



System Log Messages

This chapter lists the PIX Firewall system log messages. The messages are listed numerically by message code.



Note

The messages shown in this guide only apply to PIX Firewall version 5.3 and later. When a number is skipped from a sequence, for example, 106004 or 110001, the message is no longer in the PIX Firewall code.

This chapter includes the following sections:

- Messages 100001 to 105020
- Messages 106001 to 112001
- Messages 199001 to 209005
- Messages 210001 to 213004
- Messages 302001 to 315011
- Messages 400000 to 709007

Messages 100001 to 105020

`%PIX-1-101001: (Primary) Failover cable OK.`

Explanation This is a failover message. This message reports that the failover cable is present and functioning correctly. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action None required.

`%PIX-1-101002: (Primary) Bad failover cable.`

Explanation This is a failover message. This message reports that the failover cable is present but not functioning correctly. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action Replace the failover cable.

%PIX-1-101003: (Primary) Failover cable not connected (this unit).

%PIX-1-101004: (Primary) Failover cable not connected (other unit).

Explanation Both instances are failover messages. These messages are logged when failover mode has been enabled, but the failover cable is not connected to one unit of the failover pair. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action Connect the failover cable to both units of the failover pair.

%PIX-1-101005: (Primary) Error reading failover cable status.

Explanation This is a failover message. This message is logged if the failover cable is connected, but the primary unit is unable to determine its status.

Action Replace the cable.

%PIX-1-102001: (Primary) Power failure/System reload other side.

Explanation This is a failover message. This message is logged if the primary unit detects a power failure on the other unit. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action Verify that the secondary unit is powered on and that power cables are properly connected.

%PIX-1-103001: (Primary) No response from other firewall (reason code = *code*).

Explanation This is a failover message. This message is logged if the primary unit is unable to communicate with the secondary unit over the failover cable. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action Verify that the secondary unit has the exact same hardware, software version level, and configuration as the primary unit.

%PIX-1-103002: (Primary) Other firewall network interface *interface_number* OK.

Explanation This is a failover message. This message is logged when the primary unit detects that the network interface on the secondary unit is okay. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit. Refer to Table 1-3 in Chapter 1, “Introduction,” for possible values for the *interface_number* variable.

Action None required.

%PIX-1-103003: (Primary) Other firewall network interface *interface_number* failed.

Explanation This is a failover message. This message is logged if the primary unit detects a bad network interface on the secondary unit. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit. Refer to Table 1-3 in Chapter 1, “Introduction,” for possible values for the *interface_number* variable.

Action Check the network connections on the secondary unit. Also, check the network hub connection. If necessary, replace the failed network interface.

%PIX-1-103004: (Primary) Other firewall reports this firewall failed.

Explanation This is a failover message. This message is logged if the primary unit receives a message from the secondary unit indicating that the primary has failed. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action Verify the status of the primary unit.

%PIX-1-103005: (Primary) Other firewall reporting failure.

Explanation This is a failover message. This message is logged if the secondary unit reports a failure to the primary unit. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action Verify the status of the secondary unit.

%PIX-1-104001: (Primary) Switching to ACTIVE (cause: *reason*).

%PIX-1-104002: (Primary) Switching to STNDBY (cause: *reason*).

Explanation Both instances are failover messages. These messages usually are logged when you force the pair to switch roles, either by entering the **failover active** command on the secondary unit, or the **no failover active** command on the primary unit. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit. Possible values for the *reason* variable are as follows:

- state check
- bad/incompleted config
- ifc [interface] check, mate is healthier
- the otherside want me standby
- in failed state, can not be Active
- switch to failed state

Action If the message occurs because of manual intervention, no action is required. Otherwise, use the cause reported by the secondary unit to verify the status of both units of the pair.

%PIX-1-104003: (Primary) Switching to FAILED.

Explanation This is a failover message. This message is logged when the primary unit fails.

Action Check the system log messages for the primary unit for an indication of the nature of the problem (see message 104001). “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

%PIX-1-104004: (Primary) Switching to OK.

Explanation This is a failover message. This message is logged when a previously failed unit now reports that it is operating again. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action None required.

%PIX-1-105001: (Primary) Disabling failover.

Explanation This is a failover message. This message is logged when you enter the **no failover** command on the console. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action None required.

%PIX-1-105002: (Primary) Enabling failover.

Explanation This is a failover message. This message is logged when you enter the **failover** command with no arguments on the console, after having previously disabled failover. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action None required.

%PIX-1-105003: (Primary) Monitoring on interface *int_name* waiting

Explanation This is a failover message. The PIX Firewall is testing the specified network interface with the other unit of the failover pair. Refer to Table 1-3 in Chapter 1, “Introduction,” for possible values for the *interface_number* variable. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action None required. The PIX Firewall monitors its network interfaces frequently during normal operations.

%PIX-1-105004: (Primary) Monitoring on interface *int_name* normal

Explanation This is a failover message. The test of the specified network interface was successful. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action None required.

%PIX-1-105005: (Primary) Lost Failover communications with mate on interface *int_name*.

Explanation This is a failover message. This message is logged if this unit of the failover pair can no longer communicate with the other unit of the pair. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action Verify that the network connected to the specified interface is functioning correctly.

%PIX-1-105006: (Primary) Link status 'Up' on interface *int_name*.

%PIX-1-105007: (Primary) Link status 'Down' on interface *int_name*.

Explanation Both instances are failover messages. These messages report the results of monitoring the link status of the specified interface. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action If the link status is down, verify that the network connected to the specified interface is operating correctly.

%PIX-1-105008: (Primary) Testing interface *int_name*.

Explanation This is a failover message. This message is logged when the PIX Firewall tests a specified network interface. This testing is performed only if the PIX Firewall fails to receive a message from the Standby unit on that interface after the expected interval. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action None required.

%PIX-1-105009: (Primary) Testing on interface *int_name* result.

Explanation This is a failover message. This message reports the result (either “Passed” or “Failed”) of a previous interface test. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action None required if the result is “Passed.” If the result is “Failed,” you should check to be sure the network cable is properly connected to both failover units and that the network itself is functioning correctly, and verify the status of the Standby unit.

%PIX-3-105010: (Primary) Failover message block alloc failed

Explanation Block memory has been depleted. This is a transient message and the PIX Firewall should recover. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action Use the **show blocks** command to monitor the current block memory.

%PIX-1-105011: (Primary) Failover cable communication failure

Explanation The failover cable is not permitting communication between the Primary and Secondary units. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action Ensure that the cable is properly connected.

%PIX-1-105020: (Primary) Incomplete/slow config replication

Explanation When a failover occurs, the active PIX Firewall detects a partial configuration in memory. Normally, this is caused by an interruption in the replication service. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action Once the failover is detected by the PIX Firewall, the PIX Firewall automatically reloads itself and loads configuration from Flash and/or resyncs with another PIX Firewall. If failovers happen continuously, check the failover configuration and make sure both PIX Firewalls can communicate with each other.

Messages 106001 to 112001

%PIX-2-106001: Inbound TCP connection denied from *IP_addr/port* to *IP_addr/port* flags *TCP_flags* on interface *int_name*

Explanation This is a connection-related message. This message occurs when an attempt to connect to an inside address is denied by your security policy. Possible *TCP_flags* values correspond to the flags in the TCP header that were present when the connection was denied. For example, a TCP packet arrived for which no connection state exists in the PIX Firewall, and it was dropped. The *TCP_flags* in this packet are FIN,ACK.

The *TCP_flags* are as follows:

- ACK—The acknowledgment number was received.
- FIN—Data was sent.
- PSH—The receiver passed data to the application.
- RST—The connection was reset.
- SYN—Sequence numbers were synchronized to start a connection.
- URG—The urgent pointer was declared valid.

Action None required.

%PIX-2-106002: *protocol* Connection denied by outbound list *list_ID* src *laddr* dest *faddr*

Explanation This is a connection-related message. This message is logged if the specified connection fails because of an **outbound deny** command statement. The *protocol* variable can be ICMP, TCP, or UDP.

Action Use the **show outbound** command to check outbound lists.

```
%PIX-2-106006: Deny inbound UDP from faddr/fport to laddr/lport on interface
int_name.
```

Explanation This is a connection-related message. This message is logged if an inbound UDP packet is denied by your security policy.

Action None required.

```
%PIX-2-106007: Deny inbound UDP from faddr/fport to laddr/lport due to DNS flag.
```

Explanation This is a connection-related message. This message is logged if a UDP packet containing a DNS query or response is denied. The *flag* variable is either Response or Query.

Action If the inside port number is 53, it is likely that the inside host is set up as a caching nameserver. Add an **access-list** command statement to permit traffic on UDP port 53. If the outside port number is 53, the most likely cause is that a DNS server was too slow to respond, and the query was answered by another server.

```
%PIX-3-106010: Deny inbound icmp src outside: IP_addr dst inside: IP_addr (type
dec, code dec)
```

Explanation This is a connection-related message. This message is logged if an inbound connection is denied by your security policy.

Action None required.

```
%PIX-7-106011: Deny inbound (No xlate) chars
```

Explanation This is a connection-related message. This message occurs when a packet is sent to the same interface that it arrived on. This usually indicates that a security breach is occurring. When the PIX Firewall receives a packet, it tries to establish a translation slot based on the security policy you set with the **global** and **conduit** commands, and your routing policy set with the **route** command.

Failing both policies, PIX Firewall allows the packet to flow from the higher priority network to a lower priority network, if it is consistent with the security policy. If a packet comes from a lower priority network and the security policy does not allow it, PIX Firewall routes the packet back to the same interface.

To provide access from an interface with a higher security to a lower security, use the **nat** and **global** commands. For example, use the **nat** command to let inside users access outside servers, to let inside users access perimeter servers, and to let perimeter users access outside servers.

To provide access from an interface with a lower security to higher security, use the **static** and **conduit** commands. For example, use the **static** and **conduit** commands to let outside users access inside servers, outside users access perimeter servers, or perimeter servers access inside servers.

Action Fix your configuration to reflect your security policy for handling these attack events.

%PIX-2-106012: Deny IP from *IP_addr* to *IP_addr*, IP options *hex*.

Explanation This is a connection-related message. A IP packet was seen with IP options. Because IP options are considered a security risk, the packet was discarded.

Action A security breach was probably attempted. Check the local site for loose source or strict source routing.

%PIX-2-106013: Dropping echo request from *IP_addr* to PAT address *IP_Addr*

Explanation This message is logged when the PIX Firewall discards an inbound ICMP Echo Request packet with a destination address that corresponds to a PAT global address. It is discarded because the inbound packet can not specify which PAT host should receive the packet.

Action None required.

%PIX-3-106014: Deny inbound icmp src *interface name: IP_addr* dst *interface name: IP_addr* (type *dec*, code *dec*)

Explanation This message is logged when the PIX Firewall denies any inbound ICMP packet access. By default, all ICMP packets are denied access unless specifically permitted using the conduit permit icmp command.

Action None required.

%PIX-6-106015: Deny TCP (no connection) from *IP_addr/port* to *IP_addr/port* flags *flags* on interface *int_name*.

Explanation This message is logged when the PIX Firewall discards a TCP packet that has no associated connection in the PIX Firewall unit's connection table. PIX Firewall looks for a SYN flag in the packet, which indicates a request to establish a new connection. If the SYN flag is not set, and there is not an existing connection, the PIX Firewall discards the packet.

Action None required unless the PIX Firewall receives a large volume of these invalid TCP packets. If this is the case, trace the packets to the source and determine the reason these packets were sent.

%PIX-2-106016: Deny IP spoof from (*IP_addr*) to *IP_addr* on interface *int_name*.

Explanation This message is logged when the PIX Firewall discards a packet with an invalid source address. Invalid sources addresses are those addresses belonging to the following:

- Loopback network (127.0.0.0)
- Broadcast (limited, net-directed, subnet-directed, and all-subnets-directed)
- The destination host (land.c)

Furthermore, if **sysopt connection enforcesubnet** is enabled, PIX Firewall discards packets with a source address belonging to the destination subnet from traversing the PIX Firewall and logs this message.

To further enhance spoof packet detection, use the **conduit** command to configure the PIX Firewall to discard packets with source addresses belonging to the internal network.

Action Determine if an external user is trying to compromise the protected network. Check for misconfigured clients.

```
%PIX-2-106017: Deny IP due to Land Attack from IP_addr to IP_addr
```

Explanation This message appears when PIX Firewall receives a packet with the IP source address equal to the IP destination and the destination port equal to the source port. This indicates a spoofed packet designed to attack systems. This attack is referred to as a Land Attack.

Action If this message persists, an attack may be in progress. The packet does not provide enough information to determine where the attack originates.

```
%PIX-2-106018: ICMP packet type ICMP_type denied by outbound list list_ID src  
laddr dest faddr
```

Explanation This message is logged because outgoing ICMP packet with type *ICMP_type* from local host *laddr* to foreign host *faddr* is denied by outbound list *list_ID*.

Action None required.

```
%PIX-4-106019: IP packet from src_addr to dest_addr, protocol protocol received  
from interface int_name deny by access-group acl_ID
```

Explanation This message is logged when an IP packet is denied by the parameters you specified in the access list with the ID *acl_ID*.

Action None required.

```
%PIX-2-106020: Deny IP teardrop fragment (size = num, offset = num) from IP_addr  
to IP_addr
```

Explanation The PIX Firewall discarded an IP packet with a teardrop signature containing either a small offset or fragment overlapping. This is a hostile event to circumvent the PIX Firewall or an Intrusion Detection System.

Action Contact the remote peer administrator or escalate this issue according to your security policy.

```
%PIX-1-106021: Deny protocol reverse path check from src_addr to dest_addr on
interface int_name
```

Explanation Someone is attempting to spoof an IP address on an inbound connection. Unicast Reverse Path Forwarding, also known as reverse route lookup, detected a packet that does not have a source address represented by a route and assumes it to be part of an attack on your PIX Firewall.

Action This message appears when you have enabled Unicast Reverse Path Forwarding with the **ip verify reverse-path** command. This feature works on packets input to an interface; if it is configured on the outside, then PIX Firewall checks packets arriving from the outside.

PIX Firewall looks up a route based on the *src_addr*. If an entry is not found and a route is not defined, then this syslog message appears and the connection is dropped.

If there is a route, PIX Firewall checks which interface it corresponds to. If the packet arrived on another interface, then it is a spoof or there is an asymmetric routing environment. PIX Firewall does not support asymmetric routing (where there is more than one path to a destination).

If configured on an internal interface, PIX Firewall checks static **route** command statements or RIP and if the *src_addr* is not found, then an internal user is spoofing their address.

An attack is in progress. With this feature enabled, no user action is required. PIX Firewall repels the attack.

```
%PIX-1-106022: Deny protocol connection spoof from src_addr to dest_addr on
interface int_name
```

Explanation This message only happens if a connection exists and a packet matching the connection arrives on a different interface than what interfaces the connection began on. For example, if a user starts a connection on the inside interface, but the PIX Firewall detects the same connection arriving on a perimeter interface, then either the PIX Firewall has more than one path to a destination, which is known as asymmetric routing and is not supported on the PIX Firewall, or an attacker is attempting to append packets from one connection to another as a way to break into the PIX Firewall. In either case, PIX Firewall displays this message and drops the connection.

Action This message appears when **ip verify reverse-path** is not configured. Ensure routing is not asymmetric.

```
%PIX-1-107001: RIP auth failed from IP_addr: version=vers, type=type, mode=mode,
sequence=seq on interface int_name
```

Explanation This is an alert log message. PIX Firewall received a RIP reply message with bad authentication. This could be due to misconfiguration on the router or the PIX Firewall or it could be a unsuccessful attempt to attack the PIX Firewall unit's routing table.

Action This may be an attack and should be monitored. If you are not familiar with the source IP address listed in this message, change your RIP authentication keys between trusted entities. An attacker may be trying to deduce the existing keys.

%PIX-1-107002: RIP pkt failed from *IP_addr*: version=*vers* on interface *int_name*

Explanation This is an alert message. This could be a router bug, a packet with non-RFC values inside, or malformed entries. This should not happen and may be an attempt to exploit the PIX Firewall unit's routing table.

Action This may be an attack and should be monitored. The packet has passed authentication, if enabled, and bad data is in the packet. The situation should be monitored and the keys should be changed if there are any doubts as to the originator of the packets.

%PIX-2-108002: SMTP replaced *chars*: out *src_addr* in *laddr* data: *chars*

Explanation This is a Mail Guard (SMTP) message generated by the **fixup protocol smtp** command. This message is logged if the PIX Firewall replaces an invalid character in an email address with a space.

Action None required.

%PIX-6-109001: Auth start for user '*username*' from *laddr/lport* to *faddr/fport*

Explanation This is an AAA message. This message is logged if the PIX Firewall is configured for AAA and detects an authentication request by the specified user.

Action None required.

%PIX-6-109002: Auth from *laddr/lport* to *faddr/fport* failed (server *IP_addr* failed) on interface *int_name*.

Explanation This is an AAA message. This message is logged if an authentication request fails because the specified authentication server cannot be contacted by the PIX Firewall.

Action Check to be sure the authentication daemon is running on the specified authentication server.

%PIX-6-109003: Auth from *laddr* to *faddr/fport* failed (all servers failed) on interface *int_name*.

Explanation This is an AAA message. This message is logged if no authentication server can be found.

Action Ping the authentication server(s) from the PIX Firewall. Make sure the daemon(s) are running.

%PIX-6-109005: Authentication succeeded for user '*user*' from *laddr/lport* to *faddr/fport* on interface *int_name*.

Explanation This is an AAA message. This message is logged when the specified authentication request succeeds.

Action None required.

%PIX-6-109006: Authentication failed for user 'user' from *laddr/lport* to *faddr/fport* on interface *int_name*.

Explanation This is an AAA message. This message is logged if the specified authentication request fails, possibly because of a mistyped password.

Action None required.

%PIX-6-109007: Authorization permitted for user 'user' from *laddr/lport* to *faddr/fport* on interface *int_name*.

Explanation This is an AAA message. This message is logged when the specified authorization request succeeds.

Action None required.

%PIX-6-109008: Authorization denied for user 'user' from *faddr/fport* to *laddr/lport* on interface *int_name*.

Explanation This is an AAA message. This message is logged if a user is not authorized to access the specified address, possibly because of a mistyped password.

Action None required.

%PIX-6-109009: Authorization denied from *laddr/lport* to *faddr/fport* (not authenticated) on interface *int_name*.

Explanation This is an AAA message. This message is logged if the PIX Firewall is configured for AAA and a user attempted to make a TCP connection across the PIX Firewall without prior authentication.

Action None required.

%PIX-3-109010: Auth from *laddr/lport* to *faddr/fport* failed (too many pending auths) on interface *int_name*.

Explanation This is an AAA message. This message is logged if an authentication request cannot be processed because the server has too many requests pending.

Action Check to see if the authentication server is too slow to respond to authentication requests. Enable floodguard with the **floodguard enable** command.

%PIX-2-109011: Authen Session Start: user 'user', sid *session_num*

Explanation An authentication session started between the host and the PIX Firewall and has not yet completed.

Action None required.

%PIX-5-109012: Authen Session End: user '*user*', sid *session_num*, elapsed *num* seconds

Explanation The authentication cache has timed out. Users will need to reauthenticate on their next connection. You can change the duration of this timer with the **timeout uauth** command.

Action None required.

%PIX-3-109013: User must authenticate before using this service

Explanation The user must be authenticated before using the service.

Action Authenticate using FTP, Telnet, or HTTP before using the service.

%PIX-7-109014: uauth_lookup_net fail for uauth_in()

Explanation A request to authenticate did not have a corresponding request for authorization.

Action Ensure that both the **aaa authentication** and **aaa authorization** command statements are provided in the configuration.

%PIX-6-109015: Authorization denied (acl=*acl_ID*) for user '*username*' from *src_addr/src_port* to *dest_addr/dest_port* on interface *int_name*

Explanation The access list check failed; either it matched a deny, or it matched nothing, such as an implicit deny. Connection denied by user access list *acl_ID*, which was defined per the AAA authorization policy on CiscoSecure ACS.

Action None required.

%PIX-3-109016: Downloaded authorization access-list *acl_ID* not found for user '*username*'

Explanation The AAA authorization **access-list** command statement ID **acl=*acl_ID*** defined on the remote AAA server has not been configured on the PIX Firewall unit. This error can occur if you configure the AAA server before configuring the PIX Firewall.

Action Use the same **access-list** command statement ID on the PIX Firewall as you specified on the AAA server.

%PIX-6-110001: No route to *dest_addr* from *src_addr*

Explanation This message indicates a route lookup failure. A packet is looking for a destination IP address which is not in the routing table.

Action Check the routing table and make sure there is a route to the destination.

%PIX-3-110002: No ARP for host *IP_addr*

Explanation This is a routing message. This message is logged if the PIX Firewall cannot resolve the address of a host on one of its immediately connected networks. This usually occurs if the specified host does not exist or is not reachable on the network the PIX Firewall expects it to be on, for example, if the host's address is incorrectly subnetted.

Action Check the ARP table and ensure the host is available. If necessary, add a static ARP statement with the **arp** command or set the **arp timeout** value lower so the ARP table will refresh sooner.

Also, check to be sure that the host's IP address is appropriate to the network topology and your subnet scheme. Verify that the host is reachable by pinging it from another host. Use the **show arp** command to display the PIX Firewall unit's ARP table. At the very least, the PIX Firewall must be able to resolve the addresses of its SNMP server, routers, and syslog host.

%PIX-5-111001: Begin configuration: *IP_addr* writing to device

Explanation This message is logged when you enter the **write** command to store your configuration on a *device* (either floppy, Flash memory, TFTP, the failover Standby unit, or the console terminal). The *IP_addr* indicates whether the login was made at the console port or via a Telnet connection.

Action None required.

%PIX-5-111003: *IP_addr* Erase configuration

Explanation This is a PIX Firewall Manager message. This message is logged when you erase the contents of Flash memory, either by entering the **write erase** command at the console, or by clicking OK to clear Flash memory in the PIX Firewall Manager. The *IP_addr* indicates whether the login was made at the console port or via a Telnet connection.

Action After erasing the configuration, you must reconfigure the PIX Firewall and save the new configuration. Alternatively, you can restore information from a configuration that was previously saved, either on floppy or on a TFTP server elsewhere on the network.

%PIX-5-111004: *IP_addr* end configuration: [FAILED]|[OK]

Explanation This is a PIX Firewall Manager message. This message is logged when you enter the **config floppy/memory/ network** command, or the **write floppy/memory/network/standby** command. The *IP_addr* indicates whether the login was made at the console port or via a Telnet connection.

Action None required if the message ends with OK. If the message indicates a failure, try to fix the problem. For example, if writing to a floppy, ensure that the floppy is not write protected; if writing to a TFTP server, ensure that the server is up.

```
%PIX-5-111005: IP_addr end configuration: OK
```

Explanation This is a PIX Firewall Manager message. This message is logged when you exit configuration mode. The *IP_addr* indicates whether the login was made at the console port or via a Telnet connection.

Action None required.

```
%PIX-5-111006: Console Login from user at IP_addr
```

Explanation This is a PIX Firewall Manager message. This message is logged when you connect to the PIX Firewall. If authentication is enabled, the username is reported; otherwise, the string “nobody” appears. The *IP_addr* indicates whether the login was made at the console port or via a Telnet connection.

Action None required.

```
%PIX-5-111007: Begin configuration: IP_addr reading from device.
```

Explanation This is a PIX Firewall Manager message. This message is logged when you enter the **reload** or **configure** command to read in a configuration. The *device* text can be floppy, memory, net, standby, or terminal. The *IP_addr* indicates whether the login was made at the console port or via a Telnet connection.

Action None required.

```
%PIX-5-111008: User 'user' executed the 'cmd' command.
```

Explanation This message indicates that a command change to the configuration has been made from an AAA authenticated session.

Action None required.

```
%PIX-2-112001: (chars:dec) pix clear finished.
```

Explanation This is a PIX Firewall Manager message. This message is logged when a request to clear the PIX Firewall configuration has finished. The source file and line number are identified.

Action None required.

Messages 199001 to 209005

```
%PIX-5-199001: PIX reload command executed from IP_addr.
```

Explanation This is a PIX Firewall Manager message. This message logs the address of the host initiating a PIX Firewall reboot with the **reload** command.

Action None required.

%PIX-6-199002: PIX startup completed. Beginning operation.

Explanation This is a PIX Firewall Manager message. This message is logged after the PIX Firewall finishes its initial boot and Flash memory reading sequence, and is ready to begin operating normally.



Note This message cannot be blocked using the **no logging message** command.

Action None required.

%PIX-6-199003: Reducing Link MTU *dec*.

Explanation This is a PIX Firewall Manager message. This message is logged when the PIX Firewall receives a packet from the outside network that uses a larger MTU than the inside network. The PIX Firewall then sends an ICMP message to the outside host to negotiate an appropriate MTU. The log message includes the ICMP message's sequence number.

Action None required.

%PIX-6-199005: PIX Startup begin

Explanation This message is logged when the PIX Firewall starts.

Action None required.

%PIX-3-201002: Too many connections on static|xlate *gaddr! econns nconns*

Explanation This is a connection-related message. This is a connection-related message. This message is logged when the maximum number of connections to the specified static address has been exceeded. The *econns* variable is the maximum number of embryonic connections and *nconns* is the maximum number of connections permitted for the static or xlate.

Action Use the **show static** command to check the limit imposed on connections to a static address. The limit is configurable.

%PIX-2-201003: Embryonic limit exceeded *neconns/elimit* for *faddr/fport (gaddr) laddr/lport* on interface *int_name*

Explanation This is a connection-related message. This message is logged when the maximum number of embryonic connections from the specified foreign address via the specified static global address to the specified local address has been exceeded. When the limit on embryonic connections is reached, the PIX Firewall attempts to accept them anyway, but puts a time limit on the connections. This allows some connections to succeed even if the PIX Firewall is very busy. The *neconns* variable lists the number of embryonic connections received and *elimit* lists the maximum number of embryonic connections specified in the **static** or **nat** command.

Action This message indicates a more serious overload than message 201002. It could be caused by a SYN attack, or simply a very heavy load of legitimate traffic. Use the **show static** command to check the limit imposed on embryonic connections to a static address.

%PIX-3-201005: FTP data connection failed for *IP_addr*

Explanation This is a connection-related message. This message is logged when the PIX Firewall is unable to allocate a structure to track the data connection for FTP because of insufficient memory.

Action Reduce the amount of memory usage, or purchase additional memory.

%PIX-3-201006: RCMD backconnection failed for *IP_addr/port*

Explanation This is a connection-related message. This message is logged if the PIX Firewall is unable to preallocate connections for inbound standard output for **rsh** commands due to insufficient memory.

Action Check the **rsh** client version; the PIX Firewall only supports the Berkeley **rsh**. Also, reduce the amount of memory usage, or purchase additional memory.

%PIX-3-201008: The PIX is disallowing new connections.

Explanation This message occurs when you have enabled TCP syslogging and the syslog server cannot be reached, or when using PFSS (PIX Firewall Syslog Server) and the disk on the Windows NT system is full.

Action Disable TCP syslogging. If using PFSS, free up space on the Windows NT system where PFSS resides. Also make sure that the syslog host is up and you can ping the host from the PIX Firewall console. Then restart TCP syslogging to allow traffic.

%PIX-3-202001: Out of address translation slots!

Explanation This is a connection-related message. This message is logged if the PIX Firewall has no more address translation slots available.

Action Check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of *xlates* and connections. This could also be caused by insufficient memory; reduce the amount of memory usage, or purchase additional memory.

%PIX-3-202005: Non-embryonic in embryonic list *faddr/fport laddr/lport*

Explanation This is a connection-related message. This message is logged when a connection object (*xlate*) is in the wrong list.

Action Contact customer support. This should never happen.

```
%PIX-3-208005: (function:line_num) pix clear command return return_code
```

Explanation The PIX Firewall received a non-zero value (an internal error) when attempting to clear the configuration in Flash memory. The message includes the reporting subroutine's filename and line number.

Action For performance reasons, the end host should be configured to not inject IP fragments. This is most likely due to NFS. Set the read and write size to be the interface MTU for NFS.

```
%PIX-4-209003: Fragment database limit of bytes exceeded: src = IP_addr,
dest = IP_addr, proto = protocol, id = ID
```

Explanation Too many IP fragments are currently awaiting reassembly. The PIX Firewall limits the number of IP fragments that can be concurrently reassembled. This restriction prevents memory depletion at the firewall under abnormal network conditions. In general, fragmented traffic should be a small percentage of the total traffic mix. A noticeable exception is in the network environment with NFS over UDP. Consider NFS over TCP in such environment, if such traffic is to be relayed through the PIX Firewall. Refer to the **sysopt connection tpmss bytes** command page in Chapter 5, "Command Reference" of the *Configuration Guide for the Cisco Secure PIX Firewall Version 5.3* for more information.

Action If this message persists, a DoS (denial of service) attack might be in progress. Contact the remote peer's administrator or upstream provider.

```
%PIX-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes:
src = IP_addr, dest = IP_addr, proto = protocol, id = ID
```

Explanation An IP fragment is malformed. The total size of the reassembled IP packet exceeds the maximum possible size of 65,535 bytes.

Action A possible intrusion event may be in progress. If this message persists, contact the remote peer's administrator or upstream provider.

```
%PIX-4-209005: Discard IP fragment set with more than number elements:
src = IP_addr, dest = IP_addr, proto = protocol, id = ID
```

Explanation Too many elements are in a fragment set. The PIX Firewall disallows any IP packet that is fragmented into more than 12 fragments.

Action A possible intrusion event may be in progress. If the message persists, contact the remote peer's administrator or upstream provider.

Messages 210001 to 213004

%PIX-3-210001: LU *SW_Module_Name* error = *error_code*

Explanation This message is logged if a Stateful Failover error occurred.

Action If this error persists after traffic lessens through the PIX Firewall, report this error to customer support.

%PIX-3-210002: LU allocate block (*size*) failed.

Explanation Stateful Failover could not allocate a block of memory to transmit stateful information to the Standby PIX Firewall.

Action Check the failover interface to make sure its xmit is normal using the **show interface** command. Also check the current block memory using the **show block** command. If current available count is 0 within any of the blocks of memory, then reload the PIX Firewall software to recover the lost blocks of memory.

%PIX-3-210003: Unknown LU Object *ID*

Explanation Stateful Failover received an unsupported Logical Update object and therefore was unable to process it. This could be caused by corrupted memory, LAN transmissions, and other events.

Action If you see this error infrequently, then no action is required. If this error occurs frequently, check the Stateful Failover link LAN connection. If the error was not caused by a faulty failover link LAN connection, determine if an external user is trying to compromise the protected network. Check for misconfigured clients.

%PIX-3-210005: LU allocate connection failed

Explanation Stateful Failover cannot allocate a new connection on the Standby unit. This may be caused by little or no RAM memory available within the PIX Firewall.

Action Check the available memory using the **show mem** command to make sure the PIX Firewall has free memory in the system. If there is no available memory, add more physical memory to the PIX Firewall.

%PIX-3-210006: LU look NAT for *IP_addr* failed

Explanation Stateful Failover was unable to locate an NAT group for the *ip_address* on the Standby unit. Most likely, the active and standby PIX Firewall units are out of sync.

Action Use the **write standby** command on the Active unit to synchronize system memory with the Standby unit.

%PIX-3-210007: LU allocate xlate failed

Explanation Stateful Failover failed to allocate a translation slot (xlate) record.

Action Check the available memory using the **show mem** command to make sure the PIX Firewall has free memory in the system. If memory has been used up, you may need to add more physical memory.

%PIX-3-210008: LU no xlate for laddr/l_port faddr/f_port

Explanation Unable to find an translation slot (xlate) record for a Stateful Failover connection; unable to process the connection information.

Action Enter the **write standby** command on the Active unit to synchronize system memory between the Active and Standby units.

%PIX-3-210010: LU make UDP connection for faddr:f_port laddr:l_port failed

Explanation Stateful Failover was unable to allocate a new record for a UDP connection.

Action Check the available memory with the **show memory** command to make sure the PIX Firewall has free memory in the system. If memory has been used up, you may need to add more physical memory.

%PIX-3-210020: LU PAT port port_number reserve failed

Explanation Stateful Failover is unable to allocate a specific PAT address which is in use.

Action If this error repeats frequently, use the **write standby** command on the Active unit to synchronize system memory between the Active and Standby units.

%PIX-3-210021: LU create static xlate global_IP ifc int_name failed

Explanation Stateful Failover is unable to create a translation slot (xlate).

Action If this error repeats frequently, use the **write standby** command on the Active unit to synchronize system memory between the Active and Standby units.

%PIX-6-210022: LU missed number updates

Explanation Stateful Failover assigns a sequence number for each record sent to the Standby unit. When a received record sequence number is out of sequence with the last updated record, the information in between is assumed lost and this error message is sent.

Action Unless there are LAN interruptions, check the available memory on both PIX Firewall units to ensure there is enough memory to process the stateful information. Use the **show failover** command to monitor the quality of stateful information updates.

%PIX-3-211001: Memory allocation Error

Explanation Failed to allocate RAM system memory.

Action If this message occurs periodically, it can be ignored. If it repeats frequently, contact customer support.

%PIX-3-212001: Unable to open SNMP channel (UDP port *udp_port*) on interface *interface_number*, error code = *code*

Explanation This is an SNMP message. This message reports that the PIX Firewall is unable to receive SNMP requests destined for the PIX Firewall from SNMP management stations located on this interface. This does not affect the SNMP traffic passing through the PIX Firewall via any interface.

An error code of -1 indicates that PIX Firewall could not open the SNMP transport for the interface, an error code of -2 indicates that PIX Firewall could not bind the SNMP transport for the interface.

Action Once the PIX Firewall reclaims some of its resources when traffic is lighter, use the **snmp-server host** command for that interface again.

%PIX-3-212002: Unable to open SNMP trap channel (UDP port *udp_port*) on interface *interface_number*, error code = *code*

Explanation This is an SNMP message. This message reports that the PIX Firewall will be unable to send its SNMP traps from the PIX Firewall to SNMP management stations located on this interface. This does not affect the SNMP traffic passing through the PIX Firewall via any interface.

An error code of -1 indicates that PIX Firewall could not open the SNMP trap transport for the interface, an error code of -2 indicates that PIX Firewall could not bind the SNMP trap transport for the interface.

Action Once the PIX Firewall reclaims some of its resources when traffic is lighter, issue the **snmp-server host** command for that interface again.

%PIX-3-212003: Unable to receive an SNMP request on interface *interface_number*, error code = *code*, will try again.

Explanation This is an SNMP message. This message is logged because of an internal error in receiving an SNMP request destined for the PIX Firewall on the specified interface.

Action None required. The PIX Firewall SNMP agent will go back to wait for the next SNMP request.

%PIX-3-212004: Unable to send an SNMP response to IP Address *IP_addr* Port *port* interface *interface_number*, error code = *code*

Explanation This is an SNMP message. This message is logged because of an internal error in sending an SNMP response from the PIX Firewall to the specified host on the specified interface.

Action None required.

%PIX-3-212005: incoming SNMP request (*number bytes*) on interface *int_name* exceeds data buffer size, discarding this SNMP request.

Explanation This is an SNMP message. This message reports that the length of the incoming SNMP request, destined for the PIX Firewall, exceeds the size of the internal data buffer (512 bytes) used for storing the request during internal processing; therefore, PIX Firewall is unable to process this request. This does not affect the SNMP traffic passing through the PIX Firewall via any interface.

Action Have the SNMP management station resend the request with a shorter length, for example, instead of querying multiple MIB variables in one request, try querying only one MIB variable in a request. This may involve modifying the configuration of the SNMP manager software.

%PIX-3-213001: PPTP control daemon socket io *string*, errno = *num*.

Explanation An internal TCP socket I/O error occurred.

Action Report the problem to customer support.

%PIX-3-213002: PPTP tunnel hashtable insert failed, peer = *IP_addr*.

Explanation An internal software error occurred while creating a new PPTP tunnel.

Action Report the problem to customer support.

%PIX-3-213003: PPP virtual interface *number* isn't opened.

Explanation An internal software error occurred while closing a PPP virtual interface.

Action Report the problem to customer support.

%PIX-3-213004: PPP virtual interface *number* client ip allocation failed.

Explanation An internal software error occurred while allocating an IP address to the PPTP client.

Action This error occurs when the IP local address pool has been depleted. Consider allocating a larger pool with the **ip local pool** command.

Messages 302001 to 315011

%PIX-6-302001: Built inbound|outbound TCP connection id for *faddr faddr/fport gaddr gaddr/gport laddr laddr/lport (username)*

Explanation This is a connection-related message. This message reports that an authenticated inbound or outbound TCP connection was started to foreign address *faddr* using the global address *gaddr* from local address *laddr*. If the connection required authentication, the *username* is reported in the last field of the message.

Action None required.

```
%PIX-6-302002: Teardown TCP connection id for faddr IP_addr/port gaddr  
IP_addr/port laddr IP_addr/port (username) duration time bytes num (chars).
```

Explanation This is a connection-related message. This message is logged when a TCP connection is terminated. The duration and byte count for the session are reported. If the connection required authentication, the username is reported in the last field of the message. This message is used by the PIX Firewall Manager to generate reports.

Action None required.

```
%PIX-6-302003: Built H245 connection for faddr faddr/fport laddr laddr/lport
```

Explanation This is a connection-related message. This message is logged when an H.245 connection is started from foreign address *faddr* to local address *laddr*. This message only occurs if the PIX Firewall detects the use of an Intel Internet phone. The foreign port (*fport*) only displays on connections from outside the PIX Firewall. The local port value (*lport*) only appears on connections started on an internal interface.

Action None required.

```
%PIX-6-302004: Pre-allocate H323 UDP backconnection for faddr faddr/fport to  
laddr laddr/lport
```

Explanation This is a connection-related message. This message is logged when an H.323 UDP back-connection is preallocated to foreign address *faddr* from local address *laddr*. This message is only generated if the PIX Firewall detects the use of an Intel Internet phone. The foreign port (*fport*) only displays on connections from outside the PIX Firewall. The local port value (*lport*) only appears on connections started on an internal interface.

Action None required.

```
%PIX-6-302005: Built UDP connection for faddr faddr/fport gaddr gaddr/gport laddr  
laddr/lport
```

Explanation This is a connection-related message. This message is logged when a UDP connection is started to foreign address *faddr* using the global address *gaddr* from local address *laddr*.

Action None required.

```
%PIX-6-302006: Teardown UDP connection for faddr faddr/fport gaddr gaddr/gport  
laddr laddr/lport
```

Explanation This is a connection-related message. This message is logged when a UDP connection is terminated. The duration and byte count for the session are reported. If the connection required authentication, the username is also reported in the last field of the message. This message is used by the PIX Firewall Manager to generate reports.

Action None required.

```
%PIX-6-302009: Rebuilt TCP connection id for faddr faddr/fport gaddr gaddr/gport
laddr laddr/lport
```

Explanation This is a connection-related message. This message appears after a TCP connection is rebuilt after a failover. A sync packet is not sent to the other PIX Firewall. The *faddr* IP address is the foreign host, the *gaddr* IP address is a global address on the lower security level interface, and the *laddr* IP address is the local IP address “behind” the PIX Firewall on the higher security level interface.

Action None required.

```
%PIX-6-302010: conns in use, conns most used
```

Explanation This is a connection-related message. This message appears after a TCP connection restarts. *conns* is the number of connections.

Action None required.

```
%PIX-3-302302: ACL = deny; no sa created
```

Explanation Proxy mismatches. Proxy hosts for the negotiated SA correspond to a deny **access-list** command policy.

Action Check **access-list** command statement in the configuration. Contact the administrator for the peer.

```
%PIX-6-303002: src_addr Stored|Retrieved dest_addr: nat_addrs
```

Explanation This is an FTP/URL message. This message is logged when the specified host successfully stores or retrieves data from the specified FTP site. This message is used by the PIX Firewall Manager to generate reports.

Action None required.

```
%PIX-5-304001: user src_addr Accessed JAVA URL|URL dest_addr: url.
```

Explanation This is an FTP/URL message. This message is logged when the specified host successfully accesses the specified URL. This message is used by the PIX Firewall Manager to generate reports.

Action None required.

```
%PIX-5-304002: Access denied URL chars SRC IP_addr DEST IP_addr: chars
```

Explanation This is an FTP/URL message. This message is logged if access from the source address to the specified URL or FTP site is denied.

Action None required.

%PIX-3-304003: URL Server *IP_addr* timed out URL *string*

Explanation This message logs when a URL server times out.

Action None required.

%PIX-6-304004: URL Server *IP_addr* request failed URL *chars*

Explanation This is an FTP/URL message. This message is logged if a Websense server request fails.

Action None required.

%PIX-7-304005: URL Server *IP_addr* request pending URL *chars*

Explanation This is an FTP/URL message. This message is logged when a Websense server request is pending.

Action None required.

%PIX-3-304006: URL Server *IP_addr* not responding

Explanation This is an FTP/URL message. The Websense server is unavailable for access, and the PIX Firewall attempts to either try to access the same server if it is the only server installed, or another server if there is more than one.

Action None required.

%PIX-2-304007: URL Server *IP_addr* not responding, ENTERING ALLOW mode.

Explanation This is an FTP/URL message. This message is logged when you use the **allow** option of the **filter** command, and the Websense server(s) are not responding. The PIX Firewall allows all Web requests to continue without filtering while the server(s) are not available.

Action None required.

%PIX-2-304008: LEAVING ALLOW mode, URL Server is up.

Explanation This is an FTP/URL message. This message is logged when you use the **allow** option of the **filter** command, and the PIX Firewall receives a response message from a Websense server that previously was not responding. With this response message, the PIX Firewall exits the allow mode enabling once again the URL filtering feature.

Action None required.

```
%PIX-6-305001: Portmapped translation built for gaddr IP_addr/port laddr  
IP_addr/port
```

Explanation This is a connection-related message. This message is logged when an xlate is created for outbound traffic using a PAT global address. This applies to UDP, TCP, and ICMP packets.

Action None required.

```
%PIX-6-305002: Translation built for gaddr IP_addr to laddr IP_addr
```

Explanation This is a connection-related message. This message is logged when an xlate is created for outbound traffic using a global address, or for either outbound or inbound traffic using a static address.

Action None required.

```
%PIX-6-305003: Teardown translation for global IP_addr local IP_addr
```

Explanation This is a connection-related message. This message is logged when the PIX Firewall clears a dynamically allocated translation after the xlate timeout expires.

Action None required.

```
%PIX-6-305004: Teardown portmap translation for global IP_addr/port local  
IP_addr/port
```

Explanation This message is logged when a portmapped translation (PAT xlate) no longer in use has been reclaimed.

Action None required.

```
%PIX-3-305005: No translation group found for protocol.
```

Explanation This message logs when a **nat** and **global** command cannot be found for a protocol. The *protocol* can be TCP, UDP, or ICMP.

Action This message can be either an internal error or an error in the configuration.

```
%PIX-3-305006: Regular translation creation failed for protocol src  
int_name:IP_addr/port dst int_name:IP_addr/port
```

Explanation A protocol (UDP, TCP, or ICMP) failed to create a translation through the PIX Firewall. This message appears as a fix to caveat CSCdr0063 that requested that PIX Firewall not allow packets destined to network or broadcast addresses. PIX Firewall provides this checking for

addresses that are explicitly identified with **static** command statements. With the change, for inbound traffic, PIX Firewall denies translations for a destined IP address identified as a network or broadcast address.

PIX Firewall utilizes the global IP and mask from configured **static** command statements to differ regular IP addresses from network or broadcast IP addresses. If the global IP address is a valid network address with a matching network mask, then the PIX Firewall will not create an xlate for network or broadcast IP addresses with inbound packets. For example:

```
static (inside,outside) 10.2.2.128 10.1.1.128 netmask 255.255.255.128
```

Global address 10.2.2.128 is treated as a network address and 10.2.2.255 as the broadcast address. Without an existing xlate, PIX Firewall denies inbound packets destined for 10.2.2.128 or 10.2.2.255, and logs this syslog message.

In case the suspected IP is really a host IP, a separated **static** command statement with a host mask needs to be configured and in front of the subnet static (first match rule for **static** command statements). The following static causes PIX Firewall to treat 10.2.2.128 as a host address:

```
static (inside,outside) 10.2.2.128 10.2.2.128 netmask 255.255.255.255
static (inside,outside) 10.2.2.128 10.2.2.128 netmask 255.255.255.128
```

The xlate may be created by traffic started with the inside host with the questioned IP address. PIX Firewall treats a network or broadcast IP address as a host IP address with overlapped subnet static config, the network address translation for both static need be the same.

Action This message can be either an internal error or an error in the configuration.

```
%PIX-6-305007: Orphan IP IP_addr on interface interface_number
```

Explanation This message logs after the PIX Firewall attempts to translate an address that it cannot find in any of its global pools. The PIX Firewall assumes that the address has been deleted and drops the request.

Action None required.

```
%PIX-3-305008: Free unallocated global IP address.
```

Explanation The PIX kernel detected an inconsistency condition when trying to free an unallocated global IP address back to the address pool. This abnormal condition may occur if the PIX Firewall is running a Stateful Failover setup and some of the internal states are momentarily out of sync between the active and standby unit. This condition is not catastrophic and the PIX Firewall will recover automatically.

Action Report this condition to Cisco support if you continue to see this message.

%PIX-6-307001: Denied Telnet login session from *IP_addr* on interface *int_name*.

Explanation This is a PIX Firewall management message. This message is logged when the PIX Firewall denies an attempt to connect to the Telnet port from the specified IP address on the inside network.

Action From the console, enter the **show telnet** command to verify that the PIX Firewall is configured to permit Telnet access from that host or network. From the PIX Firewall Manager, select **Administration>Telnet Hosts** for host information.

%PIX-6-307002: Permitted Telnet login session from *IP_addr*

Explanation This is a PIX Firewall management message. This message logs a successful Telnet connection to the PIX Firewall.

Action None required.

%PIX-6-307003: telnet login session failed from *IP_addr* (*num* attempts) on interface *int_name*.

Explanation This is a PIX Firewall management message. The PIX Firewall logs this message after an incorrect Telnet password was entered *num* times for the same connection. Up to three attempts are allowed to log into a console Telnet session.

Action Verify the password and try again.

%PIX-6-308001: PIX console enable password incorrect for *num* tries (from *IP_addr*).

Explanation This is a PIX Firewall management message. This message is logged after the *num* number of times a user miss types the password to enter privileged mode. The maximum is three attempts.

Action The privileged mode password is not necessarily the same as the password for Telnet access to the PIX Firewall. Verify the password and try again.

%PIX-4-308002: static *gaddr1 laddr1 netmask mask1* overlapped with *gaddr2 laddr2*

Explanation This message occurs if the IP addresses in one or more **static** command statements overlap. *gaddr* is the global address, which is the address on the lower security interface and *laddr* is the local address, which is the address on the higher security level interface.

Action Use the **show static** command to view the **static** command statements in your configuration and fix the commands that overlap. The most common overlap occurs if you specify a network address such as 10.1.1.0 and in another **static** command statement, specify a host within that range such as 10.1.1.5.

%PIX-3-309001: Denied manager connection from *IP_addr*.

Explanation This is a PIX Firewall management message. This message is logged when the PIX Firewall Manager denies an attempt to connect to its Telnet port from the specified IP address on the inside network.

Action None required.

%PIX-6-309002: Permitted manager connection from *IP_addr*.

Explanation This is a PIX Firewall management message. This message logs a successful PIX Firewall Manager connection.

Action None required.

%PIX-6-311001: LU loading standby start

Explanation This message appears when Stateful Failover update information is sent to the Standby PIX Firewall unit when the Standby unit is first coming online.

Action None required.

%PIX-6-311002: LU loading standby end

Explanation This message appears when Stateful Failover update information is done being sent to the Standby unit.

Action None required.

%PIX-6-311003: LU rcv thread up

Explanation This message appears when an update acknowledgment has been received from the Standby unit.

Action None required.

%PIX-6-311004: LU xmit thread up

Explanation This message appears when a Stateful Failover update is transmitted to the Standby unit.

Action None required.

```
%PIX-6-312001: RIP hdr failed from IP_addr: cmd=cmd, version=vers domain=name on
interface int_name
```

Explanation PIX Firewall received a RIP message with an operation code other than reply, the message has a version number different than what is expected on this interface, and the routing domain entry was non-zero.

Action This message is informational, but may also indicate that another RIP device is not configured correctly to communicate with the PIX Firewall.

```
%PIX-3-313001: Denied ICMP type=icmp_type, code=type_code from IP_addr on
interface int_name
```

Explanation When using the **icmp** command with an access list, if the first matched entry is a permit entry, ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, PIX Firewall discards the ICMP packet and generates this syslog message. The **icmp** command enables or disables pinging to an interface. With pinging disabled, the PIX Firewall cannot be detected on the network. This feature is also referred to as configurable proxy pinging.

Action Contact the peer's administrator.

```
%PIX-6-314001: Pre-allocate RTSP UDP backconnection for faddr faddr/fport to
laddr laddr/lport
```

Explanation PIX Firewall opened an RTSP connection for the specified IP addresses and ports.

Action No action required.

```
%PIX-3-315001: Denied SSH session from IP_addr on interface int_name
```

Explanation This SSH message logs when the PIX Firewall denies an attempt to connect to the SSH port from the specified IP address on the specified network interface.

Action From the console, enter the **show ssh** command to verify that the PIX Firewall is configured to permit SSH access from the host or network.

```
%PIX-6-315002: Permitted SSH session from IP_addr on interface int_name for user
"user_id"
```

Explanation This SSH message appears when an SSH session starts. The *ip_addr*, IP address, is the address of the host with the SSH client. The *int_name*, interface name, is the interface through which the SSH session is started. The *user_ID* is the username to which the client is accessing. Use the **ssh show sessions** command to view the status of SSH sessions. If the *user_id* is **pix**, the connection is to the PIX Firewall console. For example, if host 10.21.196.38 on the outside interface starts an SSH session to the PIX Firewall console, the message text appears as follows:

```
%PIX-6-315002: Permitted SSH session from 10.21.196.38 on interface outside for user
"pix"
```

Action None required.

```
%PIX-6-315003: SSH login session failed from IP_addr on (num attempts) on
interface int_name by user "user_id"
```

Explanation This SSH message appears after an incorrect user ID or password were entered *num* times for the same connection. Up to three attempts are allowed to log into a SSH console session. The *ip_addr*, IP address, is the address of the host with the SSH client. The *int_name*, interface name, is the interface through which the SSH session is started. The *user_ID* is the username that the client is attempting to access. If the *user_id* is **pix**, the connection attempt was to the PIX Firewall console.

Action If this message appears infrequently, no action is required. If this message appears frequently, it can indicate an attack. Inform the user to verify their username and password.

```
%PIX-3-315004: Fail to establish SSH session because PIX RSA host key retrieval
failed.
```

Explanation This SSH message appears when the PIX Firewall cannot find the PIX Firewall unit's RSA host key, which is required for establishing an SSH session. The PIX Firewall host key may be absent because no PIX Firewall host key has been generated or because the license for this PIX Firewall does not allow DES or 3DES.

Action From the console, enter the **show ca mypubkey rsa** command to verify that PIX Firewall unit's RSA host key is present. If not, also enter **show version** to check whether the PIX Firewall unit's license allows DES or 3DES.

```
%PIX-6-315011: SSH session from IP_addr on interface int_name for user "user_id"
terminated normally
```

```
%PIX-6-315011: SSH session from IP_addr on interface int_name for user "user_id"
disconnected by SSH server, reason: "text"
```

Explanation This message appears after an SSH session completes. If a user enters quit or exit, this message displays "terminated normally." If the session disconnected for another reason, the text describes the reason. The following table lists the possible reasons for why a session disconnected:

Table 2-1 %PIX-6-315011 SSH Disconnect Reasons

Text String	Explanation	Action
Bad checkbytes	A mismatch was detected in the check bytes during an SSH key exchange.	Restart the SSH session.
CRC check failed	The CRC value computed for a particular packet does not match the CRC value embedded in the packet; the packet is bad.	No action required. If this message persists, call customer support.
Decryption failure	Decryption of an SSH session key failed during an SSH key exchange.	Check the RSA host key and try again.
Format error	A non-protocol version message was received during an SSH version exchange.	Check the SSH client, to ensure it is a supported version.

Table 2-1 %PIX-6-315011 SSH Disconnect Reasons (continued)

Text String	Explanation	Action
Internal error	This message indicates either an error internal to SSH on the PIX Firewall or an RSA key may not have been entered on the PIX Firewall or cannot be retrieved.	From the PIX Firewall console, enter the show ca mypubkey rsa to verify that RSA host key is present. If not, also enter the show version command to verify whether DES or 3DES is allowed. If an RSA host key is present, just restart the SSH session.
Invalid cipher type	The SSH client requested an unsupported cipher.	Enter the show version command to determine what features your license supports, then reconfigure the SSH client to use the supported cipher.
Invalid message length	The length of SSH message arriving at the PIX Firewall exceeds 262,144 bytes or is shorter than 4,096 bytes. The data may be corrupted.	No action required.
Invalid message type	PIX Firewall received a non-SSH message or an unwanted SSH message.	Check whether the peer is an SSH client.
Out of memory	This message appears when the PIX Firewall is unable to allocate memory for use by the SSH server, probably when the PIX Firewall is busy with high traffic.	Restart the SSH session later.
Rejected by server	User authentication failed.	Ask the user to verify their username and password.
Reset by client	An SSH client sent the SSH_MSG_DISCONNECT message to the PIX Firewall.	No action required.
status code: <i>hex</i> (<i>hex</i>)	Users closed the SSH client window (running on Windows) instead of entering quit or exit at the SSH console.	No action required. Encourage users to exit the client gracefully instead of just exiting.
Terminated by operator	The SSH session was terminated by entering the ssh disconnect command at the PIX Firewall console.	No action required.
Time-out activated	The SSH session timed out because the duration specified by the ssh timeout command was exceeded.	No action required. Restart the SSH connection. You can use the ssh timeout command to increase the default value of 5 minutes up to 60 minutes if required.

Messages 40000 to 709007

%PIX-4-4000nn: IDS: *sig_num sig_msg* from *IP_addr* to *IP_addr* on interface *int_name*

Explanation Messages 400000 through 400051—Cisco Secure Intrusion Detection System signature messages.

Action Refer to the *Cisco Secure Intrusion Detection System Version 2.2.1 User Guide* for more information. You can view the “NSDB and Signatures” chapter, which describes each signature number (*sig_num*) at the following site:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids1/csidsug/sigs.htm>

All signature messages are not supported by PIX Firewall in this release. IDS syslog messages all start with %PIX-4-4000nn and have the following format:

%PIX-4-4000nn IDS:sig_num sig_msg from ip_addr to ip_addr on interface int_name

Options:

sig_num The signature number. Refer to the *Cisco Secure Intrusion Detection System Version 2.2.1 User Guide* at the following site:

<http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids1/csidsug/sigs.htm>

sig_msg The signature message—approximately the same as the NetRanger signature message.

ip_addr The local to remote address to which the signature applies.

int_name The name of the interface on which the signature originated.

For example:

```
%PIX-4-400013 IDS:2003 ICMP redirect from 10.4.1.2 to 10.2.1.1 on interface dmz
```

```
%PIX-4-400032 IDS:4051 UDP Snork attack from 10.1.1.1 to 192.168.1.1 on interface outside
```

Table 2-2 lists the supported signature messages.

Table 2-2 *IDS Syslog Messages*

Message #	Signature ID	Signature Title	Signature Type
400000	1000	IP options-Bad Option List	Informational
400001	1001	IP options-Record Packet Route	Informational
400002	1002	IP options-Timestamp	Informational
400003	1003	IP options-Security	Informational
400004	1004	IP options-Loose Source Route	Informational
400005	1005	IP options-SATNET ID	Informational
400006	1006	IP options-Strict Source Route	Informational
400007	1100	IP Fragment Attack	Attack
400008	1101	IP Unknown IP Protocol	Attack
400009	1103	IP Fragments Overlap	Attack
400010	2000	ICMP Echo Reply	Informational
400011	2001	ICMP Host Unreachable	Informational
400012	2002	ICMP Source Quench	Informational
400013	2003	ICMP Redirect	Informational
400014	2004	ICMP Echo Request	Informational
400015	2005	ICMP Time Exceeded for a Datagram	Informational
400016	2006	ICMP Parameter Problem on Datagram	Informational
400017	2007	ICMP Timestamp Request	Informational
400018	2008	ICMP Timestamp Reply	Informational
400019	2009	ICMP Information Request	Informational

Table 2-2 IDS Syslog Messages (continued)

Message #	Signature ID	Signature Title	Signature Type
400020	2010	ICMP Information Reply	Informational
400021	2011	ICMP Address Mask Request	Informational
400022	2012	ICMP Address Mask Reply	Informational
400023	2150	Fragmented ICMP Traffic	Attack
400024	2151	Large ICMP Traffic	Attack
400025	2154	Ping of Death Attack	Attack
400026	3040	TCP NULL flags	Attack
400027	3041	TCP SYN+FIN flags	Attack
400028	3042	TCP FIN only flags	Attack
400029	3153	FTP Improper Address Specified	Informational
400030	3154	FTP Improper Port Specified	Informational
400031	4050	UDP Bomb attack	Attack
400032	4051	UDP Snork attack	Attack
400033	4052	UDP Chargen DoS attack	Attack
400034	6050	DNS HINFO Request	Attack
400035	6051	DNS Zone Transfer	Attack
400036	6052	DNS Zone Transfer from High Port	Attack
400037	6053	DNS Request for All Records	Attack
400038	6100	RPC Port Registration	Informational
400039	6101	RPC Port Unregistration	Informational
400040	6102	RPC Dump	Informational
400041	6103	Proxied RPC Request	Attack
400042	6150	ypserv (YP server daemon) Portmap Request	Informational
400043	6151	ybind (YP bind daemon) Portmap Request	Informational
400044	6152	yppasswdd (YP password daemon) Portmap Request	Informational
400045	6153	ypupdated (YP update daemon) Portmap Request	Informational
400046	6154	ypxfrd (YP transfer daemon) Portmap Request	Informational
400047	6155	mountd (mount daemon) Portmap Request	Informational
400048	6175	rex (remote execution daemon) Portmap Request	Informational
400049	6180	rex (remote execution daemon) Attempt	Informational
400050	6190	statd Buffer Overflow	Attack

```
%PIX-4-402101: decaps: rec'd IPSEC packet has invalid spi for destaddr=IP_addr,
prot=protocol, spi=spi
```

Explanation Received IPsec packet specifies SPI that does not exist in SADB. This may be a temporary condition due to slight differences in aging of SAs between the IPsec peers, or it may be because the local SAs have been cleared. It may also be because of incorrect packets sent by the IPsec peer. This may also be an attack.

Action The peer may not acknowledge that the local SAs have been cleared. If a new connection is established from the local router, the two peers may then reestablish successfully. Otherwise, if the problem occurs for more than a brief period, either attempt to establish a new connection or contact the peer's administrator.

```
%PIX-4-402102: decapsulate: packet missing packet_type, destaddr=dest_addr,
actual prot=protocol
```

Explanation Received IPsec packet missing an expected AH or ESP header. The peer is sending packets that do not match the negotiated security policy. This may be an attack. *packet_type* is either AH or ESP.

Action Contact the peer's administrator.

```
%PIX-4-402103: identity doesn't match negotiated identity (ip) dest_addr=
IP_addr, src_addr= IP_addr, prot= protocol, (ident) local=IP_addr,
remote=IP_addr, local_proxy=IP_addr/IP_addr/port/port,
remote_proxy=IP_addr/IP_addr/port/port
```

Explanation An unencapsulated IPsec packet does not match the negotiated identity. The peer is sending other traffic through this security association. It may be due to an security association selection error by the peer. This may be a hostile event.

Action Contact the peer's administrator to compare policy settings.

```
%PIX-4-402106: Rec'd packet not an IPSEC packet (ip) dest_addr= IP_addr,
src_addr= IP_addr, prot= protocol
```

Explanation The received packet matched the crypto map ACL, but it is not IPsec-encapsulated; the IPsec Peer is sending unencapsulated packets. This error can occur because of a policy setup error on the peer. For example, the firewall only accepts encrypted Telnet traffic to the outside interface port 23. If you attempt to Telnet without IPsec encryption to the outside interface on port 23, this message appears. This error can also signify a hostile event. This syslog message is not generated except under the conditions cited (for example, it is not generated for traffic to the firewall interfaces themselves). See messages 307001, 309001, and 315001 for messages that track some denied sessions.

Action Contact the peer's administrator to compare policy settings.

```
%PIX-4-403101: PPTP session state not established, but received an XGRE packet,  
tunnel_id=id, session_id=session
```

Explanation PIX Firewall received a PPTP XGRE packet without a corresponding control connection session.

Action If this message occurs frequently, report the problem to customer support.

```
%PIX-4-403102: PPP virtual interface int_name rcvd pkt with invalid protocol:  
protocol, reason: text.
```

Explanation PIX Firewall received an XGRE encapsulated PPP packet with an invalid protocol field.

Action If this message occurs frequently, report the problem to customer support.

```
%PIX-4-403103: PPP virtual interface max connections reached.
```

Explanation PIX Firewall cannot accept additional PPTP connections.

Action None required. Connections are allocated as soon as they are freed.

```
%PIX-4-403104: PPP virtual interface int_name requires mschap for MPPE.
```

Explanation The MPPE is configured but MS-CHAP authentication is not.

Action Add MS-CHAP authentication with the **vpdn group group_name ppp authentication** command.

```
%PIX-4-403106: PPP virtual interface int_name requires RADIUS for MPPE.
```

Explanation The MPPE is configured but RADIUS authentication is not.

Action Add RADIUS authentication with the **vpdn group group_name ppp authentication** command.

```
%PIX-4-403107: PPP virtual interface int_name missing aaa server group info
```

Explanation AAA server configuration information cannot be found.

Action Add AAA server information with the **vpdn group group_name client authentication aaa aaa_server_group** command.

```
%PIX-4-403108: PPP virtual interface int_name missing client ip address option
```

Explanation The client IP address pool information is missing.

Action Add IP address pool info with the **vpdn group group_name client configuration address local address_pool_name** command.

```
%PIX-4-403109: Rec'd packet not an PPTP packet. (ip) dest_addr= IP_addr,
src_addr= IP_addr, data: text.
```

Explanation The PIX Firewall received a spoofed PPTP packet. This may be a hostile event. The PIX Firewall received a spoofed PPTP packet. This may be a hostile event.

Action Contact the system administrator for the peer to check the PPTP configuration settings.

```
%PIX-4-403110: PPP virtual interface int_name, user: user missing MPPE key from
aaa server.
```

Explanation The AAA server is not returning the MPPE key attributes required to set up the MPPE encryption policy.

Action Check the AAA server configuration and If the AAA server cannot return MPPE key attributes, use local authentication instead with the **vpdn group group_name client authentication local** command.

```
%PIX-4-404101: ISAKMP: Failed to allocate address for client from pool pool_id
```

Explanation ISAKMP failed to allocate an IP address for the VPN Client from the pool you specified with the **ip local pool** command statement.

Action Use the **ip local pool** command to specify additional IP addresses for the pool.

```
%PIX-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for faddr
faddr[/fport] to laddr laddr[/lport]
```

Explanation PIX Firewall failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

Action If this message occurs periodically, it can be ignored. If it repeats frequently, contact customer support. Also, check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of xlates and connections. This could also be caused by insufficient memory; reduce the amount of memory usage, or purchase additional memory.

```
%PIX-4-405102: Unable to Pre-allocate H245 Connection for faddr faddr[/fport] to
laddr laddr[/lport]
```

Explanation PIX Firewall failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

Action If this message occurs periodically, it can be ignored. If it repeats frequently, contact customer support. Also, check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of xlates and connections. This could also be caused by insufficient memory; reduce the amount of memory usage, or purchase additional memory.

```
%PIX-5-500001: ActiveX content modified src IP_addr dest IP_addr on interface int_name.
```

Explanation This message is logged after you turn on the **activex** option using the **filter** command, and the PIX Firewall detects an ActiveX object. The **activex** option allows the PIX Firewall to filter out ActiveX contents by modifying it so that it no longer is tagged as an HTML object.

Action None required.

```
%PIX-5-500002: Java content modified src IP_addr dest IP_addr on interface int_name.
```

Explanation This message is logged after you turn on the **java** option using the **filter** command, and the PIX Firewall detects a Java applet. The **java** option allows the PIX Firewall to filter out Java contents by modifying it so that it no longer is tagged as an HTML object.

Action None required.

```
%PIX-5-500003: Bad TCP hdr length (hdrlen=bytes, pktlen=bytes) from src_addr/src_port to dest_addr/dport, flags: tcp_flags, on interface int_name
```

Explanation This message indicates that a header length in TCP is incorrect. Some operating systems do not handle TCP RSTs (resets) correctly when responding to a connection request to a disabled socket. If a client tries to connect to an FTP server outside the PIX Firewall and FTP is not listening, then the server sends a RST. Some operating systems send incorrect TCP header lengths which causes this problem. UDP uses ICMP port unreachable messages.

The TCP header length may indicate that it is larger than the packet length resulting in a negative number of bytes being transferred. A negative number is displayed by syslog as an unsigned number making it appear far larger than would be normal; for example, showing 4 GB transferred in 1 second.

Action None required. This message should occur infrequently.

```
%PIX-4-500004: Invalid transport field for protocol=protocol, from src_addr/src_port to dest_addr/dest_port
```

Explanation This message appears when there is an invalid transport number, in which the source or destination port number for a protocol is zero. The *protocol* field is 6 for TCP and 17 for UDP.

Action If these messages persist, contact the peer's administrator.

```
%PIX-6-602101: PMTU-D packet packet_length bytes greater than effective mtu mtu_value dest_addr=dest_ip, src_addr=source_ip, prot=protocol
```

Explanation This message occurs when the PIX Firewall sends an ICMP destination unreachable message and when fragmentation is needed, but the “don't-fragment” bit is set.

Action Ensure that the data is sent correctly.

%PIX-6-602102: Adjusting IPSec tunnel mtu...

Explanation The MTU for an IPSec tunnel is adjusted from Path MTU Discovery.

Action Check MTU of the IPSec tunnels. If effective MTU is smaller than normal, check intermediate links.

%PIX-6-602301: sa created...

Explanation A new SA (security association) was created.

Explanation Informational message.

%PIX-6-602302: deleting sa...

Explanation An SA was deleted.

Action Informational message.

%PIX-6-603101: PPTP received out of seq or duplicate pkt, tnl_id=*id*, sess_id=*session*, seq=*num*.

Explanation PIX Firewall received a PPTP packet that was out of sequence or duplicated.

Action If the packet count is high, contact the peer administrator to check client PPTP configuration.

%PIX-6-603102: PPP virtual interface *int_name* - user: *user* aaa authentication started.

Explanation PIX Firewall sent an authentication request to the AAA server.

Action None required.

%PIX-6-603103: PPP virtual interface *int_name* - user: *user* aaa authentication *status*.

Explanation PIX Firewall received an authentication response from the AAA server.

Action None required.

%PIX-6-603104: PPTP Tunnel created, tunnel_id is *id*, remote_peer_ip is *IP_addr*, ppp_virtual_interface_id is *id*, client_dynamic_ip is *IP_addr*, username is *login*, MPPE_key_strength is *chars*

Explanation A PPTP tunnel was created.

Action None required.

```
%PIX-6-603105: PPTP Tunnel deleted, tunnel_id = id, remote_peer_ip= IP_addr
```

Explanation A PPTP tunnel was deleted.

Action None required.

```
%PIX-6-604101: DHCP client interface int_name: Allocated ip = ip_address,  
mask = mask, gw = gateway_address
```

Explanation The PIX Firewall DHCP client successfully obtained an IP address from a DHCP server. The **dhcpc** command statement lets PIX Firewall obtain an *ip_address* and network *mask* for a network interface from a DHCP server as well as a default route. The default route statement uses the *gateway_address* as the address of the default router.

Action None required.

```
%PIX-6-604102: DHCP client interface int_name: address released
```

Explanation The PIX Firewall DHCP client released an allocated IP address back to the DHCP server.

Action None required.

```
%PIX-6-604103: DHCP daemon interface int_name: address granted MAC_addr (IP_addr)
```

Explanation The PIX Firewall DHCP server granted an IP address to an external client.

Action None required.

```
%PIX-6-604104: DHCP daemon interface int_name: address released
```

Explanation An external client released an IP address back to the PIX Firewall DHCP server.

Action None required.

```
%PIX-7-701001: alloc_user() out of Tcp_user objects
```

Explanation This is an AAA message. This message is logged if the user authentication rate is too high for the PIX Firewall to handle new **aaa** requests.

Action Enable **floodguard** with the **floodguard enable** command.

```
%PIX-7-702301: lifetime expiring...
```

Explanation An SA lifetime has expired.

Action Debugging message.

%PIX-3-702302: replay rollover detected...

Explanation More than 4 billion packets have been received in the IPsec tunnel and a new tunnel will now be negotiated.

Explanation Contact the peer's administrator to compare the SA lifetime setting.

%PIX-7-702303: sa_request...

Explanation IPsec has requested IKE for new SAs.

Action Debugging message.

%PIX-7-709001: FO replication failed: cmd=*command* returned=*code*

%PIX-7-709002: FO unreplicable: cmd=*command*

Explanation These failover messages only appear during the development debug testing phase.

Action None required.

%PIX-1-709003: (Primary) Beginning configuration replication: Receiving from mate.

Explanation This is a failover message. This message is logged when the Active unit starts replicating its configuration to the Standby unit. "(Primary)" can also be listed as "(Secondary)" for the Secondary unit.

Action None required.

%PIX-1-709004: (Primary) End Configuration Replication (ACT)

Explanation This is a failover message. This message is logged when the Active unit completes replicating its configuration on the Standby unit. "(Primary)" can also be listed as "(Secondary)" for the Secondary unit.

Action None required.

%PIX-1-709005: (Primary) Beginning configuration replication: Receiving from mate.

Explanation This message indicates that the standby PIX Firewall received the first part of the configuration replication from the active PIX Firewall. "(Primary)" can also be listed as "(Secondary)" for the Secondary unit.

Action None required.

%PIX-1-709006: (Primary) End Configuration Replication (STB)

Explanation This is a failover message. This message is logged when the Standby unit completes replicating a configuration sent by the Active unit. “(Primary)” can also be listed as “(Secondary)” for the Secondary unit.

Action None required.

%PIX-2-709007: Configuration replication failed for command *command_name*

Explanation This is a failover message. This message is logged when the Standby unit is unable to complete replicating a configuration sent by the Active unit. The command at which the failure occurs displays at the end of the message.

Action Write down the command name and inform customer support.

