

System Log Messages

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

Note The messages shown in this guide only apply to PIX Firewall version 5.0 and later. When a number is skipped from a sequence, for example, 106004 or 110001, the message is no longer in the PIX Firewall code.

This chapter includes the following sections:

- Messages 101001 to 105020
- Messages 106001 to 112001
- Messages 199001 to 201008
- Messages 202001 to 209002
- Messages 210001 to 212004
- Messages 302001 to 311004
- Messages 402101 to 709006

Refer to “How to Read System Log Messages” in Chapter 1, “Introduction,” for more information on how to interpret the `%PIX-severity_level-message_number` string that precedes each syslog message.

Messages 101001 to 105020

Log 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.

Log 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.

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

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

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

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

Log 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.

Log 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.

Log Message %PIX-1-103001: (Primary) No response from other firewall.

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.

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

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

Explanation This is a failover message. This message is logged if the primary unit detects a bad network interface on the secondary unit. "(Primary)" can also be listed as "(Secondary)" for the Secondary unit. Refer to Table 1-3 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.

Log 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.

Log 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.

Log Message %PIX-1-104001: Secondary: Switching to ACTIVE (cause: *reason*).

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

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

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

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.

Log 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.

Log 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.

Log Message %PIX-1-105001: Disabling failover.

Explanation This is a failover message. This message is logged when you enter the **no failover** command on the console.

Recommended Action None required.

Log Message %PIX-1-105002: 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.

Recommended Action None required.

Log Message %PIX-1-105003: Monitoring on interface *interface_number* waiting.

Explanation This is a failover message. The PIX Firewall is testing the specified network interface with the other unit of the failover pair. Refer to Table 1-3 for possible values for the *interface_number* variable.

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

Log Message %PIX-1-105004: Monitoring on interface *interface_number* normal.

Explanation This is a failover message. The test of the specified network interface was successful. Refer to Table 1-3 for possible values for the *interface_number* variable.

Recommended Action None required.

Log Message %PIX-1-105005: Lost Failover communications with mate on interface *interface_number*.

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. Refer to Table 1-3 for possible values for the *interface_number* variable.

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

Log Message %PIX-1-105006: Link status 'Up' on interface *interface_number*.

Log Message %PIX-1-105007: Link status 'Down' on interface *interface_number*.

Explanation Both instances are failover messages. These messages report the results of monitoring the link status of the specified interface. Refer to Table 1-3 for possible values for the *interface_number* variable.

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

Log Message %PIX-1-105008: Testing Interface *interface_number*.

Explanation This is a failover message. This message is logged when the PIX Firewall tests a specified network interface. This testing is performed only if the PIX Firewall fails to receive a message from the Standby unit on that interface after the expected interval. Refer to Table 1-3 for possible values for the *interface_number* variable.

Recommended Action None required.

Log Message %PIX-1-105009: Testing on interface *interface_number* result.

Explanation This is a failover message. This message reports the result (either "Passed" or "Failed") of a previous interface test. Refer to Table 1-3 for possible values for the *interface_number* variable.

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

Log Message %PIX-3-105010: (Primary) failover message block alloc failed

Explanation Block memory has been depleted. This is a transient message and the PIX Firewall should recover.

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

Log 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.

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

Messages 106001 to 112001

Log Message %PIX-2-106001: Inbound TCP connection denied from *IP_addr/port* to *IP_addr/port* flags *TCP_flags*

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

The *TCP_flags* are as follows:

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

Recommended Action None required.

Log Message %PIX-2-106002: *protocol#* Connection denied by outbound list *list_ID* src *laddr/lport* dest *faddr/fport*

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 is 1 for ICMP, 6 for TCP, and 17 for UDP.

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

Log Message %PIX-2-106003: Connection denied src *laddr* dest *faddr* due to JAVA Applet.

Explanation This is a connection-related message. This message is logged if JAVA filtering is enabled, and a JAVA applet is prevented from downloading to a user on the inside network.

Recommended Action Use the **show outbound** command to check outbound lists for JAVA access restrictions.

Log Message %PIX-2-106006: Deny inbound UDP from *faddr/fport* to *laddr/lport*

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.

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

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

Recommended Action If the inside port number is 53, it is likely that the inside host is set up as a caching nameserver. Set up a conduit for 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 already answered by another server.

Log Message %PIX-2-106008: Translation for *src_addr* to *dest_addr/dport* denied by outbound (source is denied) *chars*

Explanation This is a connection-related message. This message is logged if the specified outbound list prevents an address translation request from being fulfilled.

Recommended Action Use the **show outbound** command to verify the outbound list.

Log Message %PIX-2-106009: Translation for *src_addr* to *dest_addr/dport* denied by outbound (destination is denied) *chars*

Explanation This is a connection-related message. This message is logged if the specified outbound list prevents an address translation request from being fulfilled.

Recommended Action Use the **show outbound** command to verify the outbound list.

Log Message %PIX-3-106010: Deny inbound from outside: *IP_addr* to inside: *IP_addr chars*.

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

Recommended Action None required.

Log Message %PIX-7-106011: Deny inbound (no xlate) *chars*

Explanation This is a connection-related message. This message occurs when a packet is sent to the same interface that it arrived on. This usually indicates that a security breach is occurring. When the PIX Firewall receives a packet, it tries to establish a translation slot based on the security policy you set with the **global** and **conduit** commands, and your routing policy set with the **route** command. Failing both policies, PIX Firewall allows the packet to flow from the higher priority network to a lower priority network, if it is consistent with the security policy. If a packet comes from a lower priority network and the security policy does not allow it, PIX Firewall routes the packet back to the same interface.

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

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

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

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

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

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

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

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

Recommended Action None required.

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

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

Recommended Action None required.

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

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

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

Log Message %PIX-2-106016: Deny IP spoof from (*IP_addr*) to *IP_addr*

Explanation This message is logged when the PIX Firewall discards a packet with an invalid source address. Invalid sources addresses are those addresses belonging to (i) loopback network (127.0.0.0), (ii) broadcast (limited, net-directed, subnet-directed, and all-subnets-directed), or (iii) the destination host (land.c). Furthermore, if **sysopt connection enforcesubnet** is enabled, PIX Firewall discards packets with a source address belonging to the destination subnet from traversing the PIX Firewall and logs this message.

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

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

Log Message %PIX-2-106017: Packet contains ActiveX content and has been modified src *IP_addr* dest to *IP_addr*

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

Recommended Action None required.

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

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

Recommended Action None required.

Log Message %PIX-4-106019: IP packet from *src_addr* to *dest_addr*, protocol *protocol* received from interface *int_name* deny by access-group *list_name*

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

Recommended Action None required.

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

Explanation This is a Mail Guard (SMTP) message. This message is logged if the PIX Firewall replaces an invalid character in an email address with a space.

Recommended Action None required.

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

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

Recommended Action None required.

Log Message %PIX-6-109002: Auth from *laddr/lport* to *faddr/fport* failed (server *IP_addr* failed)

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

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

Log Message %PIX-6-109003: Auth from *laddr* to *faddr/fport* failed (all servers failed)

Explanation This is an 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.

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

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

Recommended Action None required.

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

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

Recommended Action None required.

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

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

Recommended Action None required.

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

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

Recommended Action None required.

Log Message %PIX-6-109009: Authorization denied from *laddr/lport* to *faddr/fport* (not authenticated)

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

Recommended Action None required.

Log Message %PIX-3-109010: Auth from *laddr/lport* to *faddr/fport* failed (too many pending auths)

Explanation This is an AAA message. This message is logged if an authentication request can not 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 floodguard with the **floodguard 1** command.

Log Message %PIX-5-109011: Authen Session Start: user 'user', sid *session_num*

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

Recommended Action None required.

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

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

Recommended Action None required.

Log 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.

Log 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 provided in the configuration.

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

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

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

Log Message %PIX-2-110003: No interface is configured (with nameif).

Explanation This is a routing or interface naming error message. This message is logged if the specified interface name does not exist. This could occur if you specify an interface that has not yet been defined with the **nameif** command, or if you mistype the interface name in a command such as **outbound**, **static**, or **conduit**.

Recommended Action Check the spelling of the interface parameters in the **outbound**, **static**, and **conduit** commands. Use the **show nameif** command to confirm the correct spellings and to verify that the interface has been defined.

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

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

Recommended Action None required.

Log Message %PIX-5-111003: *IP_addr* erase configuration

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

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

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

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

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.

Log Message %PIX-5-111005: *IP_addr* end configuration: OK

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

Recommended Action None required.

Log Message %PIX-5-111006: Console login from *user* at *IP_addr*

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

Recommended Action None required.

Log Message %PIX-5-111007: Begin configuration: *IP_addr* reading from *device*.

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

Recommended Action None required.

Log Message %PIX-5-111008: User 'user' executed the 'chars' command.

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

Recommended Action None required.

Log Message %PIX-2-112001: (*chars:dec*) pix clear finished.

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

Recommended Action None required.

Messages 199001 to 201008

Log Message %PIX-5-199001: PIX reload command executed from *IP_addr*.

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

Recommended Action None required.

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

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

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

Recommended Action None required.

Log Message %PIX-6-199003: Reducing link MTU *dec*.

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

Recommended Action None required.

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

Explanation This message is logged when the PIX Firewall starts.

Recommended Action None. required.

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

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

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

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

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

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.

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

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

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

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

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

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

Log Message %PIX-3-201007: Unable to allocate new udp connections (*faddr/fport-laddr/lport*)

Explanation This is a connection-related message. This message is logged if the PIX Firewall cannot allocate new UDP connections between the specified foreign address and port and the specified local address and port, due to insufficient memory.

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

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

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

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

Messages 202001 to 209002

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

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

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.

Log Message %PIX-3-202002: getxlate failed *int_name*.

Explanation This is a connection-related message. The PIX Firewall was unable to find a translation slot for an incoming packet. Where possible, the PIX Firewall provides the more detailed form of the message. The error could occur because the translation slot timeout is set too low, and the slot resource was freed; or because the specified inside address is not a valid NAT address; or because of a routing problem (possibly an asymmetric routing loop).

Recommended Action Use the **show timeout** command to display the translation timeout. Use the **show nat** command to determine whether the inside address is a valid destination. Use the **show route** command to display the PIX Firewall unit's routing table.

Log Message %PIX-3-202003: Couldn't find xlate *gaddr laddr dest_addr int_name int_name*

Explanation This is a connection-related message, and applies to outbound connections. This message can occur if an outbound list blocks connections to the specified address, or if the inside address is not part of a NAT group. A less likely possibility is that there are too many current PAT connections, and the PIX Firewall cannot allocate a PAT address for the connection.

Recommended Action Use the **show outbound** command to verify that connections to the specified address are blocked. Use the **show nat** command to determine if the inside address is included in a NAT group. Make sure the global pool is not running out of addresses.

Log Message %PIX-3-202004: Couldn't find xlate *gaddr laddr dest_addr int_name*

Explanation This is a connection-related message, and applies to outbound connections. This message can occur if an outbound list blocks connections to the specified address, or if the inside address is not part of a NAT group. A less likely possibility is that there are too many current PAT connections, and the PIX Firewall cannot allocate a PAT address for the connection.

Recommended Action Use the **show outbound** command to verify that connections to the specified address are blocked. Use the **show nat** command to determine if the inside address is included in a NAT group. Make sure the global pool is not running out of addresses.

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

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

Recommended Action Contact customer support. This should never happen.

Log Message %PIX-3-203001: ESP Error: No Key SPI *hex SRC IP_addr DEST IP_addr*

Explanation This is a Private Link message. This message is logged if no encryption key could be found to match the key specified by the remote Private Link unit.

Recommended Action Use the **show link** command to display information about the keys. If you recently changed keys, you must change keys on both PIX Firewall units, and you should reboot both units to activate the new keys.

Log Message %PIX-3-209001: IPFRAG: Unable to allocate frag record for *src_addr/src_port to dest_addr/dest_port*

Explanation More than 1024 IP fragment packets were received within 10 seconds. PIX Firewall was unable to allocate a record for each fragment. This could be an indication of a fragment attack or a host injecting IP fragments, which can occur with NFS when the MTU is set incorrectly.

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

Log Message %PIX-3-209002: IPFRAG: First Frag have not been seen *src_addr to dest_addr*

Explanation A noninitial IP fragment was found because either a denial of service attack is occurring or a remote host is injecting out of order IP fragments, which can occur with NFS. The *src_addr* is the IP address of the host sending the packet and the *dest_addr* is the host to which the packet was sent.

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

Messages 210001 to 212004

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

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

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

Log Message %PIX-3-210002: LU allocate block *size* failed.

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

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 PIX Firewall software to recover the lost blocks of memory.

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

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

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.

Log 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 PIX Firewall.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.

Log Message %PIX-3-210021: LU create static xlate *global_IP ifc int_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.

Log 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.

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.

Log 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 customer support.

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

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

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

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

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

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

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

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

Log 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 PIX Firewall on the specified interface.

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

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

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

Recommended Action None required.

Messages 302001 to 311004

Log Message %PIX-6-302001: Built inbound|outbound TCP connection *id* for *faddr faddr/fport gaddr gaddr/gport laddr laddr/lport {username}*

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

Recommended Action None required.

Log Message %PIX-6-302002: Teardown TCP connection *id* for *faddr* *IP_addr/port* *gaddr* *IP_addr/port* *laddr* *IP_addr/port* {*username*}

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

Recommended Action None required.

Log Message %PIX-6-302003: Built H245 connection for *faddr* *faddr/fport* *laddr* *laddr/lport*

Explanation This is a connection-related message. This message is logged when an H.245 connection is started from foreign address *faddr* to local address *laddr*. This message only occurs if the PIX Firewall detects the use of an Intel Internet phone.

Recommended Action None required.

Log Message %PIX-6-302004: Pre-allocate H323 UDP backconnection for *faddr* *faddr/fport* to *laddr* *laddr/port*

Explanation This is a connection-related message. This message is logged when an H.323 UDP back-connection is preallocated to foreign address *faddr* from local address *laddr*. This message is only generated if the PIX Firewall detects the use of an Intel Internet phone.

Recommended Action None required.

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

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

Recommended Action None required.

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

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

Recommended Action None required.

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

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

Recommended Action None required.

Log Message %PIX-6-302010: *conns* in use, *conns* most used

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

Recommended Action None required.

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

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

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

Log Message %PIX-6-303002: *src_addr* Stored|Retrieved *dest_addr: nat_addr*s

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

Recommended Action None required.

Log Message %PIX-5-304001: *user src_addr* Accessed JAVA URL|URL *dest_addr: url*.

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

Recommended Action None required.

Log Message %PIX-5-304002: Access denied URL *chars SRC IP_addr* DEST *IP_addr: chars*

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

Recommended Action None required.

Log Message %PIX-7-304003: URL Server *IP_addr* timed out URL *string*

Explanation This message logs when a URL server times out.

Recommended Action None required.

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

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

Recommended Action None required.

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

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

Recommended Action None required.

Log Message %PIX-3-304006: URL Server *IP_addr* not responding, trying *IP_addr*

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.

Log Message %PIX-3-304007: URL Server *IP_addr* not responding, ENTERING ALLOW mode

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

Recommended Action None required.

Log Message %PIX-3-304008: 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.

Log Message %PIX-6-305001: Portmapped translation built for *gaddr IP_addr/port* *laddr IP_addr/port*

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

Recommended Action None required.

Log Message %PIX-6-305002: Translation built for *gaddr IP_addr* to *laddr IP_addr*

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

Recommended Action None required.

Log Message %PIX-6-305003: Teardown translation for global *IP_addr* local *IP_addr*

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

Recommended Action None required.

Log Message %PIX-6-305004: Teardown portmap translation for global *IP_addr/port* local *IP_addr/port*

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

Recommended Action None required.

Log Message %PIX-3-305005: No translation group found for *protocol*

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

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

Log Message %PIX-3-305006: *type* translation creation failed for *protocol*

Explanation A protocol (UDP, TCP, or ICMP) failed to create a translation through the PIX Firewall. The *type* can be static, portmapped (PAT), or regular.

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

Log Message %PIX-6-305007: Orphan IP *IP_addr* on interface *interface_number*

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

Recommended Action None required.

Log Message %PIX-3-307001: Denied Telnet login session from *IP_addr*.

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

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

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

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

Recommended Action None required.

Log Message %PIX-6-307003: telnet login session failed from *IP_addr* (*num* attempts).

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

Recommended Action Verify the password and try again.

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

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

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

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

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

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.

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

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

Recommended Action None required.

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

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

Recommended Action None required.

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

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

Recommended Action None required.

Log 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.

Log Message %PIX-6-311003: LU recv thread up

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

Recommended Action None required.

Log 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.

Messages 402101 to 709006

Log Message %PIX-4-402101: decaps: rec'd IPSEC packet has invalid spi for destaddr=*ip-addr*, prot=*protocol*, spi=*spi*

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

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.

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

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

Recommended Action Contact the peer's administrator.

Log Message %PIX-4-402103: identity doesn't match negotiated identity..

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

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

Log Message %PIX-4-402106: Rec'd packet not an IPSEC packet...

Explanation Received packet matched crypto map ACL, but is not IPSEC-encapsulated. IPSEC Peer is sending unencapsulated packets. This may occur because of a policy setup error on the peer. This may also be a hostile event.

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

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

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

Recommended Action Ensure that the data is sent correctly.

Log 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.

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

Explanation A new SA (security association) was created.

Explanation Informational message.

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

Explanation An SA was deleted.

Recommended Action Informational message.

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

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

Recommended Action Enable floodguard with the **floodguard 1** command.

Log Message %PIX-3-702301: lifetime expiring...

Explanation An SA lifetime has expired.

Recommended Action Debugging message.

Log Message %PIX-7-702302: replay rollover detected...

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

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

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

Explanation IPSec has requested IKE for new SAs.

Recommended Action Debugging message.

Log Message %PIX-7-709001: FO replication failed: cmd=*chars* returned=*chars*

Log Message %PIX-7-709002: FO unreplicable: cmd=*chars*

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

Recommended Action None required.

Log Message %PIX-1-709003: (Primary) Beginning configuration replication:
Send to 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.

Log 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.

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

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

Recommended Action None required.

Log Message %PIX-7-709006: (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.