



System Log Messages

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



Note

The messages shown in this guide apply to Cisco PIX Firewall Version 6.3 and higher. When a number is skipped from a sequence, the message is no longer in the PIX Firewall code.

This chapter includes the following sections:

- [Messages 101001 to 199005, page 2-1](#)
- [Messages 201002 to 215001, page 2-25](#)
- [Messages 302003 to 320001, page 2-36](#)
- [Messages 400000 to 409023, page 2-54](#)
- [Messages 410001 to 410001, page 2-71](#)
- [Messages 411001 to 416001, page 2-71](#)
- [Messages 500001 to 503001, page 2-73](#)
- [Messages 602101 to 620002, page 2-75](#)
- [Messages 701001 to 710006, page 2-92](#)

Messages 101001 to 199005

This section contains messages from 101001 to 199005.

101001

Error Message %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.

Recommended Action None required.

101002

Error Message %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.

Recommended Action Replace the failover cable.

101003, 101004

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

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

Explanation Both instances are failover messages. These messages are logged when failover mode is 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.

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

101005

Error Message %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.

Recommended Action Replace the cable.

102001

Error Message %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.

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

103001

Error Message %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. [Table 2-1](#) lists the Reason Codes and the descriptions to determine why the failover occurred.

Table 2-1 Reason Codes

Reason Code	Description
1	No failover hello seen on Serial cable for 30 + seconds. This ensures that failover is running properly on the other firewall unit.
2	An interface did not pass one of the 4 failover tests. The 4 tests are: 1) Link Up, 2) Monitor for Network Traffic, 3) ARP test, 4) Broadcast Ping test.
3	No proper ACK for 15+ seconds after a command was sent on the serial cable.

Recommended Action Verify the failover cable is connected properly and both units have the same hardware, software, and configuration; otherwise contact Cisco TAC.

103002

Error Message %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 1-4 in Chapter 1, “Introduction,”](#) for possible values for the *interface_number* variable.

Recommended Action None required.

103003

Error Message %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 1-4 on page 1-17](#) for possible values for the *interface_number* variable.

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

103004

Error Message %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.

Recommended Action Verify the status of the primary unit.

103005

Error Message %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.

Recommended Action Verify the status of the secondary unit.

104001, 104002

Error Message %PIX-1-104001: (Primary) Switching to ACTIVE (cause: *string*).

Error Message %PIX-1-104002: (Primary) Switching to STNDBY (cause: *string*).

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 *string* variable are as follows:

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

Recommended 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.

104003

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

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

Recommended 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.

104004

Error Message %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.

Recommended Action None required.

105001

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

Explanation In version 6.x and earlier, this message is generated when the switching of active and standby roles is detected. In this case, the secondary unit disables failover automatically. Failover is also disabled if a version mismatch between the primary and secondary units occurs. “(Primary)” can also be listed as “(Secondary)” for the secondary unit.

Recommended Action None required.

105002

Error Message %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.

Recommended Action None required.

105003

Error Message %PIX-1-105003: (Primary) Monitoring on interface *interface_name* waiting

Explanation This is a failover message. The firewall is testing the specified network interface with the other unit of the failover pair. “(Primary)” can also be listed as “(Secondary)” for the secondary unit.

Recommended Action None required. The firewall monitors its network interfaces frequently during normal operations.

105004

Error Message %PIX-1-105004: (Primary) Monitoring on interface *interface_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.

Recommended Action None required.

105005

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

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

105006, 105007

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

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

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

105008

Error Message %PIX-1-105008: (Primary) Testing interface *interface_name*.

Explanation This is a failover message. This message is logged when the firewall tests a specified network interface. This testing is performed only if the 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.

Recommended Action None required.

105009

Error Message %PIX-1-105009: (Primary) Testing on interface *interface_name* {Passed|Failed}.

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.

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

105010

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

Explanation Block memory was depleted. This is a transient message and the firewall should recover. “(Primary)” can also be listed as “(Secondary)” for the secondary unit.

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

105011

Error Message %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.

Recommended Action Ensure that the cable is properly connected.

105020

Error Message %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.

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

105031

Error Message %PIX-1-105031: Failover LAN interface is up

Explanation LAN failover interface link is up.

Recommended Action None required.

105032

Error Message %PIX-1-105032: LAN Failover interface is down

Explanation LAN failover interface link is down.

Recommended Action Check the connectivity of the LAN failover interface. Make sure the speed/duplex setting is correct.

105034

Error Message %PIX-1-105034: Receive a LAN_FAILOVER_UP message from peer.

Explanation The peer has just booted and sent the initial contact message.

Recommended Action None required.

105035

Error Message %PIX-1-105035: Receive a LAN failover interface down msg from peer.

Explanation The peer LAN failover interface link is down. The unit switches to active mode if it is in standby mode.

Recommended Action Check the connectivity of the peer's LAN failover interface.

105036

Error Message %PIX-1-105036: PIX dropped a LAN Failover command message.

Explanation The firewall dropped an unacknowledged LAN failover command message, indicating a connectivity problem on the LAN failover interface.

Recommended Action Check that the LAN interface cable is connected.

105037

Error Message %PIX-1-105037: The primary and standby units are switching back and forth as the active unit.

Explanation The primary and standby units are switching back and forth as the active unit, indicating a LAN failover connectivity problem or software bug.

Recommended Action Check that the LAN interface cable is connected.

106001

Error Message %PIX-2-106001: Inbound TCP connection denied from *IP_address/port* to *IP_address/port* flags *tcp_flags* on interface *interface_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 and 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.

Recommended Action None required.

106002

Error Message %PIX-2-106002: *protocol* Connection denied by outbound list *acl_ID* src *inside_address* dest *outside_address*

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.

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

106006

Error Message %PIX-2-106006: Deny inbound UDP from *outside_address/outside_port* to *inside_address/inside_port* on interface *interface_name*.

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

Recommended Action None required.

106007

Error Message %PIX-2-106007: Deny inbound UDP from *outside_address/outside_port* to *inside_address/inside_port* due to DNS {Response|Query}.

Explanation This is a connection-related message. This message is logged if a UDP packet containing a DNS query or response is denied.

Recommended 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.

106010

Error Message %PIX-3-106010: Deny inbound *protocol* src
interface_name:dest_address/dest_port dst
interface_name:source_address/source_port

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

Recommended Action Modify the security policy if traffic should be permitted. If the message occurs at regular intervals, contact the remote peer administrator.

106011

Error Message %PIX-3-106011: Deny inbound (No xlate) *string*

Explanation The message will appear under normal traffic conditions if there are internal users that are accessing the Internet via a web browser. Anytime a connection is reset, when the host at the end of the connection sends a packet after the firewall receives the reset, this message will appear. It can typically be ignored.

Recommended Action Disable this syslog message from getting logged to the syslog server by entering the **no logging message 106011** command.

106012

Error Message %PIX-2-106012: Deny IP from *IP_address* to *IP_address*, IP options *hex*.

Explanation This is a packet integrity check message. An IP packet was seen with IP options. Because IP options are considered a security risk, the packet was discarded.

Recommended Action Contact the remote host system administrator to determine the problem. Check the local site for loose source or strict source routing.

106013

Error Message %PIX-2-106013: Dropping echo request from *IP_address* to PAT address
IP_address

Explanation This message is logged when the 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 cannot specify which PAT host should receive the packet.

Recommended Action None required.

106014

Error Message %PIX-3-106014: Deny inbound icmp src *interface_name: IP_address* dst *interface_name: IP_address* (type *dec*, code *dec*)

Explanation This message is logged when the firewall denies any inbound ICMP packet access. By default, all ICMP packets are denied access unless specifically permitted using the **conduit permit icmp** command. Now that the **icmp** command has been implemented, the **conduit** command has been deprecated and is no longer guaranteed to work properly.

Recommended Action None required.

106015

Error Message %PIX-6-106015: Deny TCP (no connection) from *IP_address/port* to *IP_address/port* flags *tcp_flags* on interface *interface_name*.

Explanation This message is logged when the firewall discards a TCP packet that has no associated connection in the firewall unit's connection table. The 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 firewall discards the packet.

Recommended Action None required unless the 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.

106016

Error Message %PIX-2-106016: Deny IP spoof from (*IP_address*) to *IP_address* on interface *interface_name*.

Explanation This message is generated when a packet arrives at the PIX interface that has a destination IP address of 0.0.0.0 and a destination MAC address of the PIX interface. In addition, this message is logged when the firewall discards a packet with an invalid source address. Invalid source 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 the **sysopt connection enforcesubnet** command is enabled, the PIX firewall discards packets with a source address belonging to the destination subnet from traversing the firewall and logs this message.

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

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

106017

Error Message %PIX-2-106017: Deny IP due to Land Attack from *IP_address* to *IP_address*

Explanation This message appears when the firewall receives a packet with the IP source address equal to the IP destination, and the destination port need not be equal to the source port. This indicates a spoofed packet designed to attack systems. This attack is referred to as a Land Attack.

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

106018

Error Message %PIX-2-106018: ICMP packet type *ICMP_type* denied by outbound list *acl_ID* src *inside_address* dest *outside_address*

Explanation This message is logged because the outgoing ICMP packet with type *ICMP_type* from local host *inside_address* to foreign host *outside_address* is denied by outbound list *acl_ID*.

Recommended Action None required.

106020

Error Message %PIX-2-106020: Deny IP teardrop fragment (size = *number*, offset = *number*) from *IP_address* to *IP_address*

Explanation The 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 firewall or an Intrusion Detection System.

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

106021

Error Message %PIX-1-106021: Deny *protocol* reverse path check from *source_address* to *dest_address* on interface *interface_name*

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

Recommended 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 the firewall checks packets arriving from the outside.

The firewall looks up a route based on the *source_address*. 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, the firewall checks which interface it corresponds to. If the packet arrived on another interface, it is either a spoof or there is an asymmetric routing environment that has more than one path to a destination. The firewall does not support asymmetric routing.

If configured on an internal interface, the firewall checks static **route** command statements or RIP and if the *source_address* 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. The firewall repels the attack.

106022

Error Message %PIX-1-106022: Deny *protocol* connection spoof from *source_address* to *dest_address* on interface *interface_name*

Explanation This message only appears if a connection exists and a packet matching the connection arrives on a different interface than the interface the connection began on.

For example, if a user starts a connection on the inside interface, but the firewall detects the same connection arriving on a perimeter interface, the firewall has more than one path to a destination. This is known as asymmetric routing and is not supported on the firewall.

Alternately, an attacker is attempting to append packets from one connection to another as a way to break into the firewall. In either case, the firewall displays this message and drops the connection.

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

106023

Error Message %PIX-4-106023: Deny *protocol* src
 [*interface_name:source_address/source_port*] dst
interface_name:dest_address/dest_port [type {*string*}, code {*code*}] by
 access_group *acl_ID*

Explanation An IP packet was denied by the ACL. This message displays even if you do not have the **log** option enabled for an ACL.

Recommended Action If messages persist from the same source address, messages could indicate a foot printing or port scanning attempt. Contact the remote host administrators.

106028

Error Message %PIX-2-106028: Dropping invalid echo {*request|reply*} from
interface:address to *interface:address*, {*destination|source*} address *address*
 should not match dynamic port translation, real *interface:address/ICMP-ID*, mapped
interface:address/ICMP-ID

Explanation An ICMP echo request or echo reply message is dropped because of an invalid destination or source address. NAT prohibits one host from pinging another host that is configured for dynamic port translation.

Recommended Action Check the adjacent device for routing misconfiguration. If this message occurs on a regular interval, and from an echo reply message, check the payload for a possible covert channel.

106100

Error Message %PIX-*n*-106100: access-list *acl_ID* {*permitted | denied | est-allowed*}
protocol interface_name/source_address(source_port) ->
interface_name/dest_address(dest_port) hit-cnt number ({*first hit |*
number-second interval})

Explanation This message reports when packets match an ACL statement, if you configured the **log** option for the **access-list** command. The message level depends on the level set in the **access-list** command (by default, the level is 6). The message indicates either the initial occurrence or the total number of occurrences during an interval. This message provides more information than message 106023, which only logs denied packets, and does not include the hit count or a configurable level. See the following descriptions:

- {*permitted | denied | est-allowed*}—These values specify if the packet was permitted or denied by the ACL. If the value is *est-allowed*, then the packet was denied by the ACL, but the packet was allowed for an already established session (for example, an internal user is allowed to access the Internet, and responding packets are allowed back).
- *protocol*—**tcp**, **udp**, **icmp**, or an IP protocol number.

- *interface_name*—The interface name for the source or destination of the logged flow. The VLAN interfaces are supported.
- *source_address*—The source IP address of the logged flow.
- *dest_address*—The destination IP address of the logged flow.
- *source_port*—The source port of the logged flow (TCP or UDP). For ICMP, this field is 0.
- *dest_port*—The destination port of the logged flow (TCP or UDP). For ICMP, this field is *icmp-type*.
- *hit-cnt number*—The number of times this flow was permitted or denied by this ACL entry in the configured time interval. The value is 1, however, when the firewall generates the first syslog message for this flow.
- *first hit*—The first message generated for this flow.
- *number-second interval*—The interval in which the hit count is accumulated. Set this interval using the **access-list** command **interval** option.

Recommended Action None required.

106101

Error Message %PIX-1-106101 The number of ACL log deny-flows has reached limit (*number*).

Explanation If you configured the **log** option for an ACL **deny** statement (**access-list id deny** command), and a traffic flow matches the ACL statement, the firewall caches the flow information. When the number of matching flows that are cached on the firewall exceeds the user-configured limit (**access-list deny-flow-max** command), this message is logged. See the following description:

- *number*—The limit configured using the **access-list deny-flow-max** command.

Recommended Action None required. This message might be generated as a result of a DoS attack.

107001

Error Message %PIX-1-107001: RIP auth failed from *IP_address*: *version=number*, *type=string*, *mode=string*, *sequence=number* on interface *interface_name*

Explanation This is an alert log message. The firewall received a RIP reply message with bad authentication. This could be due to misconfiguration on the router or the firewall, or it could be an unsuccessful attempt to attack the firewall routing table.

Recommended 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.

107002

Error Message %PIX-1-107002: RIP pkt failed from *IP_address*: version=*number* on interface *interface_name*

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

Recommended 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 packet.

108002

Error Message %PIX-2-108002: SMTP replaced *string*: out *source_address* in *inside_address* data: *string*

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.

Recommended Action None required.

109001

Error Message %PIX-6-109001: Auth start for user *user* from *inside_address/inside_port* to *outside_address/outside_port*

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

Recommended Action None required.

109002

Error Message %PIX-6-109002: Auth from *inside_address/inside_port* to *outside_address/outside_port* failed (server *IP_address* failed) on interface *interface_name*.

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

Recommended Action Check that the authentication daemon is running on the specified authentication server.

109003

Error Message %PIX-6-109003: Auth from *inside_address* to *outside_address/outside_port* failed (all servers failed) on interface *interface_name*.

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

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

109005

Error Message %PIX-6-109005: Authentication succeeded for user '*user*' from *inside_address/inside_port* to *outside_address/outside_port* on interface *interface_name*.

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

Recommended Action None required.

109006

Error Message %PIX-6-109006: Authentication failed for user '*user*' from *inside_address/inside_port* to *outside_address/outside_port* on interface *interface_name*.

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

Recommended Action None required.

109007

Error Message %PIX-6-109007: Authorization permitted for user '*user*' from *inside_address/inside_port* to *outside_address/outside_port* on interface *interface_name*.

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

Recommended Action None required.

109008

Error Message %PIX-6-109008: Authorization denied for user '*user*' from *source_address/source_port* to *destination_address/destination_port* on interface *interface_name*.

Explanation This is a AAA message. This message is logged if a user is not authorized to access the specified address, possibly because of an incorrect password. This message works only with TACACS+ protocol.

Recommended Action None required.

109010

Error Message %PIX-3-109010: Auth from *inside_address/inside_port* to *outside_address/outside_port* failed (too many pending auths) on interface *interface_name*.

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

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

109011

Error Message %PIX-2-109011: Authen Session Start: user '*user*', sid *number*

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

Recommended Action None required.

109012

Error Message %PIX-5-109012: Authen Session End: user '*user*', sid *number*, elapsed *number* seconds

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

Recommended Action None required.

109013

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

Explanation The user must be authenticated before using the service.

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

109014

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

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

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

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

109016

Error Message %PIX-3-109016: Can't find authorization ACL *acl_ID* on 'PIX' for user '*user*'

Explanation The access control list (ACL) specified on the AAA server for this user does not exist on the firewall. This error can occur if you configure the AAA server before you configure the firewall. The Vendor-Specific Attribute (VSA) on your AAA server might be one of the following values:

- `acl=acl_ID`
- `shell:acl=acl_ID`
- `ACS:CiscoSecured-Defined-ACL=acl_ID`

Recommended Action Add the ACL to the firewall, making sure to use the same name specified on the AAA server.

109017

Error Message %PIX-4-109017: User at *IP_address* exceeded auth proxy connection limit (*max*)

Explanation A user has exceeded the user authentication proxy limit, and has opened too many connections to the proxy.

Recommended Action Increase the proxy limit by entering the **aaa proxy-limit** *proxy_limit* command, or make the user close unused connections. If the error persists, it may indicate a possible DoS attack.

109018

Error Message %PIX-3-109018: Downloaded ACL *acl_ID* is empty

Explanation The downloaded authorization access list has no ACEs. This might be caused by the misspelled attribute string 'ip:inacl#' or omission of the **access-list** command.

```
junk:junk# 1=permit tcp any any eq junk "ip:inacl#1="
```

Recommended Action Correct the ACL elements that have the indicated error on the AAA server.

109019

Error Message %PIX-3-109019: Downloaded ACL *acl_ID* has parsing error; ACE *string*

Explanation An error is encountered during parsing the sequence number NNN in the attribute string 'ip:inacl#NNN=' of a downloaded authorization access list. The reasons include: - missing '=' - contains non-numeric, non-space characters between '#' and '=' - NNN is greater than 999999999.

```
ip:inacl# 1 permit tcp any any
ip:inacl# 1junk2=permit tcp any any
ip:inacl# 1000000000=permit tcp any any
```

Recommended Action Correct the ACL element that has the indicated error on the AAA server.

109020

Error Message %PIX-3-109020: Downloaded ACL has config error; ACE

Explanation One of the elements of the downloaded authorization access list has a configuration error. The entire text of the element is included in the syslog message. This message is usually caused by an invalid **access-list** command statement.

```
ip:inacl# 1=permit junk any any
ip:inacl# 1=permit tcp any any eq junk
```

Recommended Action Correct the ACL element that has the indicated error on the AAA server.

109021

Error Message %PIX-7-109021: Uauth null proxy error

Explanation This message indicates an internal User Authentication error.

Recommended Action None required. However, if this error appears repeatedly, contact Cisco TAC.

109022

Error Message %PIX-4-109022: exceeded HTTPS proxy process limit

Explanation For each HTTPS authentication, the firewall dedicates a process to service the authentication request. When the number of concurrently running processes exceeds the system-imposed limit, the firewall does not perform the authentication, and this message displays.

Recommended Action None required.

109023

Error Message %PIX-3-109023: User from src_IP_Address/src_port to dest_IP_Address/dest_port on interface outside must authenticate before using this service.

Explanation This is a AAA message. Based on the configured policies, you need to be authenticated before you can use this service (port).

Recommended Action Have the user authenticate using Telnet, FTP or HTTP before attempting to use the above service (port).

109024

Error Message %PIX-6-109024: Authorization denied from source_IP_Address/src_port to dest_IP_Address/dest_port (not authenticated) on interface interface_name using protocol

Explanation (not authenticated) on interface interface_name using protocol(not authenticated) on interface interface_name using protocol. This is a 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.

Recommended Action None required.

109025

Error Message %PIX-6-109025: Authorization denied (acl=acl_ID) for user 'user' from source_address/source_port to dest_address/dest_port on interface interface_name using protocol

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. This message works only with RADIUS protocol.

Recommended Action None required.

110001

Error Message %PIX-6-110001: No route to *dest_address* from *source_address*

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

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

111002

Error Message %PIX-5-111002: Begin configuration: *IP_address* 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_address* indicates whether the login was made at the console port or via a Telnet connection.

Recommended Action None required.

111003

Error Message %PIX-5-111003: *IP_address* Erase configuration

Explanation This is a firewall management message. This message is logged when you erase the contents of Flash memory by entering the **write erase** command at the console. The *IP_address* indicates whether the login was made at the console port or via a Telnet connection.

Recommended Action After erasing the configuration, reconfigure the 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.

111004

Error Message %PIX-5-111004: *IP_address* end configuration: {FAILED|OK}

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

Recommended 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.

111005

Error Message %PIX-5-111005: *IP_address* end configuration: OK

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

Recommended Action None required.

111007

Error Message %PIX-5-111007: Begin configuration: *IP_address* reading from *device*.

Explanation 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_address* indicates whether the login was made at the console port or via a Telnet connection.

Recommended Action None required.

111008

Error Message %PIX-5-111008: User *user* executed the command *string*

Explanation This syslog message is for accounting purposes. The user entered a command that modified the configuration.

Recommended Action None required.

111009

Error Message %PIX-7-111009:User *user* executed cmd:*string*

Explanation This syslog message is for accounting purposes. The user entered a command that does not modify the configuration.

Recommended Action None required.

112001

Error Message %PIX-2-112001: (*string:dec*) PIX Clear complete.

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

Recommended Action None required.

199001

Error Message %PIX-5-199001: PIX reload command executed from telnet (*remote IP_address*).

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

Recommended Action None required.

199002

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

Explanation 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 by using the **no logging message** command.

Recommended Action None required.

199005

Error Message %PIX-6-199005: PIX Startup begin

Explanation This message is logged when the PIX Firewall starts.

Recommended Action None required.

Messages 201002 to 215001

This section contains messages from 201002 to 215001.

201002

Error Message %PIX-3-201002: Too many connections on {static|xlate} *global_address!*
econns nconns

Explanation This is a connection-related message. This message is logged when the maximum number of connections to the specified static address was 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.

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

201003

Error Message %PIX-2-201003: Embryonic limit exceeded *nconns/elimit* for
outside_address/outside_port (global_address) inside_address/inside_port on
interface *interface_name*

Explanation This is a connection-related message regarding traffic to the firewall. This message is logged when the number of embryonic connections from the specified foreign address via the specified static global address to the specified local address exceeds the embryonic limit. When the limit on embryonic connections to the firewall is reached, the 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 *nconns* variable lists the number of embryonic connections received and *elimit* lists the maximum number of embryonic connections specified in the **static** or **nat** command.

Recommended 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.

201005

Error Message %PIX-3-201005: FTP data connection failed for *IP_address*

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

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

201006

Error Message %PIX-3-201006: RCMD backconnection failed for *IP_address/port*

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

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

201008

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

Explanation This message occurs when you have enabled TCP system log messaging and the syslog server cannot be reached, or when using PIX Firewall Syslog Server (PFSS) and the disk on the Windows NT system is full, or when the auto-update timeout is configured and the auto-update server is not reachable.

Recommended Action Disable TCP system log messaging. 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 system message logging to allow traffic. If the Auto Update Server has not been contacted for a certain period of time, the following command will cause it to cease sending packets: [no] auto-update timeout period.

201009

Error Message %PIX-3-201009: TCP connection limit of *number* for host *IP_address* on *interface_name* exceeded

Explanation This is a connection-related message. This message is logged when the maximum number of connections to the specified static address was exceeded. The *limit-count* variable is the maximum of connections permitted for the host specified by the *host-address* variable.

Recommended Action Use the **show static** and **show nat** commands to check the limit imposed on connections to an address. The limit is configurable.

202001

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

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

Recommended 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.

202005

Error Message %PIX-3-202005: Non-embryonic in embryonic list
outside_address/outside_port inside_address/inside_port

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

Recommended Action Contact Cisco TAC.

208005

Error Message %PIX-3-208005: (*function:line_num*) pix clear command return code

Explanation The 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.

Recommended Action Re-try the clear command. If the problem persists, Contact Cisco TAC.

209003

Error Message %PIX-4-209003: Fragment database limit of *number* exceeded: src =
IP_address,dest = IP_address, proto = protocol, id = number

Explanation Too many IP fragments are currently awaiting reassembly. By default, the maximum number of fragments is 200 (refer to the **fragment size** command in the *Cisco PIX Firewall Command Reference* to raise the maximum). The 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 a network environment with NFS over UDP; if this type of

traffic is relayed through the firewall, consider using NFS over TCP instead. To prevent fragmentation, see the **sysopt connection tcpmss bytes** command in the *Cisco PIX Firewall Command Reference*.

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

209004

Error Message %PIX-4-209004: Invalid IP fragment, size = *bytes* exceeds maximum size = *bytes*: src = *IP_address*, dest = *IP_address*, proto = *protocol*, id = *number*

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

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

209005

Error Message %PIX-4-209005: Discard IP fragment set with more than *number* elements: src = *IP_address*, dest = *IP_address*, proto = *protocol*, id = *number*

Explanation Too many elements are in a fragment set. The firewall disallows any IP packet that is fragmented into more than 12 fragments. Refer to the **fragment** command in the *Cisco PIX Firewall Command Reference* for more information.

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

210001

Error Message %PIX-3-210001: LU *SW_Module_Name* error = *number*

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

Recommended Action If this error persists after traffic lessens through the firewall, report this error to Cisco TAC.

210002

Error Message %PIX-3-210002: LU allocate block (*bytes*) failed.

Explanation Stateful Failover could not allocate a block of memory to transmit stateful information to the standby firewall.

Recommended 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 firewall software to recover the lost blocks of memory.

210003

Error Message %PIX-3-210003: Unknown LU Object *number*

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.

Recommended 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.

210005

Error Message %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 firewall.

Recommended Action Check the available memory using the **show memory** 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 firewall.

210006

Error Message %PIX-3-210006: LU look NAT for *IP_address* failed

Explanation Stateful Failover was unable to locate a NAT group for the *IP_address* on the standby unit. Most likely, the active and standby firewall units are out of sync.

Recommended Action Use the **write standby** command on the active unit to synchronize system memory with the standby unit.

210007

Error Message %PIX-3-210007: LU allocate xlate failed

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

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

210008

Error Message %PIX-3-210008: LU no xlate for *inside_address/inside_port*
outside_address/outside_port

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

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

210010

Error Message %PIX-3-210010: LU make UDP connection for *outside_address:outside_port*
inside_address:inside_port failed

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

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

210020

Error Message %PIX-3-210020: LU PAT port *port* reserve failed

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

Recommended 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.

210021

Error Message %PIX-3-210021: LU create static xlate *global_address* ifc *interface_name* failed

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

Recommended 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.

210022

Error Message %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.

Recommended 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.

211001

Error Message %PIX-3-211001: Memory allocation Error

Explanation Failed to allocate RAM system memory.

Recommended Action If this message occurs periodically, it can be ignored. If it repeats frequently, contact Cisco TAC.

211003

Error Message %PIX-3-211003: CPU utilization for *number* seconds = *percent*

Explanation This message is displayed if the percentage of CPU usage is greater than 100% for *number* seconds.

Recommended Action If this message occurs frequently, contact Cisco TAC.

212001

Error Message %PIX-3-212001: Unable to open SNMP channel (UDP port *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 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 the firewall could not open the SNMP transport for the interface.

An error code of -2 indicates that the firewall could not bind the SNMP transport for the interface.

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

212002

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

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

An error code of -1 indicates that the firewall could not open the SNMP trap transport for the interface.

An error code of -2 indicates that the firewall could not bind the SNMP trap transport for the interface.

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

212003

Error Message %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 firewall on the specified interface.

Recommended Action None required. The firewall SNMP agent goes back to wait for the next SNMP request.

212004

Error Message %PIX-3-212004: Unable to send an SNMP response to IP Address *IP_address* 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 firewall to the specified host on the specified interface.

Recommended Action None required.

212005

Error Message %PIX-3-212005: incoming SNMP request (*number* bytes) on interface *interface_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 firewall, exceeds the size of the internal data buffer (512 bytes) used for storing the request during internal processing; therefore, the firewall is unable to process this request. This does not affect the SNMP traffic passing through the firewall via any interface.

Recommended 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.

213001

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

Explanation An internal TCP socket I/O error occurred.

Recommended Action Report the problem to Cisco TAC.

213002

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

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

Recommended Action Report the problem to Cisco TAC.

213003

Error Message %PIX-3-213003: PPP virtual interface *interface_number* isn't opened.

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

Recommended Action Report the problem to Cisco TAC.

213004

Error Message %PIX-3-213004: PPP virtual interface *interface_number* client ip allocation failed.

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

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

214001

Error Message %PIX-2-214001: Terminating manager session from *IP_address* on interface *interface_name*. Reason: incoming encrypted data (*number* bytes) longer than *number* bytes

Explanation An incoming encrypted data packet destined for the PIX Firewall management port indicates a packet length exceeding the specified upper limit. This may be a hostile event. The firewall immediately terminates this management connection.

Recommended Action Ensure that the management connection was initiated by Cisco Secure Policy Manager.

215001

Error Message %PIX-2-215001:Bad route_compress() call, sdb= *number*

Explanation An internal software error occurred.

Recommended Action Contact Cisco TAC.

Messages 302003 to 320001

This section contains messages from 302003 to 320001.

302003

Error Message %PIX-6-302003: Built H245 connection for foreign_address outside_address/outside_port local_address inside_address/inside_port

Explanation This is a connection-related message. This message is logged when an H.245 connection is started from foreign address *outside_address* to local address *inside_address*. This message only occurs if the firewall detects the use of an Intel Internet phone. The foreign port (*outside_port*) only displays on connections from outside the firewall. The local port value (*inside_port*) only appears on connections started on an internal interface.

Recommended Action None required.

302004

Error Message %PIX-6-302004: Pre-allocate H323 UDP backconnection for foreign_address outside_address/outside_port to local_address inside_address/inside_port

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

Recommended Action None required.

302009

Error Message %PIX-6-302009: Rebuilt TCP connection number for foreign_address outside_address/outside_port global_address/global_port local_address inside_address/inside_port

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 *outside_address* IP address is the foreign host, the *global_address* IP address is a global address on the lower security level interface, and the *inside_address* IP address is the local IP address “behind” the PIX Firewall on the higher security level interface.

Recommended Action None required.

302010

Error Message %PIX-6-302010: *connections* in use, *connections* most used

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

Recommended Action None required.

302013

Error Message %PIX-6-302013: Built {inbound|outbound} TCP connection *number* for *interface_name:real_address/real_port* (*mapped_address/mapped_port*) to *interface_name:real_address/real_port* (*mapped_address/mapped_port*) [(*user*)]

Explanation A TCP connection slot between two hosts was created.

Where:

connection number is a unique identifier.

interface, real_address, real_port identify the actual sockets.

mapped_address, mapped_port identify the mapped sockets.

user is the AAA name of the user.

If inbound is specified, then the original control connection was initiated from the outside. For example, for FTP, all data transfer channels are inbound if the original control channel is inbound. If outbound is specified, then the original control connection was initiated from the inside.

Recommended Action None required.

302014

Error Message %PIX-6-302014: Teardown TCP connection *number* for *interface_name:real_address/real_port* to *interface_name:real_address/real_port* duration *time* bytes *number* [*reason*] [(*user*)]

Explanation A TCP connection between two hosts was deleted.

Where:

connection number is an unique identifier.

interface, real_address, real_port identify the actual sockets.

time is the lifetime of the connection.

bytes number is the data transfer of the connection.

user is the AAA name of the user.

The *reason* variable presents the action that causes the connection to terminate. Set the *reason* variable to one of the TCP termination reasons listed in [Table 2-2](#).

Table 2-2 TCP Termination Reasons

Reason	Description
Reset-I	Reset was from the inside
Reset-O	Reset was from the outside
TCP FINs	Normal close down sequence
FIN Timeout	Force termination after ten minutes awaiting the last ACK or after half-closed timeout
SYN Timeout	Force termination after two minutes awaiting three-way handshake completion
Xlate Clear	Command-line removal
Deny	Terminate by application inspection
SYN Control	Back channel initiation from wrong side
Uauth Deny	Deny by URL filter
Unknown	Catch-all error
Conn-timeout	Connection was torn down because it was idle longer than the configured idle timeout

Recommended Action None required.

302015

Error Message %PIX-6-302015: Built {inbound|outbound} UDP connection *number* for *interface_name:real_address/real_port (mapped_address/mapped_port)* to *interface_name:real_address/real_port (mapped_address/mapped_port)* [(*user*)]

Explanation A UDP connection slot between two hosts is created.

See the following descriptions:

- *connection number*—A unique identifier.
- *interface, real_address, real_port*—The actual sockets.
- *mapped_address* and *mapped_port*—The mapped sockets.
- *user*—The AAA name of the user.

If inbound is specified, then the original control connection is initiated from the outside. For example, for UDP, all data transfer channels are inbound if the original control channel is inbound. If outbound is specified, then the original control connection is initiated from the inside.

Recommended Action None required.

302016

Error Message %PIX-6-302016: Teardown UDP connection *number* for *interface_name:real_address/real_port* to *interface_name:real_address/real_port* duration *time* bytes *number* [(*user*)]

Explanation A UDP connection slot between two hosts was deleted.

Where:

connection *number* is an unique identifier.

interface, *real_address*, *real_port* are the actual sockets.

time is the lifetime of the connection.

bytes *bytes* is the data transfer of the connection.

user is the AAA name of the user.

Recommended Action None required.

302017

Error Message %PIX-6-302017: Built {*inbound|outbound*} GRE connection *id* from *interface:real_address (translated_address)* to *interface:real_address/real_cid (translated_address/translated_cid)* [(*user*)]

Explanation A GRE connection slot between two hosts is created. The *id* is an unique identifier. The *interface*, *real_address*, *real_cid* tuple identifies the one of the two simplex PPTP GRE streams. The parenthetical *translated_address*, *translated_cid* tuple identifies the translated value with NAT.

If *inbound* is indicated, then the connection can only be used inbound. If *outbound* is indicated, then the connection can only be used for outbound. The following list describes the message values:

- *id*—Unique number identifying the connection.
- *inbound*—Control connection is for inbound PPTP GRE flow.
- *outbound*—Control connection is for outbound PPTP GRE flow.
- *interface_name*—The interface name.
- *real_address*—IP address of the actual host.
- *real_cid*—Untranslated call-ID for the connection.
- *translated_address*—IP address after translation.
- *translated_cid*—Translated call.
- *user*—AAA user name.

Recommended Action This is an informational message.

302018

Error Message %PIX-6-302018: Teardown GRE connection *id* from *interface:real_address (translated_address)* to *interface:real_address/real_cid (translated_address/translated_cid)*
duration *hh:mm:ss* bytes *bytes* [(*user*)]

Explanation A GRE connection slot between two hosts is deleted. The *interface*, *real_address*, *real_port* tuples identify the actual sockets. *Duration* accounts the lifetime of the connection. The following list describes the message values:

- *id*—Unique number identifying the connection.
- *interface*—The interface name.
- *real_address*—IP address of the actual host.
- *real_port*—Port number of the actual host.
- *hh:mm:ss*—Time in hour:minute:second format.
- *bytes*—Number of PPP bytes transferred in the GRE session.
- *reason*—Reason why the connection was terminated.
- *user*—AAA user name.

Recommended Action This is an informational message.

302019

Error Message %PIX-3-302019: H.323 *library_name* ASN Library failed to initialize, error code *number*

Explanation The specified ASN library that the firewall uses for decoding the H.323 messages failed to initialize; the firewall cannot decode or inspect the arriving H.323 packet. The firewall allows the H.323 packet to pass through without any modification. When the next H.323 message arrives, the firewall attempts to initialize the library again.

Recommended Action If this message is generated consistently for a particular library, contact Cisco TAC and provide them with all log messages (preferably with timestamps).

302302

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

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

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

303002

Error Message %PIX-6-303002: *source_address* {Stored|Retrieved} *dest_address*:
mapped_address

Explanation This is an FTP/URL message. This message is logged when the specified host attempts to store or retrieve data from the specified FTP site.

Recommended Action None required.

304001

Error Message %PIX-5-304001: *user source_address* Accessed {JAVA URL|URL}
dest_address: url.

Explanation This is an FTP/URL message. This message is logged when the specified host attempts to access the specified URL.

Recommended Action None required.

304002

Error Message %PIX-5-304002: Access denied URL *url* SRC *IP_address* DEST *IP_address*:
url

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.

Recommended Action None required.

304003

Error Message %PIX-3-304003: URL Server *IP_address* timed out URL *url*

Explanation This message logs when a URL server times out.

Recommended Action None required.

304004

Error Message %PIX-6-304004: URL Server *IP_address* request failed URL *url*

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

Recommended Action None required.

304005

Error Message %PIX-7-304005: URL Server *IP_address* request pending URL *url*

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

Recommended Action None required.

304006

Error Message %PIX-3-304006: URL Server *IP_address* 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.

Recommended Action None required.

304007

Error Message %PIX-2-304007: URL Server *IP_address* 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.

Recommended Action None required.

304008

Error Message %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.

Recommended Action None required.

304009

Error Message %PIX-2-304009: Ran out of buffer blocks specified by url-block command

Explanation The URL pending buffer block is running out of space.

Recommended Action Change the buffer block size by entering the **url-block block** *block_size* command.

305005

Error Message %PIX-3-305005: No translation group found for *protocol src interface_name:dest_address/dest_port dst interface_name:source_address/source_port*

Explanation A packet does not match any of the outbound **nat** rules.

Recommended Action This message signals a configuration error. If dynamic NAT is desired for the source host, ensure that the **nat** command matches the source IP address. If static NAT is desired for the source host, ensure that the local IP address of the **static** command matches. If no NAT is desired for the source host, check the ACL bound to the nat 0 ACL.

305006

Error Message %PIX-3-305006: {outbound static|identity|portmap|regular) translation creation failed for *protocol src interface_name:source_address/source_port dst interface_name:dest_address/dest_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, the firewall denies translations for a destined IP address identified as a network or broadcast address.

The PIX Firewall does not PAT all ICMP message types; it only PATs ICMP echo and echo-reply packets (types 8 and 0). Specifically, only ICMP echo or echo-reply packets create a PAT xlate. So, when the other ICMP messages types are dropped, syslog message 305006 (on the PIX Firewall) is generated.

The 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 firewall does 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.

To handle the case where the suspected IP is a host IP, configure a separated **static** command statement with a host mask 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. Because the PIX Firewall treats a network or broadcast IP address as a host IP address with overlapped subnet static configuration, the network address translation for both **static** command statements must be the same.

Recommended Action This message can be either an internal error or an error in the configuration, and will be generated any time the firewall is unable to create a translation.

305007

Error Message %PIX-6-305007: addrpool_free(): Orphan IP *IP_address* on interface *interface_number*

Explanation The PIX Firewall has attempted to translate an address that it cannot find in any of its global pools. The PIX Firewall assumes that the address was deleted and drops the request.

Recommended Action None required.

305008

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

Explanation The firewall 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 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 recovers automatically.

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

305009

Error Message %PIX-3-305009: Teardown <type> translation from <interface>:<address> to <interface>[<acl>]:<address> duration <HH:MM:SS>

Explanation An address translation slot was created. The slot is used to translate the source address from the local side to the global side. In reverse, the slot is used to translate the destination address from the global side to the local side.

Recommended Action None required.

305010

Error Message %PIX-6-305010: Teardown {dynamic|static} translation from *interface_name* [(*<acl-name>*)]:*real_address* to *interface_name:mapped_address* duration *time*

Explanation The address translation slot was deleted.

Recommended Action None required.

305011

Error Message %PIX-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from *interface_name* [(*<acl-name>*)]:*real_address/real_port* to *interface_name:mapped_address/mapped_port*

Explanation A TCP, UDP, or ICMP address translation slot was created. The slot is used to translate the source socket from the local side to the global side. In reverse, the slot is used to translate the destination socket from the global side to the local side.

Recommended Action None required.

305012

Error Message %PIX-6-305012: Teardown {dynamic|static} {TCP|UDP|ICMP} translation from *interface_name* [(*<acl-name>*)]:*real_address*/*{real_port|real_ICMP_ID}* to *interface_name*:*mapped_address*/*{mapped_port|mapped_ICMP_ID}* duration time

Explanation The address translation slot was deleted.

Recommended Action None required.

308001

Error Message %PIX-6-308001: PIX console enable password incorrect for *number* tries (from *IP_address*)

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

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

308002

Error Message %PIX-4-308002: static *global_address* *inside_address* netmask *netmask* overlapped with *global_address* *inside_address*

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

Recommended 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.

309002

Error Message %PIX-6-309002: Permitted manager connection from *IP_address*.

Explanation This is a firewall management message. This message logs a successful connection to the firewall management port from the specified address.

Recommended Action None required.

311001

Error Message %PIX-6-311001: LU loading standby start

Explanation This message appears when Stateful Failover update information is sent to the standby firewall unit when the standby unit is first coming on line.

Recommended Action None required.

311002

Error Message %PIX-6-311002: LU loading standby end

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

Recommended Action None required.

311003

Error Message %PIX-6-311003: LU rcv thread up

Explanation This message appears when an update acknowledgment is received from the standby unit.

Recommended Action None required.

311004

Error Message %PIX-6-311004: LU xmit thread up

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

Recommended Action None required.

312001

Error Message %PIX-6-312001: RIP hdr failed from *IP_address*: cmd=*string*, version=*number* domain=*string* on interface *interface_name*

Explanation The 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.

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

313001

Error Message %PIX-3-313001: Denied ICMP type=*number*, code=*code* from *IP_address* on interface *interface_name*

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

Recommended Action Contact the administrator of the peer device.

313003

Error Message %PIX-4-313003: Invalid destination for ICMP error

Explanation The destination for the ICMP error message is different than the source of the IP packet that induced the ICMP error message.

Recommended Action If the message occurs frequently, this could be an active network probe, an attempt to use the ICMP error message as a covert channel, or a misbehaving IP host. Contact the administrator of the host that originated the ICMP error message.

314001

Error Message %PIX-6-314001: Pre-allocate RTSP UDP backconnection for *foreign_address outside_address/outside_port* to *local_address inside_address/inside_port*

Explanation The firewall opened an RTSP connection for the specified IP addresses and ports.

Recommended Action No action required.

315004

Error Message %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 firewall host key may be absent because no PIX Firewall host key was generated or because the license for this PIX Firewall does not allow DES or 3DES.

Recommended 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 the **show version** command to check whether the PIX Firewall unit's license allows DES or 3DES.

315011

Error Message %PIX-6-315011: SSH session from *IP_address* on interface *interface_name* for user *user* disconnected by SSH server, reason: *reason*

Explanation This message appears after an SSH session completes. If a user enters **quit** or **exit**, the "terminated normally" message displays. If the session disconnected for another reason, the text describes the reason. [Table 2-3](#) lists the possible reasons why a session disconnected.

Table 2-3 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 Cisco TAC.
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.
Internal error	This message indicates either an error internal to SSH on the firewall or an RSA key may not have been entered on the firewall or cannot be retrieved.	From the firewall console, enter the show ca mypubkey rsa to verify that the 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, simply restart the SSH session.

Table 2-3 SSH Disconnect Reasons (continued)

Text String	Explanation	Action
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 firewall exceeds 262,144 bytes or is shorter than 4096 bytes. The data may be corrupted.	No action required.
Invalid message type	The firewall received a non-SSH message, or an unsupported or unwanted SSH message.	Check whether the peer is an SSH client. If it is a client supporting SSHv1, and this message persists, from the firewall serial console enter the debug ssh command and capture the debug messages. Then contact Cisco TAC.
Out of memory	This message appears when the PIX Firewall is unable to allocate memory for use by the SSH server, probably when the 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 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 firewall console.	No action required.
Time-out activated	The SSH session timed out because the duration specified by the ssh timeout command was exceeded.	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.

316001

Error Message %PIX-2-316001: Denied new tunnel to *IP_address*. VPN peer limit (*platform_vpn_peer_limit*) exceeded

Explanation If more VPN tunnels (ISAKMP/IPSec) are concurrently attempting to be established than supported by the platform VPN peer limit, then the excess tunnels are aborted.

Recommended Action None required.

317001

Error Message %PIX-3-317001: No memory available for limit_slow

Explanation The requested operation failed because of a low memory condition.

Recommended Action Reduce other system activity to ease memory demands. If conditions warrant, upgrade to a larger memory configuration.

317002

Error Message %PIX-3-317002: Bad path index of *number* for *IP_address*, *number* max

Explanation A software error occurred.

Recommended Action To determine the cause of the problem, contact Cisco TAC for assistance.

317003

Error Message %PIX-3-317003: IP routing table creation failure - *reason*

Explanation An internal software error occurred, which prevented the creation of new IP routing table.

Recommended Action Copy the message exactly as it appears, and report it to Cisco TAC.

317004

Error Message %PIX-3-317004: IP routing table limit warning

Explanation The number of routes in the named IP routing table has reached the configured warning limit.

Recommended Action Reduce the number of routes in the table, or reconfigure the limit.

317005

Error Message %PIX-3-317005: IP routing table limit exceeded - *reason*, *IP_address* *netmask*

Explanation Further routes will be added to the table.

Recommended Action Reduce the number of routes in the table, or reconfigure the limit.

318001

Error Message %PIX-3-318001: Internal error: *reason*

Explanation An internal software error occurred. This message occurs at 5 second intervals.

Recommended Action To determine the cause of the problem, contact Cisco TAC for assistance.

318002

Error Message %PIX-3-318002: Flagged as being an ABR without a backbone area

Explanation The router was flagged as an area border router without a backbone area configured in the router. This message occurs at 5 second intervals.

Recommended Action Restart the OSPF process.

318003

Error Message %PIX-3-318003: Reached unknown state in neighbor state machine

Explanation An internal software error occurred. This message occurs at 5 second intervals.

Recommended Action None required.

318004

Error Message %PIX-3-318004: area *string* lsid *IP_address* mask *netmask* adv *IP_address*
type *number*

Explanation OSPF had a problem locating the LSA, which might lead to a memory leak.

Recommended Action To determine the cause of the problem, contact Cisco TAC for assistance.

318005

Error Message %PIX-3-318005: lsid *IP_address* adv *IP_address* type *number* gateway
gateway_address metric *number* network *IP_address* mask *netmask* protocol *hex* attr
hex net-metric *number*

Explanation OSPF found an inconsistency between its database and the IP routing table.

Recommended Action To determine the cause of the problem, contact Cisco TAC for assistance.

318006

Error Message %PIX-3-318006: if *interface_name* if_state *number*

Explanation An internal error occurred.

Recommended Action To determine the cause of the problem, contact Cisco TAC for assistance.

318007

Error Message %PIX-3-318007: OSPF is enabled on *interface_name* during idb initialization

Explanation An internal error occurred.

Recommended Action To determine the cause of the problem, contact Cisco TAC for assistance.

318008

Error Message %PIX-3-318008: OSPF process *number* is changing router-id. Reconfigure virtual link neighbors with our new router-id

Explanation The OSPF process is being reset, and it is going to select a new router-id. This action will bring down all virtual links. To make them work again, virtual link configuration needs to be changed on all virtual link neighbors.

Recommended Action Change virtual link configuration on all the virtual link neighbors, to reflect our new router-id.

320001

Error Message %PIX-3-320001: The subject name of the peer cert is not allowed for connection

Explanation When the firewall is an Easy VPN Remote device or Server, the peer certificate contains a subject name that does not match the **ca verifycertdn** command.

Recommended Action This message might indicate a man in the middle attack, where a device spoofs the peer IP address and attempts to intercept a VPN connection from the firewall.

Messages 400000 to 409023

This section contains messages from 400000 to 409023.

4000nn

Error Message %PIX-4-4000nn: IDS:number string from IP_address to IP_address on interface interface_name

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

Recommended Action Refer to the *Cisco 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 (*number*) at the following website:

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/tsd_products_support_model_home.html

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

%PIX-4-4000nn IDS:number string from IP_address to IP_address on interface interface_name

Options:

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

http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/tsd_products_support_model_home.html

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

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

interface_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 2-4 lists the supported signature messages.

Table 2-4 IDS Syslog Messages

Message Number	Signature ID	Signature Title	Signature Type
400000	1000	IP options-Bad Option List	Informational
400001	1001	IP options-Record Packet Route	Informational

Table 2-4 IDS Syslog Messages (continued)

Message Number	Signature ID	Signature Title	Signature Type
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	1102	IP Impossible Packet	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
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	Informational
400035	6051	DNS Zone Transfer	Informational
400036	6052	DNS Zone Transfer from High Port	Informational
400037	6053	DNS Request for All Records	Informational

Table 2-4 IDS Syslog Messages (continued)

Message Number	Signature ID	Signature Title	Signature Type
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	yplib (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

401001

Error Message %PIX-4-401001: Shuns cleared

Explanation The **clear shun** command was entered to remove existing shuns from memory.

Recommended Action None required. This message is issued to allow an institution to keep a record of shunning activity.

401002

Error Message %PIX-4-401002: Shun added: *IP_address IP_address port port*

Explanation A **shun** command was entered, where the first IP address is the shunned host. The other addresses and ports are optional and are used to terminate the connection if available.

Recommended Action None required. This message is issued to allow an institution to keep a record of shunning activity.

401003

Error Message %PIX-4-401003: Shun deleted: *IP_address*

Explanation A single shunned host was removed from the shun database.

Recommended Action None required. This message is issued to allow an institution to keep a record of shunning activity.

401004

Error Message %PIX-4-401004: Shunned packet: *IP_address* ==> *IP_address* on interface *interface_name*

Explanation A packet was dropped because the host defined by IP src is a host in the shun database. A shunned host cannot pass traffic on the interface on which it is shunned. For example, an external host on the Internet can be shunned on the outside interface.

Recommended Action None required. This message provides a record of the activity of shunned hosts. This message and %PIX-4-401005 can be used to evaluate further risk assessment concerning this host.

401005

Error Message %PIX-4-401005: Shun add failed: unable to allocate resources for *IP_address IP_address port port*

Explanation The firewall is out of memory; a shun could not be applied.

Recommended Action The Cisco Intrusion Detection System should continue to attempt to apply this rule. Attempt to reclaim memory and reapply shun manually, or wait for the Cisco Intrusion Detection System to do this.

402101

Error Message %PIX-4-402101: decaps: rec'd IPSEC packet has invalid spi for
destaddr=*dest_address*, prot=*protocol*, spi=*number*

Explanation Received IPsec packet specifies a Security Parameters Index (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.

Recommended 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.

402102

Error Message %PIX-4-402102: decapsulate: packet missing {AH|ESP},
destaddr=*dest_address*, 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.

Recommended Action Contact the peer's administrator.

402103

Error Message %PIX-4-402103: identity doesn't match negotiated identity (ip)
dest_address= *dest_address*, src_addr= *source_address*, prot= *protocol*, (ident)
local=*inside_address*, remote=*remote_address*,
local_proxy=*IP_address/IP_address/port/port*,
remote_proxy=*IP_address/IP_address/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 a security association selection error by the peer. This may be a hostile event.

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

402106

Error Message %PIX-4-402106: Rec'd packet not an IPSEC packet (ip) dest_address= dest_address, src_addr= source_address, 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, but not on a telnet or traffic to the outside interface on ports other than 23. 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 710001, 710002, and 710003 for messages that track TCP and UDP requests.

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

403101

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

Explanation The firewall received a PPTP XGRE packet without a corresponding control connection session.

Recommended Action If this message occurs frequently, report the problem to Cisco TAC.

403102

Error Message %PIX-4-403102: PPP virtual interface *interface_name* rcvd pkt with invalid protocol: *protocol*, reason: *reason*.

Explanation The firewall received an XGRE encapsulated PPP packet with an invalid protocol field.

Recommended Action If this message occurs frequently, report the problem to Cisco TAC.

403103

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

Explanation The firewall cannot accept additional PPTP connections.

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

403104

Error Message %PIX-4-403104: PPP virtual interface *interface_name* requires mschap for MPPE.

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

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

403106

Error Message %PIX-4-403106: PPP virtual interface *interface_name* requires RADIUS for MPPE.

Explanation The MPPE is configured but RADIUS authentication is not.

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

403107

Error Message %PIX-4-403107: PPP virtual interface *interface_name* missing aaa server group info

Explanation AAA server configuration information cannot be found.

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

403108

Error Message %PIX-4-403108: PPP virtual interface *interface_name* missing client ip address option

Explanation The client IP address pool information is missing.

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

403109

Error Message %PIX-4-403109: Rec'd packet not an PPTP packet. (ip) dest_address= dest_address, src_addr= source_address, data: string.

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

Recommended Action Contact the peer's administrator to check the PPTP configuration settings.

403110

Error Message %PIX-4-403110: PPP virtual interface *interface_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.

Recommended 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.

403500

Error Message %PIX-6-403500: PPPoE - Service name 'any' not received in PADO.
Intf: *interface_name* AC: *ac_name*.

Explanation The firewall requested the PPPoE service “any” from the access controller at the Internet service provider. The response from the service provider includes other services but does not include the service “any.” This is a discrepancy in the implementation of the protocol. The PADO packet is processed normally and connection negotiations continue.

Recommended Action None required.

403501

Error Message %PIX-3-403501: PPPoE - Bad host-unique in PADO - packet dropped.
Intf: *interface_name* AC: *ac_name*

Explanation The firewall sent an identifier called the “host-unique” value to the access controller. The access controller responded with a different “host-unique” value. The PIX Firewall is unable to identify the corresponding connection request for this response. The packet is dropped and connection negotiations are aborted.

Recommended Action Contact the Internet service provider. Either the access controller at the service provider is mishandling the “host-unique” value or the PADO packet is being forged.

403502

Error Message %PIX-3-403502: PPPoE - Bad host-unique in PADS - dropping packet.
Intf: *interface_name* AC: *ac_name*

Explanation The firewall sent an identifier called the “host-unique” value to the access controller. The access controller responded with a different “host-unique” value. The PIX Firewall is unable to identify the corresponding connection request for this response. The packet was dropped and connection negotiations were aborted.

Recommended Action The Internet service provider should be contacted. Either the access controller at the service provider is mishandling the “host-unique” value or the PADO packet is being forged.

403503

Error Message %PIX-3-403503: PPPoE:PPP link down:*reason*

Explanation The PPP link has gone down. There are many reasons why this could happen. The first format will display a reason if PPP provides one.

Recommended Action Check the network link to ensure that the link is connected. The access concentrator could be down. Ensure that your authentication protocol matches the access concentrator. Ensure that your name and password are correct. Check with your ISP or network support person.

403504

Error Message %PIX-3-403504: PPPoE:No 'vpdn group' for PPPoE is created

Explanation PPPoE requires a dial-out configuration before starting a PPPoE session. In general, the configuration should specify a dialing policy, the PPP authentication, the username and a password. The following example configures the firewall for PPPoE dialout. It also uses **my-username** and **my-password** to authenticate the access concentrator, using PAP if necessary.

For example:

```
vpdn group my-pppoe request dialout pppoe
vpdn group my-pppoe ppp authentication pap
vpdn group my-pppoe localname my-username
vpdn username my-username password my-password
ip address outside pppoe setroute
```

Recommended Action The user should configure a VPDN group for PPPoE.

403505d

Error Message %PIX-3-403505d: PPPoE:PPP - Unable to set default route to *IP_address* at *interface_name*

Explanation Usually this message is followed by “- default route already exists.”

Recommended Action Remove the current default route or remove the “setroute” parameter so that there is no conflict between PPPoE and the manually configured route.

403506

Error Message %PIX-3-403506: PPPoE:failed to assign PPP *IP_address* netmask *netmask* at *interface_name*

Explanation This message is followed by “- subnet is the same as interface,” or “on failover channel.”

Recommended Action In the first case, change the address causing the conflict. In the second case, configure the PPPoE on an interface other than the failover interface.

404101

Error Message %PIX-4-404101: ISAKMP: Failed to allocate address for client from pool *string*

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

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

405001

Error Message %PIX-4-405001: Received ARP {request | response} collision from *IP_address/mac_address* on interface *interface_name*

Explanation The firewall received an ARP packet, and the MAC address in the packet differs from the ARP cache entry.

Recommended Action This traffic might be legitimate, or it might indicate that an ARP poisoning attack is in progress. Check the source MAC address to determine where the packets are coming from and check to see if it belongs to a valid host.

405002

Error Message %PIX-4-405002: Received mac mismatch collision from *IP_address/mac_address* for authenticated host

Explanation This packet appears for one of the following conditions:

- The firewall received a packet with the same IP address but a different MAC address from one of its uauth entries.
- You configured the **vpnclient mac-exempt** command on the firewall, and the firewall receives a packet with an exempt MAC address but a different IP address from the corresponding uauth entry.

Recommended Action This traffic might be legitimate, or it might indicate that a spoofing attack is in progress. Check the source MAC address and IP address to determine where the packets are coming from and check to see if they belong to a valid host.

405101

Error Message %PIX-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for *foreign_address outside_address[/outside_port]* to *local_address inside_address[/inside_port]*

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

Recommended Action If this message occurs periodically, it can be ignored. If it repeats frequently, contact Cisco TAC. 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.

405102

Error Message %PIX-4-405102: Unable to Pre-allocate H245 Connection for *foreign_address outside_address[/outside_port]* to *local_address inside_address[/inside_port]*

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

Recommended Action If this message occurs periodically, it can be ignored. If it repeats frequently, contact Cisco TAC. 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.

405103

Error Message %PIX-4-405103: H225 message from <src_ip/src_port> to <dest_ip/dest_port> contains bad protocol discriminator <hex_value>

Explanation This event is logged when PIX is expecting the protocol discriminator, 0x08, but it received something other than 0x08. This could happen because the endpoint is sending a bad packet, or PIX received a message segment other than the first.

Recommended Action Packet is let through since we currently do not handle segments.

405104

Error Message %PIX-4-405104: H225 message received from *outside_address/outside_port* to *inside_address/inside_port* before SETUP

Explanation This message appears after an H.225 message is received out of order. The H.225 message was received before the initial SETUP message, which is not allowed. The PIX Firewall must receive an initial SETUP message for that H.225 call signalling channel before accepting any other H.225 messages.

Recommended Action None required.

406001

Error Message %PIX-4-406001: FTP port command low port: *IP_address/port* to *IP_address* on interface *interface_name*

Explanation A client issued an ftp port command and supplied a port lesser than 1024 (in the well-known port range typically devoted to server ports). This is indicative of an attempt to avert the site's security policy. The firewall drops the packet, terminates the connection, and logs the event.

Recommended Action None required.

406002

Error Message %PIX-4-406002: FTP port command different address:
IP_address(IP_address) to IP_address on interface interface_name

Explanation A client issued an FTP port command and supplied an address other than the address used in the connection. This error message is indicative of an attempt to avert the site's security policy. For example, one might attempt to hijack an FTP session by changing the packet on the way, and putting different source information instead of the correct source information. The PIX Firewall drops the packet, terminates the connection, and logs the event. In the error message displayed, the IP address in parentheses is the address from the **PORT** command.

Recommended Action None required.

407001

Error Message %PIX-4-407001: Deny traffic for local-host
interface_name:inside_address, license limit of number exceeded

Explanation The host limit was exceeded. An inside host is counted toward the limit when one of the following conditions is true:

- The inside host has forwarded traffic through the PIX Firewall within the last five minutes.
- The inside host currently reserved an xlate connection or user authentication at the PIX Firewall.

Recommended Action The host limit is enforced on the low-end platforms. Use the **show version** command to view the host limit. Use the **show local-host** command to view the current active hosts and the inside users that have sessions at the firewall. To force disconnect one or more users, use the **clear local-host** command. To expire the inside users more quickly from the limit, set the xlate, connection, and uauth timeouts to the recommended values or lower. (See [Table 2-5](#).)

Table 2-5 Timeouts and Recommended Values

Timeout	Recommended Value
xlate	00:05:00 (five minutes)
conn	00:01:00 (one hour)
uauth	00:05:00 (five minutes)

407002

Error Message %PIX-3-407002: Embryonic limit *neconns/elimit* for through connections exceeded. *outside_address/outside_port* to *global_address (inside_address)/inside_port* on interface *interface_name*

Explanation This message is about connections through the firewall. This message is logged when the number of connections from specified foreign address over specified global address to the specified local address exceeds the maximum embryonic limit for that static. The firewall attempts to accept the connection if it can allocate memory for that connection. It proxies on behalf of local host and sends a SYN_ACK packet to the foreign host. The firewall retains pertinent state information, drops the packet, and waits for the client's acknowledgment.

Recommended Action It might be legitimate traffic, or indicate that a denial of service (DoS) attack is in progress. Check the source address to determine where the packets are coming from and whether it is a valid host.

408001

Error Message %PIX-4-408001: IP route counter negative - *reason*, *IP_address* Attempt: *number*

Explanation An attempt to decrement the IP route counter into a negative value failed.

Recommended Action Enter the **clear ip route *** command to reset the route counter. If the message continues to appear consistently, copy the messages exactly as they appear, and report it to Cisco TAC.

409001

Error Message %PIX-4-409001: Database scanner: external LSA *IP_address netmask* is lost, reinstalls

Explanation The software detected an unexpected condition. The router will take corrective action and continue.

Recommended Action None required.

409002

Error Message %PIX-4-409002: db_free: external LSA *IP_address netmask*

Explanation An internal software error occurred.

Recommended Action None required.

409003

Error Message %PIX-4-409003: Received invalid packet: *reason* from *IP_address*, *interface_name*

Explanation An invalid OSPF packet was received. Details are included in the error message. The cause might be an incorrect OSPF configuration or an internal error in the sender.

Recommended Action Check the OSPF configuration of the receiver and the sender configuration for inconsistency.

409004

Error Message %PIX-4-409004: Received *reason* from unknown neighbor *IP_address*

Explanation The OSPF hello, database description, or database request packet was received, but the router could not identify the sender.

Recommended Action This situation should correct itself.

409005

Error Message %PIX-4-409005: Invalid length number in OSPF packet from *IP_address* (ID *IP_address*), *interface_name*

Explanation The system received an OSPF packet with a field length of less than normal header size or inconsistent with the size of the IP packet in which it arrived. This indicates a configuration error in the sender of the packet.

Recommended Action From a neighboring address, locate the problem router and reboot it.

409006

Error Message %PIX-4-409006: Invalid lsa: *reason* Type *number*, LSID *IP_address* from *IP_address*, *IP_address*, *interface_name*

Explanation The router received an LSA with an invalid LSA type. The cause is either memory corruption or unexpected behavior on a router.

Recommended Action From a neighboring address, locate the problem router and reboot it. To determine what is causing this problem, contact Cisco TAC for assistance.

409007

Error Message %PIX-4-409007: Found LSA with the same host bit set but using different mask LSA ID *IP_address netmask* New: Destination *IP_address netmask*

Explanation An internal software error occurred.

Recommended Action To determine what is causing this problem, contact Cisco TAC for assistance.

409008

Error Message %PIX-4-409008: Found generating default LSA with non-zero mask LSA type : *number* Mask: *IP_address* metric : *number* area : *string*

Explanation The router tried to generate a default LSA with the wrong mask and possibly wrong metric due to an internal software error.

Recommended Action To determine what is causing this problem, contact Cisco TAC for assistance.

409009

Error Message %PIX-4-409009: OSPF process number cannot start. There must be at least one up IP interface, for OSPF to use as router ID

Explanation OSPF failed while attempting to allocate a router ID from the IP address of one of its interfaces.

Recommended Action Make sure that there is at least one interface that is up and has a valid IP address. If there are multiple OSPF processes running on the router, each requires a unique router ID. You must have enough interfaces up so that each of them can obtain a router ID.

409010

Error Message %PIX-4-409010: Virtual link information found in non-backbone area: *string*

Explanation An internal error occurred.

Recommended Action To determine what is causing this problem, contact Cisco TAC for assistance.

409011

Error Message %PIX-4-409011: OSPF detected duplicate router-id *IP_address* from *IP_address* on interface *interface_name*

Explanation OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

Recommended Action The OSPF router ID should be unique. Change the neighbor's router ID.

409012

Error Message %PIX-4-409012: Detected router with duplicate router ID *IP_address* in area *string*

Explanation OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

Recommended Action The OSPF router ID should be unique. Change the neighbor's router ID.

409013

Error Message %PIX-4-409013: Detected router with duplicate router ID *IP_address* in Type-4 LSA advertised by *IP_address*

Explanation OSPF received a hello packet from a neighbor that has the same router ID as this routing process. A full adjacency cannot be established.

Recommended Action The OSPF router ID should be unique. Change the neighbor's router ID.

409023

Error Message %PIX-4-409023: Attempting AAA Fallback method <method_name> for <request_type> request for user <username> :Auth-server group <server_tag> unreachable

Explanation When transitioning from one method to a second method, the PIX will issue the above message

Recommended Action Investigate any connectivity problems with AAA servers configured in the first method. Ping the authentication server(s) from the PIX. Make sure the daemon(s) are running on your AAA server.

Messages 410001 to 410001

This section contains messages from 410001 to 411002.

410001

Error Message %PIX-4-410001: UDP DNS packet dropped due to domainname length check of 255 bytes: actual length:<n> bytes

Explanation This message is printed when the domain-name length exceeds 255 bytes in a UDP DNS packet. (See rfc1035 section 3.1)

Recommended Action None required.

Error Message %PIX-4-410001:UDP DNS packet dropped due to label length check of 63 bytes actual length:<n> bytes

Explanation This message is printed when the label length exceeds 63 bytes in a UDP DNS packet. (See rfc1035 section 3.1)

Recommended Action None required.

Error Message %PIX-4-410001:UDP DNS packet dropped due to packet length check of <n> bytes: actual length:<n1> bytes

Explanation This message is printed when the packet length of a UDP DNS packet exceeds the maximum-length value which is configured along with the fixup protocol DNS command. (See EDCS-275620) <n> is the maximum-length configured in the command, <n1> is the actual length of the packet dropped.

Recommended Action None required.

Error Message %PIX-4-410001:UDP DNS packet dropped due to compression length check of <n> bytes: actual length:<n1> bytes

Explanation This message is printed when a compression pointer loop is detected and the number of bytes read exceeds the size of the packet. <n> size of the packet, <n1> number of bytes parsed in the packet. (with a compression pointer to pointer loop we parse the same bytes repeatedly)

Recommended Action None required.

Messages 411001 to 416001

This section contains messages from 411001 to 416001.

411001

Error Message %PIX-4-411001:Line protocol on interface *interface_name* changed state to up

Explanation The status of the line protocol has changed from down to up.

Recommended Action None required.

411002

Error Message %PIX-4-411002:Line protocol on interface *interface_name* changed state to down

Explanation The status of the line protocol has changed from up to down.

Recommended Action If this is an unexpected event, check the physical line.

416001

Error Message %PIX-4-416001: Dropped UDP SNMP packet from <source interface> :<source> IP>/<source port> to <dest interface>:<dest IP>/<dest port>; version> (<version>) is not allowed through the firewall

Explanation an SNMP packet was denied passage through the firewall because of a fixup configuration or a packet format check failed.

Recommended Action None necessary. If passing the traffic is desired, remove the denying configuration. Otherwise, identify denied SNMP traffic sender by examining IP and interface information.

Messages 500001 to 503001

This section contains messages from 500001 to 503001.

500001

Error Message %PIX-5-500001: ActiveX content modified src *IP_address* dest *IP_address* on interface *interface_name*.

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

Recommended Action None required.

500002

Error Message %PIX-5-500002: Java content modified src *IP_address* dest *IP_address* on interface *interface_name*.

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

Recommended Action None required.

500003

Error Message %PIX-5-500003: Bad TCP hdr length (hdrhlen=*bytes*, pktlen=*bytes*) from *source_address/source_port* to *dest_address/dest_port*, flags: *tcp_flags*, on interface *interface_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 firewall and FTP is not listening, then the server sends an 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.

Recommended Action None required. This message should occur infrequently.

500004

Error Message %PIX-4-500004: Invalid transport field for protocol=*protocol*, from *source_address/source_port* to *dest_address/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.

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

501101

Error Message %PIX-5-501101: User transitioning priv level

Explanation The privilege level of a command was changed.

Recommended Action None required.

502101

Error Message %PIX-5-502101: New user added to local dbase: Uname: *user* Priv: *privilege_level* Encpass: *string*

Explanation A new username record was created. The message lists the username, privilege level, and encrypted password.

Recommended Action None required.

502102

Error Message %PIX-5-502102: User deleted from local dbase: Uname: *user* Priv: *privilege_level* Encpass: *string*

Explanation A username record was deleted. The message lists the username, privilege level, and encrypted password.

Recommended Action None required.

502103

Error Message %PIX-5-502103: User priv level changed: Uname: *user* From: *privilege_level* To: *privilege_level*

Explanation The privilege level of a user changed.

Recommended Action None required.

503001

Error Message %PIX-5-503001: Process number, Nbr *IP_address* on *interface_name* from *string* to *string*, *reason*

Explanation An OSPF neighbor has changed its state. The message describes the change and the reason for it. This message appears only if the **log-adjacency-changes** command is configured for the OSPF process.

Recommended Action To determine what is causing this problem, contact Cisco TAC for assistance.

Messages 602101 to 620002

This section contains messages from 602101 to 620002.

602101

Error Message %PIX-6-602101: PMTU-D packet *number* bytes greater than effective mtu *number* dest_addr=*dest_address*, src_addr=*source_address*, prot=*protocol*

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

Recommended Action Ensure that the data is sent correctly.

602102

Error Message %PIX-6-602102: Adjusting IPsec tunnel mtu...

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

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

602201

Error Message %PIX-6-602201: ISAKMP Phase 1 SA created (local <ip>/<port> (initiator|responder), remote <ip>/<port>, authentication=<auth_type>, encryption=<encr_alg>, hash=<hash_alg>, group=<DH_grp>, lifetime=<seconds>)

Explanation This message is logged when an ISAKMP SA is created.

Recommended Action N/A

602301

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

Explanation A new security association (SA) was created.

Recommended Action Informational message.

602302

Error Message %PIX-6-602302: deleting sa

Explanation An SA was deleted.

Recommended Action Informational message.

603101

Error Message %PIX-6-603101: PPTP received out of seq or duplicate pkt, tnl_id=number, sess_id=number, seq=number.

Explanation The firewall received a PPTP packet that was out of sequence or duplicated.

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

603102

Error Message %PIX-6-603102: PPP virtual interface *interface_name* - user: *user* aaa authentication started.

Explanation The firewall sent an authentication request to the AAA server.

Recommended Action None required.

603103

Error Message %PIX-6-603103: PPP virtual interface *interface_name* - user: *user* aaa authentication *status*

Explanation The firewall received an authentication response from the AAA server.

Recommended Action None required.

603104

Error Message %PIX-6-603104: PPTP Tunnel created, *tunnel_id* is *number*, *remote_peer_ip* is *remote_address*, *ppp_virtual_interface_id* is *number*, *client_dynamic_ip* is *IP_address*, *username* is *user*, *MPPE_key_strength* is *string*

Explanation A PPTP tunnel was created.

Recommended Action None required.

603105

Error Message %PIX-6-603105: PPTP Tunnel deleted, *tunnel_id* = *number*, *remote_peer_ip*= *remote_address*

Explanation A PPTP tunnel was deleted.

Recommended Action None required.

603106

Error Message %PIX-6-603106: L2TP Tunnel created, *tunnel_id* is *number*, *remote_peer_ip* is *remote_address*, *ppp_virtual_interface_id* is *number*, *client_dynamic_ip* is *IP_address*, *username* is *user*

Explanation An L2TP tunnel was created.

Recommended Action None required.

603107

Error Message %PIX-6-603107: L2TP Tunnel deleted, tunnel_id = *number*, remote_peer_ip = *remote_address*

Explanation An L2TP tunnel was deleted.

Recommended Action None required.

603108

Error Message %PIX-6-603108: Built PPTP Tunnel at *interface_name*, tunnel-id = *number*, remote-peer = *IP_address*, virtual-interface = *number*, client-dynamic-ip = *IP_address*, username = *user*, MPPE-key-strength = *number*

Explanation This message is displayed each time a new PPPoE tunnel is created.

Recommended Action None required.

603109

Error Message %PIX-6-603109: Teardown PPPOE Tunnel at *interface_name*, tunnel-id = *number*, remote-peer = *IP_address*

Explanation This message is displayed each time a new PPPoE tunnel is deleted.

Recommended Action None required.

604101

Error Message %PIX-6-604101: DHCP client interface *interface_name*: Allocated ip = *IP_address*, mask = *netmask*, gw = *gateway_address*

Explanation The firewall DHCP client successfully obtained an IP address from a DHCP server. The **dhcpc** command statement lets the 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.

Recommended Action None required.

604102

Error Message %PIX-6-604102: DHCP client interface *interface_name*: address released

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

Recommended Action None required.

604103

Error Message %PIX-6-604103: DHCP daemon interface *interface_name*: address granted
MAC_address (*IP_address*)

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

Recommended Action None required.

604104

Error Message %PIX-6-604104: DHCP daemon interface *interface_name*: address released

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

Recommended Action None required.

605004

Error Message %PIX-6-605004: Login denied from {*source_address/source_port* | *serial*}
to {*interface_name:dest_address/service* | *console*} for user "*user*"

Explanation This message appears after an incorrect login attempt. The firewall allows 3 login attempts per session. After the third attempt, the firewall terminates the session. For SSH and Telnet logins, the firewall generates a message either after the third failure or if at least one failed attempt has been tried, and the TCP session is terminated before the third attempt. For all other management logins, each failed attempt generates a message.

Recommended 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.

605005

Error Message %PIX-6-605005: Login permitted from {*source_address/source_port* | *serial*} to {*interface_name:dest_address/service* | *console*} for user "user"

Explanation This message appears when a user is authenticated successfully and a management session starts.

Recommended Action None required.

606001

Error Message %PIX-6-606001: PDM session number *number* from *IP_address* started

Explanation This message indicates that an administrator has been authenticated successfully and a PDM session was started.

Recommended Action None required.

606002

Error Message %PIX-6-606002: PDM session number *number* from *IP_address* ended

Explanation This message indicates that a PDM session ended.

Recommended Action None required.

607001

Error Message %PIX-6-607001: Pre-allocate SIP *connection_type* secondary channel for *interface_name:IP_address/port* to *interface_name:IP_address* from *string* message

Explanation This message indicates that the **fixup sip** command pre-allocated a SIP connection after inspecting a SIP message. The *connection_type* is one of the following strings:

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route

- RTP
- RTCP

Recommended Action None required.

608001

Error Message %PIX-6-608001: Pre-allocate Skinny *connection_type* secondary channel for *interface_name:IP_address* to *interface_name:IP_address/port* from *string* message

Explanation This message indicates that the **fixup skinny** command pre-allocated a Skinny connection after inspecting a Skinny message. The *connection_type* is one of the following strings:

- SIGNALLING UDP
- SIGNALLING TCP
- SUBSCRIBE UDP
- SUBSCRIBE TCP
- Via UDP
- Route
- RTP
- RTCP

Recommended Action None required.

609001

Error Message %PIX-6-609001: Built local-host *interface_name:IP_address*

Explanation A network state container is reserved for host *IP_address* connected to interface *interface_name*. This is an informational message.

Recommended Action None required.

609002

Error Message %PIX-6-609002: Teardown local-host *interface_name:IP_address* duration *time*

Explanation A network state container for host *IP_address* connected to interface *interface_name* is removed. This is an informational message.

Recommended Action None required.

610001

Error Message %PIX-3-610001: NTP daemon interface *interface_name*: Packet denied from *IP_address*

Explanation An NTP packet was received from a host that does not match one of the configured NTP servers. The firewall is only an NTP client; it is not a time server and does not respond to NTP requests.

Recommended Action None required.

610002

Error Message %PIX-3-610002: NTP daemon interface *interface_name*: Authentication failed for packet from *IP_address*

Explanation The received NTP packet failed the authentication check.

Recommended Action Ensure that both the firewall and the NTP server are set to use authentication, and the same key number and value.

610101

Error Message %PIX-6-610101: Authorization failed: Cmd: *command* Cmdtype: *command_modifier*

Explanation Command authorization failed for the specified command. The *command_modifier* is one of the following strings:

- **cmd** (this string means the command has no modifier)
- **clear**
- **no**
- **show**

Explanation If the firewall encounters any other value other than the four command types listed, the following message displays: “unknown command type.”

Recommended Action None required.

611101

Error Message %PIX-6-611101: User authentication succeeded: Uname: *user*

Explanation User authentication when accessing the firewall succeeded.

Recommended Action None required.

611102

Error Message %PIX-6-611102: User authentication failed: Uname: *user*

Explanation User authentication failed when attempting to access the firewall.

Recommended Action None required.

611103

Error Message %PIX-5-611103: User logged out: Uname: *user*

Explanation The specified user logged out.

Recommended Action None required.

611104

Error Message %PIX-5-611104: Serial console idle timeout exceeded

Explanation The configured idle timeout for the firewall serial console was exceeded because of no user activity.

Recommended Action None required.

611301

Error Message %PIX-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT addr: *mapped_address*

Explanation The VPN client policy for client mode with no split tunneling was installed.

Recommended Action None required.

611302

Error Message %PIX-6-611302: VPNClient: NAT exemption configured for Network Extension Mode with no split tunneling

Explanation VPN client policy for network extension mode with no split tunneling was installed.

Recommended Action None required.

611303

Error Message %PIX-6-611303: VPNClient: NAT configured for Client Mode with split tunneling: NAT addr: *mapped_address* Split Tunnel Networks: *IP_address/netmask* *IP_address/netmask* ...

Explanation VPN client policy for client mode with split tunneling was installed.

Recommended Action None required.

611304

Error Message %PIX-6-611304: VPNClient: NAT exemption configured for Network Extension Mode with split tunneling: Split Tunnel Networks: *IP_address/netmask* *IP_address/netmask* ...

Explanation VPN client policy for network extension mode with split tunneling was installed.

Recommended Action None required.

611305

Error Message %PIX-6-611305: VPNClient: DHCP Policy installed: Primary DNS: *IP_address* Secondary DNS: *IP_address* Primary WINS: *IP_address* Secondary WINS: *IP_address*

Explanation VPN client policy for DHCP was installed.

Recommended Action None required.

611306

Error Message %PIX-6-611306: VPNClient: Perfect Forward Secrecy Policy installed

Explanation Perfect forward secrecy was configured as part of the VPN client download policy.

Recommended Action None required.

611307

Error Message %PIX-6-611307: VPNClient: Head end : *IP_address*

Explanation The VPN client is connected to the specified headend.

Recommended Action None required.

611308

Error Message %PIX-6-611308: VPNClient: Split DNS Policy installed: List of domains:
string string ...

Explanation A split DNS policy was installed as part of the VPN client downloaded policy.

Recommended Action None required.

611309

Error Message %PIX-6-611309: VPNClient: Disconnecting from head end and uninstalling
previously downloaded policy: Head End : *IP_address*

Explanation A VPN client is disconnecting and uninstalling a previously installed policy.

Recommended Action None required.

611310

Error Message %PIX-6-611310: VNPCClient: XAUTH Succeeded: Peer: *IP_address*

Explanation The VPN client Xauth succeeded with the specified headend.

Recommended Action None required.

611311

Error Message %PIX-6-611311: VPNClient: XAUTH Failed: Peer: *IP_address*

Explanation The VPN client Xauth failed with the specified headend.

Recommended Action None required.

611312

Error Message %PIX-6-611312: VPNClient: Backup Server List: *reason*

Explanation When the firewall is an Easy VPN Remote device, this message indicates that the Easy VPN Server downloaded a list of backup servers to the firewall. This list overrides any backup servers you configured locally. If the downloaded list is empty, then the firewall uses no backup servers. The *reason* is one of the following messages:

- A list of backup server IP addresses
- Received NULL list. Deleting current backup servers.

Recommended Action None required.

611313

Error Message %PIX-3-611313: VPNClient: Backup Server List Error: *reason*

Explanation When the firewall is an Easy VPN Remote device, and the Easy VPN Server downloads a backup server list to the firewall, this message indicates that the list contains an invalid IP address or a host name. The firewall does not support DNS, and therefore does not support host names for servers unless you manually map a name to an IP address using the **name** command.

Recommended Action On the Easy VPN Server, make sure the server IP addresses are correct, and configure the servers as IP addresses instead of host names. If you must use host names on the server, use the **name** command on the Easy VPN Remote device to map the IP addresses to names.

611314

Error Message %PIX-6-611314: VPNClient: Load Balancing Cluster with Virtual IP: *IP_address* has redirected the PIX to server *IP_address*

Explanation When the firewall is an Easy VPN Remote device, the master server of the load balancing cluster redirected the firewall to connect to a particular server.

Recommended Action None required.

611315

Error Message %PIX-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member *IP_address*

Explanation When the firewall is an Easy VPN Remote device, this message indicates that it disconnected from a load balancing cluster server.

Recommended Action None required.

611316

Error Message %PIX-6-611316: VPNClient: Secure Unit Authentication Enabled

Explanation When the firewall is an Easy VPN Remote device, the downloaded VPN policy enabled secure unit authentication (SUA).

Recommended Action None required.

611317

Error Message %PIX-6-611317: VPNClient: Secure Unit Authentication Disabled

Explanation When the firewall is an Easy VPN Remote device, the downloaded VPN policy disabled secure unit authentication (SUA).

Recommended Action None required.

611318

Error Message %PIX-6-611318: VPNClient: User Authentication Enabled: Auth Server IP: *IP_address* Auth Server Port: *port* Idle Timeout: *time*

Explanation When the firewall is an Easy VPN Remote device, the downloaded VPN policy enabled individual user authentication (IUA) for users on the firewall's inside network.

- *IP_address*—The server IP address to which the firewall sends authentication requests.
- *port*—The server port to which the firewall sends authentication requests.
- *time*—The idle timeout value for authentication credentials.

Recommended Action None required.

611319

Error Message %PIX-6-611319: VPNClient: User Authentication Disabled

Explanation When the firewall is an Easy VPN Remote device, the downloaded VPN policy disabled individual user authentication (IUA) for users on the firewall's inside network.

Recommended Action None required.

611320

Error Message %PIX-6-611320: VPNClient: Device Pass Thru Enabled

Explanation When the firewall is an Easy VPN Remote device, the downloaded VPN policy enabled device pass through. The device pass through feature allows devices that cannot perform authentication (such as an IP phone) to be exempt from authentication when Individual User Authentication (IUA) is enabled.

Recommended Action None required. If the Easy VPN Server enables this feature, you can specify the devices that should be exempt from authentication (IUA) using the **vpnclient mac-exempt** command on the firewall.

611321

Error Message %PIX-6-611321: VPNClient: Device Pass Thru Disabled

Explanation When the firewall is an Easy VPN Remote device, the downloaded VPN policy disabled device pass through.

Recommended Action None required.

611322

Error Message %PIX-6-611322: VPNClient: Extended XAUTH conversation initiated when SUA disabled

Explanation When the firewall is an Easy VPN Remote device and the downloaded VPN policy disabled secure unit authentication (SUA), the Easy VPN Server uses two-factor/SecurID/cryptocard-based authentication mechanisms to authenticate the firewall using XAUTH.

Recommended Action If you want the Easy VPN Remote device to be authenticated using two-factor/SecureID/cryptocard-based authentication mechanisms, enable SUA on the server.

611323

Error Message %PIX-6-611323: VPNClient: Duplicate split nw entry

Explanation When the firewall is an Easy VPN Remote device, this message indicates that the downloaded VPN policy contains duplicate split network entries. An entry is considered a duplicate if it matches both the network address and the network mask.

Recommended Action Remove duplicate split network entries from the VPN policy on the Easy VPN Server.

612001

Error Message %PIX-5-612001: Auto Update succeeded: *filename*, version: *number*

Explanation An update from an Auto Update Server was successful. The *filename* variable is **PIX image, PDM file, or configuration**. The *version number* variable is the version number of the update.

Recommended Action None required.

612002

Error Message %PIX-4-612002: Auto Update failed: *filename*, version: *number*, reason: *reason*

Explanation This message indicates that an update from an Auto Update Server failed. The *filename* variable is **PIX image, PDM file, or configuration**. The *version number* variable is the version number of the update. The *reason* variable describes why the update failed. Possible reasons for the failure include invalid image file, connection lost to server, configuration errors, etc.

Recommended Action Check the configuration of the Auto Update Server.

612003

Error Message %PIX-4-612003: Auto Update failed to contact: *url*, reason: *reason*

Explanation This indicates that the Auto Update daemon was unable to contact the specified URL *url*. This could be the URL of the Auto Update Server or one of the file server URLs returned by the Auto Update Server. The *reason* field describes why the contact failed. Possible reasons for the failure include no response from server, authentication failed, file not found, etc.

Recommended Action Check the configuration of the Auto Update Server.

613001

Error Message %PIX-6-613001: Checksum Failure in database in area *string* Link State Id *IP_address* Old Checksum *number* New Checksum *number*

Explanation OSPF has detected a checksum error in the database due to memory corruption.

Recommended Action Restart the OSPF process.

613002

Error Message %PIX-6-613002: interface *interface_name* has zero bandwidth

Explanation The interface reports its bandwidth as zero.

Recommended Action To determine what is causing this problem, contact Cisco TAC for assistance.

613003

Error Message %PIX-6-613003: *IP_address netmask* changed from area *string* to area *string*

Explanation An OSPF configuration change has caused a network range to change areas.

Recommended Action Reconfigure OSPF with the correct network range.

614001

Error Message %PIX-6-614001: Split DNS: request patched from server: *IP_address* to server: *IP_address*

Explanation Split DNS is redirecting DNS queries from the original destination server to the primary enterprise DNS server.

Recommended Action None required.

614002

Error Message %PIX-6-614002: Split DNS: reply from server: *IP_address* reverse patched back to original server: *IP_address*

Explanation Split DNS is redirecting DNS queries from the enterprise DNS server to the original destination server.

Recommended Action None required.

620001

Error Message %PIX-6-620001: Pre-allocate CTIQBE {RTP | RTCP} secondary channel for *interface_name:outside_address[/outside_port]* to *interface_name:inside_address[/inside_port]* from *CTIQBE_message_name* message

Explanation The firewall pre-allocates a connection object for the specified CTIQBE media traffic.

Recommended Action None required.

620002

Error Message %PIX-4-620002: Unsupported CTIQBE version: *hex*: from *interface_name:IP_address/port* to *interface_name:IP_address/port*

Explanation The firewall received a CTIQBE message with an unsupported version number. The firewall drops the packet.

Recommended Action If the version number captured in the log message is unreasonably large (greater than 10), the packet could be malformed, a non-CTIQBE packet, or corrupted before it arrives at the firewall. We recommend that you determine the source of the packets. If the version number is reasonably small (less than or equal to 10), then contact Cisco TAC to see if a new firewall image that supports this CTIQBE version is available.

Messages 701001 to 710006

This section contains messages from 701001 to 710006.

701001

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

Explanation This is a AAA message. This message is logged if the user authentication rate is too high for the firewall to handle new AAA requests.

Recommended Action Enable Flood Defender with the **floodguard enable** command.

702201

Error Message %PIX-7-702201: ISAKMP Phase 1 delete received (local <ip> (initiator|responder), remote <ip>)

Explanation An ISAKMP delete message has been received.

Recommended Action N/A

702202

Error Message %PIX-7-702202: ISAKMP Phase 1 delete sent (local <ip> (initiator|responder), remote <ip>)

Explanation An ISAKMP delete message has been sent.

Recommended Action N/A

702203

Error Message %PIX-7-702203: ISAKMP DPD timed out (local <ip> (initiator|responder), remote <ip>)

Explanation Remote peer is not responding, DPD has timed out the peer.

Recommended Action Check network connectivity to remote host.

702204

Error Message %PIX-7-702204: ISAKMP Phase 1 retransmission (local <ip> (initiator|responder), remote <ip>)

Explanation Remote peer is not responding, ISAKMP is retransmitting the previous packet.

Recommended Action Check network connectivity to remote host, check VPN configuration of local and remote devices.

702205

Error Message %PIX-7-702205: ISAKMP Phase 2 retransmission (local <ip> (initiator|responder), remote <ip>)

Explanation Remote peer is not responding, ISAKMP is retransmitting the previous packet.

Recommended Action Check network connectivity to remote host, check VPN configuration of local and remote devices.

702206

Error Message %PIX-7-702206: ISAKMP malformed payload received (local <ip> (initiator|responder), remote <ip>)

Explanation ISAKMP received an illegal or malformed message. May indicate an out of sync problem with the remote peer, a problem decrypting a message, or a message received out of order.

Recommended Action If using preshared key, verify local preshared key is configured correctly on local and remote device. Check local and remote configuration, additional troubleshooting may be required if SA fails to come up.

702207

Error Message %PIX-7-702207: ISAKMP duplicate packet detected (local <ip> (initiator|responder), remote <ip>)

Explanation ISAKMP received a duplicate of the previously received packet. May occur during normal operation, or as a side effect of previous errors in an ISAKMP exchange.

Recommended Action Check connectivity, check local and remote configuration.

702208

Error Message %PIX-7-702208: ISAKMP Phase 1 exchange started (local <ip> (initiator|responder), remote <ip>)

Explanation ISAKMP has started a new Phase 1 message exchange with the remote peer.

Recommended Action N/A

702209

Error Message %PIX-7-702209: ISAKMP Phase 2 exchange started (local <ip> (initiator|responder), remote <ip>)

Explanation ISAKMP has started a new Phase 2 message exchange with the remote peer.

Recommended Action N/A

702210

Error Message %PIX-7-702210: ISAKMP Phase 1 exchange completed(local <ip> (initiator|responder), remote <ip>)

Explanation ISAKMP has finished a Phase 1 exchange.

Recommended Action N/A

702211

Error Message %PIX-7-702211: ISAKMP Phase 2 exchange completed(local <ip> (initiator|responder), remote <ip>)

Explanation ISAKMP has finished a Phase 2 exchange.

Recommended Action N/A

702212

Error Message %PIX-7-702212: ISAKMP Phase 1 initiating rekey (local <ip> (initiator|responder), remote <ip>)

Explanation ISAKMP is initiating Phase 1 rekeying.

Recommended Action N/A

702301

Error Message %PIX-7-702301: lifetime expiring...

Explanation An SA lifetime has expired.

Recommended Action Debugging message.

702302

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

Explanation More than 4 billion packets have been received in the IPSec tunnel and a new tunnel is being negotiated.

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

702303

Error Message %PIX-7-702303: sa_request...

Explanation IPSec has requested IKE for new SAs.

Recommended Action Debugging message.

703001

Error Message %PIX-7-703001: H.225 message received from
interface_name:ip_address/port to *interface_name:ip_address/port* is using an
unsupported version number

Explanation The firewall received an H.323 packet with an unsupported version number. The firewall might re-encode the protocol version field of the packet to the highest supported version.

Recommended Action Use the version of H.323 that the firewall supports in the VoIP network.

703002

Error Message %PIX-7-703002: Received H.225 Release Complete with newConnectionNeeded for *interface_name:ip_address* to *interface_name:ip_address/port*

Explanation This is debugging message indicates that the firewall received the specified H.225 message, and that the firewall opened a new signalling connection object for the two specified H.323 endpoints.

Recommended Action None required.

709001, 709002

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

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

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

Recommended Action None required.

709003

Error Message %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.

Recommended Action None required.

709004

Error Message %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.

Recommended Action None required.

709005

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

Explanation This message indicates that the standby the firewall received the first part of the configuration replication from the active the firewall. “(Primary)” can also be listed as “(Secondary)” for the secondary unit.

Recommended Action None required.

709006

Error Message %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.

Recommended Action None required.

709007

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

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.

Recommended Action Write down the command name and inform Cisco TAC.

710001

Error Message %PIX-7-710001: TCP access requested from *source_address/source_port* to *interface_name:dest_address/service*

Explanation This message appears when the first TCP packet destined to the firewall requests to establish a TCP session. This packet is the first SYN packet of the three-way handshake. This message appears when the respective access control list (telnet, http or ssh) has permitted the packet. However, the SYN cookie verification is not yet completed and no state is reserved.

Recommended Action None required.

710002

Error Message %PIX-7-710002: {TCP|UDP} access permitted from *source_address/source_port* to *interface_name:dest_address/service*

Explanation For a TCP connection, this message appears when the second TCP packet destined to the firewall requests to establish a TCP session. This packet is the final ACK of the three-way handshake. This message appears when the respective access control list (Telnet, HTTP, or SSH) has permitted the packet. Also, the SYN cookie verification is successful and the state is reserved for the TCP session. For a UDP connection, the connection was permitted. For example, this message appears (with the service **snmp**) when the firewall receives an SNMP request from an authorized SNMP management station, and the request has been processed. When the service is **snmp**, this message occurs a maximum of 1 time every 10 seconds so that the log receiver is not overwhelmed.

Recommended Action None required.

710003

Error Message %PIX-3-710003: {TCP|UDP} access denied by ACL from *source_address/source_port* to *interface_name:dest_address/service*

Explanation This message appears when the firewall denies an attempt to connect to the interface service. For example, this message appears (with the service **snmp**) when the firewall receives an SNMP request from an unauthorized SNMP management station.

Recommended Action Use the **show http**, **show ssh**, or **show telnet** command to verify that the firewall is configured to permit the service access from the host or network. If this message appears frequently, it can indicate an attack.

710004

Error Message %PIX-4-710004: TCP connection limit exceeded from *source_address/source_port* to *interface_name:dest_address/service*

Explanation The maximum number of firewall management connections for the service was exceeded. The firewall permits at most five concurrent management connections per management service.

Recommended Action From the console, use the **kill** command to release the unwanted session.

710005

Error Message %PIX-7-710005: {TCP|UDP} request discarded from *source_address/source_port* to *interface_name:dest_address/service*

Explanation This message appears when the firewall does not have a UDP server that services the UDP request. The message can also indicate a TCP packet that does not belong to any session on the firewall. In addition, this message appears (with the service **snmp**) when the firewall receives an SNMP request with an empty payload, even if it is from an authorized host. When the service is **snmp**, this message occurs a maximum of 1 time every 10 seconds so that the log receiver is not overwhelmed.

Recommended Action In networks that heavily utilize broadcasting services such as DHCP, RIP or NetBios, the frequency of this message can be high. If this message appears in excessive number, it may indicate an attack.

710006

Error Message %PIX-7-710006: *protocol* request discarded from *source_address* to *interface_name:dest_address*

Explanation This message appears when the firewall does not have an IP server that services the IP protocol request; for example, the firewall receives IP packets that are not TCP or UDP, and the firewall cannot service the request.

Recommended Action In networks that heavily utilize multicasting, the frequency of this message can be high. If this message appears in excessive number, it may indicate an attack.

