
ip address inside 192.168.2.1 255.255.255.0
ip address perimeter 192.168.70.3 255.255.255.0
```

The Current IP Addresses are the same as the System IP Addresses on the failover active unit. When the primary unit fails, the Current IP Addresses become those of the standby unit.

The standby Logical Update Statistics output that displays when you use the **show failover** command only describes Stateful Failover. The “xerrs” value does not indicate an error in failover, but rather the number of packet transmit errors.

filter

Enable or disable outbound URL or HTML object filtering. (Configuration mode.)

filteractivex *port local_ip mask foreign_ip mask*

no filteractivex *port local_ip mask foreign_ip mask*

filterjava *port[-port] local_ip mask foreign_ip mask*

no filterjava *port[-port] local_ip mask foreign_ip mask*

filterurl *port|except local_ip local_mask foreign_ip foreign_mask [allow]*

no filterurl *port | except [local_ip local_mask foreign_ip foreign_mask]*

clear filter

show filter

Syntax Description

activex	Block outbound ActiveX, Java applets, and other HTML <object> tags from outbound packets.
java	Block Java applets returning to the PIX Firewall as a result of an outbound connection.
url	Filter Universal Resource Locators (URLs) from data moving through the PIX Firewall.
except	filter url only: Create an exception to a previous filter condition.
<i>port</i>	The Web traffic port. Typically, this is port 80, but other values are accepted. The http literal can be used for port 80.
<i>port[-port]</i>	filter java only: One or more ports on which Java applets may be received.
<i>local_ip</i>	The IP address of the highest security level interface from which access is sought. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all hosts.
<i>local_mask</i>	Network mask of <i>local_ip</i> . You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
<i>foreign_ip</i>	The IP address of the lowest security level interface to which access is sought. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
<i>foreign_mask</i>	Network mask of <i>foreign_ip</i> . Always specify a specific mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
allow	filter url only: When the server is unavailable, let outbound connections pass through PIX Firewall without filtering. If you omit this option, and if the Websense server goes off line, PIX Firewall stops outbound port 80 (Web) traffic until the Websense server is back on line.

Usage Guidelines

The sections that follow describe each type of filter. The **clear filter** command removes all **filter** commands from the configuration. The **show filter** command lists all **filter** commands in the configuration.

filter activex

The **filter activex** command filters out ActiveX, Java applets, and other HTML <object> usages from outbound packets. ActiveX controls, formerly known as OLE or OCX controls, are components you can insert in a web page or other application. These controls include custom forms, calendars, or any of the extensive third-party forms for gathering or displaying information.

As a technology, it creates many potential problems for the network clients including causing workstations to fail, introducing network security problems, or be used to attack servers.

This feature blocks the HTML <object> tag and comments it out within the HTML web page.

**Note**

The <object> tag is also used for Java applets, image files, and multimedia objects, which will also be blocked by the **filter activex** command. If the <object> or </object> HTML tags split across network packets or if the code in the tags is longer than the number of bytes in the MTU, PIX Firewall cannot block the tag.

ActiveX blocking does not occur when users access an IP address referenced by the **alias** command.

To specify that all outbound connections have ActiveX blocking, use the following command:

```
filter activex 80 0 0 0 0
```

This command specifies that the ActiveX blocking applies to Web traffic on port 80 from any local host and for connections to any foreign host.

filter java

The **filter java** command filters out Java applets that return to the PIX Firewall from an outbound connection. The user still receives the HTML page, but the web page source for the applet is commented out so that the applet cannot execute. Use 0 for the *local_ip* or *foreign_ip* IP addresses to mean all hosts.

**Note**

If Java applets are known to be in <object> tags, use the **filter activex** command to remove them.

To specify that all outbound connections have Java applet blocking, use the following command:

```
filter java 80 0 0 0 0
```

This command specifies that the Java applet blocking applies to Web traffic on port 80 from any local host and for connections to any foreign host.

filter url

The **filter url** command lets you prevent outbound users from accessing World Wide Web URLs that you designate using the Websense filtering application.

The **allow** option to the **filter** command determines how the PIX Firewall behaves in the event that the Websense server goes off line. If you use the **allow** option with the **filter** command and the Websense server goes offline, port 80 traffic passes through the PIX Firewall without filtering. Used without the **allow** option and with the server offline, PIX Firewall stops outbound port 80 (Web) traffic until the server is back on line, or if another URL server is available, passes control to the next URL server.

**Note**

With the **allow** option set, PIX Firewall now passes control to an alternate server if the Websense server goes off line.

The Websense server works with the PIX Firewall to deny users from access to websites based on the company security policy.

Websense protocol version 4 enables group and username authentication between a host and a PIX Firewall. The PIX Firewall performs a username lookup, and then the Websense server handles URL filtering and username logging.

Websense protocol version 4 contains the following enhancements:

- URL filtering allows the PIX Firewall to check outgoing URL requests against the policy defined on the Websense server.
- Username logging tracks username, group, and domain name on the Websense server.
- Username lookup enables the PIX Firewall to use the user authentication table to map the host's IP address to the username.

Follow these steps to filter URLs:

-
- Step 1** Designate a Websense server with the **url-server** command.
- Step 2** Enable filtering with the **filter** command.
- Step 3** If needed, improve throughput with the **url-cache** command. However, this command does not update Websense logs, which may affect Websense accounting reports. Accumulate Websense run logs before using the **url-cache** command.
- Step 4** Use the **show url-cache stats** and the **show perfmon** commands to view run information.
-

Information on Websense is available at the following website:

<http://www.websense.com/>

Examples

The following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
url-server (perimeter) host 10.0.1.1
filter url 80 0 0 0 0
filter url except 10.0.2.54 255.255.255.255 0 0
```

The following example filters all outbound HTTP connections received from a proxy server that sends Web traffic on port 8080:

```
filter url 8080 0 0 0 0
```

fixup protocol

Change, enable, disable, or list a PIX Firewall application protocol feature. (Configuration mode.)

```

fixup protocol ftp [strict] [port]
fixup protocol http [port[-port]]
fixup protocol h323 [port[-port]]
fixup protocol rsh [514]
fixup protocol rtsp [port]
fixup protocol sip [5060]
fixup protocol smtp [port[-port]]
fixup protocol sqlnet [port[-port]]
fixup protocol [protocol [skinny | sip | ...]] [port]
no fixup protocol [protocol] [port]

clear fixup
show fixup [protocol protocol]
show conn state [skinny | sip]

show timeout sip

```

Syntax Description		
fixup protocol	Performs enabling, disabling, viewing, or changing the configuration of a service or protocol through the PIX Firewall.	
no	Disables the fixup of a protocol by removing all fixups of the protocol from the configuration using the no fixup command. After removing all fixups for a protocol, the no fixup form of the command or the default port is stored in the configuration.	
<i>port</i>	Specify the port number or range for the application protocol. The default ports are: TCP 21 for ftp , TCP 80 for http , TCP 1720 for h323 , TCP 514 for rsh , TCP 554 for rtsp , TCP 25 for smtp , TCP 1521 for sqlnet , and TCP 5060 for sip . The default port value for rsh cannot be changed, but additional port statements can be added. See the “Ports” section in Chapter 1, “Using PIX Firewall Commands” for a list of valid port literal names. The port over which the designated protocol travels.	
strict	Prevent web browsers from sending embedded commands in FTP requests. Each FTP command must be acknowledged before a new command is allowed. Connections sending embedded commands are dropped.	
protocol	Specifies the protocol to fix up.	
sip	Enable or change the port assignment for the Session Initiation Protocol (SIP) for Voice over IP TCP connections. UDP SIP is on by default and cannot be disabled and the port assignment is nonconfigurable.	

show conn state	Displays the connection state of the designated protocol.
show fixup	The show fixup command lists all values or the show fixup protocol <i>protocol</i> command lists an individual protocol.
show timeout	Displays the timeout value of the designated protocol.
show timeout skinny	Displays the timeout value of the SCCP.
skinny	Enable SCCP. SCCP protocol supports IP telephony and can coexist in an H.323 environment. An application layer ensures that all SCCP signaling and media packets can traverse the PIX Firewall and interoperate with H.323 terminals.
update timeout	Updates the timeout value of the SCCP.

Defaults

The default for the **fixup protocol sip** command is 5060.

The default for the **fixup protocol skinny** command is 2000.

Usage Guidelines

SCCP (skinny) protocol supports IP telephony and can coexist in an H.323 environment. An application layer ensures that all SCCP signaling and media packets can traverse the PIX Firewall and interoperate with H.323 terminals.

To support SIP calls through the PIX Firewall, signaling messages for the media connection addresses, media ports, and embryonic connections for the media must be inspected, because while the signaling is sent over a well known destination port (UDP/TCP 5060), the media streams are dynamically allocated. Therefore, SIP is a text-based protocol and contains the IP addresses throughout the text. The packets are inspected and NAT is provided for the IP addresses.



Note

If Call Manager (CM) is configured for NAT and outside phones register to it via TFTP, the connection will fail because PIX Firewall currently does not support NAT TFTP messages.

For additional information about the SIP protocol see RFC 2543. For additional information about the Session Description Protocol (SDP), see RFC 2327.

The **fixup protocol** commands let you view, change, enable, or disable the use of a service or protocol through the PIX Firewall. The ports you specify are those that the PIX Firewall listens at for each respective service. You can change the port value for each service except **rsh** and **sip**. The **fixup protocol** commands are always present in the configuration and are enabled by default.

The **fixup protocol** command performs the Adaptive Security Algorithm based on different port numbers other than the defaults. This command is global and changes things for both inbound and outbound connections, and cannot be restricted to any **static** command statements.

The **clear fixup** command removes **fixup** commands from the configuration that you added. It does not remove the default **fixup protocol** commands.

The **show fixup** command lists all values or the **show fixup protocol *protocol*** command lists an individual protocol.

You can disable the fixup of a protocol by removing all fixups of the protocol from the configuration using the **no fixup** command. After you remove all fixups for a protocol, the **no fixup** form of the command or the default port is stored in the configuration.

The following lists the default **fixup protocol** values (those enabled when a PIX Firewall is first installed). You can view the **fixup protocol** settings with the **show fixup** command as follows:

```
show fixup
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
```

fixup protocol ftp

The FTP port can be changed; however if you change the default of port 21, to something like 2021, all FTP control connections must happen on port 2021. FTP control connections on port 21 will no longer work.

If you disable FTP fixups with the **no fixup protocol ftp** command, outbound users can start connections only in passive mode, and all inbound FTP is disabled.

The **strict** option to the **fixup protocol ftp** command prevents web browsers from sending embedded commands in FTP requests. Each FTP command must be acknowledged before a new command is allowed. Connections sending embedded commands are dropped. The **strict** option only lets an FTP server generate the 227 command and only lets an FTP client generate the PORT command. The 227 and PORT commands are checked to ensure they do not appear in an error string.

The *port* parameter allows you to specify the port at which the PIX Firewall listens for FTP traffic. Typically, this value is 21. In addition, the FTP port can now only be in the range of 1 to 1024.

fixup protocol h323

The **fixup protocol h323** command provides support for Intel InternetPhone, CU-SeeMe, CU-SeeMe Pro, MeetingPoint, and MS NetMeeting. Version 5.3 and higher supports H.323 version 2. H.323 is a suite of protocols defined by the International Telecommunication Union (ITU) for multimedia conferences over LANs. H.323 supports VoIP gateways and VoIP gatekeepers. H.323 version 2 adds the following functionality to the PIX Firewall:

- Fast Connect or Fast Start Procedure for faster call setup
- H.245 tunneling for resource conservation, call synchronization, and reduced set up time

fixup protocol http

**Note**

If there is a **no fixup protocol http** command statement in the configuration, the **filter url** command does not work.

fixup protocol rtsp

The **fixup protocol rtsp** command lets PIX Firewall pass Real Time Streaming Protocol (RTSP) packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections. PIX Firewall does not support multicast RTSP.

If you are using Cisco IP/TV, use RTSP TCP port 554 and TCP 8554:

```
fixup protocol rtsp 554
fixup protocol rtsp 8554
```

The following restrictions apply to the **fixup protocol rtsp** command:

1. This PIX Firewall will not fix RTSP messages passing through UDP ports.
2. PIX Firewall does not support the RealNetwork's multicast mode (x-real-rdt/mcast).
3. PAT is not supported with the **fixup protocol rtsp** command.
4. PIX Firewall does not have the ability to recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.
5. PIX Firewall cannot perform NAT on RTSP messages because the embedded IP addresses are contained in the SDP files as part of HTTP or RTSP messages. Packets could be fragmented and PIX Firewall cannot perform NAT on fragmented packets.
6. With Cisco IP/TV, the number of NATs the PIX Firewall performs on the SDP part of the message is proportional to the number of program listings in the Content Manager (each program listing can have at least six embedded IP addresses).
7. You can configure NAT for Apple QuickTime 4 or RealPlayer. Cisco IP/TV only works with NAT if the Viewer and Content Manager are on the outside network and the server is on the inside network.
8. When using RealPlayer, it is important to properly configure transport mode. For the PIX Firewall, add an **access-list** command statement from the server to the client or vice versa. For RealPlayer, change transport mode by clicking **Options>Preferences>Transport>RTSP Settings**.

If using TCP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use TCP for all content** check boxes. On the PIX Firewall, there is no need to configure the fixup.

If using UDP mode on the RealPlayer, select the **Use TCP to Connect to Server** and **Attempt to use UDP for static content** check boxes, and for live content not available via Multicast. On the PIX Firewall, add a **fixup protocol rtsp port** command statement.

fixup protocol sip

The **fixup protocol sip** command enables SIP on the interface. SIP enables call handling sessions—particularly two-party audio conferences, or “calls.” SIP works with Session Description Protocol (SDP) for call signalling. SDP specifies the ports for the media stream. Using SIP, the PIX Firewall can support any SIP Voice over IP (VoIP) gateways and VoIP proxy servers.

Session Initiation Protocol (SIP), as defined by the Internet Engineering Task Force (IETF), enables call handling sessions, particularly two-party audio conferences, or “calls.” SIP works with Session Description Protocol (SDP) for call signalling. SDP specifies the ports for the media stream. Using SIP, the PIX Firewall can support any SIP Voice over IP (VoIP) gateways and VoIP proxy servers. SIP and SDP are defined in the following RFCs:

- SIP: Session Initiation Protocol, RFC 2543
- SDP: Session Description Protocol, RFC 2327

fixup protocol smtp

The **fixup protocol smtp** command enables the Mail Guard feature, which only lets mail servers receive the RFC 821, section 4.5.1 commands of HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT. All other commands are rejected with the “500 command unrecognized” reply code.

As of version 5.1 and later, the **fixup protocol smtp** command changes the characters in the SMTP banner to asterisks except for the “2”, “0”, “0 ” characters. Carriage return (CR) and linefeed (LF) characters are ignored.

In version 4.4, all characters in the SMTP banner are converted to asterisks.

fixup protocol sqlnet



Note

PIX Firewall uses port 1521 for SQL*Net. This is the default port used by Oracle for SQL*Net; however, this value does not agree with IANA port assignments.

Examples

You can add multiple port settings for each protocol with separate commands; for example:

```
fixup protocol ftp 21
fixup protocol ftp 4254
fixup protocol ftp 9090
```

These commands cause PIX Firewall to listen to the standard FTP port of 21 but also to listen for FTP traffic at ports 4254 and 9090.

The following example enables access to an inside server running Mail Guard:

```
static (inside,outside) 209.165.201.1 192.168.42.1 netmask 255.255.255.255
access-list acl_out permit tcp host 209.165.201.1 eq smtp any
access-group acl_out in interface outside
fixup protocol smtp 25
```

The following example shows the commands to disable Mail Guard:

```
static (dmz1,outside) 209.165.201.1 10.1.1.1 netmask 255.255.255.255
access-list acl_out permit tcp host 209.165.201.1 eq smtp any
access-group acl_out in interface outside
no fixup protocol smtp 25
```

In this example, the **static** command sets up a global address to permit outside hosts access to the 10.1.1.1 mail server host on the dmz1 interface. (The MX record for DNS needs to point to the 209.165.201.1 address so that mail is sent to this address.) The **access-list** command lets any outside users access the global address through the SMTP port (25). The **no fixup protocol** command disables the Mail Guard feature.

flashfs

Clear, display, or downgrade filesystem information. (Configuration mode.)

flashfs downgrade {4.x | 5.0 | 5.1}

clear flashfs

show flashfs

Syntax Description

downgrade 4.x	Clear the filesystem information from Flash memory before downgrading to version 4.0, 4.1, 4.2, 4.3, or 4.4.
downgrade 5.x	Write the filesystem to Flash memory before downgrading to the appropriate version 5.0 or higher.

Usage Guidelines

The **clear flashfs** and the **flashfs downgrade 4.x** commands clear the filesystem part of Flash memory in the PIX Firewall. Versions 4.*n* cannot use the information in the filesystem; it needs to be cleared to let the earlier version operate correctly.

The **flashfs downgrade 5.x** command reorganizes the filesystem part of Flash memory so that information stored in the filesystem can be accessed by the earlier version. The PIX Firewall maintains a filesystem in Flash memory to store system information, IPSec private keys, certificates, and CRLs. It is crucial that you clear or reformat the filesystem before downgrading to a previous PIX Firewall version. Otherwise, your filesystem will get out of sync with the actual contents of the Flash memory and cause problems when the unit is later upgraded.

You only need to use the **flashfs downgrade 5.x** command if your PIX Firewall has 16 MB of Flash memory, if you have IPSec private keys, certificates, or CRLs stored in Flash memory, and you used the **ca save all** command to save these items in Flash memory. The **flashfs downgrade 5.x** command fails if the filesystem indicates that any part of the image, configuration, or private data in the Flash memory device is unusable.



Note

When downgrading to PIX Firewall Versions 5.0 or 5.1, which support a maximum 4 MB of Flash memory, configuration files larger than 4 MB will be truncated and some configuration information will be lost.

The **clear flashfs** and **flashfs downgrade** commands do not affect the configuration stored in Flash memory.

The **clear flashfs** command is the same as the **flashfs downgrade 4.x** command.

The **show flashfs** command displays the size in bytes of each filesystem sector and the current state of the filesystem. The data in each sector is as follows:

- file 0—PIX Firewall binary image, where the .bin file is stored.
- file 1—PIX Firewall configuration data that you can view with the **show config** command.
- file 2—PIX Firewall datafile that stores IPSec key and certificate information.
- file 3—**flashfs downgrade** information for the **show flashfs** command.

Examples

Use the following command to write the filesystem to Flash memory before downgrading to a lower version of software:

```
flashfs downgrade 5.3
```

The following commands display the filesystem sector sizes:

```
show flashfs  
flash file system: version:1 magic:0x12345679  
  file 0: origin:      0 length:1794104  
  file 1: origin: 2095104 length:1496  
  file 2: origin:      0 length:0  
  file 3: origin: 2096640 length:140
```

```
flashfs downgrade 5.3
```

```
show flashfs  
flash file system: version:0 magic:0x0  
  file 0: origin:      0 length:0  
  file 1: origin:      0 length:0  
  file 2: origin:      0 length:0  
  file 3: origin:      0 length:0
```

The origin values are integer multiples of the underlying filesystem sector size.

floodguard

Enable or disable Flood Defender to protect against flood attacks. (Configuration mode.)

floodguard enable | disable

show floodguard

clear floodguard

Syntax Description

enable	Enable Flood Defender.
disable	Disable Flood Defender.

Usage Guidelines

The **floodguard** command allows you to reclaim PIX Firewall resources if the user authentication (uauth) subsystem runs out of resources. If an inbound or outbound uauth connection is being attacked or overused, the PIX Firewall will actively reclaim TCP user resources.

When the resources deplete, the PIX Firewall lists messages about it being out of resources or out of tcpusers.

If the PIX Firewall uauth subsystem is depleted, TCP user resources in different states are reclaimed depending on urgency in the following order:

1. Timewait
2. LastAck
3. FinWait
4. Embryonic
5. Idle

The **floodguard** command is enabled by default.

Examples

The following example enables the **floodguard** command and lists the **floodguard** command statement in the configuration:

```
floodguard enable
show floodguard
floodguard enable
```

fragment

The **fragment** command provides additional management of packet fragmentation and improves compatibility with NFS. (Configuration Mode.)

```

fragment size database-limit [interface]
fragment chain chain-limit [interface]
fragment timeout seconds [interface]
clear fragment
show fragment [interface]

```

Syntax Description

size	Sets the maximum number of packets in the fragment database. The default is 200.
chain	Specifies the maximum number of packets into which a full IP packet can be fragmented. The default is 24.
timeout	Specifies the maximum number of seconds that a packet fragment will wait to be reassembled after the first fragment is received before being discarded. The default is 5 seconds.
clear	Resets the fragment databases and defaults. All fragments currently waiting for reassembly are discarded and the size , chain , and timeout options are reset to their default values.
show	<ul style="list-style-type: none"> • Displays the state of the fragment database: • Size—Maximum packets set by the size option. • Chain—Maximum fragments for a single packet set by the chain option. • Timeout—Maximum seconds set by the timeout option. • Queue—Number of packets currently awaiting reassembly. • Assemble—Number of packets successfully reassembled. • Fail—Number of packets which failed to be reassembled. • Overflow—Number of packets which overflowed the fragment database.
<i>database-limit</i>	The default is 200. The maximum is 1,000,000 or the total number of blocks.
<i>chain-limit</i>	The default is 24. The maximum is 8200.
<i>seconds</i>	The default is 5 seconds. The maximum is 30 seconds.
<i>interface</i>	The PIX Firewall interface. If not specified, the command will apply to all interfaces.

Usage Guidelines

In general, the default values should be used. However, if a large percentage of the network traffic through the PIX Firewall is NFS, additional tuning may be necessary to avoid database overflow. See system log message 209003 for additional information.

In an environment where the MTU between the NFS server and client is small, such as a WAN interface, the **chain** option may require additional tuning. In this case, NFS over TCP is highly recommended to improve efficiency.

Setting the *database-limit* of the **size** option to a large value can make the PIX Firewall more vulnerable to a DoS attack by fragment flooding. Do not set the *database-limit* equal to or greater than the total number of blocks in the 1550 or 16384 pool. See the **show block** command for more details. The default values will limit DoS due to fragment flooding to that interface only.

Examples

The following example configures the outside fragment database to limit a maximum size of 2000, a maximum chain length of 45, and a wait time of 10 seconds:

```
pixfirewall(config)#
pixfirewall(config)# fragment outside size 2000
pixfirewall(config)# fragment chain 45 outside
pixfirewall(config)# fragment outside timeout 10
pixfirewall(config)#
```

The **clear fragment** command resets the fragment databases. Specifically, all fragments awaiting re-assembly are discarded. In addition, the size is reset to 200; the chain limit is reset to 24; and the timeout is reset to 5 seconds.

The **show fragment** command displays the states of the fragment databases. If the interface name is specified, only the database residing at the specified interface is displayed.

```
pixfirewall(config)# show fragment outside
Interface:outside
Size:2000, Chain:45, Timeout:10
Queue:1060, Assemble:809, Fail:0, Overflow:0
```

The preceding example shows that the "outside" fragment database has the following:

- A database size limit of 2000 packets.
- The chain length limit of 45 fragments.
- A timeout of ten seconds.
- 1060 packets is currently awaiting re-assembly.
- 809 packets has been fully reassembled.
- No failure.
- No overflow.

This fragment database is under heavy usage.