CHAPTER 1

Syslog Messages

This chapter lists the syslog messages in numerical order.

Note When a number is skipped in a sequence, the message is no longer in the adaptive security appliance code.

For information about how to configure logging and SNMP, see the *Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide*.

Table 1-1 lists the syslog message classes and the ranges of syslog message IDs associated with each class.

Table 1-1 Syslog Message Classes and Associated Message ID Numbers

Class	Definition	Syslog Message ID Numbers
auth	User Authentication	109, 113
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
config	Command Interface	111, 112, 208, 308
dap	Dynamic Access Policies	734
e-mail	E-mail Proxy	719
ha	High Availability (Failover)	101, 102, 103, 104, 210, 311, 709
ip	IP Stack	209, 215, 313, 317, 408
ips	Intrusion Protection Service	400, 401, 415
np	Network Processor	319
npssl	NP SSL	725
ospf	OSPF Routing	318, 409, 503, 613
rip	RIP Routing	107, 312
rm	Resource Manager	321
session	User Session	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
snmp	SNMP	212

Table 1-1 Syslog Message Classes and Associated Message ID Numbers (continued)

Class (continued)	Definition	Syslog Message ID Numbers
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711
vpdn	PPTP and L2TP Sessions	213, 403, 603
vpn	IKE and IPSec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN Client	611
vpnfo	VPN Failover	720
vpnlb	VPN Load Balancing	718
webvpn	Web-based VPN	716

This chapter includes the following sections:

Messages 101001 to 199012

This section contains messages from 101001 to 199012.

101001

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

Error Message `%ASA-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 `%ASA-1-101005: (Primary) Error reading failover cable status.`

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

Recommended Action Replace the cable.

102001

Error Message `%ASA-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 system reload or a power failure on the other unit. “Primary” can also be listed as “Secondary” for the secondary unit.

Recommended Action On the unit that experienced the reload, issue the **show crashinfo** command to determine if there is a traceback associated with the reload. Also verify that the unit is powered on and that power cables are correctly connected.

103001

Error Message `%ASA-1-103001: (Primary) No response from other firewall (reason code = code).`

Explanation This is a failover message. This message is displayed 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 1-2 lists the reason codes and the descriptions to determine why the failover occurred.

Table 1-2 Reason Codes

Reason Code	Description
1	No failover hello seen on serial cable for 30+ seconds. This ensures that failover is running correctly on the other unit.
2	An interface did not pass one of the four failover tests. The four tests are as follows: 1) Link Up, 2) Monitor for Network Traffic, 3) ARP test, 4) Broadcast Ping test.
3	No correct ACK for 15+ seconds after a command was sent on the serial cable.
4	The local unit is not receiving the hello packet on the failover LAN and other data interfaces and it is declaring that the peer is down.
5	The standby peer went down during the configuration synchronization process.

Recommended Action Verify that the failover cable is connected correctly and both units have the same hardware, software, and configuration. If the problem persists, contact the Cisco TAC.

103002

Error Message `%ASA-1-103002: (Primary) Other firewall network interface interface_number OK.`

Explanation This is a failover message. This message is displayed 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.

Recommended Action None required.

103003

Error Message `%ASA-1-103003: (Primary) Other firewall network interface` *`interface_number`* `failed.`

Explanation This is a failover message. This message is displayed if the primary unit detects a bad network interface on the secondary unit. (Primary) can also be listed as (Secondary) for the secondary unit.

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

103004

Error Message `%ASA-1-103004: (Primary) Other firewall reports this firewall failed.`

Explanation This is a failover message. This message is displayed 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 `%ASA-1-103005: (Primary) Other firewall reporting failure.`

Explanation This is a failover message. This message is displayed 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.

103006

Error Message `%ASA-1-103006: (Primary|Secondary) Mate version` *`ver_num`* `is not compatible with ours` *`ver_num`*

Explanation This message appears when the firewall detects peer unit is running a version that is not the same as local unit and also is not compatible with HA Hitless Upgrade feature.

- *ver_num*—Version number

Recommended Action Install same or compatible versions image on both firewall units.

103007

Error Message `%ASA-1-103007: (Primary|Secondary) Mate version ver_num is not identical with ours ver_num`

Explanation This message appears when the security appliance detects that a peer unit is running a version that is not identical, but does support Hitless Upgrade and is compatible with the local unit. The system performance could be degraded because of the different image version, and you could encounter a stability issue if the different image version runs for an extended period.

- *ver_num*—Version number

Recommended Action Install same version image on both units as soon as possible.

104001, 104002

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

Error Message `%ASA-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 standby unit, or the **no failover active** command on the active unit. (Primary) can also be listed as (Secondary) for the secondary unit. Possible values for the *string* variable are as follows:

- state check
- bad/incomplete config
- ifc [interface] check, mate is healthier
- the other side wants me to standby
- in failed state, cannot be active
- switch to failed state

Recommended Action If the message occurs because of manual intervention, none required. Otherwise, use the cause reported by the secondary unit to verify the status of both units of the pair.

104003

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

Explanation This is a failover message. This message is displayed 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 `%ASA-1-104004: (Primary) Switching to OK.`

Explanation This is a failover message. This message is displayed 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 `%ASA-1-105001: (Primary) Disabling failover.`

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

Recommended Action None required.

105002

Error Message `%ASA-1-105002: (Primary) Enabling failover.`

Explanation This is a failover message. This message is displayed 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 `%ASA-1-105003: (Primary) Monitoring on interface` *`interface_name`* `waiting`

Explanation This is a failover message. The security appliance 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 security appliance monitors its network interfaces frequently during normal operations.

105004

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

Explanation This is a failover message. This message is displayed 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 %ASA-1-105006: (Primary) Link status 'Up' on interface *interface_name*.

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

Explanation This is a failover message. This message is displayed when the tests a specified network interface. This testing is performed only if the security appliance 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 `%ASA-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 `%ASA-3-105010: (Primary) Failover message block alloc failed`

Explanation Block memory was depleted. This is a transient message and the security appliance 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 `%ASA-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 correctly connected.

105020

Error Message `%ASA-1-105020: (Primary) Incomplete/slow config replication`

Explanation When a failover occurs, the active security appliance 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 security appliance, the security appliance automatically reloads itself and loads configuration from flash memory and/or resynchronizes with another security appliance. If failovers happen continuously, check the failover configuration and make sure both security appliance units can communicate with each other.

105021

Error Message `%ASA-1-105021: (failover_unit) Standby unit failed to sync due to a locked context_name config. Lock held by lock_owner_name`

Explanation During configuration synchronizing, a standby unit will reload itself if some other process locks the configuration for more than five minutes, which prevents the failover process from applying the new configuration. This can occur when an administrator pages through a running configuration on the standby unit while configuration synchronization is in process. See also the **show running-config** EXEC command and the **pager lines** *num* CONFIG command.

Recommended Action Avoid viewing or modifying configuration on standby unit when it first comes up and is in the process of establishing a failover connection with the active unit.

105031

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

Explanation LAN failover interface link is up.

Recommended Action None required.

105032

Error Message `%ASA-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 that the speed/duplex setting is correct.

105034

Error Message `%ASA-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 `%ASA-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 LAN failover interface.

105036

Error Message `%ASA-1-105036: Dropped a LAN Failover command message.`

Explanation The security appliance 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 `%ASA-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.

105038

Error Message `%ASA-1-105038: (Primary) Interface count mismatch`

Explanation When a failover occurs, the active security appliance 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 security appliance, the security appliance automatically reloads itself and loads the configuration from flash memory and/or resyncs with another security appliance. If failovers happen continuously, check the failover configuration and make sure that both security appliance units can communicate with each other.

105039

Error Message `%ASA-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.`

Explanation Failover initially verifies that the number of interfaces configured on the primary and secondary security appliances are the same. This message indicates that the primary security appliance is not able to verify the number of interfaces configured on the secondary security appliance. This message indicates that the primary security appliance is not able communicate with the secondary security appliance over the failover interface. (Primary) can also be listed as (Secondary) for the secondary security appliance.

Recommended Action Verify the failover LAN, interface configuration, and status on the primary and secondary security appliances. Make sure that the secondary security appliance is running the security appliance application and that failover is enabled.

105040

Error Message `%ASA-1-105040: (Primary) Mate failover version is not compatible.`

Explanation The primary and secondary security appliance should run the same failover software version to act as a failover pair. This message indicates that the secondary security appliance failover software version is not compatible with the primary security appliance. Failover is disabled on the primary security appliance. (Primary) can also be listed as (Secondary) for the secondary security appliance.

Recommended Action Maintain consistent software versions between the primary and secondary security appliances to enable failover.

105042

Error Message `%ASA-1-105042: (Primary) Failover interface OK`

Explanation LAN failover interface link is up.

Explanation The interface used to send failover messages to the secondary security appliance is functioning. (Primary) can also be listed as (Secondary) for the secondary security appliance.

Recommended Action None required.

105043

Error Message `%ASA-1-105043: (Primary) Failover interface failed`

Explanation LAN failover interface link is down.

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

105044

Error Message `%ASA-1-105044: (Primary) Mate operational mode` *`mode`* `is not compatible with my mode` *`mode`*`.`

Explanation When the operational mode (single or multi) does not match between failover peers, failover will be disabled.

Recommended Action Configure the failover peers to have the same operational mode, and then reenable failover.

105045

Error Message `%ASA-1-105045: (Primary) Mate license (`*`number`* `contexts) is not compatible with my license (`*`number`* `contexts).`

Explanation When the feature licenses do not match between failover peers, failover will be disabled.

Recommended Action Configure the failover peers to have the same feature license, and then reenable failover.

105046

Error Message `%ASA-1-105046 (Primary|Secondary) Mate has a different chassis`

Explanation This message is issued when two failover units have a different type of chassis. For example, one is an ASA-5510, the other is an ASA-5520, or one has a three-slot chassis, and the other has a six-slot chassis.

Recommended Action Make sure that the two failover units are the same.

105047

Error Message `%ASA-1-105047: Mate has an io_card_name1 card in slot slot_number which is different from my io_card_name2`

Explanation The two failover units have different types of cards in their respective slots.

Recommended Action Make sure that the card configurations for the failover units are the same.

105048

Error Message `%ASA-1-105048: (unit) Mate's service module (application) is different from mine (application)`

Explanation The failover process detected that different applications are running on the service modules in the active and standby units. The two failover units are incompatible if different service modules are used.

- *unit*—Primary or secondary.
- *application*—The name of the application, such as InterScan Security Card.

Recommended Action Make sure that both units have identical service modules before trying to re-enable failover.

106001

Error Message `%ASA-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 the security policy that is defined for the specified traffic type. 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 security appliance, 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 `%ASA-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 displayed if the specified connection fails because of an **outbound deny** command. The *protocol* variable can be ICMP, TCP, or UDP.

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

106006

Error Message `%ASA-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 displayed if an inbound UDP packet is denied by the security policy that is defined by the specified traffic type.

Recommended Action None required.

106007

Error Message `%ASA-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 displayed if a UDP packet containing a DNS query or response is denied.

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

106010

Error Message `%ASA-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 displayed 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 `%ASA-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 through a web browser. Any time a connection is reset, when the host at the end of the connection sends a packet after the security appliance receives the reset, this message will appear. It can typically be ignored.

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

106012

Error Message `%ASA-6-106012: 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 routing or strict source routing.

106013

Error Message `%ASA-2-106013: Dropping echo request from IP_address to PAT address IP_address`

Explanation The security appliance discarded an inbound ICMP Echo Request packet with a destination address that corresponds to a PAT global address. The inbound packet is discarded because it cannot specify which PAT host should receive the packet.

Recommended Action None required.

106014

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

Explanation The security appliance denied any inbound ICMP packet access. By default, all ICMP packets are denied access unless specifically permitted.

Recommended Action None required.

106015

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

Explanation The security appliance discarded a TCP packet that has no associated connection in the security appliance connection table. The security appliance 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 security appliance discards the packet.

Recommended Action None required unless the security appliance 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 `%ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.`

Explanation The security appliance discarded a packet with an invalid source address, which may include one of the following or some other invalid address:

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

To further enhance spoof packet detection, use the **access-list** command to configure the security appliance to discard packets with source addresses belonging to the internal network. Now that the **icmp** command has been implemented, the **access-list** command has been deprecated and is no longer guaranteed to work correctly.

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

106017

Error Message `%ASA-2-106017: Deny IP due to Land Attack from IP_address to IP_address`

Explanation The security appliance received a packet with the IP source address equal to the IP destination, and the destination port equal to the source port. This message indicates a spoofed packet that is 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 `%ASA-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address`

Explanation The outgoing ICMP packet with the specified ICMP from local host (*inside_address*) to the foreign host (*outside_address*) was denied by the outbound ACL list.

Recommended Action None required.

106020

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

Explanation The security appliance discarded an IP packet with a teardrop signature containing either a small offset or fragment overlapping. This is a hostile event that circumvents the security appliance or an Intrusion Detection System.

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

106021

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

Explanation An attack is in progress. Someone is attempting to spoof an IP address on an inbound connection. 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 security appliance.

This message appears when you have enabled Unicast RPF 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 security appliance checks packets arriving from the outside.

The security appliance 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 security appliance 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 security appliance does not support asymmetric routing.

If the security appliance is configured on an internal interface, it checks static **route** command statements or RIP, and if the source_address is not found, then an internal user is spoofing their address.

Recommended Action Even though an attack is in progress, if this feature is enabled, no user action is required. The security appliance repels the attack.

106022

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

Explanation A packet matching a connection arrives on a different interface from the interface that the connection began on.

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

An attacker also might be attempting to append packets from one connection to another as a way to break into the security appliance. In either case, the security appliance displays this message and drops the connection.

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

106023

Error Message `%ASA-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 extended ACL.

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

106024

Error Message `%ASA-2-106024: Access rules memory exhausted`

Explanation The access list compilation process has run out of memory. All configuration information that has been added since the last successful access list was removed from the system, and the most recently compiled set of access lists will continue to be used.

Recommended Action Access lists, AAA, ICMP, SSH, Telnet, and other rule types are stored and compiled as access list rule types. Remove some of these rule types so that others can be added.

106025, 106026

Error Message %ASA-6-106025: Failed to determine the security context for the *packet*:*sourceVlan:source_address dest_address source_port dest_port protocol*

Error Message %ASA-6-106026: Failed to determine the security context for the *packet:sourceVlan*:*source_address dest_address source_port dest_port protocol*

Explanation The security context of the packet in multiple context mode cannot be determined. Both messages can be generated for IP packets being dropped in either router and transparent mode.

Recommended Action None required.

106027

Error Message %ASA-4-106027:Failed to determine the security context for the *packet*:*vlansource Vlan#*:*ethertype* src *sourceMAC* dst *destMAC*

Explanation The security context of the packet in multiple context mode cannot be determined. This message is generated for non-IP packets being dropped in transparent mode only.

Recommended Action None required.

106100

Error Message %ASA-6-106100: 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 If you configured the *log* argument for the **access-list** command, the packets matched an ACL statement. The message severity level depends on the level set in the **access-list** command. The message indicates either the initial occurrence or the total number of occurrences during an interval. This message provides more information than message 106027, which only logs denied non-IP packets, and does not include the hit count or a configurable level.

When an access-list line has the *log* argument, it is expected that this syslog ID might be triggered because of a non-synchronized packet reaching the security appliance and being evaluated by the access-list. For example, if an ACK packet is received on the security appliance (for which no TCP connection exists in the connection table), the device might generate syslog 106100, indicating that the packet was permitted; however, the packet is later correctly dropped because of no matching connection.

The following list describes the message values:

- permitted | denied | est-allowed—These values specify if the packet was permitted or denied by the ACL. If the value is est-allowed, the packet was denied by the ACL but was allowed for an already established session (for example, an internal user is allowed to accesss the Internet, and responding packets that would normally be denied by the ACL are accepted).

- *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 *src_addr*.
- 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 when the security appliance 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 with the **interval** option.

Recommended Action None required.

106101

Error Message `%ASA-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 security appliance caches the flow information. This message indicates that the number of matching flows that are cached on the security appliance exceeds the user-configured limit (using the **access-list deny-flow-max** command). This message might be generated as a result of a DoS attack.

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

Recommended Action None required.

106102

Error Message `%ASA-6-106102: access-list acl_ID {permitted|denied} protocol interface_name/source_address source_port interface_name/dest_address dest_port hit-cnt number {first hit|number-second interval}`

Explanation This message indicates that a packet was either permitted or denied by an access-list that is applied through a VPN filter.

Recommended Action None required.

107001

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

Explanation The security appliance received a RIP reply message with bad authentication. This message might be caused by a misconfiguration on the router or the security appliance or by an unsuccessful attempt to attack the routing table of the security appliance.

Recommended Action This message indicates a possible 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 might be trying to determine the existing keys.

107002

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

Explanation This message could be caused by 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 routing table of the security appliance.

Recommended Action This message indicates a possible attack and should be monitored. The packet has passed authentication, if enabled, and bad data is in the packet. Monitor the situation and change the keys if there are any doubts about the originator of the packet.

108002

Error Message `%ASA-2-108002: SMTP replaced string: out source_address in inside_address data: string`

Explanation This is a Mail Guard (SMTP) message generated by the **inspect esmtp** command. This message is displayed if the security appliance replaces an invalid character in an e-mail address with a space.

Recommended Action None required.

108003

Error Message `%ASA-2-108003: Terminating ESMTP/SMTP connection; malicious pattern detected in the mail address from source_interface:source_address/source_port to dest_interface:dest_address/dset_port. Data:string`

Explanation This message is generated by Mail Guard (SMTP). This message is displayed if the security appliance detects malicious pattern in an e-mail address and drops the connection. This indicates an attack in progress.

Recommended Action None required.

108004

Error Message `%ASA-4-108004: action_class: action ESMTP req_resp from src_ifc:sip|sport to dest_ifc:dip|dport;further_info`

Explanation This event is generated when a ESMTP classification is performed on a ESMTP message and the specified criteria are satisfied. The configured action is taken.

- *action_class*—The class of action: “ESMTP Classification” for ESMTP match commands; “ESMTP Parameter” for parameter commands.
- *action*—action taken: “Dropped,” “Dropped connection for,” “Reset connection for,” or “Masked header flags for”
- *req_resp*—”Request” or “Response”
- *src_ifc*—Source interface name
- *sip|sport*—Source IP address or source port
- *dest_ifc*—Destination interface name
- *dip|dport*—Destination IP address or destination port
- *further info*—One of the following:

  For single match command: matched Class *id*: *match_command* (for example, matched Class 1234: match body length 100).

  For parameter commands: *parameter-command*: *descriptive-message* (for example, mail-relay: No Mail Relay allowed).

Recommended Action None required.

108005

Error Message `%ASA-6-108005: action_class: Received ESMTP req_resp from src_ifc:sip/sport to dest_ifc:dip/dport;further_info`

Explanation This message is generated when a ESMTP classification is performed on a ESMTP message, and the specified criteria are satisfied. The standalone log action is taken.

- *action_class*—The class of action: "ESMTP Classification" for ESMTP match commands; "ESMTP Parameter" for parameter commands.
- *req_resp*—"Request" or "Response"
- *src_ifc*—Source interface name
- *sip/sport*—Source IP address or source port
- *dest_ifc*—Destination interface name
- *dip/dport*—Destination IP address or destination port
- *further info*—One of the following:

  For single match command: matched Class *id*: *match_command* (for example, matched Class 1234: match body length 100).

  For parameter commands (commands under parameter section): *parameter-command*: *descriptive-message* (for example, mail-relay: No Mail Relay allowed).

Recommended Action None required.

108006

Error Message `%ASA-7-108006: Detected ESMTP size violation from src_ifc:sip/sport to dest_ifc:dip/dport;declared size is: decl_size, actual size is act_size.`

Explanation This message is generated when an ESMTP message size exceeds the size declared in the RCPT command.

- *src_ifc*—Source interface name
- *sip/sport*—Source IP address or source port
- *dest_ifc*—Destination interface name
- *dip/dport*—Destination IP address or destination port
- *decl_size*—Declared size
- *act_size*—Actual size

Recommended Action None required.

108007

Error Message `%ASA-6-108007: TLS started on ESMTP session between client client-side interface-name: clientIP address/client port and server server-side interface-name: server IP address/server port`

Explanation This message indicates that on an ESMTP connection, the server has responded with a 220 reply code to the client STARTTLS command. The ESMTP inspection engine no longer inspects the traffic on this connection.

- *client-side interface-name*—The name for the interface that faces the client side
- *client IP address*—The IP address of the client
- *client port*—The TCP port number for the client
- *server-side interface-name*—The name for the interface that faces the server side
- *server IP address*—The IP address of the server
- *server port*—The TCP port number for the server

Recommended Action Log and review the message. Check whether the ESMTP policy map associated with this connection has the following setting: "allow-tls action log." If not, contact the Cisco TAC.

109001

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

Explanation This is an authentication, authorization and accounting (AAA) message. This message is displayed if the security appliance is configured for AAA and detects an authentication request by the specified user.

Recommended Action None required.

109002

Error Message `%ASA-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 displayed if an authentication request fails, because the specified authentication server cannot be contacted by the module.

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

109003

Error Message `%ASA-6-109003: Auth from inside_address to outside_address/outside_port failed (all servers failed) on interface interface_name, >, so marking all servers ACTIVE again.`

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

Recommended Action Ping the authentication servers from the security appliance. Make sure that the daemons are running.

109005

Error Message `%ASA-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 displayed when the specified authentication request succeeds.

Recommended Action None required.

109006

Error Message `%ASA-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 displayed if the specified authentication request fails, possibly because of an incorrect password.

Recommended Action None required.

109007

Error Message `%ASA-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 displayed when the specified authorization request succeeds.

Recommended Action None required.

109008

Error Message `%ASA-6-109008: Authorization denied for user user from outside_address/outside_port to inside_address/ inside_port on interface interface_name.`

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

Recommended Action None required.

109010

Error Message `%ASA-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 displayed 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 the Flood Defender feature with the **floodguard enable** command.

109011

Error Message `%ASA-2-109011: Authen Session Start: user 'user', sid number`

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

Recommended Action None required.

109012

Error Message `%ASA-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 `%ASA-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 `%ASA-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.

109016

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

Explanation The access control list specified on the AAA server for this user does not exist on the security appliance. This error can occur if you configure the AAA server before you configure the security appliance. The Vender-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 security appliance, making sure to use the same name specified on the AAA server.

109017

Error Message `%ASA-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 **proxy-limit** *proxy_limit* command, or ask the user to close unused connections. If the error persists, it may indicate a possible DoS attack.

109018

Error Message `%ASA-3-109018: Downloaded ACL acl_ID is empty`

Explanation The downloaded authorization access control list has no ACEs. This situation might be caused by misspelling the attribute string “ip:inacl#” or omitting the **access-list** command.

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

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

109019

Error Message `%ASA-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 control 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 `%ASA-3-109020: Downloaded ACL has config error; ACE`

Explanation One of the components of the downloaded authorization access control 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.

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

109021

Error Message `%ASA-7-109021: Uauth null proxy error`

Explanation An internal user authentication error has occurred.

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

109022

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

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

Recommended Action None required.

109023

Error Message `%ASA-3-109023: User from source_address/source_port to dest_address/dest_port on interface outside_interface 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 Authenticate using Telnet, FTP, or HTTP before attempting to use the above service port.

109024

Error Message `%ASA-6-109024: Authorization denied from source_address/source_port to dest_address/dest_port (not authenticated) on interface interface_name using protocol`

Explanation This is a AAA message. This message is displayed if the security appliance is configured for AAA and a user attempted to make a TCP connection across the security appliance without prior authentication.

Recommended Action None required.

109025

Error Message `%ASA-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 control list check failed. The check either matched a deny or did not match anything, such as an implicit deny. The connection was denied by the user access control list *acl_ID*, which was defined per the AAA authorization policy on Cisco Secure Access Control Server (ACS).

Recommended Action None required.

109026

Error Message `%ASA-3-109026: [aaa protocol] Invalid reply digest received; shared server key may be mismatched.`

Explanation The response from the AAA server could not be validated. It is likely that the configured server key is incorrect. This event may be generated during transactions with RADIUS or TACACS+ servers.

Recommended Action Verify that the server key, configured using the **aaa-server** command, is correct.

109027

Error Message `%ASA-4-109027: [aaa protocol] Unable to decipher response message Server = server_IP_address, User = user`

Explanation The response from the AAA server could not be validated. The configured server key is probably incorrect. This message may be displayed during transactions with RADIUS or TACACS+ servers. The *server_IP_address* is the IP address of the relevant AAA server. The *user* is the username associated with the connection.

Recommended Action Verify that the server key, configured using the **aaa-server** command, is correct.

109028

Error Message `%ASA-4-109028: aaa bypassed for same-security traffic from ingress_interface:source_address/source_port to egress_interface:dest_address/dest_port`

Explanation AAA is being bypassed for same security traffic that matches a configured AAA rule. This can only occur when traffic passes between two interfaces that have the same configured security level, when the same security traffic is permitted, and if the AAA configuration uses the include or exclude syntax.

Recommended Action None required.

109029

Error Message `%ASA-5-109029: Parsing downloaded ACL: string`

Explanation A syntax error was encountered while parsing an access list that was downloaded from a RADIUS server during user authentication.

- *string*—An error message detailing the syntax error that prevented the access list from parsing correctly.

Recommended Action Use the information presented in this message to identify and correct the syntax error in the access list definition within the RADIUS server configuration.

109030

Error Message `%ASA-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list source | dest netmask netmask.`

Explanation This message is displayed when a dynamic ACL that is configured on a RADIUS server is not converted by the mechanism for automatically detecting wildcard netmasks. The problem occurs because this mechanism could not determine if the netmask is a wildcard or a normal netmask.

- *access_list*—The access list that could not be converted
- *source*—The source IP address.
- *dest*—The destination IP address.
- *netmask*—The subnet mask for the destination or source address in dotted-decimal notation.

Recommended Action Check the access list netmask on the RADIUS server for wildcard configuration. If it is meant to be a wildcard, and if all access list netmasks on that server are wildcard then use the **wildcard** setting for **acl-netmask-convert** for the AAA server. Otherwise, change the netmask to a normal netmask or to a wildcard netmask that does not contain holes. In other words, where the netmask presents consecutive binary 1s. For example, 00000000.00000000.00011111.11111111 or hex 0.0.31.255. If the mask is meant to be normal and all access list netmasks on that server are normal then use the **normal** setting **acl-netmask-convert** for the AAA server.

109031

Error Message `%ASA-4-109031: NT Domain Authentication Failed: rejecting guest login for username.`

Explanation This message is displayed when a user tries to authenticate to an NT Auth domain that was configured for guest account access and the username is not a valid username on the NT server. The connection is denied.

Recommended Action If the user is a valid user, add an account to the NT server. If the user is not allowed access, none required.

109032

Error Message `%ASA-3-109032: Unable to install ACL access_list, downloaded for user username; Error in ACE: ace.`

Explanation This message is displayed when an access control list is received from a RADIUS server during the authentication of a network user. The log event indicates a syntax error in one of the elements of the access list. When this occurs, the element is discarded but the rest of access list is still applied. The entire text of the malformed element is included in the message. Note that this condition does not result in an authentication failure.

- *access_list*—The name assigned to the dynamic access list as it would appear in the output of the **show access-list** command.
- *username*—The name of the user whose connection will be subject to this access list.
- *ace*—The access list entry that was being processed when the error was detected.

Recommended Action Correct the access list definition in the RADIUS server configuration.

109033

Error Message `%ASA-4-109033: Authentication failed for admin user user from src_IP. Interactive challenge processing is not supported for protocol connections`

Explanation AAA challenge processing was triggered during authentication of an administrative connection, but the security appliance cannot initiate interactive challenge processing with the client application. When this occurs, the authentication attempt will be rejected and the connection denied.

- *user*—The name of the user being authenticated.
- *src_IP*—The IP address of the client host.
- *protocol*—The client connection protocol. Possible values: "SSH v1" or "administrative HTTP."

Recommended Action Reconfigure AAA so that challenge processing does not occur for these connection types. This generally means to avoid authenticating these connection types to RSA SecurID servers or to any token-based AAA server via RADIUS.

109034

Error Message `%ASA-4-109034: Authentication failed for network user user from src_IP/port to dst_IP/port. Interactive challenge processing is not supported for protocol connections`

Explanation AAA challenge processing was triggered during authentication of a network connection, but the security appliance cannot initiate interactive challenge processing with the client application. When this occurs, the authentication attempt will be rejected and the connection denied.

- *user*—The name of the user being authenticated.
- *src_IP/port*—The IP address and port of the client host.

- *dst_IP/port*—The IP address and port of the server to which the client is attempting to connect.
- *protocol*—The client connection protocol. Possible value: "FTP."

Recommended Action Reconfigure AAA so that challenge processing does not occur for these connection types. This generally means to avoid authenticating these connection types to RSA SecurID servers or to any token-based AAA server via RADIUS.

109035

Error Message `%ASA-3-109035: Exceeded maximum number (999) of DAP attribute instances for user string.`

Explanation The Dynamic Access Policy supports multiple values of the same attribute received from an AAA server. If the AAA server should send a response containing more than 999 values for the same attribute, then the ASA will treat this response message as being malformed and reject the authentication. This condition has only been seen in lab environments using specialized test tools. It is unlikely that the condition should occur in a real-world production network.

- *string*—The username at login

Recommended Action If this message is generated, it would be helpful to capture the authentication traffic between the ASA and AAA server using a protocol sniffer (such as WireShark) and forward the trace file to Cisco Engineering for analysis.

110002

Error Message `%ASA-6-110002: Failed to locate egress interface for protocol from src-interface: src IP/src port to dest IP/dest port`

Explanation An error occurred when the security appliance tried to find the interface through which to send the packet.

- *protocol*—The protocol of the packet
- *src interface*—The interface on which the packet was received from
- *src IP*—The source IP address of the packet
- *src port*—The source port number
- *dest interface*—The interface to which the packet is forwarded
- *dest IP*— The destination IP address of the packet
- *dest port*—The destination port number

Recommended Action Copy the error message together with the configuration and any events leading up to the error, and submit this information to Cisco TAC. In addition, use the **show asp table routing** command to view routing table details.

110003

Error Message `%ASA-6-110003: Routing failed to locate next hop for` *`protocol`* `from` *`src interface`*`: src IP/src port to dest interface: dest IP/dest port`

Explanation An error occurred when the security appliance tried to find the next hop on the interface's routing table.

- *protocol*—The protocol of the packet
- *src interface*—The interface on which the packet was received from
- *src IP*—The source IP address of the packet
- *src port*—The source port number
- *dest interface*—The interface to which the packet is forwarded
- *dest IP*— The destination IP address of the packet
- *dest port*—The destination port number

Recommended Action Copy the error message together with the configuration and any events leading up to the error, and submit this information to Cisco TAC. In addition, use the **show asp table routing** command to view routing table details.

111001

Error Message `%ASA-5-111001: Begin configuration:` *`IP_address`* `writing to` *`device`*

Explanation This message is displayed 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 with a Telnet connection.

Recommended Action None required.

111002

Error Message `%ASA-5-111002: Begin configuration:` *`IP_address`* `reading from` *`device`*

Explanation This message is displayed when you enter the **read** command to read your configuration from 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 with a Telnet connection.

Recommended Action None required.

111003

Error Message `%ASA-5-111003: IP_address Erase configuration`

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

Recommended Action After erasing the configuration, reconfigure the security appliance 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 `%ASA-5-111004: IP_address end configuration: {FAILED|OK}`

Explanation This message is displayed when you enter the **config floppy/memory/ network** command or the **write floppy/memory/network/standby** command. The *IP_address* value indicates whether the login was made at the console port or through 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 disk, ensure that the floppy disk is not write protected; if writing to a TFTP server, ensure that the server is up.

111005

Error Message `%ASA-5-111005: IP_address end configuration: OK`

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

Recommended Action None required.

111007

Error Message `%ASA-5-111007: Begin configuration: IP_address reading from device.`

Explanation This message is displayed 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* value indicates whether the login was made at the console port or through a Telnet connection.

Recommended Action None required.

111008

Error Message `%ASA-5-111008: User user executed the command string`

Explanation The user entered any command, with the exception of a **show** command.

Recommended Action None required.

111009

Error Message `%ASA-7-111009:User user executed cmd:string`

Explanation The user entered a command that does not modify the configuration. This message appears only for **show** commands.

Recommended Action None required.

111111

Error Message `%ASA-1-111111 error_message`

Explanation System or infrastructure error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

112001

Error Message `%ASA-2-112001: (string:dec) Clear complete.`

Explanation This message is displayed when a request to clear the module configuration is completed. The source file and line number are identified.

Recommended Action None required.

113001

Error Message `%ASA-3-113001: Unable to open AAA session. Session limit [limit] reached.`

Explanation The AAA operation on an IPsec tunnel or WebVPN connection could not be performed because of the unavailability of system resources. The *limit* value indicates the maximum number of concurrent AAA transactions.

Recommended Action Reduce the demand for AAA resources if possible.

113003

Error Message `%ASA-6-113003: AAA group policy for user user is being set to policy_name.`

Explanation The group policy that is associated with the tunnel-group is being overridden with a user specific policy, *policy_name*. The *policy_name* is specified using the **username** command when LOCAL authentication is configured or is returned in the RADIUS CLASS attribute when RADIUS authentication is configured.

Recommended Action None required.

113004

Error Message `%ASA-6-113004: AAA user aaa_type Successful: server = server_IP_address, User = user`

Explanation This is an indication that a AAA operation on an IPsec or WebVPN connection has been completed successfully. The AAA types are “authentication,” “authorization,” or “accounting.” The *server_IP_address* is the IP address of the relevant AAA server. The *user* is the username associated with the connection.

Recommended Action None required.

113005

Error Message `%ASA-6-113005: AAA user authentication Rejected: reason = string: server = server_IP_address, User = user`

Explanation This is an indication that either an authentication or authorization request for a user associated with an IPsec or WebVPN connection has been rejected. Details of why the request was rejected are provided in the *reason* field. *server_IP_address* is the IP address of the relevant AAA server. *user* is the username associated with the connection. *aaa_operation* is either authentication or authorization.

Recommended Action None required.

113006

Error Message `%ASA-6-113006: User user locked out on exceeding number successive failed authentication attempts`

Explanation A locally configured user is being locked out. This happens when a configured number of consecutive authentication failures have occurred for this user and indicates that all future authentication attempts by this user will be rejected until an administrator unlocks the user using the **clear aaa local user lockout** command. *user* is the user that is now locked and *number* is the consecutive failure threshold configured with the **aaa local authentication attempts max-fail** command.

Recommended Action Try unlocking the user using the **clear_aaa_local_user_lockout** command or adjusting the maximum number of consecutive authentication failures that are tolerated.

113007

Error Message `%ASA-6-113007: User user unlocked by administrator`

Explanation A locally configured user that was locked out after exceeding the maximum number of consecutive authentication failures set by the **aaa local authentication attempts max-fail** command has been unlocked by the indicated administrator.

Recommended Action None required.

113008

Error Message `%ASA-6-113008: AAA transaction status ACCEPT: user = user`

Explanation The AAA transaction for a user associated with an IPsec or WebVPN connection was completed successfully. The *user* is the username associated with the connection.

Recommended Action None required.

113009

Error Message `%ASA-6-113009: AAA retrieved default group policy` *`policy`* `for user` *`user`*

Explanation This message may be generated during the authentication or authorization of an IPsec or WebVPN connection. The attributes of the group policy that were specified with the **tunnel-group** or **webvpn** commands have been retrieved.

Recommended Action None required.

113010

Error Message `%ASA-6-113010: AAA challenge received for user` *`user`* `from server` *`server_IP_address`*

Explanation This message may be generated during the authentication of an IPsec connection when the authentication is done with a SecurID server. The user will be prompted to provide further information prior to being authenticated. *server _IP_address* is the IP address of the relevant AAA server. *user* is the username associated with the connection.

Recommended Action None required.

113011

Error Message `%ASA-6-113011: AAA retrieved user specific group policy` *`policy`* `for user` *`user`*

Explanation This event may be generated during the authentication or authorization of an IPsec or WebVPN connection. The attributes of the group policy that was specified with the **tunnel-group** or **webvpn** commands have been retrieved.

Recommended Action None required.

113012

Error Message `%ASA-6-113012: AAA user authentication Successful: local database: user = user`

Explanation The user associated with a IPsec or WebVPN connection has been successfully authenticated to the local user database. *user* is the username associated with the connection.

Recommended Action None required.

113013

Error Message `%ASA-6-113013: AAA unable to complete the request Error: reason = reason: user = user`

Explanation The AAA transaction for a user associated with an IPsec or WebVPN connection has failed due to an error or has been rejected due to a policy violation. Details are provided in the *reason* field. *user* is the username associated with the connection.

Recommended Action None required.

113014

Error Message `%ASA-6-113014: AAA authentication server not accessible: server = server_IP_address: user = user`

Explanation The device was unable to communicate with the configured AAA server during the AAA transaction associated with an IPsec or WebVPN connection. This may or may not result in a failure of the user connection attempt depending on the backup servers configured in the *aaa-server* group and the availability of those servers.

Recommended Action Verify connectivity with the configured AAA servers.

113015

Error Message `%ASA-6-113015: AAA user authentication Rejected: reason = reason: local database: user = user`

Explanation A request for authentication to the local user database for a user associated with an IPsec or WebVPN connection has been rejected. Details of why the request was rejected are provided in the *reason* field. *user* is the username associated with the connection.

Recommended Action None required.

113016

Error Message `%ASA-6-113016: AAA credentials rejected: reason = reason: server = server_IP_address: user = user`

Explanation The AAA transaction for a user associated with an IPsec or WebVPN connection has failed due to an error or rejected due to a policy violation. Details are provided in the *reason* field. *server_IP_address* is the IP address of the relevant AAA server. *user* is the username associated with the connection.

Recommended Action None required.

113017

Error Message `%ASA-6-113017: AAA credentials rejected: reason = reason: local database: user = user\`

Explanation This is an indication that the AAA transaction for a user associated with an IPsec or WebVPN connection has failed due to an error or rejected due to a policy violation. Details are provided in the *reason* field. This event only appears when the AAA transaction is with the local user database rather than with an external AAA server. *user* is the username associated with the connection.

Recommended Action None required.

113018

Error Message `%ASA-3-113018: User: user, Unsupported downloaded ACL Entry: ACL_entry, Action: action`

Explanation An ACL entry in unsupported format was downloaded from the authentication server. The following list describes the message values:

- *user*—User trying to login.
- *ACL_entry*—Unsupported ACL entry downloaded from the authentication server.
- *action*—Action taken on encountering the unsupported ACL Entry.

Recommended Action The ACL entry on the authentication server has to be changed appropriately by the administrator to conform with the supported ACL entry formats.

113019

Error Message `%ASA-4-113019: Group = group, Username = user, IP = peer_address, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason`

Explanation This is an informational message.

- *group*—group name
- *user*—username
- *peer_address*—peer address
- *type*—session type (for example, IPsec/UDP)
- *duration*—connect duration
- *count*—number of bytes
- *reason*—reason for disconnection

Port preempted. This reason indicates that the allowed number of simultaneous (same user) logins has been exceeded. To resolve this problem, increase the number of simultaneous logins or have users only log in once with a given username and password.

Recommended Action None required.

113020

Error Message `%ASA-3-113020: Kerberos error: Clock skew with server ip_address greater than 300 seconds`

Explanation This message is displayed when authentication for an IPsec or WebVPN user through a Kerberos server fails because the clocks on the security appliance the server are more than five minutes (300 seconds) apart. When this occurs, the connection attempt is rejected.

- *ip_address*—The IP address of the Kerberos server.

Recommended Action Synchronize the clocks on the security appliance and the Kerberos server.

113021

Error Message `%ASA-3-113021: Attempted console login failed. User username did NOT have appropriate Admin Rights.`

Explanation A user has attempted access to the management console and was denied.

- *username*—The username entered by the user.

Recommended Action If the user is a newly added Admin Rights user, check that the service-type (LOCAL or RADIUS authentication server) for that user is set to allow access:

- nas-prompt - Allows login to the console and exec privileges at the required level, but not enable (configuration modification) access.
- admin - Allows all access and can be further constrained by command privilege.

Otherwise, the user is inappropriately attempting to access the management console; the action to be taken should be consistent with company policy for these matters.

113022

Error Message `%ASA-2-113022: AAA Marking protocol server ip-addr in server group tag as FAILED`

Explanation This syslog message indicates that the security appliance has tried an authentication, authorization, or accounting request to the AAA server and did not receive a response within the configured timeout window. The AAA server will be marked as "failed" and has been removed from service.

- *protocol*—The type of authentication protocol, which can be one of the following:

- RADIUS
- TACACS+
- NT
- RSA SecurID
- Kerberos
- LDAP

- *ip-addr*—The IP address of the AAA server
- *tag*—The server group name

Recommended Action Verify that the AAA server is online and is accessible from the security appliance.

113023

Error Message `%ASA-2-113023: AAA Marking protocol server ip-addr in server group tag as ACTIVE`

Explanation This syslog message indicates that the security appliance has reactivated the AAA server that was previously marked as "failed." The AAA server is now available to service AAA requests.

- *protocol*—The type of authentication protocol, which can be one of the following:
  - RADIUS
  - TACACS+
  - NT
  - RSA SecurID
  - Kerberos
  - LDAP
- *ip-addr*—The IP address of the AAA server
- *tag*—The server group name

Recommended Action None required.

113024

Error Message `%ASA-5-113024: Group tg: Authenticating type connection from ip with username, user_name, from client certificate`

Explanation This message is generated when the pre-fill username feature overrides the username with one derived from the client certificate for use in AAA.

- *tg*—The tunnel group
- *type*—The type of connection (ssl-client or clientless)

- *ip*—The IP address of the connecting user
- *user_name*—The name extracted from the client certificate for use in AAA

Recommended Action None required.

113025

Error Message `%ASA-5-113025: Group tg: FAILED to extract username from certificate while authenticating type connection from ip`

Explanation This message indicates that a username could not be successfully extracted from the certificate for use in AAA.

- *tg*—The tunnel group
- *type*—The type of connection (SSL client or clientless)
- *ip*—The IP address of the connecting user

Recommended Action The administrator should check that the **authentication aaa certificate**, **ssl certificate-authentication**, and **authorization-dn-attributes** keywords are all set correctly.

114001

Error Message `%ASA-1-114001: Failed to initialize 4GE SSM I/O card (error error_string).`

Explanation This message is displayed when the system fails to initialize a 4GE SSM I/O card due to an I2C error or a switch initialization error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.

3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114002

Error Message `%ASA-1-114002: Failed to initialize SFP in 4GE SSM I/O card (error error_string).`

This message is displayed when the system fails to initialize an SFP connector in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114003

Error Message `%ASA-1-114003: Failed to run cached commands in 4GE SSM I/O card (error error_string).`

Explanation This message is displayed when the system fails to run cached commands in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C_BUS_TRANSACTION_ERROR
- I2C_CHKSUM_ERROR
- I2C_TIMEOUT_ERROR
- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114004

Error Message `%ASA-6-114004: 4GE SSM I/O Initialization start.`

Explanation This message is displayed to notify the user that an 4GE SSM I/O Initialization is starting.

- *syslog_id*—Message identifier

Recommended Action None required.

114005

Error Message `%ASA-6-114005: 4GE SSM I/O Initialization end.`

Explanation This message is displayed to notify user that an 4GE SSM I/O Initialization is finished.

- *syslog_id*—Message identifier

Recommended Action None required.

114006

Error Message `%ASA-3-114006: Failed to get port statistics in 4GE SSM I/O card (error error_string).`

Explanation This message is displayed when the system fails to get port statistics in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114007

Error Message `%ASA-3-114007: Failed to get current msr in 4GE SSM I/O card (error error_string).`

Explanation This message is displayed when the system fails to get the current module status register information in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114008

Error Message `%ASA-3-114008: Failed to enable port after link is up in 4GE SSM I/O card due to either I2C serial bus access error or switch access error.`

Explanation This message is displayed when the system fails to enable a port after the link transition to Up state is detected in an 4GE SSM I/O card due to either an I2C serial bus access error or a switch access error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C_BUS_TRANSACTION_ERROR
- I2C_CHKSUM_ERROR
- I2C_TIMEOUT_ERROR
- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114009

Error Message `%ASA-3-114009: Failed to set multicast address in 4GE SSM I/O card (error error_string).`

Explanation This message is displayed when the system fails to set the multicast address in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114010

Error Message `%ASA-3-114010: Failed to set multicast hardware address in 4GE SSM I/O card (error error_string).`

Explanation This message is displayed when the system fails to set the multicast hardware address in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR
- I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114011

Error Message `%ASA-3-114011: Failed to delete multicast address in 4GE SSM I/O card (error error_string).`

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C_BUS_TRANSACTION_ERROR
- I2C_CHKSUM_ERROR
- I2C_TIMEOUT_ERROR
- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

Explanation This message is displayed when the system fails to delete the multicast address in an 4GE SSM I/O card due to either an I2C error or a switch initialization error.

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114012

Error Message `%ASA-3-114012: Failed to delete multicast hardware address in 4GE SSM I/O card (error error_string).`

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Explanation This message is displayed when the system fails to delete the multicast hardware address in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114013

Error Message `%ASA-3-114013: Failed to set mac address table in 4GE SSM I/O card (error error_string).`

Explanation This message is displayed when the system fails to set the MAC address table in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114014

Error Message `%ASA-3-114014: Failed to set mac address in 4GE SSM I/O card (error error_string).`

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- I2C_BUS_TRANSACTION_ERROR
- I2C_CHKSUM_ERROR
- I2C_TIMEOUT_ERROR
- I2C_BUS_COLLISION_ERROR
- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

Explanation This message is displayed when the system fails to set the MAC address in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114015

Error Message `%ASA-3-114015: Failed to set mode in 4GE SSM I/O card (error error_string).`

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Explanation This message is displayed when the system fails to set individual/promiscuous mode in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114016

Error Message `%ASA-3-114016: Failed to set multicast mode in 4GE SSM I/O card (error error_string).`

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR

– I2C_SMBUS_UNSUPPORT
– I2C_BYTE_COUNT_ERROR
– I2C_DATA_PTR_ERROR

Explanation This message is displayed when the system fails to set the multicast mode in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114017

Error Message `%ASA-3-114017: Failed to get link status in 4GE SSM I/O card (error error_string).`

Explanation This message is displayed when the system fails to get link status in an 4GE SSM I/O card due to either an I2C serial bus access error or a switch access error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

– I2C_BUS_TRANSACTION_ERROR
– I2C_CHKSUM_ERROR
– I2C_TIMEOUT_ERROR
– I2C_BUS_COLLISION_ERROR
– I2C_HOST_BUSY_ERROR
– I2C_UNPOPULATED_ERROR
– I2C_SMBUS_UNSUPPORT
– I2C_BYTE_COUNT_ERROR
– I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Notify the system administrator
2. Log and review the messages and the errors associated with the event.
3. Reboot the software running on the system.
4. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
5. If the problem persists, contact the Cisco TAC.

114018

Error Message `%ASA-3-114018: Failed to set port speed in 4GE SSM I/O card (error error_string).`

Explanation This message is displayed when the system fails to set the port speed in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114019

Error Message `%ASA-3-114019: Failed to set media type in 4GE SSM I/O card (error error_string).`

Explanation This message is displayed when the system fails to set the media type in an 4GE SSM I/O card due to an I2C error or a switch initialization error.

- *syslog_id*—Message identifier
- *error_string*—Describes either an I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR

- I2C_HOST_BUSY_ERROR
- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

114020

Error Message `%ASA-3-114020: Port link speed is unknown in 4GE SSM I/O card.`

Explanation This message is displayed when the system cannot detect the port link speed in an 4GE SSM I/O card.

Recommended Action Perform the following steps:

1. Log and review the messages associated with the event.
2. Reset the 4GE SSM I/O card and observe if the software automatically recovers from the event.
3. If the software does not recover automatically, power cycle the box. When you turn off the power, make sure you wait several seconds before you turn the power on.
4. If the problem persists, contact the Cisco TAC.

114021

Error Message `%ASA-3-114021: Failed to set multicast address table in 4GE SSM I/O card due to` *`error`*`.`

Explanation This message is displayed when the system fails to set the multicast address table in the 4GE SSM I/O card due to either I2C serial bus access error, or to switch access error.

- *error*—Describes either a switch access error (which is a decimal error code), or an I2C serial bus error. Possible I2C serial bus errors include:

  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR

- I2C_UNPOPULATED_ERROR
- I2C_SMBUS_UNSUPPORT
- I2C_BYTE_COUNT_ERROR
- I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages associated with the event.
2. Try to reboot the box.
3. If the software does not recover automatically, power cycle the box. When you turn off the power, make sure you wait several seconds before you turn the power on again.
4. If the problem persists, contact the Cisco TAC.

115000

Error Message `%ASA-2-115000: %d: Critical assertion in process: %s, fiber: %s, component: %s, subcomponent: %s, file: %s, line: %d`

Explanation An important software event has occurred.

Recommended Action Contact the Cisco TAC.

115001

Error Message `%ASA-3-115001: %d: Error in process: %s, fiber: %s, component: %s, subcomponent: %s, file: %s, line: %d`

Explanation An important software event has occurred.

Recommended Action Contact the Cisco TAC.

115002

Error Message `%ASA-4-115002: %d: Warning in process: %s, fiber: %s, component: %s, subcomponent: %s, file: %s, line: %d`

Explanation An important software event has occurred.

Recommended Action Contact the Cisco TAC.

199001

Error Message `%ASA-5-199001: Reload command executed from telnet (remote IP_address).`

Explanation This message logs the address of the host that is initiating a security appliance reboot with the **reload** command.

Recommended Action None required.

199002

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

Explanation The security appliance finished its initial boot and the 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.

199003

Error Message `%ASA-6-199003: Reducing link MTU dec.`

Explanation The security appliance received a packet from the outside network that uses a larger MTU than the inside network. The security appliance then sent an ICMP message to the outside host to negotiate an appropriate MTU. The log message includes the sequence number of the ICMP message.

Recommended Action None required.

199005

Error Message `%ASA-6-199005: Startup begin`

Explanation The security appliance started.

Recommended Action None required.

199006

Error Message `%ASA-5-199006: Orderly reload started at` *`when`* `by` *`whom`*`. Reload reason:` *`reason`*

Explanation This message is generated when a reload operation is started.

- *when*—The time at which orderly reload operation begins. The time is in the format of *hh:mm:ss timezone weekday month day year*, for example "13:23:45 UTC Sun Dec 28 2007."
- *whom*—The user or system that scheduled the reload.
- *reason*—The reload reason. String will be *unspecified* if a more complete reason is not displayed.

Recommended Action None required.

199907

Error Message `%ASA-5-1999007:IP detected an attached application using port` *`port`* `while removing context`

Explanation When an interface or context is removed, all applications should close all channels for that context or interface. This message indicates that an application had not closed all channels for a removed interface or application and is doing so now.

Recommended Action None required.

199909

Error Message `%ASA-7-199009: ICMP detected an attached application while removing a context`

Explanation When an interface or context is removed, all applications should close all channels for that context or interface. This message indicates that an application had not closed all channels for a removed interface or application and is doing so now.

Recommended Action None required.

199010

Error Message `%ASA-1-199010: Signal 11 caught in process/fiber (rtcli async executor process)/(rtcli async executor) at address 0xf132e03b, corrective action at 0xca1961a0`

Explanation The crash recovery mechanism generates this message after a system has recovered from a serious error.

Recommended Action Contact the Cisco TAC.

199011

Error Message `%ASA-2-199011: Close on bad channel in process/fiber` *`process/fiber`*`, channel ID` *`p`*`, channel state` *`s process/fiber`* `name of the process/fiber that caused the bad channel close operation.`

Explanation An unexpected channel close condition has been detected.

- *p*—The channel ID.
- *process/fiber*—The name of the process/fiber that caused the bad channel close operation.
- *s*—The channel state.

Recommended Action Contact Cisco TAC and attach a log file.

199012

Error Message `%ASA-1-199012: Stack smash during new_stack_call in process/fiber` *`process/fiber`*`, call target` *`f`*`, stack size` *`s`*`,` *`process/fiber`* `name of the process/fiber that caused the stack smash`

Explanation A stack smash condition has been detected.

- *f*—The target of the new_stack_call.
- *process/fiber*—The name of the process/fiber that caused the stack smash.
- *s*—The new stack size specified in new_stack_call.

Recommended Action Contact Cisco TAC and attach a log file.

Messages 201002 to 219002

This section contains messages from 201002 to 219002.

201002

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

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

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

201003

Error Message `%ASA-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 security appliance. This message is displayed when the number of embryonic connections from the specified foreign address with the specified static global address to the specified local address exceeds the embryonic limit. When the limit on embryonic connections to the security appliance is reached, the security appliance attempts to accept them anyway, but puts a time limit on the connections. The time limit allows some connections to succeed even if the security appliance is very busy. The *nconns* variable lists the number of embryonic connections received and the *elimit* variable 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 by a very heavy load of legitimate traffic. Use the **show static** command to check the limit imposed on embryonic connections to a static address.

201004

Error Message `%ASA-3-201004: Too many UDP connections on {static|xlate} global_address! udp connections limit`

Explanation This is a connection-related message. This message is displayed when the maximum number of UDP connections to the specified global address was exceeded. The *udp conn limit* variable is the maximum number of UDP connections permitted for the static or translation.

Recommended Action Use the **show static** or **show nat** command to check the limit imposed on connections to a static address. You can configure the limit.

201005

Error Message `%ASA-3-201005: FTP data connection failed for IP_address IP_address`

Explanation The security appliance could not 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 `%ASA-3-201006: RCMD backconnection failed for IP_address/port.`

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

Recommended Action Check the **rsh** client version; the security appliance only supports the Berkeley **rsh**. You can also reduce the amount of memory usage, or purchase additional memory.

201008

Error Message `%ASA-3-201008: The security appliance is disallowing new connections.`

Explanation This message appears when you have enabled TCP system log messaging and the syslog server cannot be reached, or when using security appliance 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 server is up and you can ping the host from the security appliance 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 `%ASA-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 displayed when the maximum number of connections to the specified static address was exceeded. The *number* variable is the maximum of connections permitted for the host specified by the *IP_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.

201010

Error Message `%ASA-3-201010: Embryonic connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name`

Explanation An attempt to establish a TCP connection failed due to an exceeded embryonic connection limit, which was configured with the **set connection embryonic-conn-max** MPC command for a traffic class.

- *econns*—The current count of embryonic connections associated to the configured traffic class.
- *limit*—The configured embryonic connection limit for the traffic class.
- *dir*—
  input: The first packet that initiates the connection is an input packet on the interface *interface_name.*
  output: The first packet that initiates the connection is an output packet on the interface *interface_name.*
- *source_address/source_port*—The source IP address and the source port of the packet initiating the connection.
- *dest_address/dest_port*—The destination IP address and the destination port of the packet initiating the connection.
- *interface_name*—The name of the interface on which the policy limit is enforced.

Recommended Action None required.

201011

Error Message `%ASA-3-201011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.`

Explanation A new connection through the firewall device resulted in exceeding at least one of the configured maximum connection limits. This message applies both to connection limits configured using a static command, or to those configured using Cisco Modular Policy Framework. The new connection will not be allowed through the firewall device until one of the existing connections are torn down thereby bringing the current connection count below the configured maximum.

- *cnt*—Current connection count.
- *limit*—Configured connection limit.
- *dir*—Direction of traffic, inbound or outbound.
- *sip*—Source IP address.
- *sport*—Source Port.
- *dip*—Destination IP address.
- *dport*—Destination Port.
- *if_name*—Name of the interface on which we received the traffic.

Recommended Action None required.

201012

Error Message `%ASA-6-201012: Per-client embryonic connection limit exceeded` *`curr num/limit`* `for [input|output] packet from` *`IP_address`*`/ port to` *`ip/port`* `on interface` *`interface_name`*

Explanation An attempt to establish a TCP connection failed because the per-client embryonic connection limit was exceeded. By default, this message is rate limited to 1 message every 10 seconds.

- *curr num*—The current number.
- *limit*—The configured limit.
- [input|output]—Input or output packet on interface *interface_name.*
- *IP_address*—IP address.
- *port*—TCP or UDP port.
- *interface_name*—The name of the interface on which the policy is applied.

Recommended Action When the limit is reached, any new connection request will be proxied by the security appliance to prevent a SYN flood attack. The security appliance will only connect to the server if the client is able to finish the three-way handshake. This usually does not affect the end user or the application. However, if this creates a problem for any application that has a legitimate need for a higher number of embryonic connections, you can adjust the setting by entering the **set connection per-client-embryonic-max** command.

201013

Error Message `%ASA-3-201013: Per-client connection limit exceeded` *`curr num/limit`* `for [input|output] packet from ip/`*`port`* `to` *`ip/port`* `on interface` *`interface_name`*

Explanation A connection was rejected because the per-client connection limit was exceeded.

- *curr num*—The current number.
- *limit*—The configured limit.
- [input|output]—The input or output packet on interface *interface_name.*
- *IP_address*—The IP address.
- *port*—The TCP or UDP port.
- *interface_name*—The name of the interface on which the policy is applied.

Recommended Action When the limit is reached any new connection request will be silently dropped. Normally an application will retry. This will cause delay or even a timeout if all retries also fail. If an application has a legitimate need for a higher number of concurrent connections, you can adjust the setting by entering the **set connection per-client-max** command.

202001

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

Explanation This is a connection-related message. This message is displayed if the security appliance 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 translates and connections. This error message could also be caused by insufficient memory; reduce the amount of memory usage, or purchase additional memory usage if possible.

202005

Error Message `%ASA-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 displayed when a connection object (xlate) is in the wrong list.

Recommended Action Contact the Cisco TAC.

202011

Error Message `%ASA-3-202011: Connection limit exceeded` *`econns/limit`* `for` *`dir`* `packet from` *`source_address/source_port`* `to` *`dest_address/dest_port`* `on interface` *`interface_name`*

Explanation This message is displayed when an attempt to create a TCP or UDP connection fails due to an exceeded connection limit, which is configured with the **set connection conn-max** MPC command for a traffic class.

- *econns*—The current count of embryonic connections associated to the configured traffic class.
- *limit*—The configured embryonic connection limit for the traffic class.
- *dir*—
  input—The first packet that initiates the connection is an input packet on the interface *interface_name.*
  output—The first packet that initiates the connection is an output packet on the interface *interface_name.*
- *source_address/source_port*—The source IP address and the source port of the packet initiating the connection.
- *dest_address/dest_port*—The destination IP address and the destination port of the packet initiating the connection.
- *interface_name*—The name of the interface on which the policy limit is enforced.

Recommended Action None required.

208005

Error Message `%ASA-3-208005: (function:line_num) clear command return code`

Explanation The security appliance received a nonzero value (an internal error) when attempting to clear the configuration in flash memory. The message includes the reporting subroutine filename and line number.

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

209003

Error Message `%ASA-4-209003: Fragment database limit of number exceeded: src = source_address, dest = dest_address, proto = protocol, id = number`

Explanation Too many IP fragments are currently awaiting reassembly. By default, the maximum number of fragments is 200 (see the **fragment size** command in the *Cisco ASA 5580 Adaptive Security Appliance Command Reference* to raise the maximum). The security appliance limits the number of IP fragments that can be concurrently reassembled. This restriction prevents memory depletion at the security appliance under abnormal network conditions. In general, fragmented traffic should be a small percentage of the total traffic mix. An exception is in a network environment with NFS over UDP where a large percentage is fragmented traffic; if this type of traffic is relayed through the security appliance, consider using NFS over TCP instead. To prevent fragmentation, see the **sysopt connection tcpmss** *bytes* command in the *Cisco ASA 5580 Adaptive Security Appliance Command Reference*.

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

209004

Error Message `%ASA-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes: src = source_address, dest = dest_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 `%ASA-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.`

Explanation The security appliance disallows any IP packet that is fragmented into more than 24 fragments. Refer to the **fragment** command in the *Cisco ASA 5580 Adaptive Security Appliance Command Reference* for more information.

Recommended Action A possible intrusion event may be in progress. If the message persists, contact the remote peer administrator or upstream provider. You can change the number of fragments per packet by using the **fragment chain** *xxx interface_name* command.

210001

Error Message `%ASA-3-210001: LU sw_module_name error = number`

Explanation A Stateful Failover error occurred.

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

210002

Error Message `%ASA-3-210002: LU allocate block (bytes) failed.`

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

Recommended Action Check the failover interface using the **show interface** command to make sure its transmit is normal. 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 security appliance software to recover the lost blocks of memory.

210003

Error Message `%ASA-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, none 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 `%ASA-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 security appliance.

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

210006

Error Message `%ASA-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. The active and standby security appliance units may be out of synchronization.

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

210007

Error Message `%ASA-3-210007: LU allocate xlate failed`

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

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

210008

Error Message `%ASA-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 `%ASA-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 that the security appliance has free memory in the system. If no memory is available, add more memory.

210011

Error Message `%ASA-3-210011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.`

Explanation This syslog message indicates that establishing a new connection through the firewall device will result in exceeding at least one of the configured maximum connection limits. The syslog message applies both for connection limits configured using a static command, or to those configured using Cisco Modular Policy Framework. The new connection will not be allowed through the firewall device until one of the existing connections are torn down, thereby bringing the current connection count below the configured maximum.

- *cnt*—Current connection count
- *limit*—Configured connection limit
- *dir*—Direction of traffic, inbound or outbound
- *sip*—Source IP address
- *sport*—Source Port
- *dip*—Destination IP address
- *dport*—Destination Port
- *if_name*—Name of the interface on which we received the traffic unit, either “Primary” or “Secondary.”

Recommended Action Because connection limits are configured for a good reason, this syslog message could indicate a possible DOS attack, in which case the source of the traffic could likely be a spoofed IP address. If the source IP address is not totally random, identifying the source and blocking it using an access-list might help. In other cases getting sniffer traces and analyzing the source of the traffic would help in isolating unwanted traffic from legitimate traffic.

210020

Error Message `%ASA-3-210020: LU PAT port port reserve failed`

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

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

210021

Error Message `%ASA-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 Enter the **write standby** command on the active unit to synchronize system memory between the active and standby units.

210022

Error Message `%ASA-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 security appliance units to ensure that 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 `%ASA-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 the Cisco TAC.

211003

Error Message `%ASA-3-211003: CPU utilization for number seconds = percent`

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

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

212001

Error Message `%ASA-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 security appliance is unable to receive SNMP requests destined for the security appliance from SNMP management stations located on this interface. This does not affect the SNMP traffic passing through the security appliance through any interface.

An error code of -1 indicates that the security appliance could not open the SNMP transport for the interface. This can occur when the user attempts to change the port on which SNMP accepts queries to one that is already in use by another feature. In this case, the port used by SNMP will be reset to the default port for incoming SNMP queries (UDP/161).

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

Recommended Action After the security appliance reclaims some of its resources when traffic is lighter, reenter the **snmp-server host** command for that interface.

212002

Error Message `%ASA-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 security appliance is unable to send its SNMP traps from the security appliance to SNMP management stations located on this interface. This does not affect the SNMP traffic passing through the security appliance through any interface.

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

An error code of -2 indicates that the security appliance could not bind the SNMP trap transport for

the interface.

An error code of -3 indicates that the security appliance could not set the trap channel as write-only.

Recommended Action After the security appliance reclaims some of its resources when traffic is lighter, reenter the **snmp-server host** command for that interface.

212003

Error Message `%ASA-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 displayed because of an internal error in receiving an SNMP request destined for the security appliance on the specified interface.

An error code of -1 indicates that the security appliance could not find a supported transport type for the interface.

An error code of -5 indicates that the security appliance received no data from the UDP channel for the interface.

An error code of -7 indicates that the security appliance received an incoming request that exceeded the supported buffer size.

An error code of -14 indicates that the security appliance was unable to determine the source IP address from the UDP channel.

An error code of -22 indicates that the security appliance received an invalid parameter.

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

212004

Error Message `%ASA-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 displayed because of an internal error in sending an SNMP response from the security appliance to the specified host on the specified interface.

An error code of -1 indicates that the security appliance could not find a supported transport type for the interface.

An error code of -2 indicates that the security appliance sent an invalid parameter.

An error code of -3 indicates that the security appliance was unable to set the destination IP address in the UDP channel.

An error code of -4 indicates that the security appliance sent a PDU length that exceeded the supported UDP segment size.

An error code of -5 indicates that the security appliance was unable to allocate a system block to construct the PDU.

Recommended Action None required.

212005

Error Message `%ASA-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 which is destined for the security appliance exceeds the size of the internal data buffer (512 bytes) used for storing the request during internal processing. The security appliance is unable to process this request. This situation does not affect the SNMP traffic passing through the security appliance using 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. You may need to modify the configuration of the SNMP manager software.

212006

Error Message `%ASA-3-212006: Dropping SNMP request from` *source_address/source_port* `to` *interface_name:dest_address/dest_port* `because:` *reason*.

Explanation This is a SNMP message. This message is displayed if the device is unable to process a SNMP request to the device for the following reasons.

- The **snmp-server** command is disabled.
- SNMPv3 is not supported.

Recommended Action Make sure that the SNMP daemon is entering by issuing the **snmp-server enable** command. Only SNMPv1 and v2c packets are handled by the device.

213001

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

Explanation An internal TCP socket I/O error occurred.

Recommended Action Contact the Cisco TAC.

213002

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

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

Recommended Action Contact the Cisco TAC.

213003

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

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

Recommended Action Contact the Cisco TAC.

213004

Error Message `%ASA-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.

213005

Error Message `%ASA-3-213005%: Dynamic-Access-Policy action (DAP) action aborted`

Explanation The Dynamic Access Policy created for this connection has determined that the session should be terminated.

Recommended Action The Dynamic Access Policy is dynamically created by selecting configured access policies based on the authorization rights of the user and the posture assessment results of the remote endpoint device. The resulting dynamic policy indicates that the session should be terminated.

213006

Error Message `%ASA-3-213006%: Unable to read dynamic access policy record.`

Explanation There was either an error in retrieving the DAP policy record data or the action configuration was missing. There was an error reading the configured dynamic access policy record.

Recommended Action A configuration change might have resulted in deleting a dynamic access policy record. Use ASDM to re-create the dynamic access policy record.

214001

Error Message `%ASA-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 security appliance management port indicates a packet length exceeding the specified upper limit. This may be a hostile event. The security appliance immediately terminates this management connection.

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

215001

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

Explanation An internal software error occurred.

Recommended Action Contact the Cisco TAC.

216001

Error Message `%ASA-n-216001: internal error in: function: message`

Explanation This message reports a variety of internal errors that should not appear during normal operation. The severity level varies depending on the cause of the message.

- *n*—The message severity level.
- *function*—The affected component.
- *message*—A message describing the cause of the problem.

Recommended Action Search the Bug Toolkit for the specific text message and try to use the Output Interpreter to resolve the problem. If the problem persists, contact the Cisco TAC.

216002

Error Message `ASA-3-216002: Unexpected event (major: major_id, minor: minor_id) received by task_string in function at line: line_num`

Explanation This message is displayed when a task registers for event notification and the task cannot handle the specific event. Events that can be watched include those associated with queues, booleans, timer services, and so forth. If any of the registered events occur, the scheduler wakes up the task to process the event. This message is generated if an unexpected event woke up the task and it does not know how to handle the event.

If an event is left unprocessed, it can wake up the task very often to make sure it is processed, but this should not occur under normal conditions. If this message is displayed, it does not necessarily mean the box is unusable, but that something unusual has occurred and needs to be investigated.

- *major_id*—Event identifier
- *minor_id*— Event identifier
- *task_string*—Custom string passed by the task to identify itself
- *function*—The function that received the unexpected event
- *line_num* —Line number in the code

Recommended Action If the problem persists, contact the Cisco TAC.

216003

Error Message `%ASA-3-216003: Unrecognized timer timer_ptr, timer_id received by task_string in function at line: line_num`

Explanation This message is displayed when an unexpected timer event woke up the task and the task does not know how to handle the event. A task can register a set of timer services with the scheduler. If any of the timers expire, the scheduler wakes up the task to take action. This message is generated if the task is woken up by an unrecognized timer event.

An expired timer, if left unprocessed, wakes up the task continuously to make sure it is processed, and this is undesirable. This should not occur under normal conditions. If This message is displayed, it does not necessarily mean the box is unusable, but something unusual has occurred and needs to be investigated.

- *timer_ptr*—Pointer to the timer
- *timer_id*—Timer identifier
- *task_string*—Custom string passed by the task to identify itself
- *function*—The function that received the unexpected event
- *line_num*—Line number in the code

Recommended Action If the problem persists, contact the Cisco TAC.

216004

Error Message `%ASA-4-216004:prevented: error in function at file (line) - stack trace`

Explanation This syslog message reports an internal logic error, and should not occur during normal operation.

- *error*—Internal logic error. Possible errors include the following:
  - Exception
  - Dereferencing null pointer
  - Array index out of bounds
  - Invalid buffer size
  - Writing from input
  - Source and destination overlap
  - Invalid date
  - Access offset from array indices
- *function*—The calling function that generated the error
- *file (line)*—The file and line number that generated the error
- *stack trace*—Full call stack traceback, starting with the calling function. For example: (“0x001010a4 0x00304e58 0x00670060 0x00130b04”).

Recommended Action If the problem persists, contact the Cisco TAC.

216005

Error Message `%ASA-1-216005: ERROR: Duplex-mismatch on interface_name resulted in transmitter lockup. A soft reset of the switch was performed.`

Explanation A duplex-mismatch on the port caused a problem whereby the port could no longer transmit packets. This condition was detected, and the switch was reset to auto-recover from this condition. This message applies only to the ASA 5505 device.

- *interface_name*—The interface name that was locked up.

Recommended Action A duplex-mismatch exists between the specified port and the device that is connected to it. Correct the duplex-mismatch by either setting both devices to “auto,” or hard-coding the duplex on both sides to be the same.

217001

Error Message `%ASA-2-217001: No memory for string in string`

Explanation An operation failed due to low memory.

Recommended Action If sufficient memory exists, then copy the error message, the configuration, and any details about the events leading up the error to the Cisco TAC.

218001

Error Message `%ASA-2-218001: Failed Identification Test in slot# [fail#/res].`

Explanation The module in *slot#* of the security appliance could not be identified as a genuine Cisco product. Cisco warranties and support programs apply only to genuine Cisco products. If Cisco determines that the cause of a support issue is related to non-Cisco memory, SSM modules, SSC cards, or other modules, Cisco may deny support under your warranty or under a Cisco support program such as SmartNet.

Recommended Action If this message reoccurs, copy it exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.

218002

Error Message `%ASA-2-218002: Module (slot#) is a registered proto-type for Cisco Lab use only, and not certified for live network operation.`

Explanation Hardware in the specified location is a prototype module that came from a Cisco lab.

Recommended Action If this message reoccurs, copy it exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter. Also perform a search of the Bug Toolkit. If the problem persists, contact the Cisco TAC.

218003

Error Message `%ASA-2-218003: Module Version in <slot#> is obsolete. The module in slot = <slot#> is obsolete and must be returned via RMA to Cisco Manufacturing. If it is a lab unit, it must be returned to Proto Services for upgrade.`

Explanation This syslog message is generated when obsolete hardware is detected or when the **show module** command is entered for the module. This syslog message is generated every minute once it starts.

Recommended Action If this message recurs, copy it exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter. Also perform a search of the Bug Toolkit. If the problem persists, contact the Cisco TAC.

218004

Error Message `%ASA-2-218004: Failed Identification Test in slot# [fail#/res]`

Explanation There was a problem while identifying hardware in the specified location.

Recommended Action If this message recurs, copy it exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter. Also perform a search of the Bug Toolkit. If the problem persists, contact the Cisco TAC.

219002

Error Message `%ASA-3-219002: I2C_API_name error, slot = slot_number, device = device_number, address = address, byte count = count. Reason: reason_string`

Explanation The I2C serial bus API has failed. This might be because of a hardware or software problem.

- *I2C_API_name*—The I2C API that failed:
  - I2C_read_byte_w_wait()
  - I2C_read_word_w_wait()
  - I2C_read_block_w_wait()
  - I2C_write_byte_w_wait()
  - I2C_write_word_w_wait()
  - I2C_write_block_w_wait()
  - I2C_read_byte_w_suspend()
  - I2C_read_word_w_suspend()
  - I2C_read_block_w_suspend()
  - I2C_write_byte_w_suspend()
  - I2C_write_word_w_suspend()

  - I2C_write_block_w_suspend()
- *slot_number*—The hexadecimal number of the slot where the I/O operation that generated the syslog message occurred.The slot number cannot be unique to a slot in the chassis. Depending on the chassis, two different slots might have the same I2C slot number. Also the value is not necessarily less than or equal to the number of slots. The value depends on the way the I2C hardware is wired.
- *device_number*—The hexadecimal number of the device on the slot the I/O operation was performed.
- *address*—This is the hexadecimal address of the device on which the I/O operation occurred.
- *byte_count*—This is the byte count in decimal of the I/O operation.
- *error_string*—The reason for the error:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event. If the syslog message does not occur continuously and goes away after a few minutes, it might be because the I2C serial bus is busy.
2. Reboot the software running on the system.
3. Power cycle the box. When you turn off the power, make sure you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

Messages 302003 to 336011

This section contains messages from 302003 to 336011.

302003

Error Message `%ASA-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 displayed when an H.245 connection is started from the *outside_address* to the *inside_address*. This message only occurs if the security appliance detects the use of an Intel Internet Phone. The foreign port (outside port) only displays on connections from outside the security appliance. The local port value (inside port) only appears on connections started on an internal interface.

Recommended Action None required.

302004

Error Message `%ASA-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 displayed when an H.323 UDP back-connection is preallocated to the foreign address (*outside_address)* from the local address (*inside_address)*. This message only occurs if the security appliance detects the use of an Intel Internet Phone. The foreign port (*outside_port*) only displays on connections from outside the security appliance. The local port value (*inside_port*) only appears on connections started on an internal interface.

Recommended Action None required.

302009

Error Message `%ASA-6-302009: Rebuilt TCP connection number for foreign_address outside_address/outside_port global_address 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 security appliance. 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 security appliance on the higher security level interface.

Recommended Action None required.

302010

Error Message `%ASA-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.

302012

Error Message `%ASA-6-302012: Pre-allocate H225 Call Signalling Connection for faddr IP_address/port to laddr IP_address`

Explanation An H.225 secondary channel has been preallocated.

Recommended Action None required.

302013

Error Message `%ASA-6-302013: Built {inbound|outbound} TCP connection_id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port) [(user)]`

Explanation A TCP connection slot between two hosts was created.

- *connection_id* is a unique identifier.
- *interface*, *real-address*, and *real-port* identify the actual sockets.
- *mapped-address* and *mapped-port* identify the mapped sockets.
- *user* is the AAA name of the user.

If inbound is specified, 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, the original control connection was initiated from the inside.

Recommended Action None required.

302014

Error Message `%ASA-6-302014: Teardown TCP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [reason] [(user)]`

Explanation A TCP connection between two hosts was deleted. The following list describes the message values:

- connection *id* is an unique identifier.
- *interface, real-address,* and *real-port* identify the actual sockets.
- *duration* is the lifetime of the connection.
- bytes *bytes* 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 1-3.

Table 1-3 TCP Termination Reasons

Reason	Description
Conn-timeout	Connection ended because it was idle longer than the configured idle timeout.
Deny Terminate	Flow was terminated by application inspection.
Failover primary closed	The standby unit in a failover pair deleted a connection because of a message received from the active unit.
FIN Timeout	Force termination after 10 minutes awaiting the last ACK or after half-closed timeout.
Flow closed by inspection	Flow was terminated by inspection feature.
Flow terminated by IPS	Flow was terminated by IPS.
Flow reset by IPS	Flow was reset by IPS.
Flow terminated by TCP Intercept	Flow was terminated by TCP Intercept.
Flow timed out	Flow has timed out.
Flow timed out with reset	Flow has timed out, but was reset.
Invalid SYN	SYN packet not valid.
Idle Timeout	Connection timed out because it was idle longer than timeout value.
IPS fail-close	Flow was terminated due to IPS card down.
Pinhole Timeout	Counter is incremented to report that the appliance opened a secondary flow, but no packets passed through this flow within the timeout interval, and hence it was removed. An example of a secondary flow is the FTP data channel that is created after successful negotiation on the FTP control channel.
SYN Control	Back channel initiation from wrong side.

Table 1-3 TCP Termination Reasons (continued)

Reason	Description
SYN Timeout	Force termination after 30 seconds awaiting three-way handshake completion.
TCP bad retransmission	Connection terminated because of bad TCP retransmission.
TCP FINs	Normal close down sequence.
TCP Invalid SYN	Invalid TCP SYN packet.
TCP Reset-APPLIANCE	Reset was from the adaptive security appliance.
TCP Reset-I	Reset was from the inside.
TCP Reset-O	Reset was from the outside.
TCP segment partial overlap	Detected a partially overlapping segment.
TCP unexpected window size variation	Connection terminated due to variation in the TCP window size.
Tunnel has been torn down	Flow terminated because tunnel is down.
Unauth Deny	Denied by URL filter.
Unknown	Catch-all error.
Xlate Clear	Command-line removal.

Recommended Action None required.

302015

Error Message `%ASA-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. The following list describes the message values:

- connection *number*—A unique identifier.
- *interface, real_address,* and *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 `%ASA-6-302016: Teardown UDP connection number for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [(user)]`

Explanation A UDP connection slot between two hosts was deleted. The following list describes the message values:

- connection *number* is an unique identifier.
- *interface, real_address,* and *real_port* are the actual sockets.
- *time* is the lifetime of the connection.
- *bytes* is the data transfer of the connection.
- connection *id* is an unique identifier.
- *interface, real-address,* and *real-port* are the actual sockets.
- *duration* is the lifetime of the connection.
- *bytes* is the data transfer of the connection.
- *user* is the AAA name of the user.

Recommended Action None required.

302017

Error Message `%ASA-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 This is an informational message. 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 username.

Recommended Action None required.

302018

Error Message `%ASA-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 username.

Recommended Action This is an informational message.

302019

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

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

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

302020

Error Message `%ASA-6-302020: Built {in | out}bound ICMP connection for faddr {`*faddr* `| icmp_seq_num} gaddr {`*gaddr* `|` *cmp_type*`} laddr` *laddr*

Explanation An ICMP session was established in the fast-path when stateful ICMP is enabled using the **inspect icmp** command.

Recommended Action None required.

302021

Error Message `%ASA-6-302021: Teardown ICMP connection for faddr {`*faddr* `|` *icmp_seq_num*`} gaddr {`*gaddr* `|` *cmp_type*`} laddr` *laddr*

Explanation An ICMP session was removed in the fast-path when stateful ICMP is enabled using the **inspect icmp** command.

Recommended Action None required.

302033

Error Message `%ASA-6-302033:Pre-allocated H323 GUP Connection for faddr` *interface*`:`*foreign-address*`/`*foreign-port* `to laddr` *interface*`:`*local-address*`/`*local-port*

Explanation This is a connection-related message. This message is displayed when a GUP connection is started from the foreign_address to the local_address. The foreign port (outside port) only displays on connections from outside the security device. The local port value (inside port) only appears on connections started on an internal interface.

- *interface*—The interface name
- *foreign-address*—IP address of the foreign host
- *foreign-port*—Port number of the foreign host
- *local-address*—IP address of the local host
- *local-port*—Port number of the local host

Recommended Action None required

302034

Error Message `%ASA-4-302034: Unable to pre-allocate H323 GUP Connection for faddr` *interface*`:` *foreign address*`/`*foreign-port* `to laddr` *interface*`:`*local-address*`/`*local-port*

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

- *interface*—The interface name
- *foreign-address*—IP address of the foreign host
- *foreign-port*—Port number of the foreign host
- *local-address*—IP address of the local host
- *local-port*—Port number of the local host

Recommended Action If this message occurs periodically, it can be ignored. If it repeats frequently, contact Cisco TAC. You can check the size of the global pool compared to the number of inside network clients. Alternatively, shorten the timeout interval of translates and connections. This error message may also be caused by insufficient memory; try reducing the amount of memory usage, or purchasing additional memory.

302302

Error Message `%ASA-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.

303003

Error Message `%ASA-5-303003: FTP` *cmd_string* `command denied - failed strict inspection, terminating connection from %s:%A/%d to %s:%A/%d\n.`

Explanation This message is generated when using strict FTP inspection on FTP traffic. It is displayed if an FTP request message contains a command that is not recognized by the device.

Recommended Action None required.

303004

Error Message `%ASA-5-303004: FTP cmd_string command unsupported - failed strict inspection, terminating connection from source_interface:source_address/source_port to dest_interface:dest_address/dest_interface`

Explanation This message is generated when using strict FTP inspection on FTP traffic. It is displayed if an FTP request message contains a command that is not recognized by the device.

Recommended Action None required.

303005

Error Message `%ASA-5-303005: Strict FTP inspection matched match_string in policy-map policy-name, action_string from src_ifc:sip/sport to dest_ifc:dip/dport`

Explanation This message is generated when FTP inspection matches any of the following configured values: filename, file type, request command, server, or username. Then the action specified by the *action_string* in this syslog message occurs.

- *match_string*—The match clause in the policy-map.
- *policy-name*—The policy-map that matched.
- *action_string*—The action to take; for example, "Reset Connection."
- *src_ifc*—The source interface name.
- *sip*—The source IP address.
- *sport*—The source port.
- *dest_ifc*—The destination interface name.
- *dip*—The destination IP address.
- *dport*—The destination port.

Recommended Action None required.

304001

Error Message `%ASA-5-304001: user@source_address Accessed {JAVA URL|URL} dest_address: url`

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

Recommended Action None required.

304002

Error Message %ASA-5-304002: Access denied URL *chars* SRC *IP_address* DEST *IP_address*: *chars*

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

Recommended Action None required.

304003

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

Explanation A URL server timed out.

Recommended Action None required.

304004

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

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

Recommended Action None required.

304005

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

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

Recommended Action None required.

304006

Error Message `%ASA-3-304006: URL Server IP_address not responding`

Explanation This is an FTP/URL message. The Websense server is unavailable for access, and the security appliance 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 `%ASA-2-304007: URL Server IP_address not responding, ENTERING ALLOW mode.`

Explanation This is an FTP/URL message. This message is displayed when you use the **allow** option of the **filter** command, and the Websense servers are not responding. The security appliance allows all web requests to continue without filtering while the servers are not available.

Recommended Action None required.

304008

Error Message `%ASA-2-304008: LEAVING ALLOW mode, URL Server is up.`

Explanation This is an FTP/URL message. This message is displayed when you use the **allow** option of the **filter** command, and the security appliance receives a response message from a Websense server that previously was not responding. With this response message, the security appliance exits the allow mode, which enables the URL filtering feature again.

Recommended Action None required.

304009

Error Message `%ASA-7-304009: 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 `%ASA-3-305005: No translation group found for` *`protocol`* `src` *`interface_name:source_address/source_port`* `dst` *`interface_name`*`:` *`dest_address/dest_port`*

Explanation A packet does not match any of the outbound **nat** command rules. If NAT is not configured for the specified source and destination systems, this message will be generated frequently.

Recommended Action This message indicates 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 `%ASA-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 security appliance. This message appears as a fix to caveat CSCdr00663, which requested that security appliance not allow packets that are destined for network or broadcast addresses. The security appliance provides checking for addresses that are explicitly identified with **static** command statements. With the change, for inbound traffic, the security appliance denies translations for a destined IP address identified as a network or broadcast address.

The security appliance does not apply PAT to all ICMP message types; it only applies PAT 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 security appliance) is generated.

The security appliance uses the global IP and mask from configured **static** command statements to differentiate 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 security appliance does not create a translation 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 responded to as a network address and 10.2.2.255 is responded to as the broadcast address. Without an existing translation, security appliance denies inbound packets destined for 10.2.2.128 or 10.2.2.255, and logs this syslog message.

When 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 the security appliance to respond to 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 translation may be created by traffic started with the inside host with the questioned IP address. Because the security appliance views 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 None required.

305007

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

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

Recommended Action None required.

305008

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

Explanation The security appliance 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 security appliance is running a Stateful Failover setup and some of the internal states are momentarily out of synchronization between the active unit and the standby unit. This condition is not catastrophic, and the sync recovers automatically.

Recommended Action If the problem persists, contact the Cisco TAC.

305009

Error Message %ASA-6-305009: Built {dynamic|static} translation from *interface_name [(acl-name)]*:*real_address* to *interface_name*:*mapped_address*

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

Recommended Action None required.

305010

Error Message %ASA-6-305010: Teardown {dynamic|static} translation from *interface_name:real_address* to *interface_name:mapped_address* duration *time*

Explanation The address translation slot was deleted.

Recommended Action None required.

305011

Error Message %ASA-6-305011: Built {dynamic|static} {TCP|UDP|ICMP} translation from *interface_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 translates the source socket from the local side to the global side. In reverse, the slot translates the destination socket from the global side to the local side.

Recommended Action None required.

305012

Error Message %ASA-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.

305013

Error Message `%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows; Connection` *`protocol`* `src` *`interface_name`*`:`*`source_address`*`/`*`source_port`* `dest` *`interface_name`*`:`*`dest_address`*`/`*`dest_port`* `denied due to NAT reverse path failure.`

Explanation An attempt to connect to a mapped host using its actual address was rejected.

Recommended Action When not on the same interface as the host using NAT, use the mapped address instead of the real address to connect to the host. In addition, enable the applicable **inspect** command if the application embeds the IP address.

308001

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

Explanation This is a security appliance management message. This message is displayed after the specified number of times a user incorrectly types the password to enter privileged mode. The maximum is three attempts.

Recommended Action Verify the password and try again.

308002

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

Explanation 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 you specify a host within that range such as 10.1.1.5.

311001

Error Message `%ASA-6-311001: LU loading standby start`

Explanation Stateful Failover update information was sent to the standby security appliance when the standby security appliance is first to be online.

Recommended Action None required.

311002

Error Message `%ASA-6-311002: LU loading standby end`

Explanation Stateful Failover update information stopped sending to the standby security appliance.

Recommended Action None required.

311003

Error Message `%ASA-6-311003: LU recv thread up`

Explanation An update acknowledgment was received from the standby security appliance.

Recommended Action None required.

311004

Error Message `%ASA-6-311004: LU xmit thread up`

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

Recommended Action None required.

312001

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

Explanation The security appliance received a RIP message with an operation code other than reply, the message has a version number different from what is expected on this interface, and the routing domain entry was nonzero.

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

313001

Error Message %ASA-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 security appliance discards the ICMP packet and generates this syslog message. The **icmp** command enables or disables pinging to an interface. With pinging disabled, the security appliance cannot be detected on the network. This feature is also referred to as configurable proxy pinging.

Recommended Action Contact the administrator of the peer device.

313004

Error Message %ASA-4-313004: Denied ICMP type=*icmp_type*, from *source_address* oninterface *interface_name* to *dest_address*:no matching session

Explanation ICMP packets were dropped by the security appliance because of security checks added by the stateful ICMP feature that are usually either ICMP echo replies without a valid echo request already passed across the security appliance or ICMP error messages not related to any TCP, UDP, or ICMP session already established in the security appliance.

Recommended Action None required.

313005

Error Message %ASA-4-313005: No matching connection for ICMP error message: *icmp_msg_info* on *interface_name* interface. Original IP payload: *embedded_frame_info icmp_msg_info* = icmp src *src_interface_name*:*src_address* dst *dest_interface_name*:*dest_address* (type *icmp_type*, code *icmp_code*) *embedded_frame_info* = *prot* src *source_address*/*source_port* dst *dest_address*/*dest_port*

Explanation ICMP error packets were dropped by the security appliance because the ICMP error messages are not related to any session already established in the security appliance.

Recommended Action If the cause is an attack, you can deny the host by using ACLs.

313008

Error Message `%ASA-3-313008: Denied ICMPv6 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 ICMPv6 packet continues processing. If the first matched entry is a deny entry, or an entry is not matched, the security appliance discards the ICMPv6 packet and generates this syslog message.

The **icmp** command enables or disables pinging to an interface. When pinging is disabled, the security appliance is undetectable on the network. This feature is also referred to as "configurable proxy pinging."

Recommended Action Contact the administrator of the peer device.

314001

Error Message `%ASA-6-314001: Pre-allocated RTSP UDP backconnection for src_intf:src_IP to dst_intf:dst_IP/dst_port.`

Explanation Open UDP media channel for RTSP client receiving data from server

- *src_intf*—Source interface name
- *src_IP*—Source interface IP address
- *dst_intf*—Destination interface name
- *dst_IP*—Destination IP address
- *dst_port*—Destination port

Recommended Action None required.

314002

Error Message `%ASA-6-314002: RTSP failed to allocate UDP media connection from src_intf:src_IP to dst_intf:dst_IP/dst_port: reason_string.`

Explanation The security appliance cannot open a new pinhole for the media channel.

- *src_intf*—Source interface name.
- *src_IP*—Source interface IP address.
- *dst_intf*—Destination interface name.
- *dst_IP*—Destination IP address.
- *dst_port*—Destination port.

- *reason_string*—Pinhole already exists | Unknown.

Recommended Action If the reason is "unknown," check the free memory available (**show memory**), or number of connections used (**show conn**), because the security device is low on memory.

314003

Error Message `%ASA-6-314003: Dropped RTSP traffic from src_intf:src_ip due to: reason.`

Explanation The RTSP message violated the user-configured RTSP security policy, either because it contains a port from the reserve port range, or it contains a URL with a length greater than the maximum limit allowed.

- *src_intf*—Source interface name
- *src_IP*—Source interface IP address
- *reason*—One of the following two reasons pertain:
  - Endpoint negotiating media ports in the reserved port range from 0 to 1024
  - URL length of <url length> bytes exceeds the maximum <url length limit> bytes

Recommended Action Investigate why the RTSP client sends messages that violate the security policy. If the requested URL is legitimate, you can relax the policy by specifying a longer URL length limit in the RTSP policy-map.

314004

Error Message `%ASA-6-314004: RTSP client src_intf:src_IP accessed RTSP URL RTSP URL`

Explanation RTSP client attempt to access an RTSP server.

- *src_intf*—Source interface name
- *src_IP*—Source interface IP address
- *RTSP URL*—RTSP server URL

Recommended Action None required.

314005

Error Message `%ASA-6-314005: RTSP client src_intf:src_IP denied access to URL RTSP_URL.`

Explanation RTSP client attempt to access prohibited site, as configured on the security appliance.

- *src_intf*—Source interface name
- *src_IP*—Source interface IP address

- *RTSP_URL*—RTSP server URL

Recommended Action None required.

314006

Error Message `%ASA-6-314006: RTSP client src_intf:src_IP exceeds configured rate limit of rate for request_method messages.`

Explanation A specific RTSP request message exceeded the configured rate limit of RTSP policy.

- *src_intf*—Source interface name
- *src_IP*—Source interface IP address
- *rate*—Configured rate limit
- *request_method*—Type of request message

Recommended Action Investigate why the specific RTSP request message from the client exceeded the rate limit.

315004

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

Explanation The security appliance could not find the security appliance RSA host key, which is required for establishing an SSH session. The security appliance host key may be absent because it was not generated or because the license for this security appliance does not allow DES or 3DES.

Recommended Action From the security appliance console, enter the **show crypto key mypubkey rsa** command to verify that the RSA host key is present. If the host key is not present, enter the **show version** command to verify that DES or 3DES is allowed. If an RSA host key is present, restart the SSH session. To generate the RSA host key, enter the **crypto key mypubkey rsa** command.

315011

Error Message `%ASA-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 1-4 lists the possible reasons why a session disconnected.

Table 1-4 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.	None 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 security appliance or an RSA key may not have been entered on the security appliance or cannot be retrieved.	From the security appliance console, enter the **show crypto key mypubkey rsa** command to verify that the RSA host key is present. If the host key is not present, enter the **show version** command to verify that DES or 3DES is allowed. If an RSA host key is present, restart the SSH session. To generate the RSA host key, enter the **crypto key mypubkey rsa** command.
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 security appliance exceeds 262,144 bytes or is shorter than 4096 bytes. The data may be corrupted.	None required.
Invalid message type	The security appliance 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 security appliance serial console enter the **debug ssh** command and capture the debug messages. contact the Cisco TAC.

Table 1-4 SSH Disconnect Reasons (continued)

Text String	Explanation	Action
Out of memory	This message appears when the security appliance cannot allocate memory for use by the SSH server, probably when the security appliance 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 security appliance.	None required.
status code: *hex* (*hex*)	Users closed the SSH client window (running on Windows) instead of entering **quit** or **exit** at the SSH console.	None 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 security appliance console.	None 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.

Recommended Action None required.

316001

Error Message `%ASA-3-316001: 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.

316002

Error Message `%ASA-3-316002: VPN Handle error: protocol=protocol, src in_if_num:src_addr, dst out_if_num:dst_addr`

Explanation This message is generated when the security appliance is unable to create a VPN handle, because the VPN handle already exists.

- *protocol*—The protocol of the VPN flow
- *in_if_num*—The ingress interface number of the VPN flow

- *src_addr*—The source IP address of the VPN flow
- *out_if_num*—The egress interface number of the VPN flow
- *dst_addr*—The destination IP address of the VPN flow

Recommended Action This message may occur during normal operation; however, if the message occurs repeatedly and a major malfunction of VPN-based applications occurs, a software defect may be the cause. Enter the following commands to collect more information and contact the Cisco TAC to investigate the issue further.

```
capture name type asp-drop vpn-handle-error
show asp table classify crypto detail
show asp table vpn-context
```

317001

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

Explanation A software error occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

317003

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

Explanation Additional routes will be added to the table.

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

317006

Error Message `%ASA-3-317006: Pdb index error pdb, pdb_index, pdb_type`

Explanation The index into the pdb is out of range.

- *pdb*—Protocol Descriptor Block, the descriptor of the Pdb index error
- *pdb_index*—The Pdb index identifier
- *pdb_type*—The type of the Pdb index error

Recommended Action If the problem persists, copy the error message exactly as it appears on the console or in the system log, contact the Cisco TAC, and provide the representative with the gathered information.

318001

Error Message `%ASA-3-318001: Internal error: reason`

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

Recommended Action If the problem persists, contact the Cisco TAC.

318002

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

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

Recommended Action Restart the OSPF process.

318003

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

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

Recommended Action None required.

318004

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

Explanation OSPF had a problem locating the link state advertisement (LSA), which might lead to a memory leak.

Recommended Action If the problem persists, contact the Cisco TAC.

318005

Error Message `%ASA-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 If the problem persists, contact the Cisco TAC.

318006

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

Explanation An internal error occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

318007

Error Message `%ASA-3-318007: OSPF is enabled on interface_name during idb initialization`

Explanation An internal error occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

318008

Error Message `%ASA-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.

Recommended Action Change virtual link configuration on all of the virtual link neighbors to reflect the new router ID.

318009

Error Message `%ASA-3-318009: OSPF: Attempted reference of stale data encountered in function, line: line_num`

Explanation This message is displayed when OSPF is running and tries to reference some related data structures that have been removed elsewhere. Clearing interface and router configurations may resolve the problem. However, if this message appears, some sequence of steps caused premature deletion of data structures and this needs to be investigated.

- *function*—The function that received the unexpected event
- *line_num* —Line number in the code

Recommended Action If the problem persists, contact the Cisco TAC.

319001

Error Message `%ASA-3-319001: Acknowledge for arp update for IP address dest_address not received (number).`

Explanation The ARP process in the security appliance lost internal synchronization because the system was overloaded.

Recommended Action No immediate action is required. The failure is only temporary. Check the average load of the system and make sure it is not used beyond its capabilities.

319002

Error Message `%ASA-3-319002: Acknowledge for route update for IP address dest_address not received (number).`

Explanation The routing module in the security appliance lost internal synchronization because the system was overloaded.

Recommended Action No immediate action required. The failure is only temporary. Check the average load of the system and make sure it is not used beyond its capabilities.

319003

Error Message `%ASA-3-319003: Arp update for IP address address to NPn failed.`

Explanation When an ARP entry has to be updated, a message is sent to the network processor (NP) in order to update the internal ARP table. If the module is experiencing high utilization of memory or if the internal table is full, the message to the NP may be rejected and this message generated.

Recommended Action Verify if the ARP table is full. If it is not full, check the load of the module with respect to the CPU utilization and connections per second. If CPU utilization is high and/or there is a large number of connections per second, normal operations will resume when the load returns to normal.

319004

Error Message `%ASA-3-319004: Route update for IP address dest_address failed (number).`

Explanation The routing module in the FWSM lost internal synchronization because the system was overloaded.

Recommended Action No immediate action required. The failure is only temporary. Check the average load of the system and make sure it is not used beyond its capabilities.

320001

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

Explanation When the security appliance 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 security appliance.

321001

Error Message %ASA-5-321001: Resource *var1* limit of *var2* reached.

Explanation A configured resource usage or rate limit for the indicated resource was reached.

Recommended Action None required.

321002

Error Message %ASA-5-321002: Resource *var1* rate limit of *var2* reached.

Explanation A configured resource usage or rate limit for the indicated resource was reached.

Recommended Action None required.

321003

Error Message %ASA-6-321003: Resource *var1* log level of *var2* reached.

Explanation A configured resource usage or rate log level for the indicated resource was reached.

Recommended Action None required.

321004

Error Message %ASA-6-321004: Resource *var1* rate log level of *var2* reached

Explanation A configured resource usage or rate log level for the indicated resource was reached.

Recommended Action None required.

322001

Error Message `%ASA-3-322001: Deny MAC address MAC_address, possible spoof attempt on interface interface`

Explanation The security appliance received a packet from the offending MAC address on the specified interface but the source MAC address in the packet is statically bound to another interface in your configuration. This could be caused by either be a MAC-spoofing attack or a misconfiguration.

Recommended Action Check the configuration and take appropriate action by either finding the offending host or correcting the configuration.

322002

Error Message `%ASA-3-322002: ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface. This host is advertising MAC Address MAC_address_1 for IP Address IP_address, which is {statically|dynamically} bound to MAC Address MAC_address_2.`

Explanation If the ARP inspection module is enabled, it checks whether a new ARP entry advertised in the packet conforms to the statically configured or dynamically learned IP-MAC address binding before forwarding ARP packets across the security appliance. If this check fails, the ARP inspection module drops the ARP packet and generates this message. This situation may be caused by either ARP spoofing attacks in the network or an invalid configuration (IP-MAC binding).

Recommended Action If the cause is an attack, you can deny the host using the ACLs. If the cause is an invalid configuration, correct the binding.

322003

Error Message `%ASA-3-322003:ARP inspection check failed for arp {request|response} received from host MAC_address on interface interface. This host is advertising MAC Address MAC_address_1 for IP Address IP_address, which is not bound to any MAC Address.`

Explanation If the ARP inspection module is enabled, it checks whether a new ARP entry advertised in the packet conforms to the statically configured IP-MAC address binding before forwarding ARP packets across the security appliance. If this check fails, the ARP inspection module drops the ARP packet and generates this message. This situation may be caused by either ARP spoofing attacks in the network or an invalid configuration (IP-MAC binding).

Recommended Action If the cause is an attack, you can deny the host using the ACLs. If the cause is an invalid configuration, correct the binding.

322004

Error Message `%ASA-6-322004: No management IP address configured for transparent firewall. Dropping protocol protocol packet from interface_in:source_address/source_port to interface_out:dest_address/dest_port`

Explanation The security appliance dropped a packet because no management IP address was configured in the transparent mode.

- *protocol*—Protocol string or value
- *interface_in*—Input interface name
- *source_address*—Source IP address of the packet
- *source_port*—Source port of the packet
- *interface_out*—Output interface name
- *dest_address*—Destination IP address of the packet
- *dest_port*—Destination port of the packet

Recommended Action Configure the device with the management IP address and mask values.

323001

Error Message `%ASA-3-323001: Module in slot slotnum experienced a control channel communications failure.`

Explanation The system is unable to communicate via the control channel with the module installed in slot *slotnum*.

- *slotnum*—The slot in which the failure occurred. Slot 0 indicates the system main board and slot 1 indicates the module installed in the expansion slot. For this error, the slot should always be 1.

Recommended Action If the problem persists, contact the Cisco TAC.

323002

Error Message `%ASA-3-323002: Module in slot slotnum is not able to shut down, shut down request not answered.`

Explanation The module installed in slot *slotnum* did not respond to a shutdown request.

- *slotnum*—The slot in which the failure occurred. Slot 0 indicates the system main board and slot 1 indicates the module installed in the expansion slot. For this error, the slot should always be 1.

Recommended Action If the problem persists, contact the Cisco TAC.

323003

Error Message `%ASA-3-323003: Module in slot slotnum is not able to reload, reload request not answered.`

Explanation The module installed in slot *slotnum* did not respond to a reload request.

- *slotnum*—The slot in which the failure occurred. Slot 0 indicates the system main board and slot 1 indicates the module installed in the expansion slot. For this error, the slot should always be 1.

Recommended Action If the problem persists, contact the Cisco TAC.

323004

Error Message `%ASA-3-323004: Module in slot slotnum failed to write software vnewver (currently vver), reason. Hw-module reset is required before further use.`

Explanation The module in the specified slot number failed to accept a software version, and will be transitioned to an UNRESPONSIVE state. The module is not usable until the software is updated.

- *slotnum*—The slot number containing the module
- *newver*—The new version number of software that was not successfully written to the module (for example, 1.0(1)0)
- *ver*—The current version number of the software on the module (for example, 1.0(1)0)
- *reason*—The reason the new version could not be written to the module. The possible values for *reason* include the following:
  - –write failure
  - –failed to create a thread to write the image

Recommended Action The module must be reset by using the **hw-module module** *slotnum* **reset** before further upgrade attempts will be made. If the module software can not be updated, it will not be usable. Ensure the module is completely seated in the chassis. If the problem persists, contact the Cisco TAC.

323005

Error Message `%ASA-3-323005: Module in slot slotnum can not be powered on completely`

Explanation This message indicates that the module can not be powered up completely. The module will remain in the UNRESPONSIVE state until this condition is corrected. A likely cause of this is a module that is not fully seated in the slot.

- *slotnum*—The slot number containing the module

Recommended Action Verify that the module is fully seated in the slot and check if any status LEDs on the module are on. It may take a minute after fully reseating the module for the system to recognize that it is powered up. If this message appears after verifying that the module is seated and after resetting the module using the **hw-module module** *slotnum* **reset** command, contact the Cisco TAC.

323006

Error Message `%ASA-3-323006: Module in slot slot experienced a data channel communication failure, data channel is DOWN.`

Explanation This message indicates that a data channel communication failure occurred and the system was unable to forward traffic to the SSM. This failure triggers a failover when the failover occurs on the active appliance in an HA configuration. The failure also results in the configured fail open or fail closed policy being enforced on traffic that would normally be sent to the SSM. This message is generated whenever a communication problem occurs over the security appliance dataplane between the system module and the SSM. This message can be caused when the SSM stops, resets, or is removed.

- *slot*—The slot in which the failure occurred

Recommended Action If this is not the result of the SSM reloading or resetting and a corresponding message 5-505010 is not seen after the SSM returns to an UP state, the module may need to be reset using the **hw-module module 1 reset** command.

324000

Error Message `%ASA-3-324000: Drop GTPv version message msg_type from source_interface:source_address/source_port to dest_interface:dest_address/dest_port Reason: reason`

Explanation The packet being processed did not meet the filtering requirements as described in the *reason* variable and is being dropped.

Recommended Action None required.

324001

Error Message `%ASA-3-324001: GTPv0 packet parsing error from` *source_interface:source_address/source_port* `to` *dest_interface:dest_address/dest_port*`, TID:` *tid_value*`, Reason:` *reason*

Explanation There was an error processing the packet. The following are possible reasons:

- Mandatory IE is missing
- Mandatory IE incorrect
- IE out of sequence
- Invalid message format.
- Optional IE incorrect
- Invalid TEID
- Unknown IE
- Bad length field
- Unknown GTP message.
- Message too short
- Unexpected message seen
- Null TID
- Version not supported

Recommended Action If this message is seen periodically, it can be ignored. If it is seen frequently, then the endpoint maybe sending out bad packets as part of an attack.

324002

Error Message `%ASA-3-324002: No PDP[MCB] exists to process GTPv0` *msg_type* `from` *source_interface:source_address/source_port* `to` *dest_interface:dest_address/dest_port*`, TID:` *tid_value*

Explanation If this message was preceded by syslog message 321100: Memory Allocation Error, the message indicates that there were not enough resources to create the PDP Context. If it was not preceded by message 321100, for version 0 it indicates that the corresponding PDP context could not be found. For version 1, if this message was preceded by message 324001, then a packet-processing error occurred, and the operation stopped.

Note When GTP HA messages are not delivered successfully from the active unit to the standby unit or if these messages are processed incorrectly on the standby unit, the following additional syslog message is generated:

```
%ASA-3-324002: No PDP exists to update the data sgsn PDPMCB Info
```

Recommended Action If the problem persists, contact the Cisco TAC.

324003

Error Message %ASA-3-324003: No matching request to process GTPv *version msg_type* from *source_interface:source_address/source_port* to *source_interface:dest_address/dest_port*

Explanation The response received does not have a matching request in the request queue and should not be processed further.

Recommended Action If this message is seen periodically, it can be ignored. But if it is seen frequently, then the endpoint maybe sending out bad packets as part of an attack.

324004

Error Message %ASA-3-324004: GTP packet with version%d from *source_interface:source_address/source_port* to *dest_interface:dest_address/dest_port* is not supported

Explanation The packet being processed has a version other than the currently supported version, which is 0 or 1. If the version number printed out is an incorrect number and is seen frequently, then the endpoint may be sending out bad packets as part of an attack.

Recommended Action None required.

324005

Error Message %ASA-3-324005: Unable to create tunnel from *source_interface:source_address/source_port* to *dest_interface:dest_address/dest_port*

Explanation An error occurred while trying to create the tunnel for the TPDUs.

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

324006

Error Message %ASA-3-324006:GSN *IP_address* tunnel limit *tunnel_limit* exceeded, PDP Context TID *tid* failed

Explanation The GSN sending the request has exceeded the maximum allowed tunnels created, so no tunnel will be created.

Recommended Action Check to see whether the tunnel limit should be increased or if there is a possible attack on the network.

324007

Error Message `%ASA-3-324007: Unable to create GTP connection for response from source_interface:source_address/0 to dest_interface:dest_address/dest_port`

Explanation An error occurred while trying to create the tunnel for the TPDUs for a different SGSN or GGSN.

Recommended Action Check debugs and messages to see why the connection was not created correctly. If the problem persists, contact the Cisco TAC.

324300

Error Message `%ASA-3-324300: Radius Accounting Request from from_addr has an incorrect request authenticator`

Explanation When a shared secret is configured for a host, the device verifies the request-authenticator with that secret. If the validation fails, it is logged and the device stops processing the packet.

- *from_addr*—The IP address of the host that is sending the Radius Accounting Request.

Recommended Action Verify that the correct shared secret was configured. If it is, double-check the source of the packet to make sure it is not spoofed.

324301

Error Message `%ASA-3-324301: Radius Accounting Request has a bad header length hdr_len, packet length pkt_len`

Explanation The accounting request message has a header length that is not the same as the actual packet length, so packet processing stops.

- *hdr_len*— The length indicated in the request header.
- *pkt_len*—The actual packet length.

Recommended Action Make sure the packet is not spoofed. If the packet is legitimate, then capture the packet and make sure the header length is incorrect as indicated by the syslog message. If the header length is correct, of the problem persists, contact the Cisco TAC.

325001

Error Message `%ASA-3-325001: Router ipv6_address on interface has conflicting ND (Neighbor Discovery) settings`

Explanation Another router on the link sent router advertisements with conflicting parameters. *ipv6_address* is the IPv6 address of the other router. *interface* is the interface name of the link with the other router.

Recommended Action Verify that all IPv6 routers on the link have the same parameters in the router advertisement for *hop_limit*, *managed_config_flag*, *other_config_flag*, *reachable_time* and *ns_interval*, and that preferred and valid lifetimes for the same prefix, advertised by several routers are the same. To list the parameters per interface, enter the **show ipv6** *interface* command.

325002

Error Message `%ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface`

Explanation Another system is using your IPv6 address. *ipv6_address* is the IPv6 address of the other router. *MAC_address* is the MAC address of the other system if known, otherwise "unknown." *interface* is the interface name of the link with the other system.

Recommended Action Change the IPv6 address of one of the two systems.

326001

Error Message `%ASA-3-326001: Unexpected error in the timer library: error_message`

Explanation A managed timer event was received without a context or a correct type or no handler exists. This message will also be displayed if the number of events queued exceed a system limit and will be attempted to be processed at a later time.

Recommended Action If the problem persists, contact the Cisco TAC.

326002

Error Message `%ASA-3-326002: Error in error_message: error_message`

Explanation The IGMP process failed to shut down upon request. Events that are performed in preparation for this shut down may be out of synchronization.

Recommended Action If the problem persists, contact the Cisco TAC.

326004

Error Message `%ASA-3-326004: An internal error occurred while processing a packet queue`

Explanation The IGMP packet queue received a signal without a packet.

Recommended Action If the problem persists, contact the Cisco TAC.

326005

Error Message `%ASA-3-326005: Mrib notification failed for (IP_address, IP_address)`

Explanation A packet triggering a data-driven event was received, and the attempt to notify the MRIB failed.

Recommended Action If the problem persists, contact the Cisco TAC.

326006

Error Message `%ASA-3-326006: Entry-creation failed for (IP_address, IP_address)`

Explanation The MFIB received an entry update from the MRIB, but failed to create the entry related to the addresses displayed, which can cause insufficient memory.

Recommended Action If the problem persists, contact the Cisco TAC.

326007

Error Message `%ASA-3-326007: Entry-update failed for (IP_address, IP_address)`

Explanation The MFIB received an interface update from the MRIB, but failed to create the interface related to the addresses displayed. The likely result is insufficient memory.

Recommended Action If the problem persists, contact the Cisco TAC.

326008

Error Message `%ASA-3-326008: MRIB registration failed`

Explanation The MFIB failed to register with the MRIB.

Recommended Action If the problem persists, contact the Cisco TAC.

326009

Error Message `%ASA-3-326009: MRIB connection-open failed`

Explanation The MFIB failed to open a connection to the MRIB.

Recommended Action If the problem persists, contact the Cisco TAC.

326010

Error Message `%ASA-3-326010: MRIB unbind failed`

Explanation The MFIB failed to unbind from the MRIB.

Recommended Action If the problem persists, contact the Cisco TAC.

326011

Error Message `%ASA-3-326011: MRIB table deletion failed`

Explanation The MFIB failed to retrieve the table that was supposed to be deleted.

Recommended Action If the problem persists, contact the Cisco TAC.

326012

Error Message `%ASA-3-326012: Initialization of` *`string`* `functionality failed`

Explanation The initialization of a functionality failed. This component might still operate without the functionality.

Recommended Action If the problem persists, contact the Cisco TAC.

326013

Error Message `%ASA-3-326013: Internal error:` *`string`* `in` *`string`* `line` *`%d`* `(`*`%s`*`)`

Explanation A fundamental error occurred in the MRIB.

Recommended Action If the problem persists, contact the Cisco TAC.

326014

Error Message `%ASA-3-326014: Initialization failed: error_message` *`error_message`*

Explanation The MRIB failed to initialize.

Recommended Action If the problem persists, contact the Cisco TAC.

326015

Error Message `%ASA-3-326015: Communication error: error_message` *`error_message`*

Explanation The MRIB received a malformed update.

Recommended Action If the problem persists, contact the Cisco TAC.

326016

Error Message `%ASA-3-326016: Failed to set un-numbered interface for` *`interface_name`* `(`*`string`*`)`

Explanation The PIM tunnel is not usable without a source address. This situation occurs because a numbered interface could not be found, or because of some internal error.

Recommended Action If the problem persists, contact the Cisco TAC.

326017

Error Message `%ASA-3-326017: Interface Manager error -` *`string`* `in` *`string`*`:` *`string`*

Explanation An error occurred while creating a PIM tunnel interface.

Recommended Action If the problem persists, contact the Cisco TAC.

326019

Error Message `%ASA-3-326019:` *`string`* `in` *`string`*`:` *`string`*

Explanation An error occurred while creating a PIM RP tunnel interface.

Recommended Action If the problem persists, contact the Cisco TAC.

326020

Error Message `%ASA-3-326020: List error in string: string`

Explanation An error occurred while processing a PIM interface list.

Recommended Action If the problem persists, contact the Cisco TAC.

326021

Error Message `%ASA-3-326021: Error in string: string`

Explanation An error occurred while setting the SRC of a PIM tunnel interface.

Recommended Action If the problem persists, contact the Cisco TAC.

326022

Error Message `%ASA-3-326022: Error in string: string`

Explanation The PIM process failed to shut down upon request. Events that are performed in preparation for this shut down may be out of sync.

Recommended Action If the problem persists, contact the Cisco TAC.

326023

Error Message `%ASA-3-326023: string - IP_address: string`

Explanation An error occurred while processing a PIM group range.

Recommended Action If the problem persists, contact the Cisco TAC.

326024

Error Message `%ASA-3-326024: An internal error occurred while processing a packet queue.`

Explanation The PIM packet queue received a signal without a packet.

Recommended Action If the problem persists, contact the Cisco TAC.

326025

Error Message `%ASA-3-326025: string`

Explanation An internal error occurred while trying to send a message. Events scheduled to happen on receipt of the message such as deletion of the PIM tunnel IDB may not take place.

Recommended Action If the problem persists, contact the Cisco TAC.

326026

Error Message `%ASA-3-326026: Server unexpected error: error_messsage`

Explanation The MRIB failed to register a client.

Recommended Action If the problem persists, contact the Cisco TAC.

326027

Error Message `%ASA-3-326027: Corrupted update: error_messsage`

Explanation The MRIB received a corrupt update.

Recommended Action If the problem persists, contact the Cisco TAC.

326028

Error Message `%ASA-3-326028: Asynchronous error: error_messsage`

Explanation An unhandled asynchronous error occurred in the MRIB API.

Recommended Action If the problem persists, contact the Cisco TAC.

327001

Error Message `%ASA-3-327001: IP SLA Monitor: Cannot create a new process`

Explanation IP SLA Monitor was unable to start a new process.

Recommended Action Check the system memory. If memory is low, then this is the likely cause. Try to reenter the commands when memory is available. If the problem persists, contact the Cisco TAC.

327002

Error Message `%ASA-3-327002: IP SLA Monitor: Failed to initialize, IP SLA Monitor functionality will not work`

Explanation IP SLA monitor failed to initialize. This condition is caused by either the timer wheel timer functionality failed to initialize or a process could not be created. A likely cause of this condition is that sufficient memory is not available to complete the task.

Recommended Action Check the system memory. If memory is low, then this is the likely cause. Try to reenter the commands when memory is available. If the problem persists, contact the Cisco TAC.

327003

Error Message `%ASA-3-327003: IP SLA Monitor: Generic Timer wheel timer functionality failed to initialize`

Explanation IP SLA monitor could not initialize the timer wheel.

Recommended Action Check the system memory. If memory is low, then the timer wheel functionality did not initialize. Try to reenter the commands when memory is available. If the problem persists, contact the Cisco TAC

328001

Error Message `%ASA-3-328001: Attempt made to overwrite a set stub function in` *`string`*`.`

Explanation A single function can be set as a callback for when a stub w/ check registry is invoked. This message indicates that an attempt to set a new callback failed because a callback function has already been set.

- *string*—The name of the function.

Recommended Action If the problem persists, contact the Cisco TAC.

329001

Error Message `%ASA-3-329001: The` *`string0`* `subblock named` *`string1`* `was not removed`

Explanation A software error has occurred. This message displays when IDB subblocks cannot be removed.

- *string0*—SWIDB or HWIDB.
- *string1*—The name of the subblock.

Recommended Action If the problem persists, contact the Cisco TAC.

331001

Error Message `ASA-3-331001: Dynamic DNS Update for 'fqdn_name' <=> ip_address failed`

Explanation This message is generated when the dynamic DNS subsystem fails to update the resource records on the DNS server. This failure might occur if the security appliance is unable to contact the DNS server or DNS service is not running on the destination system.

- *fqdn_name*—The fully qualified domain name for which the DNS update was attempted.
- *ip_address*—The IP address of the DNS update.

Recommended Action Make sure a DNS server is configured and reachable by the security appliance. If the problem persists, contact the Cisco TAC.

331002

Error Message `ASA-5-331002: Dynamic DNS type RR for ('fqdn_name' -> ip_address | ip_address -> 'fqdn_name') successfully updated in DNS server dns_server_ip`

Explanation This message is generated when a dynamic DNS update succeeds in the DNS server.

- *type*—The type of resource record, could be “A” or “PTR”.
- *fqdn_name*—The fully qualified domain name for which the DNS update was attempted.
- *ip_address*—The IP address of the DNS update.
- *dns_server_ip*—The IP address of the DNS server.

Recommended Action None required.

332001

Error Message `%ASA-3-332001: Unable to open cache discovery socket, WCCP V2 closing down.`

Explanation An internal error that indicates the WCCP process was unable to open the UDP socket used to listen for protocol messages from caches.

Recommended Action Ensure that the IP configuration is correct and that at least one IP address is configured.

332002

Error Message `%ASA-3-332002: Unable to allocate message buffer, WCCP V2 closing down.`

Explanation An internal error that indicates the WCCP process was unable to allocate memory to hold incoming protocol messages.

Recommended Action Ensure that there is enough memory available for all processes.

332003

Error Message `%ASA-5-332003: Web Cache` *`IP_address/service_ID`* `acquired`

Explanation A service from the web cache of the security appliance was acquired.

- *IP_address*—The IP address of the web cache.
- *service_ID*—The WCCP service identifier.

Recommended Action None required.

332004

Error Message `%ASA-1-332004: Web Cache` *`IP_address/service_ID`* `lost`

Explanation A service from the web cache of the security appliance was lost.

- *IP_address*—The IP address of the web cache.
- *service_ID*—The WCCP service identifier.

Recommended Action Verify operation of specified web cache.

333001

Error Message `%ASA-6-333001: EAP association initiated - context:` *`EAP-context`*

Explanation An EAP association has been initiated with a remote host.

- *EAP-context*—A unique identifier for the EAP session, displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

Recommended Action None required.

333002

Error Message `%ASA-5-333002: Timeout waiting for EAP response - context:EAP-context`

Explanation A timeout occurred while waiting for an EAP response.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

Recommended Action None required.

333003

Error Message `%ASA-6-333003: EAP association terminated - context:EAP-context`

Explanation The EAP association has been terminated with the remote host.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

Recommended Action None required.

333004

Error Message `%ASA-7-333004: EAP-SQ response invalid - context:EAP-context`

Explanation The EAP-Status Query response failed basic packet validation.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

Recommended Action If the problem persists, contact the Cisco TAC.

333005

Error Message `%ASA-7-333005: EAP-SQ response contains invalid TLV(s) - context:EAP-context`

Explanation The EAP-Status Query response has one or more invalid TLVs.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

Recommended Action If the problem persists, contact the Cisco TAC.

333006

Error Message `%ASA-7-333006: EAP-SQ response with missing TLV(s) - context:EAP-context`

Explanation The EAP-Status Query response is missing one or more mandatory TLVs.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

Recommended Action If the problem persists, contact the Cisco TAC.

333007

Error Message `%ASA-7-333007: EAP-SQ response TLV has invalid length - context:EAP-context`

Explanation The EAP-Status Query response contains a TLV with an invalid length.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

Recommended Action If the problem persists, contact the Cisco TAC.

333008

Error Message `%ASA-7-333008: EAP-SQ response has invalid nonce TLV - context:EAP-context`

Explanation The EAP-Status Query response contains an invalid nonce TLV.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

Recommended Action If the problem persists, contact the Cisco TAC.

333009

Error Message `%ASA-6-333009: EAP-SQ response MAC TLV is invalid - context:EAP-context`

Explanation The EAP-Status Query response contains a MAC which does not match the calculated MAC.

- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

Recommended Action If the problem persists, contact the Cisco TAC.

333010

Error Message `%ASA-5-333010: EAP-SQ response Validation Flags TLV indicates PV request - context:EAP-context`

Explanation The EAP-Status Query response contains a Validation Flags TLV which indicates that the peer requested a full posture validation.

Recommended Action None required.

334001

Error Message `%ASA-6-334001: EAPoUDP association initiated - <host-address>`

Explanation An EAPoUDP association has been initiated with a remote host.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

Recommended Action None required.

334002

Error Message `%ASA-5-334002: EAPoUDP association successfully established - host-address`

Explanation An EAPoUDP association has been successfully established with the host.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

Recommended Action None required.

334003

Error Message `%ASA-5-334003: EAPoUDP association failed to establish - host-address`

Explanation An EAPoUDP association has failed to establish with the host.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

Recommended Action Verify configuration of Cisco Secure Access Control Server.

334004

Error Message `%ASA-6-334004: Authentication request for NAC Clientless host-` *`host-address`*

Explanation An authentication request was made for a NAC Clientless host.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101)

Recommended Action None required.

334005

Error Message `%ASA-5-334005: Host put into NAC Hold state -` *`host-address`*

Explanation The NAC session for the host was put into the Hold state.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101)

Recommended Action None required.

334006

Error Message `%ASA-5-334006: EAPoUDP failed to get a response from host -` *`host-address`*

Explanation An EAPoUDP response was not received from the host.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101)

Recommended Action None required.

334007

Error Message `%ASA-6-334007: EAPoUDP association terminated -` *`host-address`*

Explanation An EAPoUDP association has terminated with the host.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101)

Recommended Action None required.

334008

Error Message `%ASA-6-334008: NAC EAP association initiated - host-address, EAP context: EAP-context`

Explanation EAPoUDP has initiated EAP with the host.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).
- *EAP-context*—A unique identifier for the EAP session displayed as an eight-digit hexadecimal number (for example, 0x2D890AE0).

Recommended Action None required.

334009

Error Message `%ASA-6-334009: Audit request for NAC Clientless host - Assigned_IP`

Explanation This is an informational message indicating that an audit request is being sent for the specified assigned IP address.

- *Assigned_IP*—The IP address assigned to the client

Recommended Action None required.

335001

Error Message `%ASA-6-335001: NAC session initialized - host-address`

Explanation A NAC session has started for a remote host.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101)

Recommended Action None required.

335002

Error Message `%ASA-5-335002: Host is on the NAC Exception List - host-address, OS: oper-sys`

Explanation The client is on the NAC Exception List is therefore not subject toPosture Validation.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101)
- *oper-sys*—The operating system (e.g., Windows XP) of the host

Recommended Action None required.

335003

Error Message %ASA-5-335003: NAC Default ACL applied, ACL:*ACL-name - host-address*

Explanation The NAC Default ACL has been applied for the client.

- *ACL-name*—The name of the ACL being applied.
- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

Recommended Action None required.

335004

Error Message %ASA-6-335004: NAC is disabled for host - *host-address*

Explanation NAC is disabled for the remote host.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101)

Recommended Action None required.

335005

Error Message %ASA-4-335005: NAC Downloaded ACL parse failure - *host-address*

Explanation Parsing of a downloaded ACL failed.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101)

Recommended Action Verify configuration of Cisco Secure Access Control Server.

335006

Error Message %ASA-6-335006: NAC Applying ACL: *ACL-name - host-address*

Explanation Name of the ACL being applied as a result of NAC Posture Validation.

- *ACL-name*—The name of the ACL being applied.
- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

Recommended Action None required.

335007

Error Message `%ASA-7-335007: NAC Default ACL not configured - host-address`

Explanation NAC Default ACL has not been configured.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

Recommended Action None required.

335008

Error Message `%ASA-5-335008:` NAC IPsec terminate from dynamic ACL:*ACL-name* - `host-address`

Explanation A dynamic ACL obtained as a result of PV warrants IPsec termination.

- *ACL-name*—The name of the ACL being applied.
- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

Recommended Action None required.

335009

Error Message `%ASA-6-335009:` NAC 'Revalidate' request by administrative action - `host-address`

Explanation NAC Revalidate was requested by the administrator.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

Recommended Action None required.

335010

Error Message `%ASA-6-335010: NAC 'Revalidate All' request by administrative action - num sessions`

Explanation NAC Revalidate All was requested by the administrator.

- *num*—A decimal integer that indicates the number of sessions to be revalidated.

Recommended Action None required.

335011

Error Message `%ASA-6-335011: NAC 'Revalidate Group' request by administrative action for group-name group - num sessions`

Explanation NAC “Revalidate Group” was requested by the administrator.

- *group-name*—The VPN group name.
- *num*—A decimal integer that indicates the number of sessions to be revalidated.

Recommended Action None required.

335012

Error Message `%ASA-6-335012: NAC 'Initialize' request by administrative action - host-address`

Explanation NAC “Initialize” was requested by the administrator.

- *host-address*—The IP address of the host, in dotted decimal format (for example, 10.86.7.101).

Recommended Action None required.

335013

Error Message `%ASA-6-335013:` NAC 'Initialize All' request by administrative action - *num* sessions

Explanation NAC Initialize All was requested by the administrator.

- *num*—A decimal integer that indicates the number of sessions to be revalidated.

Recommended Action None required.

335014

Error Message `%ASA-6-335014: NAC 'Initialize Group' request by administrative action for group-name group - num sessions`

Explanation NAC Initialize Group was requested by the administrator.

- *group-name*—The VPN group name
- *num*—A decimal integer that indicates the number of sessions to be revalidated

Recommended Action None required.

336001

Error Message `%ASA-3-336001 Route desination_network stuck-in-active state in EIGRP-ddb_name as_num. Cleaning up`

Explanation The stuck-in-active (SIA) state means that an EIGRP router has not received a reply to a query from one or more neighbors within the time allotted (approximately three minutes). When this happens, EIGRP clears the neighbors that did not send a reply and logs an error message for the route that went active.

- *desination_network*—The route that went active
- *ddb_name*—IPv4
- *as_num*—The EIGRP router

Recommended Action Check to see why the router did not get a response from all of its neighbors and why the route disappeared. For more information on this type of problem, see the Technote at: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008010f016.shtml

336002

Error Message `%ASA-3-336002: Handle handle_id is not allocated in pool.`

Explanation Handle not allocated. The EIGRP router is unable to find the handle for the next hop.

- *handle_id*—The identity of the unfound handle

Recommended Action If the problem persists, contact the Cisco TAC.

336003

Error Message `%ASA-3-336003: No buffers available for bytes byte packet`

Explanation No Buffer. The Diffusing Update Algorithm (DUAL) software was unable to allocate a packet buffer. The system may be out of memory.

- *bytes*—Number of bytes in the packet

Recommended Action Check to see whether the system is out of memory by entering a **show mem** or **show tech** command. If the problem persists, contact the Cisco TAC.

336004

Error Message `%ASA-3-336004: Negative refcount in pakdesc pakdesc.`

Explanation Negative reference count. The reference count packet count that went negative.

- *pakdesc*—Packet identifier

Recommended Action If the problem persists, contact the Cisco TAC.

336005

Error Message `%ASA-3-336005: Flow control error, error, on interface_name.`

Explanation This log is issued when the interface is flow-blocked for multicast. Qelm is the queue element, in this case, the last multicast packet on the queue for this particular interface.

- *error*—Error statement "Qelm on flow ready"
- *interface_name*—Name of the interface on which the error occurred

Recommended Action If the problem persists, contact the Cisco TAC.

336006

Error Message `%ASA-3-336006: num peers exist on IIDB interface_name.`

Explanation Peers still exist on a particular interface during or after clean up of the IDB of the EIGRP.

- *num*—The number of peers
- *interface_name*—The interface name

Recommended Action If the problem persists, contact the Cisco TAC.

336007

Error Message `%ASA-3-336007: Anchor count negative`

Explanation Negative Anchor Count. An error occurred and the count of the anchor became negative when it was released.

Recommended Action If the problem persists, contact the Cisco TAC.

336008

Error Message `%ASA-3-336008: Lingering DRDB deleting IIDB, dest network, nexthop address (interface), origin origin_str`

Explanation Lingering DRDB. An interface is being deleted and some lingering DRDB exists.

- *network*—The destination network
- *address*—The nexthop address
- *interface*—The nexthop interface
- *origin_str*—String defining the origin

Recommended Action If the problem persists, contact the Cisco TAC.

336009

Error Message `%ASA-3-336009 ddb_name as_id: Internal Error`

Explanation An internal error occurred.

- *ddb_name*—Protocol Dependent Module (PDM) name, for example, IPv4 PDM
- *as_id*—Autonomous system ID

Recommended Action If the problem persists, contact the Cisco TAC.

336010

Error Message `%ASA-5-336010 EIGRP-<ddb_name> tableid as_id: Neighbor address (%interface) is event_msg: msg`

Explanation Neighbor Change. A neighbor went up or down.

- *ddb_name*—IPv4
- *tableid*— Internal ID for the RIB
- *as_id*—Autonomous system ID
- *address*—IP address of the neighbor
- *interface*—Name of the interface
- *event_msg*— Event that is occurring for the neighbor (that is, up or down)
- *msg*—Reason for the event. Possible *event_msg* and *msg* value pairs include:
  - resync: Peer graceful-restart
  - down: Holding timer expired
  - up: New adjacency
  - down: Auth failure

- down: Stuck in Active
- down: Interface PEER-TERMINATION received
- down: K-value mismatch
- down: Peer Termination received
- down: Stuck in INIT state
- down: Peer info changed
- down: Summary configured
- down: Max hopcount changed
- down: Metric changed
- down: [No reason]

Recommended Action Check to see why the link on the neighbor is going down or is flapping. This may be a sign of a problem, or a problem might start occurring because of this.

336011

Error Message `%ASA-6-336011: event event`

Explanation A dual event occurred. The events can be one of the following:

- Redist rt change
- SIA Query while Active

Recommended Action If the problem persists, contact the Cisco TAC.

Messages 400000 to 450001

This section contains messages from 400000 to 450001.

4000*nn*

Error Message `%ASA-4-4000nn: IPS:number string from IP_address to IP_address on interface interface_name`

Explanation Messages 400000 through 400051 are Cisco Intrusion Prevention Service signature messages.

Recommended Action Refer to the *Cisco Intrusion Prevention Service User Guide* at the following URL:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_user_guide_list.html

All signature messages are not supported by the security appliance in this release. IPS syslog messages all start with 4-4000*nn* and have the following format:

Options:

number	The signature number. For more information, see the *Cisco Intrusion Prevention Service User Guide* at the following website: http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_user_guide_list.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:

```
%ASA-4-400013 IPS:2003 ICMP redirect from 10.4.1.2 to 10.2.1.1 on interface dmz
%ASA-4-400032 IPS:4051 UDP Snork attack from 10.1.1.1 to 192.168.1.1 on interface outside
```

Table 1-5 lists the supported signature messages.

Table 1-5 IPS System Log 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
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

Table 1-5 IPS System Log Messages (continued)

Message Number	Signature ID	Signature Title	Signature Type
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
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	ypbind (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	rexd (remote execution daemon) Portmap Request	Informational
400049	6180	rexd (remote execution daemon) Attempt	Informational
400050	6190	statd Buffer Overflow	Attack

401001

Error Message `%ASA-4-401001: Shuns cleared`

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

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

401002

Error Message `%ASA-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 displayed to allow an institution to keep a record of shunning activity.

401003

Error Message `%ASA-4-401003: Shun deleted:` *`IP_address`*

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

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

401004

Error Message `%ASA-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 `%ASA-4-401005` can be used to evaluate further risk assessment concerning this host.

401005

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

Explanation The security appliance 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 a shun manually, or wait for the Cisco Intrusion Detection System to do this.

402114

Error Message `%ASA-4-402114: IPsec: Received a protocol packet (SPI=spi, sequence number=seq_num) from remote_IP to local_IP with an invalid SPI.`

- *protocol*—IPsec protocol
- *spi*—IPsec Security Parameter Index
- *seq_num*—IPsec sequence number
- *remote_IP*—IP address of the remote endpoint of the tunnel
- *username*—Username associated with the IPsec tunnel
- *local_IP*—IP address of the local endpoint of the tunnel

Explanation This message is displayed when an IPsec packet is received that specifies an SPI that does not exist in the SA database. 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 indicate incorrect packets sent by the IPsec peer, which may be part of an attack. This message is rate limited to no more than one message every five seconds.

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 administrator.

402115

Error Message `%ASA-4-402115: IPsec: Received a packet from remote_IP to local_IP containing act_prot data instead of exp_prot data.`

Explanation This message is displayed when an IPsec packet is received that is missing the expected ESP header. The peer is sending packets that do not match the negotiated security policy. This may indicate an attack. This message is rate limited to no more than one message every five seconds.

- *remote_IP*—IP address of the remote endpoint of the tunnel
- *local_IP*—IP address of the local endpoint of the tunnel
- *act_prot*—Received IPsec protocol

- *exp_prot*—Expected IPsec protocol

Recommended Action Contact the peer administrator.

402116

Error Message `%ASA-4-402116: IPsec: Received an protocol packet (SPI=spi, sequence number=seq_num) from remote_IP (username) to local_IP. The decapsulated inner packet doesn't match the negotiated policy in the SA. The packet specifies its destination as pkt_daddr, its source as pkt_saddr, and its protocol as pkt_prot. The SA specifies its local proxy as id_daddr/id_dmask/id_dprot/id_dport and its remote proxy as id_saddr/id_smask/id_sprot/id_sport.`

Explanation This message is displayed when a decapsulated 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, or it may be part of an attack. This message is rate limited to no more than one message every five seconds.

- *protocol*—IPsec protocol
- *spi*—IPsec Security Parameter Index
- *seq_num*—IPsec sequence number
- *remote_IP*—IP address of the remote endpoint of the tunnel
- *username*—Username associated with the IPsec tunnel
- *local_IP*—IP address of the local endpoint of the tunnel
- *pkt_daddr*—Destination address from the decapsulated packet
- *pkt_saddr*—Source address from the decapsulated packet
- *pkt_prot*—Transport protocol from the decapsulated packet
- *id_daddr*—Local proxy IP address
- *id_dmask*—Local proxy IP subnet mask
- *id_dprot*—Local proxy transport protocol
- *id_dport*—Local proxy port
- *id_saddr*—Remote proxy IP address
- *id_smask*—Remote proxy IP subnet mask
- *id_sprot*—Remote proxy transport protocol
- *id_sport*—Remote proxy port

Recommended Action Contact the peer administrator and compare policy settings.

402117

Error Message `%ASA-4-402117: IPsec: Received a non-IPsec (protocol) packet from remote_IP to local_IP.`

Explanation This message is displayed when 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 may be configured to only accept 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 telnet or traffic to the outside interface on ports other than 23. This error can also indicate an attack. This syslog message is not generated except under these conditions (for example, it is not generated for traffic to the firewall interfaces themselves). See system log messages 710001, 710002, and 710003 that track TCP and UDP requests. This message is rate limited to no more than one message every five seconds.

- *protocol*—IPsec protocol
- *remote_IP*—IP address of the remote endpoint of the tunnel
- *local_IP*—IP address of the local endpoint of the tunnel

Recommended Action Contact the peer administrator to compare policy settings.

402118

Error Message `%ASA-4-402118: IPsec: Received an protocol packet (SPI=spi, sequence number seq_num) from remote_IP (username) to local_IP containing an illegal IP fragment of length frag_len with offset frag_offset.`

Explanation This message is displayed when a decapsulatd IPsec packet contains an IP fragment with an offset less than or equal to 128 bytes. The latest version of the Security Architecture for IP RFC recommends 128 bytes as the minimum IP fragment offset to prevent reassembly attacks. This may be part of an attack. This message is rate limited to no more than one message every five seconds.

- *protocol*—IPsec protocol
- *spi*—IPsec Security Parameter Index
- *seq_num*—IPsec sequence number
- *remote_IP*—IP address of the remote endpoint of the tunnel
- *username*—Username associated with the IPsec tunnel
- *local_IP*—IP address of the local endpoint of the tunnel
- *frag_len*—IP fragment length
- *frag_offset*—IP fragment offset in bytes

Recommended Action Contact the administrator of the remote peer to compare policy settings.

402119

Error Message `%ASA-4-402119: IPsec: Received an protocol packet (SPI=spi, sequence number=seq_num) from remote_IP (username) to local_IP that failed anti-replay checking.`

Explanation This message is displayed when an IPsec packet is received with an invalid sequence number. The peer is sending packets containing sequence numbers that may have been previously used. This syslog message indicates that an IPsec packet has been received with a sequence number outside of the acceptable window. This packet will be dropped by IPsec as part of a possible attack. This message is rate limited to no more than one message every five seconds.

- *protocol*—IPsec protocol
- *spi*—IPsec Security Parameter Index
- *seq_num*—IPsec sequence number
- *remote_IP*—IP address of the remote endpoint of the tunnel
- *username*—Username associated with the IPsec tunnel
- *local_IP*—IP address of the local endpoint of the tunnel

Recommended Action Contact the peer administrator.

402120

Error Message `%ASA-4-402120: IPsec: Received an protocol packet (SPI=spi, sequence number=seq_num) from remote_IP (username) to local_IP that failed authentication.`

Explanation This message is displayed when an IPsec packet is received and fails authentication. The packet is dropped. The packet may have been corrupted in transit or the peer may be sending invalid IPsec packets. This may indicate an attack if many of these packets are received from the same peer. This message is rate limited to no more than one message every five seconds.

- *protocol*—IPsec protocol
- *spi*—IPsec Security Parameter Index
- *seq_num*—IPsec sequence number
- *remote_IP*—IP address of the remote endpoint of the tunnel
- *username*—Username associated with the IPsec tunnel
- *local_IP*—IP address of the local endpoint of the tunnel

Recommended Action Contact the administrator of the remote peer if many failed packets are received.

402121

Error Message `%ASA-4-402121: IPsec: Received an protocol packet (SPI=spi, sequence number=seq_num) from peer_addr (username) to lcl_addr that was dropped by IPsec (drop_reason).`

Explanation This message is displayed when an IPsec packet to be decapsulated was received and subsequently dropped by the IPsec subsystem. This could indicate a problem with the device configuration or with the device itself.

- *protocol*—IPsec protocol
- *spi*—IPsec Security Parameter Index
- *seq_num*—IPsec sequence number
- *peer_addr*—IP address of the tunnel remote endpoint
- *username*—Username associated with the IPsec tunnel
- *lcl_addr*—IP address of the local endpoint of the tunnel
- *drop_reason*—Reason that the packet was dropped

Recommended Action If the problem persists, contact the Cisco TAC.

402122

Error Message `%ASA-4-402122: Received a cleartext packet from src_addr to dest_addr that was to be encapsulated in IPsec that was dropped by IPsec (drop_reason).`

Explanation A packet to be encapsulated in IPsec was received and subsequently dropped by the IPsec subsystem. This could indicate a problem with the device configuration or with the device itself.

- *src_addr*—Source IP address
- *dest_addr*—Destination IP address
- *drop_reason*—Reason that the packet was dropped

Recommended Action If the problem persists, contact the Cisco TAC.

402123

Error Message `%ASA-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (code= error_string) while executing crypto command command.`

Explanation This message is displayed when an error is detected while running a crypto command with a hardware accelerator. This could indicate a problem with the accelerator. This type of error may occur for a variety of reasons, and this message supplements the crypto accelerator counters to help determine the cause.

- *accel_type*—Hardware accelerator type

- *error_string*—Code indicating the type of error
- *command*—Crypto command that generated the error

Recommended Action If the problem persists, contact the Cisco TAC.

402124

Error Message `%ASA-4-402124: CRYPTO: The ASA hardware accelerator encountered an error (Hardware error address, Core, Hardware error code, IstatReg, PciErrReg, CoreErrStat, CoreErrAddr, Doorbell Size,DoorBell Outstanding, SWReset).`

Explanation This syslog message appears when the crypto hardware chip has reported a fatal error, indicating the chip is inoperable. The information from this syslog message captures information to allow further analysis of this problem. The crypto chip is reset when this condition is detected, to unobtrusively allow the security appliance to continue functioning. Also, the crypto environment at the time this issue is detected is written to a crypto archive directory on flash, to provide further debugging information. Various parameters related to the crypto hardware are contained in this syslog message; these include the following:

- `HWErrAddr—Hardware address (set by crypto chip)`
- `Core—Crypto core experiencing the error`
- `HwErrCode—Hardware error code (set by crypto chip)`
- `IstatReg—Interrupt status register (set by crypto chip)`
- `PciErrReg—PCI error register (set by crypto chip)`
- `CoreErrStat—Core error status (set by crypto chip)`
- `CoreErrAddr—Core error address (set by crypto chip)`
- `Doorbell Size—Maximum crypto commands allowed`
- `DoorBell Outstanding—Crypto commands outstanding`
- `SWReset—Number of crypto chip resets since boot`

Recommended Action Forward the syslog message information to Cisco TAC for further analysis.

402125

Error Message `%ASA-4-402125: The ASA hardware accelerator` *`ring`* `timed out (`*`parameters`*`).`

Explanation The crypto driver has detected either the IPsec or SSL/Admin descriptor ring is no longer progressing, meaning the crypto chip no longer appears to be functioning. The crypto chip is reset when this condition is detected, to unobtrusively allow the security appliance to continue functioning. Also the crypto environment at the time this issue is detected is written to a crypto archive directory on flash, to provide further debugging information.

- *ring*—IPsec ring or Admin ring
- *parameters*—Include the following:

  - Desc—Descriptor address

- CtrlStat—Control/status value
- ResultP—Success pointer
- ResultVal—Success value
- Cmd—Crypto command
- CmdSize—Command size
- Param—Command parameters
- Dlen—Data length
- DataP—Data pointer
- CtxtP—VPN context pointer
- SWReset—Number of crypto chip resets since boot

Recommended Action Forward the syslog message information to Cisco TAC for further analysis.

402126

Error Message `%ASA-4-402126: CRYPTO: The ASA created Crypto Archive File` *`Archive Filename`* `as a Soft Reset was necessary. Please forward this archived information to Cisco.`

Explanation A functional problem was detected with the hardware crypto chip (see system log messages 4402124 and 4402125). To further debug the crypto problem, a crypto archive file is generated, containing the current crypto hardware environment (hardware registers, Crypto Desc Entries, and so on….). At boot time, a crypto_archive directory is automatically created on the flash file system (if it did not previously exist). A maximum of two crypto archive files are allowed to exist in this directory.

- *Archive Filename*—The name of the crypto archive file name. The crypto archive file names are of the form, "crypto_arch_x.bin," where "x" = (1 or 2).

Recommended Action Forward the crypto archive file(s) to Cisco TAC for further analysis.

402127

Error Message `%ASA-4-402127: CRYPTO: The ASA is skipping the writing of latest Crypto Archive File as the maximum # of files,` *`max_number,`* `allowed have been written to` *`archive_directory`*`. Please archive & remove files from` *`Archive Directory`* `if you want more Crypto Archive Files saved.`

Explanation There was a functional problem detected with the HW Crypto chip (see syslog messages 4402124 and 4402125). This syslog message indicates a crypto archive file was not written, because the maximum number of crypto archive files already existed.

- *`max_number`*—Maximum number of files allowed in the archive directory; currently set to two

- *archive_directory*—Name of the archive directory

Recommended Action Forward previously generated crypto archive files to Cisco. Remove the previously generated archive file(s), so more can be written (if deemed necessary).

402128

Error Message `%ASA-5-402128: CRPTO: An attempt to allocate a large memory block failed, size: size, limit: limit`

Explanation An SSL connection is attempting to use more memory than allowed. The request has been denied.

- *size*—The size of the memory block being allocated
- *limit*—The maximum size of allocated memory permitted

Recommended Action If this message persists, an SSL denial of service (DoS) attack may be in progress. Contact the remote peer administrator or upstream provider.

402129

Error Message `%ASA-6-402129: CRPTO: An attempt to release a DMA memory block failed, location: address`

Explanation An internal software error has occurred.

- *address*—The address being freed

Recommended Action Contact the Cisco TAC for assistance.

402130

Error Message `%PIX|ASA-6-402130: CRYPTO: Received an ESP packet (SPI = 0x54A5C634, sequence number= 0x7B) from 75.2.96.101 (user= user) to 85.2.96.10 with incorrect IPsec padding.`

Explanation The ASAs crypto hardware accelerator detected an IPSec packet with invalid padding.

- *SPI*—The SPI associated with the packet
- *sequence number*—The sequence number associated with packet
- *user*—username string
- *padding*—padding data from packet

Recommended Action There have been customers using the ATT VPN client that have experienced this issue due to the ATT VPN client sometimes padding Ipsec packets incorrectly. While this syslog is informational only and doesn't indicate a problem with the ASA, customers using the ATT VPN client may wish to upgrade their VPN client software.

403101

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

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

Recommended Action If the problem persists, contact the Cisco TAC.

403102

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

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

Recommended Action If the problem persists, contact the Cisco TAC.

403103

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

Explanation The module cannot accept additional PPTP connections.

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

403104

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

Explanation The Microsoft Point-to-Point Encryption (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 `%ASA-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 `%ASA-4-403107: PPP virtual interface interface_name missing aaa server group info`

Explanation The AAA server configuration information cannot be found.

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

403108

Error Message `%ASA-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 information with the **vpdn group** *group_name* **client configuration address local** *address_pool_name* command.

403109

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

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

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

403110

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

Explanation The security appliance 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 `%ASA-3-403501: PPPoE - Bad host-unique in PADO - packet dropped. Intf:interface_name AC:ac_name`

Explanation The security appliance sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The security appliance is unable to identify the corresponding connection request for this response. The packet is dropped and connection negotiations are discontinued.

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 `%ASA-3-403502: PPPoE - Bad host-unique in PADS - dropping packet. Intf:`*`interface_name`* `AC:`*`ac_name`*

Explanation The security appliance sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The security appliance is unable to identify the corresponding connection request for this response. The packet was dropped and connection negotiations were discontinued.

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.

403503

Error Message `%ASA-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 `%ASA-3-403504: PPPoE:No 'vpdn group `*`group_name`*`' 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 security appliance for PPPoE dialout. The **my-username** and **my-password** commands are used 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 Configure a VPDN group for PPPoE.

403505

Error Message `%ASA-4-403505: PPPoE:PPP - Unable to set default route to` *`IP_address`* `at` *`interface_name`*

Explanation This message is usually followed by the message - **`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 `%ASA-4-403506: PPPoE:failed to assign PPP` *IP_address* `netmask` *netmask* `at` *interface_name*

Explanation This message is followed by one of two options:

- **`subnet is the same as interface`**
- **`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.

403507

Error Message `%ASA-3-403507:PPPoE:PPPoE client on interface` *`interface`* `failed to locate PPPoE vpdn group` *`group_name`*

Explanation You can configure the PPPoE client on an interface to use a particular VPDN group by entering the **pppoe client vpdn group** *group_name* command. If a PPPoE VPDN group of the configured name is not located during system startup, this syslog message is generated.

- *interface*—The interface on which the PPPoE client failed.
- *group_name* —The VPDN group name of the PPPoe client on the interface.

Recommended Action Perform the following steps:

1. Add the required VPDN group by entering the **vpdn group** *group_name* command. Request dialout PPPoE in global configuration mode and add all the group properties.
2. Remove the **pppoe client vpdn group** *group_name* command from the interface indicated. In this case, the PPPoE client will attempt to use the first PPPoE VPDN group defined.

Note All changes take effect only after the PPPoE client on the interface is restarted by entering the **ip address pppoe** command.

404101

Error Message `%ASA-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 that you specified with the **ip local pool** command.

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

404102

Error Message `%ASA-3-404102: ISAKMP: Exceeded embryonic limit`

Explanation More than 500 embryonic security associations (SAs) exist, which could mean a DoS attack.

Recommended Action Enter the **show crypto isakmp ca** command to determine the origin of the attack. After the source is identified, deny access to the offending IP address or network.

405001

Error Message `%ASA-4-405001: Received ARP {request | response} collision from IP_address/MAC_address on interface interface_name`

Explanation The security appliance 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.

405101

Error Message `%ASA-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 module 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. You can 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 translates and connections. This error message may also be caused by insufficient memory; try reducing the amount of memory usage, or purchasing additional memory. If the problem persists, contact the Cisco TAC.

405002

Error Message `%ASA-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 security appliance 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 security appliance, and the security appliance 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 to see whether they belong to a valid host.

405101

Error Message `%ASA-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 security appliance failed to allocate RAM system memory while starting a connection or 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. If this message occurs periodically, it can be ignored. If the problem persists, contact the Cisco TAC.

405102

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

Explanation The security appliance failed to allocate RAM system memory while starting a connection or 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. If this message occurs periodically, it can be ignored. If the problem persists, contact the Cisco TAC.

405103

Error Message `%ASA-4-405103: H225 message from source_address/source_port to dest_address/dest_port contains bad protocol discriminator hex`

Explanation The security appliance is expecting the protocol discriminator, 0x08, but it received something other than 0x08. This might happen because the endpoint is sending a bad packet, or received a message segment other than the first segment.

Recommended Action None required. The packet is allowed through.

405104

Error Message `%ASA-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 security appliance must receive an initial SETUP message for that H.225 call signalling channel before accepting any other H.225 messages.

Recommended Action None required.

405105

Error Message `%ASA-4-405105: H323 RAS message AdmissionConfirm received from source_address/source_port to dest_address/dest_port without an AdmissionRequest`

Explanation A gatekeeper has sent an admission confirm (ACF), but the security appliance did not send an admission request (ARQ) to the gatekeeper.

Recommended Action Check the gatekeeper with the specified *source_address* to determine why it sent an ACF without receiving an ARQ from the security appliance.

405106

Error Message `%ASA-4-405106: H323 num channel is not created from %I/%d to %I/%d %s\n`

Explanation This syslog message is generated when the security appliance attempts to create a match condition on the H.323 media-type channel. See the **match media-type** command for more information.

Recommended Action None required.

405107

Error Message `%ASA-4-405107: H245 Tunnel is detected and connection dropped from %I/%d to %I/%d %s\n`

Explanation This syslog message is generated when an H.323 connection has been dropped because of attempted H.245 tunnel control during call setup. See the **h245-tunnel-block** command for more information.

Recommended Action None required.

405201

Error Message `%ASA-4-405201: ILS ILS_message_type from inside_interface:source_IP_address to outside_interface:/destination_IP_address has wrong embedded address embedded_IP_address`

Explanation The embedded address in the ILS packet payload is not the same as the source IP address of the IP packet header.

Recommended Action Check the host with the specified with the *source_IP_address* to determine why it sent an ILS packet with an incorrect embedded IP address.

405300

Error Message `%ASA-4-405300: Radius Accounting Request received from from_addr is not allowed`

Explanation The accounting request came from a host that was not configured in the policy-map. The message is logged and processing stops.

- *from_addr*—The IP address of the host sending the request.

Recommended Action If the host was configured to send RADIUS accounting messages to the security appliance, make sure it was configured in the correct policy-map that was applied to the service-policy. If the host was not configured to send RADIUS accounting messages to the security appliance, then check to see why the messages are being sent. If the messages are illegitimate, then create the correct ACLs to drop the packets.

405301

Error Message `%ASA-4-405301: Attribute attribute_number does not match for user user_ip`

Explanation When the **validate-attribute** command is entered, the attribute values stored in the Accounting Request Start received do not match those stored in entry, if it exists.

- *attribute_number*—The RADIUS attribute to be validated with RADIUS accounting. Values range from 1 to 191. Vendor-specific attributes are not supported.
- *user_ip*—The IP address (framed IP attribute) of the user.

Recommended Action None required.

406001

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

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

Recommended Action None required.

406002

Error Message `%ASA-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 security policy. For example, an attacker 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 security appliance drops the packet, terminates the connection, and logs the event. The address in parentheses is the address from the port command.

Recommended Action None required.

407001

Error Message `%ASA-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 security appliance within the last five minutes.
- The inside host currently reserved an xlate connection or user authentication at the security appliance.

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 security appliance. To forcefully 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 1-6.)

Table 1-6 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 `%ASA-4-407002: Embryonic limit nconns/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 security appliance. This message is displayed when the number of connections from a specified foreign address over a specified global address to the specified local address exceeds the maximum embryonic limit for that static. The security appliance 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 security appliance retains pertinent state information, drops the packet, and waits for the acknowledgment from the client.

Recommended Action The message might indicate 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.

407003

Error Message `%ASA-4-407003: Established limit for RPC services exceeded number`

Explanation The security appliance tried to open a new hole for a pair of RPC servers or services that have already been configured after the maximum number of holes has been met.

Recommended Action Wait for other holes to be closed (through associated timeout expiration) or limit the number of active pairs of servers or services.

408001

Error Message `%ASA-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 problem persists, contact the Cisco TAC.

408002

Error Message `%ASA-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1] via source IP:interface1 address2 netmask2 [distance2/metric2] interface2`

Explanation A network update was received from a different interface with the same distance and a better metric than the existing route. The new route overrides the existing route that was installed through another interface. The new route is for redundancy purposes only and means that a path has shifted in the network. This change must be controlled through topology and redistribution. Any existing connections affected by this change are probably disabled and will timeout. This path shift only occurs if the network topology has been specifically designed to support path redundancy, in which case it is expected.

Recommended Action None required.

408003

Error Message `%ASA-4-408003: can't track this type of object hex`

Explanation A component of the tracking system has encountered an object type that is not supported by the component. A STATE object was expected.

- *hex*—A hexidecimal value(s) depicting variable value(s) or addresses in memory

Recommended Action Reconfigure the track object to make it a STATE object.

409001

Error Message `%ASA-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 `%ASA-4-409002: db_free: external LSA IP_address netmask`

Explanation An internal software error occurred.

Recommended Action None required.

409003

Error Message `%ASA-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 `%ASA-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 `%ASA-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 `%ASA-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. If the problem persists, contact the Cisco TAC.

409007

Error Message `%ASA-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 If the problem persists, contact the Cisco TAC.

409008

Error Message `%ASA-4-409008: Found generating default LSA with non-zero mask LSA type : number Mask: netmask metric: number area: string`

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

Recommended Action If the problem persists, contact the Cisco TAC.

409009

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

Explanation An internal error occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

409011

Error Message `%ASA-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 router ID.

409012

Error Message `%ASA-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 router ID.

409013

Error Message `%ASA-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 router ID.

409023

Error Message `%ASA-4-409023: Attempting AAA Fallback method method_name for request_type request for user user: Auth-server group server_tag unreachable`

Explanation An authentication or authorization attempt to an external server has failed and will now be performed using the local user database. *aaa_operation* is either "authentication" or "authorization." *username* is the user associated with the connection. *server_group* is the name of the AAA server whose servers were unreachable.

Recommended Action Investigate any connectivity problems with the AAA servers configured in the first method. Ping the authentication servers from the security appliance. Make sure that the daemons are running on your AAA server.

410001

Error Message `%ASA-4-410001: UDP DNS request from source_interface:source_address/source_port to dest_interface:dest_address/dest_port; (label length | domain-name length) 52 bytes exceeds remaining packet length of 44 bytes.`

Explanation This syslog message is generated when the domain-name length exceeds 255 bytes in a UDP DNS packet. (See RFC 1035, section 3.1.)

Recommended Action None required.

410002

Error Message `%ASA-2-410002: Dropped num DNS responses with mis-matched id in the past sec second(s): from src_ifc:sip/sport to dest_ifc:dip/dport`

Explanation This syslog message is generated when the security device detects an excess number of DNS responses with a mismatched DNS identifier. The threshold is set by the **id-mismatch** DNS policy-map parameter submode command.

- *num*—The number of ID mismatch instances as configured by the **id-mismatch** command.

- *sec*—The duration in seconds as configured by the **id-mismatch** command.
- *src_ifc*—The source interface name at which the DNS message is received with a mismatched DNS identifier.
- *sip*—The source IP address.
- *sport*—The source port.
- *dest_ifc*—The destination interface name.
- *dip*—The destination IP address.
- *dport*—The destination port.

Recommended Action A high rate of mismatched DNS identifiers might indicate an attack on the cache. Check the IP address/port in the syslog message to trace the source of the attack. You can configure ACLs to block traffic permanently from the source.

410003

Error Message `%ASA-4-410003: action_class: action DNS query_response from src_ifc:sip/sport to dest_ifc:dip/dport; further_info`

Explanation This syslog message is generated when a DNS classification is performed on a DNS message and the specified criteria are satisfied. The configured action occurs as a result.

- *action_class*—The "DNS Classification" action class.
- *action*—The action taken: "Dropped," "Dropped (no TSIG)," or "Masked header flags for."
- *query_response*—Either "query" or "response."
- *src_ifc*—The source interface name.
- *sip*—The source IP address.
- *sport*—The source port.
- *dest_ifc*—The destination interface name.
- *dip*—The destination IP address.
- *dport*—The destination port.
- *further_info*—One of the following: "matched Class id: *class_name*," "matched Class id: *match_command*" (for a standalone **match** command), or "TSIG resource record not present" (for system log messages generated by the **tsig enforced** command).

Recommended Action None required.

410004

Error Message `%ASA-6-410004: action_class: action DNS query_response from src_ifc:sip/sport to dest_ifc:dip/dport; further_info`

Explanation This event is generated when a DNS classification is performed on a DNS message and the specified criteria are satisfied.

- *action_class*—The "DNS Classification" action class.
- *action*—The action taken: "Received" or "Received (no TSIG)."
- *query_response*—Either "query" or "response."
- *src_ifc*—The source interface name.
- *sip*—The source IP address.
- *sport*—The source port.
- *dest_ifc*—The destination interface name.
- *dip*—The destination IP address.
- *dport*—The destination port.
- *further_info*—One of the following: "matched Class id: *class_name*," "matched Class id: *match_command*" (for a standalone **match** command), or "TSIG resource record not present" (for system log messages generated by the **tsig enforced** command).

Recommended Action None required.

411001

Error Message `%ASA-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. If *interface_name* is a logical interface name such as "inside" and "outside," this message indicates that the logical interface line protocol has changed from down to up. If *interface_name* is a physical interface name such as "Ethernet0" and "GigabitEthernet0/1," this message indicates that the physical interface line protocol has changed from down to up.

Recommended Action None required.

411002

Error Message `%ASA-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. If *interface_name* is a logical interface name such as "inside" and "outside," this message indicates that the logical interface line protocol has changed from up to down. In this case, the physical interface line protocol

status is not affected. If *interface_name* is a physical interface name such as "Ethernet0" and "GigabitEthernet0/1," this message indicates that the physical interface line protocol has changed from up to down.

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

411003

Error Message `%ASA-4-411003: Configuration status on interface` *`interface_name`* `changed state to downup`

Explanation The configuration status of the interface has changed from down to up.

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

411004

Error Message `%ASA-4-411004: Configuration status on interface` *`interface_name`* `changed state to up`

Explanation The configuration status of the interface has changed from down to up.

Recommended Action None required.

411005

Error Message `%ASA-4-411005: Interface` *`variable 1`* `experienced a hardware transmit hang. The interface has been reset.`

Explanation The interface experienced a hardware transmit hang that required a reset of the ethernet controller to restore the interface to full operation. This is a known issue with Gigabit interfaces on ASA 5510, ASA 5520, ASA 5540, and ASA 5550 devices.

- *variable 1*—The interface name, such as GigabitEthernet0/0

Recommended Action None required.

412001

Error Message %ASA-4-412001:MAC *MAC_address* moved from *interface_1* to *interface_2*

Explanation This message is generated when a host move is detected from one module interface to another. In a transparent security appliance, mapping between the host (MAC) and security appliance port is maintained in a Layer 2 forwarding table. The table dynamically binds packet source MAC addresses to a security appliance port. In this process, whenever movement of a host from one interface to another interface is detected, this message is generated.

Recommended Action The host move might be valid or the host move might be an attempt to spoof host MACs on other interfaces. If it is a MAC spoof attempt, you can either locate vulnerable hosts on your network and remove them or configure static MAC entries, which will not allow MAC address and port binding to change. If it is a genuine host move, none required.

412002

Error Message %ASA-4-412002:Detected bridge table full while inserting MAC *MAC_address* on interface *interface*. Number of entries = *num*

Explanation This message is generated when the bridge table is full and an attempt is made to add one more entry. The security appliance maintains a separate Layer 2 forwarding table per context and the message is generated whenever a context exceeds its size limit. The MAC address will be added, but it will replace the oldest existing dynamic entry (if available) in the table

Recommended Action This might be an attempted attack. Make sure that the new bridge table entries are valid. In case of attack, use EtherType ACLs to access control vulnerable hosts.

413001

Error Message %ASA-4-413001: Module in slot *slotnum* is not able to shut down. Module Error: *errnum message*

Explanation The module in *slotnum* was not able to comply with a request from the ASA system module to shut down. It may be performing a task that could not be interrupted, like a software upgrade. The *errnum* and *message* text describes the reason why the module could not shut down, and recommends the correct action to take.

Recommended Action Wait for the task on the module to complete before shutting down the module, or use the session command to access the CLI on the module, and stop the task that is preventing the module from shutting down.

413002

Error Message `%ASA-4-413002: Module in slot slotnum is not able to reload. Module Error: errnum message`

Explanation The module in *slotnum* was not able to comply with a request from the ASA system module to reload. It may be performing a task that could not be interrupted, like a software upgrade. The *errnum* and *message* text describes the reason why the module could not reload, and the recommended action.

Recommended Action Wait for the task on the module to complete before reloading the module, or use the session command to access the CLI on the module and stop the task that is preventing the module from reloading.

413003

Error Message `%ASA-4-413003: Module in slot slotnum is not a recognized type`

Explanation Generated whenever a card is detected that is not recognized as a valid card type.

Recommended Action Upgrade to a version of security appliance system software that supports the module type installed.

413004

Error Message `%ASA-4-413004: Module in slot slotnum failed to write software vnewver (currently vver), reason. Trying again.`

Explanation The module in the specified slot number failed to accept a software version, and will be transitioned to an UNRESPONSIVE state. Another attempt will be made to update the module software.

- *slotnum*—The slot number containing the module.
- *newver*—The new version number of software that was not successfully written to the module (for example, 1.0(1)0).
- *ver*—The current version number of the software on the module (for example, 1.0(1)0).
- *reason*—The reason the new version could not be written to the module. The possible values for *reason* include the following:

  - write failure.

  - failed to create a thread to write the image.

Recommended Action None required. Subsequent attempts will either generate a message indicating a successful update or failure. You may verify the module transitions to UP after a subsequent update attempt by using the **show module** *slotnum* command.

413005

Error Message `%ASA-1-413005: prod_id Module in slot slot, application is not supported app_name version app_vers type app_type`

Explanation The module installed in slot *slot* is running an unsupported application version or type.

- *prod_id*—Product ID string.
- *slot*—Slot 0 indicates the system main board and slot 1 indicates the module installed in the expansion slot. For this error, the slot number should always be 1.
- *app_name*—Application name (string).
- *app_vers*—Application version (string).
- *app_type*—Application type (decimal).

Recommended Action If the problem persists, contact the Cisco TAC.

413006

Error Message `%ASA-4-413006: prod-id Module software version mismatch; slot slot is prod-id version running-vers. Slot slot prod-id requires required-vers.`

Explanation The version of software running on the module in slot *slot* is not the version required by another module.

- *slot*—Slot 0 indicates the system main board and slot 1 indicates the module installed in the expansion slot.
- *prod_id*—Product Id string for the device installed in slot *slot.*
- *running_vers*—Version of software currently running on the module installed in slot *slot*.
- *required_vers*—Version of software required by the module in slot *slot.*

Recommended Action If the problem persists, contact the Cisco TAC.

414001

Error Message `%ASA-3-414001: Failed to save logging buffer using file name filename to FTP server ftp_server_address on interface interface_name: [fail_reason]`

Explanation This syslog message is generated when logging module failed to save the logging buffer to external FTP server.

Recommended Action Take appropriate action based on the failed reason:

- Protocol error—Make sure no connectivity issue between the FTP server and security appliance, and FTP sever can accept FTP PORT command and put request.
- Invalid username or password—Make sure that the configured FTP client username and password are correct.

- All other errors—If the problem persists, contact the Cisco TAC.

414002

Error Message `%ASA-3-414002: Failed to save logging buffer to flash:/syslog directory using file name: filename: [fail_reason]`

Explanation This syslog message is generated when logging module failed to save the logging buffer to system flash.

Recommended Action If the failed reason is due to insufficient space, check the system flash free space, make sure that the configured limits of the logging flash-size command are set correctly. If the error is a flash file system IO error, then contact the Cisco TAC for assistance.

415001

Error Message `%ASA-6-415001: HTTP - matched matched_string in policy-map map_name, header field count exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when one of the following occurs:

– The total number of fields in the HTTP header exceeds the user-configured number of header fields. The relevant command is: **match** {**request | response**} **header count** *num*.

– The appearance of a specified field in the HTTP header exceeds the user-configured number for this header field.The relevant command is: **match** {**request | response**} **header** *header-name* **count** *num*.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface (for example, DMZ, outside, and so on).
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action Enter the **match** {**request | response**} **header** command to reconfigure the HTTP header field value.

415002

Error Message `%ASA-6-415002: HTTP - matched matched_string in policy-map map_name, header field length exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the specified HTTP header field length exceeds the user-configured length.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface (for example, DMZ, outside, and so on).
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action Enter the **match** {**request** | **response**} **header** *header_name* **length gt** *num* command to change the HTTP header field length.

415003

Error Message `%ASA-6-415003: HTTP - matched matched_string in policy-map map_name, body length exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the length of the message body exceeds user-configured length.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface (for example, DMZ, outside, and so on).
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action Enter the **match** {**request** | **response**} **body length gt** *num* command to change the length of the message body.

415004

Error Message `%ASA-5-415004: HTTP - matched matched_string in policy-map map_name, content-type verification failed connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the "magic number" in the body of the HTTP message is not the correct magic number for the mime-type specified in the "content-type" field in the HTTP message header.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface (for example, DMZ, outside, and so on).
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action Enter the **match {request | response} header content-type violation** command to correct the error.

415005

Error Message `%ASA-5-415005: HTTP - matched matched_string in policy-map map_name, URI length exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the length of the URI exceeds the user-configured length.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface, for example, DMZ, outside, and so on.
- *IP_address*—The IP address of the interface.

- *port_num*—The port number.

Recommended Action Enter the **match request uri length gt** *num* command to change the length of the URI.

415006

Error Message `%ASA-5-415006: HTTP - matched matched_string in policy-map map_name, URI matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the URI matches the regular expression that the user configured. See the **match request uri regex** {*regex-name* | **class** *class-name*} command for more information.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface, for example, DMZ, outside, and so on.
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action None required.

415007

Error Message `%ASA-5-415007: HTTP - matched matched_string in policy-map map_name, Body matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the message body matches the regular expression that the user configured. See the **match** {**request** | **response**} **body regex** {*regex-name* | **class** *class-name*} command for more information.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."

- *interface_type*—The type of interface (for example, DMZ, outside, and so on).
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action None required.

415008

Error Message `%ASA-5-415008: HTTP - matched matched_string in policy-map map_name, header matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when a value in a user-specified field in the message header matches the regular expression that the user configured. See the **match** {**request** | **response** } **header** *header-field-name* {*regex-name* | **class** *class-name*} command for more information.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface (for example, DMZ, outside, and so on).
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action None required.

415009

Error Message `%ASA-5-415009: HTTP - matched matched_string in policy-map map_name, method matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the HTTP method matches the user-configured regular expression. See the **match request method** {*regex-name* | **class** *class-name*} command for more information.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.

- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface (for example, DMZ, outside, and so on).
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action None required.

415010

Error Message `%ASA-5-415010: matched matched_string in policy-map map_name, transfer encoding matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is issued when the value in the "transfer encoding" field matches the user-configured regular expression or keyword. See the **match** {**request** | **response**} **header transfer-encoding** {{*regex-name* | **class** *class-name*} | **keyword**} command for more information.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.
- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface (for example, DMZ, outside, and so on).
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action None required.

415011

Error Message `%ASA-5-415011: HTTP - policy-map map_name:Protocol violation connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the HTTP parser cannot detect a valid HTTP message in the first few bytes of an HTTP message.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface (for example, DMZ, outside, and so on).
- *IP_address*—The IP address of the interface.

- *port_num*—The port number.

Recommended Action Enter the **protocol-violation action** {**drop** | **reset**} **log** command to correct the problem.

415012

Error Message `%ASA-5-415012: HTTP - matched matched_string in policy-map map_name, Unknown mime-type connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the "content-type" field does not contain a mime type that matches a built-in MIME type.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"- Dropping connection" or "- Resetting connection."
- *interface_type*—The type of interface, for example, DMZ, outside, and so on.
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action Enter the **match** {**request** | **response**} **header content-type unknown** command to correct the problem.

415013

Error Message `%ASA-5-415013: HTTP - policy-map map-name: Malformed chunked encoding connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when a chunked encoding is malformed and the HTTP message cannot be parse, and whenever logging for the **protocol-violation** command is configured.

- *map-name*— The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface, for example, DMZ, outside, and so on.
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action Enter the **protocol-violation action** {**drop** | **reset**} **log** command to correct the problem.

415014

Error Message `%ASA-5-415014: HTTP - matched matched_string in policy-map map_name, Mime-type in response wasn't found in the accept-types of the request connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the mime type in an HTTP response is not in the "accept" field of the request.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface, for example, DMZ, outside, and so on.
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action Enter the **match req-resp content-type mismatch** command to correct the problem.

415015

Error Message `%ASA-5-415015: HTTP - matched matched_string in policy-map map_name, transfer-encoding unknown connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the an empty transfer encoding occurs.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface, for example, DMZ, outside, and so on.
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action Enter the **match** {**request** | **response**} **header transfer-encoding empty** command to correct the problem.

415016

Error Message %ASA-4-415016: policy-map *map_name*:Maximum number of unanswered HTTP requests exceeded *connection_action* from *int_type*:*IP_address*/*port_num* to *int_type*:*IP_address*/*port_num*

Explanation This syslog message is generated when the number of unanswered HTTP requests exceeds the internal number of requests allowed.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface, for example, DMZ, outside, and so on.
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action Enter the **protocol-violation action** {**drop** | **reset**} **log** command to correct the problem.

415017

Error Message %ASA-6-415017: HTTP - *matched_string* in policy-map *map_name*, arguments matched *connection_action* from *int_type*:*IP_address*/*port_num* to *int_type*:*IP_address*/*port_num*

Explanation This syslog message is generated when a pattern in the arguments matches the user-configured regular expression or keyword. See the **match request args regex** {*regex-name* | **class** *class-name*} command for more information.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface, for example, DMZ, outside, and so on.
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action None required.

415018

Error Message `%ASA-5-415018: HTTP - matched matched_string in policy-map map_name, Header length exceeded connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the total header length exceeds the user-configured length for the header.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface, for example, DMZ, outside, and so on.
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action Enter the **match** {**request** | **response**} **header length gt** *num* command to reduce the length of the header.

415019

Error Message `%ASA-5-415019: HTTP - matched matched_string in policy-map map_name, status line matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when the status line in a response matches user-configured regex. See the **match response status-line regex** {*regex-name* | **class** *class-name*} for more information.

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface, for example, DMZ, outside, and so on.
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action None required.

415020

Error Message `%ASA-5-415020: HTTP - matched matched_string in policy-map map_name, a non-ASCII character was matched connection_action from int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation This syslog message is generated when a non-ASCII character is found.

Explanation

- *matched_string*—The matched string is one of the following:

  - The class map ID, followed by the name of the class map. This string displays when the class map is user configured.

  - The actual **match** command that initiated the syslog message. This string displays when the class map is internal.

- *map_name*—The name of the policy map.
- *connection_action*—"Dropping connection" or "Resetting connection."
- *interface_type*—The type of interface, for example, DMZ, outside, and so on.
- *IP_address*—The IP address of the interface.
- *port_num*—The port number.

Recommended Action Enter the **match** {**request** | **response**} **header non-ascii** command to correct the problem.

416001

Error Message `%ASA-4-416001: Dropped UDP SNMP packet from source_interface:source_IP/source_port to dest_interface:dest_address/dest_port; version (prot_version) is not allowed through the firewall`

Explanation An SNMP packet was denied passage through the security appliance because of a bad packet format or because the *prot_version* is not allowed through the security appliance. The field *prot_version* can be one of the following values: 1, 2, 2c, or 3.

Recommended Action Change the settings for SNMP inspection using the **snmp-map** command, which allows the user to permit or deny specific protocol versions.

417001

Error Message `%ASA-4-417001: Unexpected event received: number`

Explanation A process received a signal, but no handler was found for the event.

Recommended Action If the problem persists, contact the Cisco TAC.

417004

Error Message `%ASA-4-417004: Filter violation error: conn number (string:string) in string`

Explanation A client tried to modify a route attribute that the client does not own.

Recommended Action If the problem persists, contact the Cisco TAC.

417006

Error Message `%ASA-4-417006: No memory for string) in string. Handling: string`

Explanation An operation failed because of low memory, but will be handled with another mechanism.

Recommended Action If the problem persists, contact the Cisco TAC.

417008

Error Message `%ASA-2-417008: AutoRP: discard %s embedded group %i/%i on interface %s from %i due to overlap %i/%i\n`

Explanation The multicast boundary has a longer network mask that the AutoRP encoded group.

- First *%s*—The announcement or discovery.
- *%i*—The IPv4 address.
- Second *%s*—The interface name.

Recommended Action Adjust the boundary access rules or RP mappings.

417009

Error Message `%ASA-2-417009: AutoRP: discard %s on interface %s from %i due to zero group count\n`

Explanation The security appliance received an AutoRP packet with an RP mapping with no group.

- First *%s*—The announcement or discovery.
- *%i*—The IPv4 address.
- Second *%s*—The interface name.

Recommended Action The originating device may not be RFC compliant. Upgrade the device or notify the device owner.

418001

Error Message `%ASA-4-418001: Through-the-device packet to/from management-only network is denied: protocol_string from interface_name IP_address (port) to interface_name IP_address (port)`

Explanation A packet from the specified source to the destination is dropped, because it is traversing the security appliance to/from the management-only network.

- *protocol_string*—TCP, UDP, ICMP, or protocol ID as a decimal number.
- *interface_name*— Interface name.
- *IP_address*—IP address.
- *port*—Port number.

Recommended Action Investigate who is generating such a packet and why.

419001

Error Message `%ASA-4-419001: Dropping TCP packet from src_ifc:src_IP/src_port to dest_ifc:dest_IP/dest_port, reason: MSS exceeded, MSS size, data size`

Explanation This message is generated when the length of the TCP packet exceeds the MSS advertised in the three-way handshake.

- *src_ifc*—Input interface name.
- *src_IP*—The source IP address of the packet.
- *src_port*—The source port of the packet.
- *dest_ifc*—The output interface name.
- *dest_IP*—The destination IP address of the packet.
- *dest_port*—The destination port of the packet.

Recommended Action If there is a need to allow packets that exceed the MSS, create a TCP map using the **exceed-mss** command, as in the following example:

```
access-list http-list permit tcp any host server_ip eq 80

class-map http
 match access-list http-list

tcp-map tmap
 exceed-mss allow

policy-map global_policy
 class http
  set connection advanced-options tmap
```

419002

Error Message `%ASA-4-419002: Received duplicate TCP SYN from in_interface:src_address/src_port to out_interface:dest_address/dest_port with different initial sequence number.`

Explanation A duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number than the SYN that opened the embryonic connection. This could indicate that SYNs are being spoofed. This message occurs in Release 7.0.4.1 and later.

- *in_interface*—The input interface.
- *src_address*—The source IP address of the packet.
- *src_port*—The source port of the packet.
- *out_interface*—The output interface.
- *dest_address*—The destination IP address of the packet.
- *dest_port*—The destination port of the packet.

Recommended Action None required.

419003

Error Message `%ASA-4-419003: Cleared TCP urgent flag from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port.`

Explanation A duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number than the SYN that opened the embryonic connection. This could indicate that SYNs are being spoofed. This message occurs in Release 7.0.4.1 and later.

- *in_ifc*—The input interface
- *src_ip*—The source IP address of the packet
- *src_port*—The source port of the packet
- *out_ifc*—The output interface
- *dest_ip*—The destination IP address of the packet
- *dest_port*—The destination port of the packet

Recommended Action If users need to keep the urgent flag in TCP headers, they can use "**urgent-flag allow**" command in TCP map configuration.

420001

Error Message `%ASA-3-420001: IPS card not up and fail-close mode used, dropping ICMP packet ifc_in:SIP to ifc_out:DIP (type ICMP_TYPE, code ICMP_CODE)"`

`%ASA-3-420001: IPS card not up and fail-close mode used, dropping TCP packet from ifc_in:SIP/SPORT to ifc_out:DIP/DPORT\n"`

```
%ASA-3-420001: IPS card not up and fail-close mode used, dropping UDP packet from
ifc_in:SIP/SPORT to ifc_out:DIP/DPORT\n"
%ASA-3-420001: IPS card not up and fail-close mode used, dropping protocol protocol
packet from ifc_in:SIP to ifc_out:DIP\n"
```

Explanation This message is displayed when packets are dropped when IPS fail-close mode is used and the IPS card is not up. This message is rate limited.

- *ifc_in*—Input interface name.
- *ifc_out*—Output interface name.
- *SIP*—Source IP of the packet.
- *SPORT* —Source port of the packet.
- *DIP*—Destination IP of the packet.
- *DPORT* —Destination port of the packet.
- *ICMP_TYPE*—Type of the ICMP packet.
- *ICMP_CODE*—Code of the ICMP packet.

Recommended Action Check and bring up the IPS card.

420002

Error Message `%ASA-4-420002: IPS requested to drop ICMP packets ifc_in:SIP to ifc_out:DIP (type ICMP_TYPE, code ICMP_CODE)"`

```
%ASA-4-420002: IPS requested to drop TCP packet from ifc_in:SIP/SPORT to
ifc_out:DIP/DPORT\n"
%ASA-4-420002: IPS requested to drop UDP packet from ifc_in:SIP/SPORT to
ifc_out:DIP/DPORT\n"
%ASA-4-420002: IPS requested to drop protocol packet from ifc_in:SIP to
ifc_out:DIP\n"
```

Explanation This message is displayed when IPS requests that the packet be dropped.

- *ifc_in*—Input interface name.
- *ifc_out*—Output interface name.
- *SIP*—Source IP of the packet.
- *SPORT* —Source port of the packet.
- *DIP*—Destination IP of the packet.
- *DPORT* —Destination port of the packet.
- *ICMP_TYPE*—Type of the ICMP packet.
- *ICMP_CODE*—Code of the ICMP packet.

Recommended Action None required.

420003

Error Message `%ASA-4-420003: IPS requested to reset TCP connection from` *`ifc_in:SIP/SPORT`* `to` *`ifc_out:DIP/DPORT`*"

Explanation This message is displayed when IPS requests to reset a TCP connection.

- *ifc_in*—Input interface name.
- *ifc_out*—Output interface name.
- *SIP*—Source IP of the packet.
- *SPORT*—Source port of the packet.
- *DIP*—Destination IP of the packet.
- *DPORT*—Destination port of the packet.

Recommended Action None required.

420004

Error Message `%ASA-6-420004: Virtual Sensor` *`sensor_name`* `was added on the AIP SSM\`*`n`*

Explanation A virtual sensor was added on the AIP SSM card.

- *n*—SSM card number.

Recommended Action None required.

420005

Error Message `%ASA-6-420005: Virtual Sensor` *`sensor_name`* `was deleted from the AIP SSM\`*`n`*

Explanation A virtual sensor was deleted from the AIP SSM card.

- *n*—SSM card number

Recommended Action None required.

420006

Error Message `%ASA-3-420006: Virtual Sensor not present and fail-close mode used, dropping` *`protocol`* `packet from` *`ifc_in:SIP/SPORT`* `to` *`ifc_out:DIP/DPORT\n`*

Explanation This message is displayed when packets are dropped when IPS fail-close mode is used and the virtual sensor used for the packet is not present.

- *ifc_in*—Input interface name.

- *ifc_out*—Output interface name.
- *SIP*—Source IP of the packet.
- *SPORT*—Source port of the packet.
- *DIP*—Destination IP of the packet.
- *DPORT*—Destination port of the packet.

Recommended Action Check and add the virtual sensor.

421001

Error Message `%ASA-3-421001: TCP|UDP flow from interface_name:ip/port to interface_name:ip/port is dropped because application has failed.`

Explanation A packet was dropped because the CSC SSM application failed. By default, this message is rate limited to 1 message every 10 seconds.

- *interface_name*—The interface name.
- *IP_address*—The IP address.
- *port*—The port number.
- *application*—The CSC SSM is the only application supported in the current release.

Recommended Action Immediately investigate the problem with the service module.

421002

Error Message `%ASA-6-421002: TCP|UDP flow from interface_name:IP_address/port to interface_nam:IP_address/port bypassed application checking because the protocol is not supported.`

Explanation The connection bypassed service module security checking because the protocol it is using cannot be scanned by the service module. For example, the CSC SSM is not capable of scanning Telnet traffic. If a user configures Telnet traffic to be scanned, the traffic will bypass the scanning service. By default, this message is rate limited to 1 message every 10 seconds.

- *IP_address*—The IP address.
- *port*—The port number.
- *interface_name*—The name of the interface on which the policy is applied.
- *application*—The CSC SSM is the only application supported in the current release.

Recommended Action The configuration should be modified to only include protocols that are supported by the service module.

421003

Error Message `%ASA-3-421003: Invalid data plane encapsulation.`

Explanation A packet injected by the service module did not have the correct data plane header. Packets exchanged on data backplane adhere to a Cisco proprietary protocol called ASDP. Any packet that does not have the correct ASDP header is dropped.

Recommended Action Use the **capture** *name* **type asp-drop** [**ssm-asdp-invalid-encap**] command to capture the offending packets and contact the Cisco TAC.

421004

Error Message `%ASA-7-421004: Failed to inject {TCP|UDP} packet from IP_address/port to IP_address/port`

Explanation The security appliance has failed to inject a packet as instructed by the service module. This could happen if the security appliance tries to inject a packet into a flow that has already been released.

- *IP_address*—The IP address.
- *port*—The port number.

Recommended Action This could happen because the security appliance maintains its connection table independently from the service module. Normally it will not cause any problem. If this affects security appliance performance or if the problem persists, contact the Cisco TAC.

421005

Error Message `%ASA-6-421005: interface_name:IP_address is counted as a user of application`

Explanation A host has been counted toward the license limit. The specified host was counted as a user of *application*. The total number of users in 24 hours is calculated at midnight for license validation.

- *interface_name*—The interface name.
- *IP_address*—The IP address.
- *application*—The CSC SSM is the only application supported in the current release.

Recommended Action None required. However, if the overall count exceeds the user license you have purchased, contact Cisco to upgrade your license.

421006

Error Message `%ASA-6-421006: There are number users of application accounted during the past 24 hours.`

Explanation Identifies the total number of users who have used *application* for the past 24 hours. This message is generated every 24 hours to give the total number of hosts that have used services provided by the service module.

Recommended Action None required. However, if the overall count exceeds the user license you have purchased, contact Cisco to upgrade your license.

421007

Error Message `%ASA-3-421007: TCP|UDP flow from interface_name:IP_address/port to interface_name:IP_address/port is skipped because application has failed.`

Explanation This message is generated when a flow is skipped because the service module application has failed. By default, this message is rate limited to 1 message every 10 seconds.

- *IP_address*—The IP address.
- *port*—The port number.
- *interface_name*—The name of the interface on which the policy is applied.
- *application*—The CSC SSM is the only application supported in the current release.

Recommended Action Immediately investigate the problem with the service module.

422004

Error Message `%ASA-4-422004: IP SLA Monitor number0: Duplicate event received. Event number number1`

Explanation The IP SLA monitor process has received a duplicate event. Currently, this message applies to destroy events. Only one destroy request will be applied.

- *number0*—The SLA operation number.
- *number1*—The SLA operation event ID.

Recommended Action This is only a warning message. If this reoccurs, enter the **show sla monitor configuration** *SLA_operation_id* command and copy the output of the command. Copy the message as it appears on the console or in the system log. Then contact Cisco TAC and provide the representative with the information you gathered, along with information about the application that is configuring and polling the SLA probes.

422005

Error Message `%ASA-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.`

Explanation One or more IP SLA monitor probes could not be scheduled because the system clock is not set.

Recommended Action Ensure that the system clock is functional by using NTP or another mechanism.

422006

Error Message `%ASA-4-422006: IP SLA Monitor Probe number: string`

Explanation The IP SLA monitor probe could not be scheduled. Either the configured starting time has already occurred or the starting time is invalid.

- *number*—The SLA operation ID.
- *string*—A string describing the error.

Recommended Action Reschedule the failed probe with a valid start time.

423001

Error Message `%ASA-4-423001: {Allowed | Dropped} invalid NBNS pkt_type_name with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port.`

Explanation The NBNS packet format is incorrect.

Recommended Action None required.

423002

Error Message `%ASA-4-423002: {Allowed | Dropped} mismatched NBNS pkt_type_name with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port.`

Explanation There is an NBNS ID mismatch.

Recommended Action None required.

423003

Error Message %ASA-4-423003: {Allowed | Dropped} invalid NBDGM *pkt_type_name* with *error_reason_str* from *ifc_name*:*ip_address*/*port* to *ifc_name*:*ip_address*/*port*.

Explanation The NBDGM packet format is incorrect.

Recommended Action None required.

423004

Error Message %ASA-4-423004: {Allowed | Dropped} mismatched NBDGM *pkt_type_name* with *error_reason_str* from *ifc_name*:*ip_address*/*port* to *ifc_name*:*ip_address*/*port*.

Explanation There is an NBDGM ID mismatch.

Recommended Action None required.

423005

Error Message %ASA-4-423005: {Allowed | Dropped} NBDGM *pkt_type_name* fragment with *error_reason_str* from *ifc_name*:*ip_address*/*port* to *ifc_name*:*ip_address*/*port*.

Explanation The NBDGM fragment format is incorrect.

Recommended Action None required.

424001

Error Message %ASA-4-424001: Packet denied *protocol_string intf_in*:*src_ip*/*src_port intf_out*:*dst_ip*/*dst_port*. [Ingress|Egress] interface is in a backup state.

Explanation A packet was dropped because it was traversing the security appliance to/from a redundant interface. Interface functionality is limited on low-end platforms. The interface specified by the **backup interface** command can only be a backup for the primary interface configured. If the default route to the primary interface is up, any traffic through the device from the backup interface will be denied. Conversely, if the default route to the primary interface is down, traffic through the device from the primary interface will be denied.

- *protocol_string*—The protocol string; for example, TCP or the protocol ID (a decimal number).
- *intf_in*—The input interface name.
- *src_ip*—The source IP address of the packet.
- *src_port*—The source port of the packet.
- *intf_out*—The output interface name.

- *dst_ip*—The destination IP address of the packet.
- *dst_port*—The destination port of the packet.

Recommended Action Investigate the source of the denied packet.

424002

Error Message `%ASA-4-424002: Connection to the backup interface is denied: protocol_string intf:src_ip/src_port intf:dst_ip/dst_port`

Explanation A connection was dropped because it is in a backup state. Interface functionality is limited on low-end platforms. The backup interface can only be a backup for the primary interface specified by the **backup interface** command. If the default route to the primary interface is up, any connection to the security appliance through the backup interface will be denied. Conversely, if the default route to the primary interface is down, connections to the security appliance through the primary interface will be denied.

- *protocol_string*—The protocol string; for example, TCP or protocol ID (a decimal number).
- *intf_in*—The input interface name.
- *src_ip*—The source IP address of the packet.
- *src_port*—The source port of the packet.
- *intf_out*—The output interface name.
- *dst_ip*—The destination IP address of the packet.
- *dst_port*—The destination port of the packet.

Recommended Action Investigate the source of the denied packet.

425001

Error Message `%ASA-6-425001 Redundant interface redundant_interface_name created.`

Explanation This message indicates the specified redundant interface is created in the configuration.

- *redundant_interface_name*—Redundant interface name.

Recommended Action None required.

425002

Error Message `%ASA-6-425002 Redundant interface redundant_interface_name removed.`

Explanation This message indicates the specified redundant interface is removed from the configuration.

- *redundant_interface_name*—Redundant interface name.

Recommended Action None required.

425003

Error Message `%ASA-6-425003 Interface interface_name added into redundant interface redundant_interface_name.`

Explanation This message indicates the specified physical interface is added into the specified redundant interface as a member interface.

- *interface_name*—An interface name.
- *redundant_interface_name*—Redundant interface name.

Recommended Action None required.

425004

Error Message `%ASA-6-425004 Interface interface_name removed from redundant interface redundant_interface_name.`

Explanation This message indicates the specified redundant interface is removed from the specified redundant interface.

- *interface_name*—An interface name.
- *redundant_interface_name*—Redundant interface name.

Recommended Action None required.

425005

Error Message `%ASA-5-425005 Interface interface_name become active in redundant interface redundant_interface_name`

Explanation Within a redundant interface, one member interface is the active member. Traffic only passes through the active member interface. This message indicates the specified physical interface becomes the active member of the specified redundant interface. Member interface switchover occurs when one of the following is true:

- EXEC command **redundant-interface interface-name active-member interface-name** was executed.
- Active member interface is down while the standby member interface is up.
- Standby member interface becomes up (from down) while the active member interface remains down.

- *interface_name*—An interface name.
- *redundant_interface_name*—Redundant interface name.

Recommended Action Check the status of the member interfaces.

425006

Error Message `%ASA-3-425006 Redundant interface redundant_interface_name switch active member to interface_name failed.`

Explanation This message indicates there is an error when member interface switchover was attempted.

- *redundant_interface_name*—Redundant interface name.
- *interface_name*—An interface name.

Recommended Action If the problem persists, contact the Cisco TAC.

431001

Error Message `%ASA-4-431001: RTP conformance: Dropping RTP packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, Drop reason: drop_reason value`

Explanation The RTP packet was dropped.

- *in_ifc*—The input interface.
- *src_ip*—The source IP address of the packet.
- *src_port*—The source port of the packet.
- *out_ifc*—The output interface.
- *dest_ip*—The destination IP address of the packet.

- *dest_port*—The destination port of the packet.
- *drop_reason*—One of the following drop reasons:
  - Incorrect version *value*—The version number from the packet is incorrect.
  - Invalid payload-type *value*—The payload type from the packet is invalid.
  - Incorrect SSRC *value*—The SSRC from the packet is incorrect.
  - Out-of-range sequence number *value* sequence number from the packet.
  - Out of sequence in packet in probation *value* sequence number from the packet.

Recommended Action Examine the dropped RTP packets to determine which field the RTP source is setting incorrectly. Also examine the source to verify that it is legitimate and not an attacker trying to misuse an opening in the security appliance.

428001

Error Message `%ASA-6-428001: WAAS confirmed from in_interface:src_ip_addr/src_port to out_interface:dest_ip_addr/dest_port, inspection services bypassed on this connection.`

Explanation This syslog message is generated when WAAS optimization is detected on a connection. All L7 inspection services, including IPS, are bypassed on WAAS-optimized connections.

Recommended Action None required if the network contains WAE devices; otherwise, the network administrator should investigate the use of the WAAS option on this connection.

431002

Error Message `%ASA-4-431002: RTCP conformance: Dropping RTCP packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, Drop reason: drop_reason value`

- *in_ifc*—The input interface.
- *src_ip*—The source IP address of the packet.
- *src_port*—The source port of the packet.
- *out_ifc*—The output interface.
- *dest_ip*—The destination IP address of the packet.
- *dest_port*—The destination port of the packet.
- *drop_reason*—One of the following drop reasons:
  - Incorrect version *value*—The version number from the packet is incorrect.
  - Invalid payload-type *value*—The payload type from the packet is incorrect.

Recommended Action Examine the dropped RTP packets to determine which field the RTP source is setting incorrectly. Also examine the source to verify that it is legitimate and not an attacker trying to misuse an opening in the security appliance.

444004

Error Message `%ASA-2-444004: Temporary license key key has expired. Applying permanent license key permkey.`

Explanation The temporary license that was installed has expired. The features that the license provided are no longer available.

- *key*—The temporary activation key.
- *permkey*—The permanent license key.

Recommended Action Purchase and install a permanent license.

444005

Error Message `%ASA-4-444005: Temporary license key key will expire in days days.`

Explanation The temporary license will expire in the specified time. After that date, the features that the license provided will no longer be available.

- *key*—The temporary activation key.
- *days*—The number of days left before license expiration.

Recommended Action Purchase and install a permanent license before the temporary license expires.

446001

Error Message `%ASA-4-446001: Maximum TLS Proxy session limit of max_sess reached.`

Explanation A configured maximum session limit for TLS proxy was reached. New sessions beyond the limit were denied.

- *max_sess*—The currently effective maximum session limit.

Recommended Action If more TLS sessions are needed, use the **tls-proxy maximum-sessions <max_sess>** command to increase the limit. Alternatively, you can use the **tls-proxy <proxy_name>** and **tls-proxy maximum-sessions <max_sess>** commands, and then reboot for the command to take effect.

447001

Error Message `%ASA-4-447001: ASP DP to CP queue_name was full. Queue length length, limit limit`

Explanation This message indicates a particular data path (DP) to control point (CP) event queue is full, and one or more multiple enqueue actions have failed. If the event contains a packet block, such as for CP application inspection, the packet will be dropped by the DP, and a counter from the **show asp drop** command will increment. If the event is for punt to CP, a typical counter is the Punt no memory ASP-drop counter.

- *queue*—The name of the DP-CP event queue.
- *length*—The current number of events on the queue.
- *limit*—The maximum number of events that are allowed on the queue.

Recommended Action The queue-full condition reflects the fact that the load on the CP has exceeded the CP processing ability, which may or may not be a temporary condition. You should consider reducing the feature load on the CP if this message appears repeatedly. Use the **show asp event dp-cp** command to identify the features that contribute the most load on the event queue.

450001

Error Message `ASA-4-450001: Deny traffic for protocol protocol_id src interface_name:IP_address/port dst interface_name:IP_address/port, licensed host limit of num exceeded.`

Explanation The licensed host limit was exceeded. This message applies to the ASA 5505 adaptive security appliance only.

- *protocol_id*—The protocol ID number.
- *interface_name*—The interface associated with the sender and receiver of the packet.
- *IP_address*—The IP address of the sender and receiver of the packet.
- *port*—The port number of the packet transmitted.
- *num*—The maximum host limit value.

Recommended Action None required.

Messages 500001 to 509001

This section contains messages from 500001 to 509001.

500001

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

Explanation This message is displayed after you turn on the **activex** option using the **filter** command, and the security appliance detects an ActiveX object. The **activex** option allows the security appliance 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 `%ASA-5-500002: Java content modified src IP_address dest IP_address on interface interface_name.`

Explanation This message is displayed after you turn on the **java** option using the **filter** command, and the security appliance detects an Java applet. The **java** option allows the security appliance 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 `%ASA-5-500003: Bad TCP hdr length (hdrlen=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 resets (RSTs) correctly when responding to a connection request to a disabled socket. If a client tries to connect to an FTP server outside the security appliance 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, which results in a negative number of bytes being transferred. A negative number is displayed by syslog message as an unsigned number, which makes it appear much larger than it would be normally; for example, it may show 4 GB transferred in 1 second.

Recommended Action None required. This message should occur infrequently.

500004

Error Message `%ASA-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* value is 6 for TCP and 17 for UDP.

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

500005

Error Message `%ASA-3-500005: connection terminated for `*`protocol`*` from `*`in_ifc_name`*`:`*`src_address`*`/`*`src_port`*` to `*`out_ifc_name`*`:`*`dest_address`*`/`*`dest_port`*` due to invalid combination of inspections on same flow. Inspect `*`inspect_name`*` is not compatible with inspect `*`filter_name`*`.`

Explanation This message is generated when a connection matched with single or multiple inspection and/or single or multiple filter features that are not allowed to be applied to the same connection.

- *protocol*—The name of the protocol.
- *in_ifc_name*—The input interface name.
- *src_address*—The source IP address of the connection.
- *src_port*—The source port of the connection.
- *out_ifc_name*—The output interface name.
- *dest_address*—The destination IP address of the connection.
- *dest_port*—The destination port of the packet.
- *inspect_name_1*—The inspect or filter feature name.
- *filter_name*—The filter feature name.

Recommended Action Review the **class-map**, **policy-map**, **service-policy**, and/or **filter** command configurations that are causing the referenced inspection and/or filter features that are matched for the connection. The rules for inspection and filter feature combinations for a connection are as follows:

- The **inspect http [http-policy-map]** and/or **filter url** and/or **filter http** and/or **filter java** and/or **filter activex** commands are valid.
- The **inspect ftp [ftp-policy-map]** and/or **filter ftp** commands are valid.
- The **inspect im** command with any other **inspect** command is allowed, but other inspection functionality takes precedence over the **inspect im** command.

Besides these listed combinations, any other inspection and/or filter feature combinations are not valid.

501101

Error Message `%ASA-5-501101: User transitioning priv level`

Explanation The privilege level of a command was changed.

Recommended Action None required.

502101

Error Message `%ASA-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 `%ASA-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 `%ASA-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.

502111

Error Message `%ASA-5-502111: New group policy added: name: policy_name Type: policy_type`

Explanation This is an indication that a group policy has been configured using the **group-policy** CLI command. *policy_name* is the name of the group policy. *policy_type* is either "internal" or "external."

Recommended Action None required.

502112

Error Message `%ASA-5-502112: Group policy deleted: name: policy_name Type: policy_type`

Explanation A group policy has been removed using the **group-policy** CLI command. *policy_name* is the name of the group policy. *policy_type* is either "internal" or "external."

Recommended Action None required.

503001

Error Message `%ASA-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 If the problem persists, contact the Cisco TAC.

504001

Error Message `%ASA-5-504001: Security context context_name was added to the system`

Explanation A security context was successfully added to the system.

Recommended Action None required.

504002

Error Message `%ASA-5-504002: Security context context_name was removed from the system`

Explanation A security context was successfully removed from the system.

Recommended Action None required.

505001

Error Message `%ASA-5-505001: Module in slot slotnum is shutting down. Please wait...`

Explanation This message is generated when a card is being shut down.

Recommended Action None required.

505002

Error Message `%ASA-5-505002: Module in slot slotnum is reloading. Please wait...`

Explanation This message is generated when a card is being reloaded.

Recommended Action None required.

505003

Error Message `%ASA-5-505003: Module in slot slotnum is resetting. Please wait...`

Explanation This message is generated when a module is being reset.

Recommended Action None required.

505004

Error Message `%ASA-5-505004: Module in slot slotnum shutdown is complete.`

Explanation This message is generated when a module has been shut down.

Recommended Action None required.

505005

Error Message `%ASA-5-505005: Module in slot slotnum is initializing control communication. Please wait...`

Explanation This message is generated when a module has been detected and the ASA system module is initializing control channel communication with it.

Recommended Action None required.

505006

Error Message `%ASA-5-505006: Module in slot slotnum is Up.`

Explanation This message is generated when a module has completed control channel initialization and is in the UP state.

Recommended Action None required.

505007

Error Message `%ASA-5-505007: Module in slot slotnum is recovering. Please wait...`

Explanation This message is generated when a module is being recovered with the **hw-module module** *slotnum* **recover boot** command.

Recommended Action None required.

505008

Error Message `%ASA-5-505008: Module in slot slotnum software is being updated to vnewver (currently vver)`

Explanation This message appears when the 4GE SSM module software is being upgraded by the system module.

- *slotnum*—The slot number containing the module.
- *newver*—The new version number of software that was not successfully written to the module (for example, 1.0(1)0).
- *ver*—The current version number of the software on the module (for example, 1.0(1)0).

Recommended Action None required. The update is proceeding normally.

505009

Error Message `%ASA-5-505009: Module in slot slotnum software was updated to vnewver (previously ver)`

Explanation :This message appears when the 4GE SSM module software is successfully upgraded by the system module.

- *slotnum*—The slot number containing the module.
- *newver*—The new version number of software that was not successfully written to the module (for example, 1.0(1)0).
- *ver*—The current version number of the software on the module (for example, 1.0(1)0).

Recommended Action None required. The update has completed successfully.

505010

Error Message `%ASA-5-505010: Module in slot slot data channel communication is UP.`

Explanation This message is generated whenever the data channel communication recovers from a DOWN state. This message indicates that data channel communication is operating normally. It occurs after the data channel communication fails and then recovers.

- *slot*—The slot that has established data channel communication.

Recommended Action None required unless this message was generated as a result of a previous data channel communication failure (message 3-323006). In that case, check the 4GE SSM messages to determine the cause of the communication failure.

505011

Error Message `%ASA-5-505011: Module in slot slot, application detected application, version version.`

Explanation A new application was detected on a 4GE SSM. This may occur when the system boots, when the 4GE SSM boots, or when the 4GE SSM starts a new application.

- *slot*—The slot in which the application was detected.
- *application*—The name of the application detected.
- *version*—The application version detected.

Recommended Action None required if the activity described is normal and expected.

505012

Error Message `%ASA-5-505012: Module in slot slot, application stopped application, version version`

Explanation This message is generated whenever an application is stopped or removed from a 4GE SSM. This may occur when the 4GE SSM upgrades an application or when an application on the 4GE SSM is stopped or uninstalled.

- *slot*—The slot in which the application was stopped.
- *application*—The name of the application stopped.
- *version*—The application version stopped.

Recommended Action If an upgrade was not occurring on the 4GE SSM or the application was not intentionally stopped or uninstalled, review the logs from the 4GE SSM to determine why the application stopped.

505013

Error Message `%ASA-5-505013: Module in slot slot application changed from: application version version to: newapplication version newversion.`

Explanation This message is generated whenever an application version changes, such as after an upgrade. This occurs when a software update for the application on the module is complete.

- *slot*—The slot in which the application was upgraded.
- *application*—The name of the application that was upgraded.
- *version*—The application version that was upgraded.
- *slot*—The slot in which the application was upgraded.
- *application*—The name of the application that was upgraded.
- *version*—The application version that was upgraded.
- *newapplication*—The new application name.
- *newversion*—The new application version.

Recommended Action Verify that the upgrade was expected and that the new version is correct.

505014

Error Message `%ASA-1-505014: prod_id Module in slot slot, application down name, version version reason`

Explanation The application running on the module in slot *slot* is disabled.

- *prod_id*—Product ID string for the device installed in slot *slot.*

- *slot*—Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- *name*—Application name (string).
- *application*—The name of the application that was upgraded.
- *version*—The application version (string).
- *reason*—Failure reason (string).

Recommended Action If the problem persists, contact the Cisco TAC.

505015

Error Message `%ASA-1-505015: SSM model Module in slot number, application up application, version version`

Explanation The application running on the SSM in slot *number* is up and running.

- *SSM model*—The SSM model for the device installed in slot *number.*
- *number*—Slot 0 indicates the system main board, and slot 1 indicates the SSM installed in the expansion slot.
- *application*—The application name (string).
- *version*—The application version (string).

Recommended Action None required.

505016

Error Message `%ASA-3-505016: prod_id Module in slot slot application changed from: name version version state state to: name version state state.`

Explanation The application version or name change was detected.

- *prod_id*—Product ID string for the device installed in slot *slot.*
- *slot*—Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- *name*—Application name (string).
- *version*—The application version (string).
- *state*—Application state (string).
- *application*—The name of the application that was upgraded.

Recommended Action Verify that the change was expected and that the new version is correct.

506001

Error Message `%ASA-5-506001: event_source_string event_string`

Explanation Status of a file system has changed. The message describes the event and the source of the event that caused a file system to become available or unavailable. Examples of sources and events that could cause a file system status change are as follows:

- External CompactFlash removed.
- External CompactFlash inserted.
- External CompactFlash unknown event.

Recommended Action None required.

507001

Error Message `%ASA-5-507001: Terminating TCP-Proxy connection from interface_inside:source_address/source_port to interface_outside:dest_address/dest_port - reassembly limit of limit bytes exceeded`

Explanation This message is displayed when reassembly buffer limit is exceeded during assembling TCP segments.

- *source_address/source_port*—The source IP address and the source port of the packet initiating the connection.
- *dest_address/dest_port*—The destination IP address and the destination port of the packet initiating the connection.
- *interface_inside*—The name of the interface on which the packet which initiated the connection arrives.
- *interface_outside*—The name of the interface on which the packet which initiated the connection exits.
- *limit*—The configured embryonic connection limit for the traffic class.

Recommended Action None required.

507002

Error Message `%ASA-4-507002: Data copy in proxy-mode exceeded the buffer limit`

Explanation This syslog message is generated when there is an operational error when processing a fragmented TCP message.

Recommended Action None required.

507003

Error Message `%ASA-3-507003: The flow of type protocol from the originating interface: src_ip/src_port to dest_if:dest_ip/dest_port terminated by inspection engine, reason`

Explanation This syslog message is generated when the TCP proxy/session API terminates a connection for various reasons. The reason is provided in the syslog message.

- *protocol*—The protocol for the flow.
- *src_ip*—The source IP address for the flow.
- *src_port*—The name of the source port for the flow.
- *dest_if*—The destination interface for the flow.
- *dest_ip*—The destination IP address for the flow.
- *dest_port*—The destination port for the flow.
- *reason*—The description of the reason why the flow is being terminated by the inspection engine. Valid reasons include:
  - failed to create flow
  - failed to initialize session API
  - filter rules installed/matched are incompatible
  - failed to consolidate new buffer data with original
  - reset unconditionally
  - reset based on “service resetinbound” configuration
  - disconnected, dropped packet
  - packet length changed
  - reset reflected back to sender
  - proxy inspector reset unconditionally
  - proxy inspector drop reset
  - proxy inspector received data after FIN
  - proxy inspector disconnected, dropped packet
  - inspector reset unconditionally
  - inspector drop reset
  - inspector received data after FIN
  - inspector disconnected, dropped packet
  - could not buffer unprocessed data
  - session API proxy forward failed
  - conversion of inspect data to session data failed

Recommended Action None required.

508001

Error Message `%ASA-5-508001: DCERPC message_type non-standard version_type version version_number from src_if:src_ip/src_port to dest_if:dest_ip/dest_port, terminating connection.`

Explanation This message is generated when using DCERPC inspection. It is logged when a message header contains a nonstandard major or minor version.

- *message_type*—The DCERPC message type.
- *version_type*—The version type, major or minor.
- *version_number*—The nonstandard version in the message header.

Recommended Action If this is a valid version, and the problem persists, contact the Cisco TAC.

508002

Error Message `%ASA-5-508002: DCERPC response has low endpoint port port_number from src_if:src_ip/src_port to dest_if:dest_ip/dest_port, terminating connection.`

Explanation This message is generated when using DCERPC inspection. The message is logged when a response message contains an endpoint port number less than 1024 (in the range of well-known server ports).

Recommended Action None required.

509001

Error Message `%ASA-5-509001: Connection attempt from src_intf:src_ip/src_port to dst_intf:dst_ip/dst_port was prevented by "no forward" command.`

Explanation The **no forward interface** command was entered to block traffic from the source interface to the destination interface given in the syslog message. This command is required on low-end platforms to allow the creation of interfaces beyond the licensed limit.

- *src_intf*—The name of the source interface to which the **no forward interface** command restriction applies.
- *dst_intf*—The name of the destination interface to which the **no forward interface** command restriction applies.

Recommended Action Upgrade the license to remove the requirement of this command on low-end platforms and remove the command from the configuration.

Messages 602101 to 634001

This section contains messages from 602101 to 634001.

602101

Error Message `%ASA-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 security appliance 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.

602103

Error Message `%ASA-6-602103: IPsec: Received an ICMP Destination Unreachable from src_addr with suggested PMTU of rcvd_mtu; PMTU updated for SA with peer peer_addr, SPI spi, tunnel name username, old PMTU old_mtu, new PMTU new_mtu.`

Explanation This message is displayed when the MTU of an SA is changed. When a packet is received for an IPsec tunnel, the corresponding SA is located and the MTU is updated based on the MTU suggested in the ICMP packet. If the suggested MTU is greater than 0 but less than 256, then the new MTU is set to 256. If the suggested MTU is 0, the old MTU is reduced by 256 or it is set to 256, whichever value is greater. If the suggested MTU is greater than 256, then the new MTU is set to the suggested value.

- *src_addr*—IP address of the PMTU sender.
- *rcvd_mtu*—Suggested MTU received in the PMTU message.
- *peer_addr*—IP address of the IPsec peer.
- *spi*—IPsec Security Parameter Index.
- *username*—Username associated with the IPsec tunnel.
- *old_mtu*—Previous MTU associated with the IPsec tunnel.
- *new_mtu*—New MTU associated with the IPsec tunnel.

Recommended Action None required.

602104

Error Message `%ASA-6-602104: IPsec: Received an ICMP Destination Unreachable from src_addr, PMTU is unchanged because suggested PMTU of rcvd_mtu is equal to or greater than the current PMTU of curr_mtu, for SA with peer peer_addr, SPI spi, tunnel name username.`

- *src_addr*—IP address of the PMTU sender.

- *rcvd_mtu*—Suggested MTU received in the PMTU message.
- *curr_mtu*—Current MTU associated with the IPsec tunnel.
- *peer_addr*—IP address of the IPsec peer.
- *spi*—IPsec Security Parameter Index.
- *username*—Username associated with the IPsec tunnel.

Explanation This message occurs when an ICMP message is received indicating that a packet sent over an IPsec tunnel exceeded the path MTU and the suggested MTU is greater than or equal to the current MTU. Because the MTU value is already correct, no MTU adjustment is made. This may happen when multiple PMTU messages are received from different intermediate stations and the MTU is adjusted before the current PMTU message is processed.

Recommended Action None required.

602303

Error Message `%ASA-6-602303: IPsec: A direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been created.`

- *direction*—SA direction (inbound or outbound).
- *tunnel_type*—SA type (remote access or L2L).
- *spi*—IPsec Security Parameter Index.
- *local_IP*—IP address of the tunnel local endpoint.
- *remote_IP*—IP address of the tunnel remote endpoint.
- *username*—Username associated with the IPsec tunnel.

Explanation A new security association (SA) was created.

Recommended Action None required.

602304

Error Message `%ASA-6-602304: IPsec: A direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) has been deleted.`

Explanation This message is displayed when an SA is deleted.

- *direction*—SA direction (inbound or outbound).
- *tunnel_type*—SA type (remote access or L2L).
- *spi*—IPsec Security Parameter Index.
- *local_IP*—IP address of the tunnel local endpoint.
- *remote_IP*—IP address of the tunnel remote endpoint.
- *username*—Username associated with the IPsec tunnel.

Recommended Action None required.

603101

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

Explanation The security appliance 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 `%ASA-6-603102: PPP virtual interface interface_name - user: user aaa authentication started.`

Explanation The security appliance sent an authentication request to the AAA server.

Recommended Action None required.

603103

Error Message `%ASA-6-603103: PPP virtual interface interface_name - user: user aaa authentication status`

Explanation The security appliance received an authentication response from the AAA server.

Recommended Action None required.

603104

Error Message `%ASA-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 %ASA-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 %ASA-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 %ASA-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 %ASA-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 `%ASA-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.

603110

Error Message `%ASA-7-603110: Multiple L2TP sessions added to the tunnel. tunnel_id: tunnel id, number_of_sessions: session_count`

Explanation This message is displayed when multiple sessions are added to an L2TP tunnel.

- *tunnel id*—The L2TP tunnel identifier
- *session_count*—The total number of sessions associated with the L2TP tunnel

Recommended Action None required.

604101

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

Explanation The security appliance DHCP client successfully obtained an IP address from a DHCP server. The **dhcpc** command statement allows the security appliance to 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 `%ASA-6-604102: DHCP client interface interface_name: address released`

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

Recommended Action None required.

604103

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

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

Recommended Action None required.

604104

Error Message `%ASA-6-604104: DHCP daemon interface interface_name: address released`

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

Recommended Action None required.

605004

Error Message `%ASA-6-605004: Login denied from source-address/source-port to interface:destination/service for user "username"`

The following form of the message is displayed when the user attempts to login to the console:

```
Login denied from serial to console for user "username"
```

Explanation This message appears after an incorrect login attempt or a failed login to the security appliance. For all logins, three attempts are allowed per session, and the session is terminated after three incorrect attempts. For SSH and TELNET logins, this message is generated after the third failed attempt or if the TCP session is terminated after one or more failed attempts. For other types of management sessions, this message is generated after every failed attempt.

- *source-address*—Source address of the login attempt.
- *source-port*—Source port of the login attempt.
- *interface*—Destination management interface.
- *destination*—Destination IP address.
- *service*—Destination service.
- *username* —Destination management interface.

Recommended Action If this message appears infrequently, none required. If this message appears frequently, it may indicate an attack. Communicate with the user to verify the username and password.

605005

Error Message `%ASA-6-605005: Login permitted from source-address/source-port to interface:destination/service for user "username"`

The following form of the message is displayed when the user logs in to the console:

```
Login permitted from serial to console for user "username"
```

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

- *source-address*—Source address of the login attempt.
- *source-port*—Source port of the login attempt.
- *interface*—Destination management interface.
- *destination*—Destination IP address.
- *service*—Destination service.
- *username*—Destination management interface.

Recommended Action None required.

606001

Error Message `%ASA-6-606001: ASDM session number number from IP_address started`

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

Recommended Action None required.

606002

Error Message `%ASA-6-606002: ASDM session number number from IP_address ended`

Explanation This message indicates that an ASDM session ended.

Recommended Action None required.

606003

Error Message `%ASA-6-606003: ASDM logging session number id from IP_address started id session ID assigned`

Explanation An ASDM logging connection is started by a remote management client.

- *IP_address*—IP address of remote management client.

Recommended Action None required.

606004

Error Message `%ASA-6-606004: ASDM logging session number id from IP_address ended`

Explanation An ASDM logging connection is terminated.

- *id*—Session ID assigned.
- *IP_address*—IP address of remote management client.

Recommended Action None required.

607001

Error Message `%ASA-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 preallocated 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.

607002

Error Message `%ASA-4-607002: action_class: action SIP req_resp req_resp_info from src_ifc:sip/sport to dest_ifc:dip/dport; further_info`

Explanation This message is generated when a SIP classification is performed on a SIP message and the specified criteria is satisfied. Then the configured action occurs.

- *action_class*—The class of the action: "SIP Classification" for SIP match commands or "SIP Parameter" for parameter commands.
- *action*—The action taken: "Dropped," "Dropped connection for," "Reset connection for," or "Masked header flags for."
- *req_resp*—"Request" or "Response."
- *req_resp_info*—The SIP method name if the type is "Request": INVITE, CANCEL, and so on. The SIP response code if type is "Response": 100, 183, 200, and so on.
- *src_ifc*—The source interface name.
- *sip*—The source IP address.
- *sport*—The source port.
- *dest_ifc*—The destination interface name.
- *dip*—The destination IP address.
- *dport*—The destination port.
- *further_info*—Displays more information for SIP match and SIP parameter commands, as follows:
  - For SIP match commands:

    matched Class *id*: *class-name*—For example:

    ```
    matched Class 1234: my_class
    ```

  - For SIP parameter commands:

    parameter-command: *descriptive-message*—For example:

    ```
    strict-header-validation: Mandatory header field 'Via' is missing
    state-checking: Message CANCEL is not permitted to create a Dialog.
    ```

Recommended Action None required.

607003

Error Message `%ASA-6-607003: action_class: Received SIP req_resp req_resp_info from src_ifc:sip/sport to dest_ifc:dip/dport; further_info`

Explanation This event is generated when a SIP classification is performed on a SIP message and the specified criteria is satisfied. Then the standalone log action occurs.

- *action_class*—SIP Classification for SIP match commands or SIP Parameter for parameter commands.

- *req_resp*—"Request" or "Response."
- *req_resp_info*—The SIP method name if the type is "Request": INVITE, CANCEL, and so on. The SIP response code if type is "Response": 100, 183, 200, and so on.
- *src_ifc*—The source interface name.
- *sip*—The source IP address.
- *sport*—The source port.
- *dest_ifc*—The destination interface name.
- *dip*—The destination IP address.
- *dport*—The destination port.
- *further_info*—Displays more information for SIP match and SIP parameter commands, as follows:

  –For SIP match commands:

  matched Class *id*: *class-name*—For example:

  ```
  matched Class 1234: my_class
  ```

  –For SIP parameter commands:

  parameter-command: *descriptive-message*—For example:

  ```
  strict-header-validation: Mandatory header field 'Via' is missing
  state-checking: Message CANCEL is not permitted to create a Dialog.
  ```

Recommended Action None required.

608001

Error Message `%ASA-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 **inspect skinny** command preallocated 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.

608002

Error Message `%ASA-4-608002: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, SCCPPrefix length value too small`

Explanation A Skinny (SSCP) message was received with an SCCP prefix length less than the minimum length configured.

- *in_ifc*—The input interface.
- *src_ip*—The source IP address of the packet.
- *src_port*—The source port of the packet.
- *out_ifc*—The output interface.
- *dest_ip*—The destination IP address of the packet.
- *dest_port*—The destination port of the packet.
- *value*—The SCCP prefix length of the packet.

Recommended Action If the SCCP message is valid, then customize the Skinny policy map to increase the minimum length value of the SSCP prefix.

608003

Error Message `%ASA-4-608003: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, SCCPPrefix length value too large`

Explanation A Skinny (SSCP) message was received with an SCCP prefix length greater than the maximum length configured.

- *in_ifc*—The input interface.
- *src_ip*—The source IP address of the packet.
- *src_port*—The source port of the packet.
- *out_ifc*—The output interface.
- *dest_ip*—The destination IP address of the packet.
- *dest_port*—The destination port of the packet.
- *value*—The SCCP prefix length of the packet.

Recommended Action If the SCCP message is valid, then customize the Skinny policy map to increase the maximum length value of the SCCP prefix.

608004

Error Message `%ASA-4-608004: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, message id value not allowed`

- *in_ifc*—The input interface.

- *src_ip*—The source IP address of the packet.
- *src_port*—The source port of the packet.
- *out_ifc*—The output interface.
- *dest_ip*—The destination IP address of the packet.
- *dest_port*—The destination port of the packet.
- *value*—The SCCP prefix length of the packet.

Explanation This SCCP message ID is not allowed.

Recommended Action If the SCCP messages should be allowed, then customize the Skinny policy map to allow them.

608005

Error Message `%ASA-4-608005: Dropping Skinny message for in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port, message id value registration not complete`

Explanation This SCCP message ID is not allowed because the endpoint did not complete registration.

- *in_ifc*—The input interface.
- *src_ip*—The source IP address of the packet.
- *src_port*—The source port of the packet.
- *out_ifc*—The output interface.
- *dest_ip*—The destination IP address of the packet.
- *dest_port*—The destination port of the packet.
- *value*—The SCCP prefix length of the packet.

Recommended Action If the SCCP messages that are being dropped are valid, then customize the Skinny policy map to disable registration enforcement.

609001

Error Message `%ASA-7-609001: 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 %ASA-7-609002: 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 %ASA-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 security appliance 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 %ASA-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 security appliance and the NTP server are set to use authentication, and the same key number and value.

610101

Error Message %ASA-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 security appliance encounters any other value other than the four command types listed, the message "unknown command type" is displayed.

Recommended Action None required.

611101

Error Message `%ASA-6-611101: User authentication succeeded: Uname: user`

Explanation User authentication succeeded when accessing the security appliance succeeded.

Recommended Action None required.

611102

Error Message `%ASA-6-611102: User authentication failed: Uname: user`

Explanation User authentication failed when attempting to access the security appliance.

Recommended Action None required.

611103

Error Message `%ASA-5-611103: User logged out: Uname: user`

Explanation The specified user logged out.

Recommended Action None required.

611104

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

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

Recommended Action None required.

611301

Error Message `%ASA-6-611301: VPNClient: NAT configured for Client Mode with no split tunneling: NAT address: mapped_address`

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

Recommended Action None required.

611302

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

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

Recommended Action None required.

611303

Error Message `%ASA-6-611303: VPNClient: NAT configured for Client Mode with split tunneling: NAT address: mapped_address Split Tunnel Networks: IP_address/netmask IP_address/netmask`

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

Recommended Action None required.

611304

Error Message `%ASA-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 the network extension mode with split tunneling was installed.

Recommended Action None required.

611305

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

Explanation The VPN client is connected to the specified headend.

Recommended Action None required.

611308

Error Message %ASA-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 %ASA-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 `%ASA-6-611310: VNPClient: XAUTH Succeeded: Peer: IP_address`

Explanation The VPN client Xauth succeeded with the specified headend.

Recommended Action None required.

611311

Error Message `%ASA-6-611311: VNPClient: XAUTH Failed: Peer: IP_address`

Explanation The VPN client Xauth failed with the specified headend.

Recommended Action None required.

611312

Error Message `%ASA-6-611312: VPNClient: Backup Server List: reason`

Explanation When the security appliance is an Easy VPN remote device, this message indicates that the Easy VPN server downloaded a list of backup servers to the security appliance. This list overrides any backup servers you configured locally. If the downloaded list is empty, then the security appliance 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 `%ASA-3-611313: VPNClient: Backup Server List Error: reason`

Explanation When the security appliance is an Easy VPN remote device, and the Easy VPN server downloads a backup server list to the security appliance, this message indicates that the list contains an invalid IP address or a hostname. The security appliance does not support DNS, and therefore does not support hostnames 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 that the server IP addresses are correct, and configure the servers as IP addresses instead of hostnames. If you must use hostnames on the server, use the **name** command on the Easy VPN remote device to map the IP addresses to names.

611314

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

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

Recommended Action None required.

611315

Error Message `%ASA-6-611315: VPNClient: Disconnecting from Load Balancing Cluster member IP_address`

Explanation When the security appliance 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 `%ASA-6-611316: VPNClient: Secure Unit Authentication Enabled`

Explanation When the security appliance is an Easy VPN remote device, the downloaded VPN policy enabled Secure Unit Authentication (SUA).

Recommended Action None required.

611317

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

Explanation When the security appliance is an Easy VPN remote device, the downloaded VPN policy disabled Secure Unit Authentication (SUA).

Recommended Action None required.

611318

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

Explanation When the security appliance is an Easy VPN remote device, the downloaded VPN policy enabled Individual User Authentication (IUA) for users on the security appliance inside network.

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

Recommended Action None required.

611319

Error Message `%ASA-6-611319: VPNClient: User Authentication Disabled`

Explanation When the security appliance is an Easy VPN remote device, the downloaded VPN policy disabled Individual User Authentication (IUA) for users on the security appliance inside network.

Recommended Action None required.

611320

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

Explanation When the security appliance 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 security appliance.

611321

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

Explanation When the security appliance is an Easy VPN remote device, the downloaded VPN policy disabled device pass through.

Recommended Action None required.

611322

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

Explanation When the security appliance is an Easy VPN remote device and the downloaded VPN policy disabled secure unit**5kujnm0o** authentication (SUA), the Easy VPN server uses two-factor/SecurID/cryptocard-based authentication mechansims to authenticate the security appliance 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 `%ASA-6-611323: VPNClient: Duplicate split nw entry`

Explanation When the security appliance 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 `%ASA-5-612001: Auto Update succeeded:`*`filename`*`, version:`*`number`*

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

Recommended Action None required.

612002

Error Message `%ASA-4-612002: Auto Update failed:filename, version:number, reason:reason`

Explanation This message indicates that an update from an Auto Update server failed.

- *filename*—either image file, and ASDM file, or configuration file.
- *number*—The version number of the update.
- *reason*—The failure reason, which may be one of the following:
  - –Failover module failed to open stream buffer
  - –Failover module failed to write data to stream buffer
  - –Failover module failed to perform control operation on stream buffer
  - –Failover module failed to open flash file
  - –Failover module ailed to write data to flash
  - –Failover module operation timeout
  - –Failover command link is down
  - –Failover resource is not available
  - –Invalid failover state on mate
  - –Failover module encountered file transfer data corruption
  - –Failover active state change
  - –Failover command EXEC failed
  - –Unsupported file type

Recommended Action Check the configuration of the Auto Update server. Check to see if the standby unit is in the failed state. If the Auto Update server is configured correctly, and the standby unit is not in the failed state, contact Cisco TAC.

612003

Error Message `%ASA-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, and so on.

Recommended Action Check the configuration of the Auto Update server.

613001

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

Explanation The interface reports its bandwidth as zero.

Recommended Action If the problem persists, contact the Cisco TAC.

613003

Error Message %ASA-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 %ASA-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 `%ASA-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.

615001

Error Message `%ASA-6-615001: vlan number not available for firewall interface`

Explanation The switch removed the VLAN from the FWSM.

Recommended Action This is an informational message.

615002

Error Message `%ASA-6-615002: vlan number available for firewall interface`

Explanation The switch added the VLAN to the FWSM.

Recommended Action This is an informational message.

616001

Error Message `%ASA-6-616001:Pre-allocate MGCP data_channel connection for inside_interface:inside_address to outside_interface:outside_address/port from message_type message`

Explanation An MGCP data channel connection, RTP, or RTCP is preallocated. The message text also specifies which message has triggered the connection preallocation.

Recommended Action None required.

617001

Error Message %ASA-6-617001: GTPv *version msg_type* from *source_interface:source_address/source_port* not accepted by *source_interface:dest_address/dest_port*

Explanation This message appears when a request was not accepted by the peer. This is usually seen with a Create PDP Context request.

Recommended Action None required.

617002

Error Message %ASA-6-617002: Removing v1 PDP Context with TID *tid* from GGSN *IP_address* and SGSN *IP_address*, Reason: *reason* or Removing v1 *primary*|*secondary* PDP Context with TID *tid* from GGSN *IP_address* and SGSN *IP_address*, Reason: *reason*

Explanation This message appears when a PDP context is removed from the database either because it expired, a Delete PDP Context Request/Response was exchanged, or a user removed it using the CLI.

Recommended Action None required.

617003

Error Message %ASA-6-617003: GTP Tunnel created from *source_interface:source_address/source_port* to *source_interface:dest_address/dest_port*

Explanation This message appears when a GTP tunnel was created after receiving a Create PDP Context Response that accepted the request.

Recommended Action None required.

617004

Error Message %ASA-6-617004: GTP connection created for response from *source_interface:source_address/0* to *source_interface:dest_address/dest_port*

Explanation This message appears when the SGSN or GGSN signaling address in the Create PDP Context Request or Response, respectively, is different than the SGSN/GGSN sending it.

Recommended Action None required.

617100

Error Message `ASA-6-617100: Teardown num_conns connection(s) for user user_ip`

Explanation The connections for this user were torn down because either a RADIUS accounting stop or RADIUS accounting start was received, which contains attributes configured in the policy-map for a match. The attributes did not match those stored for the user entry, if the user entry exists.

- *num_conns*—The number of connections torn down.
- *user_ip*—The IP address (framed IP attribute) of the user.

Recommended Action None required.

620001

Error Message `%ASA-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 security appliance pre-allocates a connection object for the specified CTIQBE media traffic. This message is rate limited to one message every 10 seconds.

Recommended Action None required.

620002

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

Explanation The security appliance received a CTIQBE message with an unsupported version number. The security appliance drops the packet. This message is rate limited to one message every 10 seconds.

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 security appliance. 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 the Cisco TAC to see if a new security appliance image that supports this CTIQBE version is available.

621001

Error Message `%ASA-6-621001: Interface interface_name does not support multicast, not enabled`

Explanation This message appears when an attempt was made to enable PIM on an interface that does not support multicast.

Recommended Action If the problem persists, contact the Cisco TAC.

621002

Error Message `%ASA-6-621002: Interface interface_name does not support multicast, not enabled`

Explanation This message appears when an attempt was made to enable IGMP on an interface that does not support multicast.

Recommended Action If the problem persists, contact the Cisco TAC.

621003

Error Message `%ASA-6-621003: The event queue size has exceeded number`

Explanation This message appears when the number of event managers created has exceeded the expected amount.

Recommended Action If the problem persists, contact the Cisco TAC.

621004

Error Message `%ASA-6-621004: Timer drift is accumulating, %d msecs`

Explanation There is a large amount of processing load and the timers are accumulating delays. This means that the device was unable to process all requests during the time slot allocated.

- *%d*—An integer.

Recommended Action Monitor this condition, and if multicast forwarding is interrupted, contact the Cisco TAC for assistance.

621006

Error Message `%ASA-6-621006: Mrib disconnected, (IP_address,IP_address) event cancelled`

Explanation This message appears when a packet triggering a data-driven event was received, but the connection to the MRIB was down. The notification was cancelled.

Recommended Action If the problem persists, contact the Cisco TAC.

621007

Error Message `%ASA-6-621007: Bad register from interface_name:IP_address to IP_address for (IP_address, IP_address)`

Explanation This message appears when a PIM router configured as a rendezvous point or with Network Address Translation (NAT) has received a PIM register packet from another PIM router. The data encapsulated in this packet is invalid.

Recommended Action It is likely that the sending router is erroneously sending non-RFC registers. Upgrade the sending router.

622001

Error Message `%ASA-6-622001: string tracked route network mask address, distance number, table string, on interface interface-name`

Explanation A tracked route has been added to or removed from a routing table, which means that the state of the tracked object has changed from up or down.

- *string*—"Adding" or "Removing."
- *network*—The network address.
- *mask*—The network mask.
- *address*—The gateway address.
- *number*—The route administrative distance.
- *string*—The routing table name.
- *interface-name*—The interface name as specified by the **nameif** command.

Recommended Action None required. This is an informational message that indicates a change in routing and a likely change in forwarding paths, as configured by the tracking and SLA commands.

622101

Error Message `%ASA-6-622101: Starting regex table compilation for match_command; table entries = regex_num entries`

Explanation Provides information on the background activities of regex compilation.

- *match_command*—The match command to which the regex table is associated.
- *regex_num*—The number of regex entries to be compiled.

Recommended Action None required.

622102

Error Message `%ASA-6-622102: Completed regex table compilation for match_command; table size = num bytes`

Explanation Provides information on the background activities of the regex compilation.

- *match_command*—The match command to which the regex table is associated.
- *num*—The size, in bytes, of the compiled table.

Recommended Action None required.

634001

Error Message `%ASA-6-634001: DAP: User user, Addr ipaddr, Connection connection; The following DAP records were selected for this connection: DAP Record names`

Explanation Displays the DAP records selected for the connection.

- *user*—The authenticated username.
- *ipaddr*—The IP address of the remote client.
- *connection*—The type of client connection:
  - IPsec—IPsec connection
  - AnyConnect—AnyConnect connection
  - Clientless—Web browser connection
  - Cut-Through-Proxy—Cut-Through-Proxy connection
  - L2TP—L2TP client connection
- *DAP record names*—The comma-separated list of the DAP record names.

Recommended Action None required.

Messages 701001 to 737033

This section contains messages from 701001 to 737033.

701001

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

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

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

701002

Error Message `%ASA-7-701002: alloc_user() out of Tcp_proxy objects`

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

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

702305

Error Message `%ASA-3-702305: IPsec: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) is rekeying due to sequence number rollover.`

Explanation This message is displayed when more than four billion packets have been received in the IPsec tunnel, and a new tunnel is being negotiated.

- *direction*—SA direction (inbound or outbound).
- *tunnel_type*—SA type (remote access or L2L).
- *spi*—IPsec Security Parameter Index.
- *local_IP*—IP address of the tunnel local endpoint.
- *remote_IP*—IP address of the tunnel remote endpoint.
- *username*—Username associated with the IPsec tunnel.

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

702307

Error Message `%ASA-3-702307: IPsec: An direction tunnel_type SA (SPI=spi) between local_IP and remote_IP (username) is rekeying due to data rollover.`

Explanation This message is displayed when an SA data life span expires. This message indicates that an IPsec SA is rekeying as a result of the amount of data transmitted with that SA. This information is useful for debugging rekeying issues.

- *direction*—SA direction (inbound or outbound).
- *tunnel_type*—SA type (remote access or L2L).
- *spi*—IPsec Security Parameter Index.
- *local_IP*—IP address of the tunnel local endpoint.
- *remote_IP*—IP address of the tunnel remote endpoint.
- *username*—Username associated with the IPsec tunnel.

Recommended Action None required.

703001

Error Message `%ASA-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 security appliance received an H.323 packet with an unsupported version number. The security appliance 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 security appliance supports in the VoIP network.

703002

Error Message `%ASA-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface_name:IP_address to interface_name:IP_address/port`

Explanation This debugging message indicates that the security appliance received the specified H.225 message, and that the security appliance opened a new signaling connection object for the two specified H.323 endpoints.

Recommended Action None required.

709001, 709002

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

Error Message `%ASA-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 `%ASA-1-709003: (Primary) Beginning configuration replication: Sending to mate.`

Explanation This is a failover message. This message is displayed 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 `%ASA-1-709004: (Primary) End Configuration Replication (ACT)`

Explanation This is a failover message. This message is displayed 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 `%ASA-1-709005: (Primary) Beginning configuration replication: Receiving from mate.`

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

Recommended Action None required.

709006

Error Message `%ASA-1-709006: (Primary) End Configuration Replication (STB)`

Explanation This is a failover message. This message is displayed 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 `%ASA-2-709007: Configuration replication failed for command` *`command`*

Explanation This is a failover message. This message is displayed when the standby unit is unable to complete replicating a configuration sent by the active unit. The command that caused the failure displays at the end of the message.

Recommended Action If the problem persists, contact the Cisco TAC.

710001

Error Message `%ASA-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 security appliance 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 `%ASA-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 security appliance 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 module receives an SNMP request from an authorized SNMP management station, and the request has been processed. This message is rate limited to one message every ten seconds.

Recommended Action None required.

710003

Error Message `%ASA-3-710003: {TCP|UDP} access denied by ACL from` *source_IP/source_port* `to` *interface_name:dest_IP/service*

The following is an example:

```
%ASA-3-710003: UDP access denied by ACL from 95.1.1.14/5000 to outside:95.1.1.13/1005
```

Explanation This message is displayed when the security appliance denies an attempt to connect to the interface service. For example, this message may occur when the security appliance receives an SNMP request from an unauthorized SNMP management station.

Recommended Action Use the **show run http**, **show run ssh**, or **show run telnet** commands to verify that the security appliance 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 `%ASA-7-710004: TCP connection limit exceeded from` *Src_ip/Src_port* `to` *In_name:Dest_ip/Dest_port* `(current connections/connection limit = Curr_conn/Conn_lmt)`

Explanation The maximum number of security appliance management connections for the service was exceeded. The security appliance permits at most five concurrent management connections per management service. Alternatively, this message may be generated when an error has occurred in the to-the-box connection counter.

- *Src_ip*—The source IP address of the packet.
- *Src_por*t—The source port of the packet.
- *In_ifc*—The input interface.

- *Dest_ip*—The destination IP address of the packet.
- *Dest_port*—The destination port of the packet.
- *Curr_conn*—The number of current to-the-box admin connections.
- *Conn_lmt*—The connection limit.

Recommended Action From the console, use the **kill** command to release the unwanted session. If the message was generated because of an error in the to-the-box counter, run the **show conn all** command to display connection details.

710005

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

Explanation This message appears when the security appliance 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 security appliance. In addition, this message appears (with the service **snmp**) when the security appliance 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 once every ten seconds, so that the log receiver is not overwhelmed.

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

710006

Error Message `%ASA-7-710006: protocol request discarded from source_address to interface_name:dest_address`

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

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 numbers, it may indicate an attack.

710007

Error Message %PIX|ASA-7-710007: *NAT-T keepalive received from 86.1.161.1/1028 to outside:86:1.129.1/4500*

Explanation This message appears when the ASA security appliance receives NAT-T keepalive messages.

Recommended Action None required.

711001

Error Message %ASA-7-711001: debug_trace_msg

Explanation This syslog message appears after you enter the **logging debug-trace** command for the logging feature. When the **logging debug-trace** command is enabled, all debug messages will be redirected to the syslog message for processing. For security reasons, the syslog message output must be encrypted or sent over a secure out-of-band network.

Recommended Action None required.

711003

Error Message ASA-7-711003: Unknown/Invalid interface identifier(*vpifnum*) detected.

Explanation This message reports an internal inconsistency that should not occur during normal operation. However, there is no harmful impact of this if it is seen rarely. If seen frequently, it might be worthwhile debugging.

- *vpifnum*—The 32-bit value corresponding to the interface.

Recommended Action If the problem persists, contact the Cisco TAC.

711004

Error Message %ASA-4-711004: Task ran for *msec* msec, Process = *process_name*, PC = *pc*, Call stack = *call stack*

Explanation This message appears when a process uses the CPU for more than 100 milliseconds. This message is used for debugging CPU purposes, and can appear once every five seconds for each offending process.

- *msec*—Length of the detected CPU hog in milliseconds
- *process_name*—Name of the hogging process
- *pc*—Instruction pointer of the CPU hogging process

- *call stack*—Stack trace of the CPU hogging process, which can include up to 12 addresses

Recommended Action None required.

713004

Error Message `%ASA-3-713004: device scheduled for reboot or shutdown, IKE key acquire message on interface interface num, for Peer IP_address ignored`

Explanation This message appears when the security appliance has received an IKE packet from a remote entity trying to initiate a tunnel. Because the security appliance is scheduled for a reboot or shutdown, it does not allow any more tunnels to be established. The IKE packet is ignored and dropped.

Explanation None required.

713006

Error Message `%ASA-5-713006: Failed to obtain state for message Id message_number, Peer Address: IP_address`

Explanation This message indicates that the security appliance does not know about the received message ID. The message ID is used to identify a specific IKE Phase 2 negotiation. This is most likely an error condition on the security appliance, but may indicate that the two IKE peers are not synchronized.

Recommended Action None required.

713008

Error Message `%ASA-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel`

Explanation This message indicates that a key ID value was received in the ID payload, which was longer than the maximum allowed size of a groupname for this IKE session using preshared keys authentication. This is an invalid value, and the session is rejected. Note that the key ID specified would never work, because a groupname of that size cannot be created in the security appliance. Notify the user to change the incorrect groupname on the client.

Recommended Action Make sure that the client peer (most likely an Altiga RA Client) specifies a valid groupname. The current maximum length for a groupname is 32 characters.

713009

Error Message `%ASA-3-713009: OU in DN in ID payload too big for Certs IKE tunnel`

Explanation This message indicates that an OU value in the DN was received in the ID payload, which was longer than the maximum allowed size of a groupname for this IKE session using Certs authentication. This OU is skipped, and another OU or other criteria may find a matching group.

Recommended Action For the client to be able to use an OU to find a group in the security appliance, the groupname must be a valid length. The current maximum length of a groupname is 32.

713010

Error Message `%ASA-5-713010: IKE area: failed to find centry for message Id message_number`

Explanation This message appears when an attempt is made to locate a conn_entry (IKE phase 2 struct that corresponds to an IPsec SA) by the unique message ID has failed. The internal structure was not found. This can occur if a session is terminated in a non-standard way, but it more likely indicates an internal error.

Recommended Action If this problem persists, investigate the peer.

713012

Error Message `%ASA-3-713012: Unknown protocol (protocol). Not adding SA w/spi=SPI value`

Explanation This message appears when an illegal or unsupported IPsec protocol has been received from the peer.

Recommended Action Check the ISAKMP Phase 2 configuration on peer(s) to make sure it is compatible with the security appliance.

713014

Error Message `%ASA-3-713014: Unknown Domain of Interpretation (DOI): DOI value`

Explanation This message appears when the ISAKMP Domain of Interpretation received from the peer is unsupported.

Recommended Action Check the ISAKMP DOI configuration on the peer(s).

713016

Error Message `%ASA-3-713016: Unknown identification type, Phase 1 or 2, Type ID_Type`

Explanation This message indicates that the ID received from the peer is unknown. The ID could be an unfamiliar valid ID or an invalid or corrupted ID.

Recommended Action Check the configuration on the headend and peer(s).

713017

Error Message `%ASA-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type`

Explanation This message indicates that the Phase 1 or Phase 2 ID received from the peer is legal, but not supported.

Recommended Action Check the configuration on the headend and peer(s).

713018

Error Message `%ASA-3-713018: Unknown ID type during find of group name for certs, Type ID_Type`

Explanation This message indicates that an internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713020

Error Message `%ASA-3-713020: No Group found by matching OU(s) from ID payload: OU_value`

Explanation This message indicates that an internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713022

Error Message `%ASA-3-713022: No Group found matching peer_ID or IP_address for Pre-shared key peer IP_address`

Explanation This message indicates that there was no group in the group database with the same name as the value (key ID or IP address) specified by the peer.

Recommended Action Verify the configuration on the peer.

713024

Error Message `%ASA-7-713024: Received local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port`

Explanation This message indicates that the security appliance has received the Phase 2 local proxy ID payload from the remote peer.

Recommended Action None required.

713025

Error Message `%ASA-7-713025: Received remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port`

Explanation This message indicates that the security appliance has received the Phase 2 local proxy ID payload from the remote peer.

Recommended Action None required.

713026

Error Message `%ASA-7-713026: Transmitted local Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port`

Explanation This message indicates that the security appliance has transmitted the Phase 2 local proxy ID payload.

Recommended Action None required.

713027

Error Message `%ASA-7-713027: Transmitted remote Proxy Host data in ID Payload: Address IP_address, Protocol protocol, Port port`

Explanation This message indicates that the security appliance has transmitted the Phase 2 remote proxy ID payload.

Recommended Action None required.

713028

Error Message `%ASA-7-713028: Received local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port`

Explanation This message indicates that the security appliance has received the Phase 2 local proxy ID payload of the remote peer, which contains an IP address range.

Recommended Action None required.

713029

Error Message `%ASA-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port`

Explanation This message indicates that the security appliance has received the Phase 2 local proxy ID payload of the remote peer, which contains an IP address range.

Recommended Action None required.

713030

Error Message `%ASA-7-713030: Transmitted local Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port`

Explanation This message indicates that the security appliance has transmitted the Phase 2 local proxy ID payload.

Recommended Action None required.

713031

Error Message `%ASA-7-713031: Transmitted remote Proxy Range data in ID Payload: Addresses IP_address - IP_address, Protocol protocol, Port port`

Explanation This message indicates that the security appliance has transmitted the Phase 2 remote proxy ID payload.

Recommended Action None required.

713032

Error Message `%ASA-3-713032: Received invalid local Proxy Range IP_address - IP_addresss`

Explanation This message appears when the local ID payload contained the range ID type and the specified low address was not less than the high address. This may indicate a configuration problem.

Recommended Action Check the configuration of ISAKMP Phase 2 parameters.

713033

Error Message `%ASA-3-713033: Received invalid remote Proxy Range IP_address - IP_address`

Explanation This message appears when the remote ID payload contained the range ID type, and the specified low address was not less than the high address. This may indicate a configuration problem.

Recommended Action Check the configuration of ISAKMP Phase 2 parameters.

713034

Error Message `%ASA-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port`

Explanation This message appears when the local IP Proxy Subnet data has been received in the Phase 2 ID Payload.

Recommended Action None required.

713035

Error Message `%ASA-7-713035: Received remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port`

Explanation This message appears when the remote IP Proxy Subnet data has been received in the Phase 2 ID Payload.

Recommended Action None required.

713036

Error Message `%ASA-7-713036: Transmitted local IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port`

Explanation This message appears when the local IP Proxy Subnet data in has been transferred in the Phase 2 ID Payload.

Recommended Action None required.

713037

Error Message `%ASA-7-713037: Transmitted remote IP Proxy Subnet data in ID Payload: Address IP_address, Mask netmask, Protocol protocol, Port port`

Explanation This message appears when the remote IP Proxy Subnet data has been transferred in the Phase 2 ID Payload.

Recommended Action None required.

713039

Error Message `%ASA-7-713039: Send failure: Bytes (number), Peer: IP_address`

Explanation This message appears when an internal software error has occurred and the ISAKMP packet could not be transmitted.

Recommended Action If the problem persists, contact the Cisco TAC.

713040

Error Message `%ASA-7-713040: Could not find connection entry and can not encrypt: msgid message_number`

Explanation This message indicates that an internal software error has occurred and a Phase 2 data structure could not be found.

Recommended Action If the problem persists, contact the Cisco TAC.

713041

Error Message `%ASA-5-713041: IKE Initiator: new or rekey Phase 1 or 2, Intf interface_number, IKE Peer IP_address local Proxy Address IP_address, remote Proxy Address IP_address, Crypto map (crypto map tag)`

Explanation This message indicates that the security appliance is negotiating a tunnel as the initiator.

Recommended Action None required.

713042

Error Message `%ASA-3-713042: IKE Initiator unable to find policy: Intf interface_number, Src: source_address, Dst: dest_address`

Explanation This message indicates that the IPsec fast path processed a packet that triggered IKE, but IKE's policy lookup failed. This error could be timing related. The ACLs that triggered IKE might have been deleted before IKE processed the initiation request. This problem will most likely correct itself.

Recommended Action If the condition persists, check the L2L configuration, paying special attention to the type of ACL associated with crypto maps.

713043

Error Message `%ASA-3-713043: Cookie/peer address IP_address session already in progress`

Explanation This message indicates that IKE has been triggered again while the original tunnel is in progress.

Recommended Action None required.

713048

Error Message %ASA-3-713048: Error processing payload: Payload ID: *id*

Explanation This message indicates that a packet has been received with a payload we could not process.

Recommended Action If this problem persists, there might be a misconfiguration on the peer.

713049

Error Message %ASA-5-713049: Security negotiation complete for *tunnel_type* type (*group_name*) *Initiator/Responder*, Inbound SPI = *SPI*, Outbound SPI = *SPI*

Explanation This message indicates the start of an IPsec tunnel.

Recommended Action None required.

713050

Error Message %ASA-5-713050: Connection terminated for peer *IP_address*. Reason: *termination reason* Remote Proxy *IP_address*, Local Proxy *IP_address*

Explanation This message indicates the termination of an IPsec tunnel. Possible termination reasons include:

- IPsec SA Idle Timeout
- IPsec SA Max Time Exceeded
- Administrator Reset
- Administrator Reboot
- Administrator Shutdown
- Session Disconnected
- Session Error Terminated
- Peer Terminate

Recommended Action None required.

713051

Error Message `%ASA-3-713051: Terminating connection attempt: IPsec not permitted for group (group_name)`

Explanation This message indicates that the user, group, or interface policy is rejecting IPsec tunnels.

Recommended Action To use IPsec select the appropriate tunneling protocol in the policy.

713052

Error Message `%ASA-7-713052: User (user) authenticated.`

Explanation This message indicates that the remote access user was authenticated.

Recommended Action None required.

713056

Error Message `%ASA-3-713056: Tunnel rejected: SA (SA_name) not found for group (group_name)!`

Explanation This message indicates that the IPsec SA was not found.

Recommended Action If this is a remote access tunnel, check the group and user configuration and verify that a tunnel group and group policy has been configured for the specific user group. For externally authenticated users and groups, check the returned authentication attributes.

713059

Error Message `%ASA-3-713059: Tunnel Rejected: User (user) matched with group name, group-lock check failed.`

Explanation This message indicates that the user tried to authenticate by using the same string for both the tunnel group and username.

Recommended Action The group and username must be different for the user to be authenticated.

713060

Error Message `%ASA-3-713060: Tunnel Rejected: User (`*user*`) not member of group (`*group_name*`), group-lock check failed.`

Explanation This message indicates that the user is configured for a different group than what was sent in the IPsec negotiation.

Recommended Action If you are using the Cisco VPN client and preshared keys, make sure that the group configured on the client is the same as the group associated with the user on the security appliance. If using digital certificates, the group is dictated either by the OU field of the certificate or the user will default to the remote access default group.

713061

Error Message `%ASA-3-713061: Tunnel rejected: Crypto Map Policy not found for Src: `*source_address*`, Dst: `*dest_address*`!`

Explanation This message indicates that the security appliance was not able to find security policy information for the private networks or hosts indicated in the message. These networks or hosts were sent by the initiator and do not match any crypto ACLs at the security appliance. This is most likely a misconfiguration.

Recommended Action Check the protected network configuration in the crypto ACLs on both sides and make sure that the local net on the initiator is the remote net on the responder and vice-versa. Pay special attention to wildcard masks, host addresses versus network addresses, and so on. Non-Cisco implementations may have the private addresses labeled as proxy addresses or red networks.

713062

Error Message `%ASA-3-713062: IKE Peer address same as our interface address `*IP_address*

Explanation The IP address configured as the IKE peer is the same as the IP address configured on one of the security appliance IP interfaces.

Recommended Action Check the L2L configuration and configuration of IP interface(s).

713063

Error Message `%ASA-3-713063: IKE Peer address not configured for destination` *`IP_address`*

Explanation This message appears when the IKE peer address is not configured for a L2L tunnel.

Recommended Action Check the L2L configuration.

713065

Error Message `%ASA-3-713065: IKE Remote Peer did not negotiate the following:` *`proposal attribute`*

Explanation This message indicates that an internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713066

Error Message `%ASA-7-713066: IKE Remote Peer configured for SA:` *`SA_name`*

Explanation This message indicates the crypto policy settings of the peer.

Recommended Action None required.

713068

Error Message `%ASA-5-713068: Received non-routine Notify message:` *`notify_type`* (*`notify_value`*)

Explanation This message indicates that notification messages that cause this event are not explicitly handled in the notify processing code.

Recommended Action Examine the specific reason information to determine the action to take. Many notification messages indicate a configuration mismatch between the IKE peers.

713072

Error Message %ASA-3-713072: Password for user (*user*) too long, truncating to *number* characters

Explanation This message indicates that the password of the user is too long.

Recommended Action Correct password lengths on the authentication server.

713073

Error Message %ASA-5-713073: Responder forcing change of *Phase 1/Phase 2* rekeying duration from *larger_value* to *smaller_value* seconds

Explanation Rekeying durations are always set to the lower of the values proposed by IKE peers. This message indicates that the value of the initiator is the lower one.

Recommended Action None required.

713074

Error Message %ASA-5-713074: Responder forcing change of IPsec rekeying duration from *larger_value* to *smaller_value* Kbs

Explanation Rekeying durations are always set to the lower of the values proposed by IKE peers. This message indicates that the value of the initiator is the lower one.

Recommended Action None required.

713075

Error Message %ASA-5-713075: Overriding Initiator's IPsec rekeying duration from *larger_value* to *smaller_value* seconds

Explanation Rekeying durations are always set to the lower of the values proposed by IKE peers. This message indicates that the value of the responder is the lower one.

Recommended Action None required.

713076

Error Message `%ASA-5-713076: Overriding Initiator's IPsec rekeying duration from` *`larger_value`* `to` *`smaller_value`* `Kbs`

Explanation Rekeying durations are always set to the lower of the values proposed by IKE peers. This message indicates that the value of the responder is the lower one.

Recommended Action None required.

713078

Error Message `%ASA-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size, used` *`value`*

Explanation This message indicates that an internal software error has occurred while processing modecfg attributes.

Recommended Action Disable any unnecessary tunnel group attributes or shorten any text messages that are excessively long. If the problem persists, contact the Cisco TAC.

713081

Error Message `%ASA-3-713081: Unsupported certificate encoding type` *`encoding_type`*

Explanation This message indicates that one of the loaded certificates is unreadable, and could be an unsupported encoding scheme.

Recommended Action Check the configuration of digital certificates and trustpoints.

713082

Error Message `%ASA-3-713082: Failed to retrieve identity certificate`

Explanation Could not find the Identity Certificate for this tunnel.

Recommended Action Check the configuration of digital certificates and trustpoints.

713083

Error Message `%ASA-3-713083: Invalid certificate handle`

Explanation This message indicates that the identity certificate for this tunnel could not be found.

Recommended Action Check the configuration of digital certificates and trustpoints.

713084

Error Message `%ASA-3-713084: Received invalid phase 1 port value (port) in ID payload`

Explanation This message indicates that the port value received in the IKE phase 1 ID payload was incorrect. Acceptable values are 0 or 500 (ISAKMP, also known as IKE).

Recommended Action This may indicate a peer that does not conform to the IKE standards or a network problem that results in corrupted packets.

713085

Error Message `%ASA-3-713085: Received invalid phase 1 protocol (protocol) in ID payload`

Explanation This message indicates that the protocol value received in the IKE phase 1 ID payload was incorrect. Valid values are 0 or 17 (UDP).

Recommended Action This may indicate a peer that does not conform to the IKE standards or a network problem that results in corrupted packets.

713086

Error Message `%ASA-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))`

Explanation This message appears when a cert payload was received but our internal cert handle indicates that we do not have an identity cert. This could mean that the cert handle was not obtained through a normal enrollment method. One likely reason this can happen is that the authentication method is not RSA or DSS signatures, although the IKE SA negotiation should fail if each side is misconfigured.

Recommended Action Check the trustpoint and ISAKMP configuration settings on the appliance and peer.

713088

Error Message `%ASA-3-713088: Set Cert filehandle failure: no IPsec SA in group` *`group_name`*

Explanation This message indicates that the tunnel group could not be found based on the digital certificate information.

Recommended Action Verify that the tunnel group is set up appropriately to handle the certificate information of the peer.

713092

Error Message `%ASA-5-713092: Failure during phase 1 rekeying attempt due to collision`

Explanation This message indicates that an internal software error has occurred.

Recommended Action This is often a benign event. If the problem persists, contact the Cisco TAC.

713094

Error Message `%ASA-7-713094: Cert validation failure: handle invalid for` *`Main/Aggressive Mode Initiator/Responder`*`!`

Explanation This message indicates that an internal software error has occurred.

Recommended Action You may have to reenroll the trustpoint. If the problem persists, contact the Cisco TAC.

713098

Error Message `%ASA-3-713098: Aborting: No identity cert specified in IPsec SA (`*`SA_name`*`)!`

Explanation This message appears when an attempt is made to establish a Certs-based IKE session, but no identity certificate have been specified in the crypto policy.

Recommended Action Specify the identity certificate/trustpoint that you want to transmit to peers.

713099

Error Message `%ASA-7-713099: Tunnel Rejected: Received NONCE length` *`number`* `is out of range!`

Explanation This message indicates that an internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713102

Error Message `%ASA-3-713102: Phase 1 ID Data length` *`number`* `too long - reject tunnel!`

Explanation This message indicates that IKE has received an ID payload containing an Identification Data field of 2 K or greater.

Recommended Action None required.

713103

Error Message `%ASA-7-713103: Invalid (NULL) secret key detected while computing hash`

Explanation This message indicates that an internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713104

Error Message `%ASA-7-713104: Attempt to get Phase 1 ID data failed while` *`hash computation`*

Explanation This message indicates that an internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713105

Error Message `%ASA-3-713105: Zero length data in ID payload received during phase` *`1 or 2`* `processing`

Explanation This message indicates that a peer sent an ID payload without including any ID data, which is invalid.

Recommended Action Check the configuration of the peer.

713107

Error Message `%ASA-3-713107: IP_Address request attempt failed!`

Explanation This message indicates that an internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713109

Error Message `%ASA-3-713109: Unable to process the received peer certificate`

Explanation This message indicates that the security appliance was unable to process the certificate received from the remote peer. This can occur if the certificate data was malformed or if the data in the certificate could not be stored by the appliance. One such possibility is if the public key size is larger than 4096 bits.

Recommended Action Try to reestablish the connection using a different certificate on the remote peer.

713112

Error Message `%ASA-3-713112: Failed to process CONNECTED notify (SPI` *`SPI_value`*`)!`

Explanation This message indicates that the security appliance was unable to successfully process the notify payload that contained notify type CONNECTED. This could occur if the IKE phase 2 structure could not be found using the SPI to locate it, or the commit bit had not been set in the received ISAKMP header. This later case could indicate a non-conforming IKE peer.

Recommended Action If the problem persists, check the configuration of the peer and/or disable commit bit processing.

713113

Error Message `%ASA-7-713113: Deleting IKE SA with associated IPsec connection entries. IKE peer:` *`IP_address`*`, SA address:` *`internal_SA_address`*`, tunnel count:` *`count`*

Explanation This message indicates that an IKE SA is being deleted with a non-0 tunnel count. This means that either the IKE SA tunnel count has lost synchronization with the associated connection entries or the associated connection cookie fields for the entries have lost synchronization with the cookie fields of the IKE SA that the connection entry points to. If this occurs, the IKE SA and its associated data structures will not be freed, so that the entries that may point to it will not have a stale pointer.

Recommended Action None required.

713114

Error Message `%ASA-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA_internal_address) for peer IP_address, but cookies don't match`

Explanation This message indicates that an internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713115

Error Message `%ASA-5-713115: Client rejected NAT enabled IPsec request, falling back to standard IPsec`

Explanation This message indicates the client rejected an attempt by the security appliance to use IPsec over UDP. IPsec over UDP is used to allow multiple clients to establish simultaneous tunnels to the security appliance through a NAT device. The client may have rejected the request either because it does not support this feature or because it is configured to not use it.

Recommended Action Verify the configuration on the headend and peer.

713116

Error Message `%ASA-3-713116: Terminating connection attempt: L2TP-over-IPsec attempted by group (group_name) but L2TP disabled`

Explanation This message indicates that the user or group entity has attempted an L2TP-over-IPsec connection, but the L2TP protocol is not enabled for this security appliance.

Recommended Action Verify the L2TP configuration.

713117

Error Message `%ASA-7-713117: Received Invalid SPI notify (SPI SPI_Value)!`

Explanation This message indicates the IPsec SA identified by the SPI value is no longer active on the remote peer. This might indicate that the remote peer has rebooted or been reset.

Recommended Action This problem should correct itself once DPDs recognize that the peer no longer has the appropriate SAs established. If DPD is not enabled, this may require a manual reestablishment of the affected tunnel.

713118

Error Message `%ASA-3-713118: Detected invalid Diffie-Hellman group_descriptor group_number, in IKE area`

Explanation This message indicates that the *group_descriptor* field contains an unsupported value. Currently we support only groups 1, 2, 5, and 7. In the case of a centry the *group_descriptor* field may also be set to 0, to indicate that Perfect Forward Secrecy (PFS) is disabled.

Recommended Action Check the peer Diffie-Hellman configuration.

713119

Error Message `%ASA-5-713119: PHASE 1 COMPLETED`

Explanation This message appears when IKE Phase 1 has completed successfully.

Recommended Action None required.

713120

Error Message `%ASA-5-713120: PHASE 2 COMPLETED (msgid=msg_id)`

Explanation This message appears when IKE Phase 2 has completed successfully.

Recommended Action None required.

713121

Error Message `%ASA-7-713121: Keep-alive type for this connection: keepalive_type`

Explanation This message indicates the type of keep-alive mechanism being used for this tunnel.

Recommended Action None required.

713122

Error Message `%ASA-3-713122: Keep-alives configured keepalive_type but peer IP_address support keep-alives (type = keepalive_type)`

Explanation This message indicates that keep-alives are configured on/off for this device, but the IKE peer does/does not support keep-alives.

Recommended Action None required if this is intentional. If it is not intentional, change the keepalive configuration on both devices.

713123

Error Message `%ASA-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive_type)`

Explanation This message indicates that the remote IKE peer did not respond to keep-alives within the expected window of time, so the connection to the IKE peer was terminated. The message includes the keep-alive mechanism used.

Recommended Action None required.

713124

Error Message `%ASA-3-713124: Received DPD sequence number rcv_sequence_# in DPD Action, description expected seq #`

Explanation This message indicates that the remote IKE peer sent a DPD with a sequence number that did not match the expected sequence number. The packet is discarded.

Recommended Action This might indicate a packet loss problem with the network.

713127

Error Message `%ASA-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list`

Explanation This message appears when the peer wants to perform a XAUTH, but the security appliance did not choose the XAUTH IKE proposal.

Recommended Action Check the priorities of the IKE xauth proposals in the IKE proposal list.

713128

Error Message `%ASA-6-713128: Connection attempt to VCPIP redirected to VCA peer` *`IP_address`* `via load balancing`

Explanation This message appears when a connection attempt has been made to the VCPIP and has been redirected to a less loaded peer using load balancing.

Recommended Action None required.

713129

Error Message `%ASA-3-713129: Received unexpected Transaction Exchange payload type:` *`payload_id`*

Explanation This message indicates that an unexpected payload has been received during XAUTH or Mode Cfg. This may indicate that the two peers are out of synchronization, that the XAUTH or Mode Cfg versions do not match, or that the remote peer is not complying to the appropriate RFCs.

Recommended Action Verify the configuration between peers.

713130

Error Message `%ASA-5-713130: Received unsupported transaction mode attribute:` *`attribute id`*

Explanation This message indicates that the device received a request for a valid transaction mode attribute (XAUTH or Mode Cfg) that is currently not supported. This is generally a benign condition.

Recommended Action None required.

713131

Error Message `%ASA-5-713131: Received unknown transaction mode attribute:` *`attribute_id`*

Explanation This message indicates that the security appliance has received a request for a transaction mode attribute (XAUTH or Mode Cfg) that is outside the range of known attributes. The attribute may be valid but only supported in later versions of config mode, or the peer may be sending an illegal or proprietary value. This should not cause connectivity problems but may affect the functionality of the peer.

Recommended Action None required.

713132

Error Message `%ASA-3-713132: Cannot obtain an IP_address for remote peer`

Explanation This message indicates that a request for an IP address for a remote access client from the internal utility that provides these addresses could not be satisfied.

Recommended Action Check configuration of IP address assignment methods.

713133

Error Message `%ASA-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH group_id) with phase 1 group(DH group DH group_number)`

Explanation The configured Phase 2 PFS Group differs from the DH group that was negotiated for phase 1.

Recommended Action None required.

713134

Error Message `%ASA-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection`

Explanation This message appears when the configured LAN-to-LAN proposal is different from the one accepted for the LAN-to-LAN connection. Depending on which side is the initiator, different proposals will be used.

Recommended Action None required.

713135

Error Message `%ASA-5-713135: message received, redirecting tunnel to IP_address.`

Explanation This message indicates that the tunnel is being redirected due to load balancing on the remote security appliance. This message will be seen when a REDIRECT_CONNECTION notify packet is received.

Recommended Action None required.

713136

Error Message `%ASA-5-713136: IKE session establishment timed out [IKE_state_name], aborting!`

Explanation This occurs when the reaper has detected an SA stuck in a non-active state. The reaper will try to remove the hung SA.

Recommended Action None required.

713137

Error Message `%ASA-5-713137: Reaper overriding refCnt [ref_count] and tunnelCnt [tunnel_count] -- deleting SA!`

Explanation This message indicates that an internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713138

Error Message `%ASA-3-713138: Group group_name not found and BASE GROUP default preshared key not configured`

Explanation This message appears when there is no group in the group database with the same name as the IP address of the peer. In Main Mode, the security appliance will fall back and try to use the default preshared key configured in one of the default groups. The default preshared key is not configured.

Recommended Action Verify the configuration of the preshared keys.

713139

Error Message `%ASA-5-713139: group_name not found, using BASE GROUP default preshared key`

Explanation There was no tunnel group in the group database with the same name as the IP address of the peer. In Main Mode, the security appliance will fall back and use the default preshared key configured in the default group.

Recommended Action None required.

713140

Error Message `%ASA-3-713140: Split Tunneling Policy requires network list but none configured`

Explanation This message appears when split tunneling policy is set to either split tunneling or allow local LAN access, a split tunneling ACL must be defined to represent the information required by the VPN client.

Recommended Action Check the configuration of the ACLs.

713141

Error Message `%ASA-3-713141: Client-reported firewall does not match configured firewall: action tunnel. Received -- Vendor: vendor(id), Product product(id), Caps: capability_value. Expected -- Vendor: vendor(id), Product: product(id), Caps: capability_value`

Explanation This message indicates that the security appliance installed on the client does not match the configured required security appliance. This message lists the actual and expected values, and whether the tunnel is terminated or allowed.

Recommended Action You may need to install a different personal security appliance on the client or a change of configuration on the security appliance.

713142

Error Message `%ASA-3-713142: Client did not report firewall in use, but there is a configured firewall: action tunnel. Expected -- Vendor: vendor(id), Product product(id), Caps: capability_value`

Explanation This message appears when the client did not report a security appliance in use using ModeCfg but one is required. The event lists the expected values, and whether the tunnel is terminated or allowed. Note that the number following the product string is a bitmask of all of the allowed products.

Recommended Action You may need to install a different personal security appliance on the client or a change of configuration on the security appliance.

713143

Error Message %ASA-7-713143: Processing firewall record. Vendor: *vendor(id)*, Product: *product(id)*, Caps: *capability_value*, Version Number: *version_number*, Version String: *version_text*

Explanation This message provides debug information about the security appliance installed on the client.

Recommended Action None required.

713144

Error Message %ASA-5-713144: Ignoring received malformed firewall record; reason - *error_reason* TLV type *attribute_value correction*

Explanation This message indicates that bad security appliance information was received from the client.

Recommended Action Check the personal security appliance configuration on the client and the security appliance.

713145

Error Message %ASA-6-713145: Detected Hardware Client in network extension mode, adding static route for address: *IP_address*, mask: *netmask*

Explanation This message indicates that a tunnel with a hardware client in network extension mode has been negotiated and a static route is being added for the private network behind the hardware client. This enables the security appliance to make the remote network known to all the routers on the private side of the head-end.

Recommended Action None required.

713146

Error Message %ASA-3-713146: Could not add route for Hardware Client in network extension mode, address: *IP_address*, mask: *netmask*

Explanation This message indicates that an internal software error has occurred. A tunnel with a hardware client in network extension mode has been negotiated and an attempt to add the static route for the private network behind the hardware client failed. This could indicate that the routing table is full or a possible addressing error.

Recommended Action If the problem persists, contact the Cisco TAC.

713147

Error Message `%ASA-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address, mask: netmask`

Explanation This message indicates that a tunnel to a hardware client in network extension mode is being removed and the static route for the private network is being deleted behind the hardware client.

Recommended Action None required.

713148

Error Message `%ASA-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address, mask: netmask`

Explanation This message indicates that while a tunnel to a hardware client in network extension mode was being removed, a route to the private network behind the hardware client could not be deleted.

Recommended Action This might indicate an addressing or software problem. Check the routing table to ensure that the route is not there. If it is, it may have to be removed manually, but only if the tunnel to the hardware client has been completely removed.

713149

Error Message `%ASA-3-713149: Hardware client security attribute attribute_name was enabled but not requested.`

Explanation This message indicates that the headend security appliance has the specified hardware client security attribute enabled, but the attribute was not requested by the VPN 3002 hardware client.

Recommended Action Check the configuration on the hardware client.

713152

Error Message `%ASA-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.`

Explanation This message indicates that the client is required to use CPP to provision its security appliance, but the headend device was unable to obtain any ACLs to send to the client. This is probably due to a misconfiguration.

Recommended Action Check the ACLs specified for CPP in the group policy for the client.

713154

Error Message `%ASA-4-713154: DNS lookup for peer_description Server [server_name] failed!`

Explanation This message appears when DNS lookup for the specified server has not been resolved.

Recommended Action Check DNS server configuration on the security appliance. Also check the DNS server to ensure that it is operational and has the hostname to IP address mapping.

713155

Error Message `%ASA-5-713155: DNS lookup for Primary VPN Server [server_name] successfully resolved after a previous failure. Resetting any Backup Server init.`

Explanation A previous DNS lookup failure for the primary server might have caused the system to initialize a backup peer. This message indicates that a later DNS lookup on the primary server finally succeeded and is resetting any backup server initializations. A tunnel initiated after this point will be aimed at the primary server.

Recommended Action None required.

713156

Error Message `%ASA-5-713156: Initializing Backup Server [server_name or IP_address]`

Explanation This message indicates that the client is failing over to a backup server or a failed DNS lookup for the primary server caused the system to initialize a backup server. A tunnel initiated after this point will be aimed at the specified backup server.

Recommended Action None required.

713157

Error Message `%ASA-4-713157: Timed out on initial contact to server [server_name or IP_address] Tunnel could not be established.`

Explanation This message indicates that the client tried to initiate a tunnel by sending out IKE MSG1, but did not receive a response from the security appliance on the other end. If backup servers are available, the client will attempt to connect to one of them.

Recommended Action Verify connectivity to the headend security appliance.

713158

Error Message `%ASA-5-713158: Client rejected NAT enabled IPsec Over UDP request, falling back to IPsec Over TCP`

Explanation This message indicates that the client is configured to use IPsec over TCP. The client rejected the attempt by the security appliance to use IPsec over UDP.

Recommended Action If TCP is desired, none required. Otherwise, check the client configuration.

713159

Error Message `%ASA-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access`

Explanation This message indicates that the TCP connection to the security appliance server was lost for some reason. Likely reasons are that the server has rebooted, has a network problem, has an SSL mismatch, and so on.

Recommended Action If the server connection was lost after the initial connection was made, then the server and network connections must be checked. If the initial connection is lost immediately, this could indicate an SSL authentication problem.

713160

Error Message `%ASA-7-713160: Remote user (session Id - id) has been granted access by the Firewall Server`

Explanation This message indicates normal authentication of the remote user to the security appliance server.

Recommended Action None required.

713161

Error Message `%ASA-3-713161: Remote user (session Id - id) network access has been restricted by the Firewall Server`

Explanation The security appliance server has sent the security appliance a message indicating that this user must be restricted. There are several reasons for this including security appliance software upgrades, changes in permissions, and so on. The security appliance server will transition the user back into full access mode as soon as the operation has been completed.

Recommended Action None required unless the user is never transitioned back into full access state. If this does not happen, access the security appliance server for more information on the operation that is being performed and the state of the security appliance software running on the remote machine.

713162

Error Message `%ASA-3-713162: Remote user (session Id - id) has been rejected by the Firewall Server`

Explanation This message indicates that the security appliance server has rejected this user.

Recommended Action Check the policy information on the security appliance server to make sure that the user is configured correctly.

713163

Error Message `%ASA-3-713163: Remote user (session Id - id) has been terminated by the Firewall Server`

Explanation This message indicates that the security appliance server has terminated this user session. This can happen if the integrity agent stops running on the client machine or if the security policy is modified by the remote user in any way.

Recommended Action Verify that the security appliance software on the client machine is still running and that the policy is correct.

713164

Error Message `%ASA-7-713164: The Firewall Server has requested a list of active user sessions`

Explanation This message indicates that the security appliance server will request the session information if it detects that it has stale data or if it loses the session data (as in a reboot).

Recommended Action None required.

713165

Error Message `%ASA-3-713165: Client IKE Auth mode differs from the group's configured Auth mode`

Explanation This message indicates that the client negotiated with preshared keys while its tunnel group points to a policy that is configured to use digital certificates.

Recommended Action Check the client configuration.

713166

Error Message `%ASA-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password`

Explanation This message indicates that the hardware client has failed extended authentication. This is most likely a username and password problem or server authentication issue.

Recommended Action Verify that the configured username and password values on each side match. Also verify that the authentication server at the headend is operational.

713167

Error Message `%ASA-3-713167: Remote peer has failed user authentication - check configured username and password`

Explanation This message indicates that the remote user has failed to extend authentication. This is most likely a username or password problem or server authentication issue.

Recommended Action Verify that the configured username and password values on each side match. Also verify that the authentication server being used to authenticate the remote is operational.

713168

Error Message `%ASA-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!`

Explanation This message indicates that reauthentication on rekey has been enabled but the tunnel authentication requires manual intervention.

Recommended Action If manual intervention is desired, none required. Otherwise, check the interactive authentication configuration.

713169

Error Message `%ASA-7-713169: IKE Received delete for rekeyed SA IKE peer: IP_address, SA address: internal_SA_address, tunnelCnt: tunnel_count`

Explanation This message indicates that IKE has received a delete message from the remote peer to delete its old IKE SA after a rekeying is completed.

Recommended Action None required.

713170

Error Message `%ASA-7-713170: IKE Received delete for rekeyed centry IKE peer: IP_address, centry address: internal_address, msgid: id`

Explanation IKE receives a delete message from the remote peer to delete its old centry after phase 2 rekeying is completed.

Recommended Action None required.

713171

Error Message `%ASA-7-713171: NAT-Traversal sending NAT-Original-Address payload`

Explanation UDP-Encapsulated-Transport was either proposed or selected during phase 2. Need to send this payload for NAT-Traversal in this case.

Recommended Action None required.

713172

Error Message `%ASA-6-713172: Automatic NAT Detection Status: Remote end is|is not behind a NAT device This end is|is_not behind a NAT device`

Explanation Results from NAT auto-detection by NAT-Traversal.

Recommended Action None required.

713174

Error Message `%ASA-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!`

Explanation A hardware client is attempting to tunnel in using network extension mode, but network extension mode is not allowed.

Recommended Action Verify the configuration of the network extension mode as compared to the PAT mode.

713176

Error Message `%ASA-2-713176: Device_type memory resources are critical, IKE key acquire message on interface interface_number, for Peer IP_address ignored`

Explanation This event indicates that the appliance is processing data intended to trigger an IPsec tunnel to the indicated peer. Because memory resources are at a critical state, it is not initiating any more tunnels. The data packet has been ignored and dropped.

Recommended Action If condition persists, verify that appliance is efficiently configured. This event could indicate that an appliance with increased memory is required for this application.

713177

Error Message `%ASA-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name: host_name Address IP_address, Protocol protocol, Port port`

Explanation A Phase 2 ID payload containing an FQDN has been received from the peer.

Recommended Action None required.

713178

Error Message `%ASA-5-713178: IKE Initiator received a packet from its peer without a Responder cookie`

Explanation An internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713179

Error Message `%ASA-5-713179: IKE AM Initiator received a packet from its peer without a payload_type payload`

Explanation An internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713182

Error Message `%ASA-3-713182: IKE could not recognize the version of the client! IPsec Fragmentation Policy will be ignored for this connection!`

Explanation An internal software error has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

713184

Error Message `%ASA-6-713184: Client Type: Client_type Client Application Version: Application_version_string`

Explanation This event indicates the client operating system and application version. If the information is not available, then N/A will be indicated.

Recommended Action None required.

713185

Error Message `%ASA-3-713185: Error: Username too long - connection aborted`

Explanation The client returned an invalid length username, and the tunnel was torn down.

Recommended Action Check the username and make changes if necessary.

713186

Error Message `%ASA-3-713186: Invalid secondary domain name list received from the authentication server. List Received: list_text Character index (value) is illegal`

Explanation An invalid secondary domain name list was received from an external RADIUS authentication server. When split tunnelling is used, this list identifies the domains that the client should resolve through the tunnel.

Recommended Action Correct the specification of the Secondary-Domain-Name-List attribute (vendor-specific attribute 29) on the RADIUS server. The list must be specified as a comma delimited list of domain names. Domain names may not include any characters other than alpha-numerics, hyphen, underscore, and period.

713187

Error Message `%ASA-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: IP_address, Remote peer address: IP_address`

Explanation The IKE peer that is attempting to bring up this tunnel is not the one that is configured in the ISAKMP configuration that is bound to the received remote subnet(s).

Recommended Action Verify correct L2L settings on the headend and peer.

713189

Error Message `%ASA-3-713189: Attempted to assign network or broadcast IP_address, removing (IP_address) from pool.`

Explanation The IP address from the pool is either the network or broadcast address for this subnet. This address will be marked as unavailable.

Recommended Action This error is generally benign but the IP address pool configuration should be checked.

713190

Error Message `%ASA-7-713190: Got bad refCnt (ref_count_value) assigning IP_address (IP_address)`

Explanation The reference counter for this SA is invalid.

Recommended Action This issue should correct itself.

713193

Error Message `%ASA-3-713193: Received packet with missing payload, Expected payload: payload_id`

Explanation The security appliance received an encrypted or unencrypted packet of the specified exchange type that had one or more missing payloads. This usually indicates a problem on the peer.

Recommended Action Verify that the peer is sending valid IKE messages.

713194

Error Message `%ASA-3-713194: IKE|IPsec Delete With Reason message: termination_reason`

Explanation Indicates that a delete message with a termination reason code was received.

Recommended Action None required.

713195

Error Message `%ASA-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!`

Explanation The peer can accept incoming connections only after it opens the first P2 tunnel. At that point, data from either direction can initiate additional Phase 2 tunnels.

Recommended Action If a different behavior is desired, the originate-only configuration needs to be revisited.

713196

Error Message `%ASA-5-713196: Remote L2L Peer IP_address initiated a tunnel with same outer and inner addresses. Peer could be Originator Only - Possible misconfiguration!`

Explanation The remote L2L peer has initiated a Public-Public tunnel. The remote L2L peer expects a response from the peer at the other end, but does not receive one, because of a possible misconfiguration.

Recommended Action Check the L2L configuration on both sides.

713197

Error Message `%ASA-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection. Enforcing the second default.`

Explanation The configured Confidence Interval in the group is outside of the valid range.

Recommended Action Check the Confidence Setting in the group to make sure it is within the valid range.

713198

Error Message `%ASA-3-713198: User Authorization failed: user User authorization failed.`

Explanation This event will contain a reason string.

Recommended Action Check the group configuration and client authorization.

713199

Error Message `%ASA-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter (counter_value)!`

Explanation The reaper corrected an internal software error.

Recommended Action If the problem persists, contact the Cisco TAC.

713203

Error Message `%ASA-3-713203: IKE Receiver: Error reading from socket.`

Explanation This message indicates that there was an error while reading a received IKE packet. This is generally an internal error and might indicate a software problem.

Recommended Action This problem is usually benign and the system will correct itself. If the problem persists, contact the Cisco TAC.

713204

Error Message `%ASA-7-713204: Adding static route for client address: IP_address`

Explanation This message indicates that a route to the peer-assigned address or to the networks protected by a hardware client was added to the routing table.

Recommended Action None required.

713205

Error Message `%ASA-3-713205: Could not add static route for client address: IP_address`

Explanation This message indicates a failed attempt to add a route to the client-assigned address or to the networks protected by a hardware client. This could indicate duplicate routes in the routing table or a corrupted network address. The duplicate routes could be caused by routes not cleaned up correctly or by having multiple clients sharing networks or addresses.

Recommended Action Check the IP local pool configuration as well as any other IP address-assigning mechanism being used (for example: DHCP or RADIUS). Ensure that routes are being cleared from the routing table. Also check the configuration of networks and/or addresses on the peer system.

713206

Error Message `%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy`

Explanation This message appears when a tunnel is dropped because the allowed tunnel specified in the group policy is different than the allowed tunnel in the tunnel-group configuration.

Recommended Action Check the tunnel-group and group-policy configuration.

713208

Error Message `%ASA-3-713208: Cannot create dynamic rule for Backup L2L entry rule rule_id`

Explanation This message indicates that there was a failure in creating the ACLs that trigger IKE and allow IPsec data to be processed correctly. The failure was specific to the Backup L2L configuration. This may indicate a configuration error, a capacity error or an internal software error.

Recommended Action If the device is running at maximum security appliance cons and maximum VPN tunnels, there may be a memory issue. If not, check the backup L2L and crypto map configuration, specifically the ACLs associated with the crypto maps.

713209

Error Message `%ASA-3-713209: Cannot delete dynamic rule for Backup L2L entry` *`rule id`*

Explanation This message indicates that there was a failure in deleting the ACLs that trigger IKE and allow IPsec data to be processed correctly. The failure was specific to the Backup L2L configuration. This may indicate an internal software error.

Recommended Action If the problem persists, contact the Cisco TAC.

713210

Error Message `%ASA-3-713210: Cannot create dynamic map for Backup L2L entry` *`rule_id`*

Explanation This message indicates that there was a failure in creating a run-time instance of the dynamic crypto map associated with backup L2L configuration. This may indicate a configuration error, a capacity error or an internal software error.

Recommended Action If the device is running at maximum security appliance cons and maximum VPN tunnels, there may be a memory issue. If not, check the backup L2L and crypto map configuration, specifically the ACLs associated with the crypto maps.

713211

Error Message `%ASA-6-713211: Adding static route for L2L peer coming in on a dynamic map. address:` *`IP_address`*`, mask:` *`netmask`*

Explanation This message indicates that the security appliance is adding a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

Recommended Action None required.

713212

Error Message `%ASA-3-713212: Could not add route for L2L peer coming in on a dynamic map. address: IP_address, mask: netmask`

Explanation This message appears when the security appliance failed while attempting to add a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. This could indicate duplicate routes. A full routing table or a failure of the security appliance to remove previously used routes.

Recommended Action Check the routing table to make sure that there is room for additional routes and that obsolete routes are not present. If the table is full or contains obsolete routes, remove the routes and try again. If the problem persists, contact the Cisco TAC.

713213

Error Message `%ASA-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask`

Explanation This message indicates that the security appliance is deleting a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

Recommended Action None required.

713214

Error Message `%ASA-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address, mask: netmask`

Explanation This message indicates that the security appliance experienced a failure while deleting a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. This event may indicate that the route has already been deleted or that an internal software error has occurred.

Recommended Action If the route has already been deleted, the condition is benign and the device will function normally. If the problem persists or can be linked to routing issues over VPN tunnels, then check the routing and addressing portions of the VPN L2L configuration. Check the reverse route injection and the ACLs associated with the appropriate crypto map. If the problem persists, contact the Cisco TAC.

713215

Error Message `%ASA-6-713215: No match against Client Type and Version rules. Client: type version is/is not allowed by default`

Explanation This message indicates that the client type and the version of a client did not match any of the rules configured on the security appliance. The default action is displayed.

Recommended Action Determine what the default action and deployment requirements are and make the appropriate changes.

713216

Error Message `%ASA-5-713216: Rule: action Client type: version Client: type version is/is not allowed`

Explanation This message indicates that the client type and the version of a client has matched one of the rules. The result of the match and the rule are displayed.

Recommended Action Determine what the deployment requirements are and make the appropriate changes.

713217

Error Message `%ASA-3-713217: Skipping unrecognized rule: action: action client type: client_type client version: client_version`

Explanation This message indicates that there is a malformed client type and version rule. The required format is *action client type* | *client version action* either "permit" or "deny" *client type* and *client version* are displayed under Session Management. Only one wildcard per parameter (*) is supported.

Recommended Action Correct the rule.

713218

Error Message `%ASA-3-713218: Tunnel Rejected: Client Type or Version not allowed.`

Explanation This message indicates that the client was rejected access per the configured rules.

Recommended Action None required.

713219

Error Message `%ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when P1 SA is complete.`

Explanation This message indicates that Phase 2 messages are being enqueued after Phase 1 completes.

Recommended Action None required.

713220

Error Message `%ASA-6-713220: De-queueing KEY-ACQUIRE messages that were left pending.`

Explanation This message indicates that queued Phase 2 messages are being processed.

Recommended Action None required.

713221

Error Message `%ASA-7-713221: Static Crypto Map check, checking map = crypto_map_tag, seq = seq_number...`

Explanation This message indicates that the security appliance is iterating through the crypto maps looking for configuration information.

Recommended Action None required.

713222

Error Message `%ASA-7-713222: Static Crypto Map check, map = crypto_map_tag, seq = seq_number, ACL does not match proxy IDs src: source_address dst: dest_address`

Explanation This message indicates that while iterating through the configured crypto maps, the security appliance could not match any of the associated ACLs. This generally means that an ACL was misconfigured.

Recommended Action Check the ACLs associated with this tunnel peer and make sure they specify the appropriate private networks from both sides of the VPN tunnel.

713223

Error Message `%ASA-7-713223: Static Crypto Map check, map = crypto_map_tag, seq = seq_number, no ACL configured`

Explanation This message indicates that the crypto map associated with this peer is not linked to an ACL.

Recommended Action Make sure there is an ACL associated with this crypto map and that the ACL contains the appropriate private addresses or network from both sides of the VPN tunnel.

713224

Error Message `%ASA-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!`

Explanation This message indicates that the crypto map associated with this VPN tunnel is missing critical information.

Recommended Action Verify that the crypto map is configured correctly with both the VPN peer, a transform set, and an associated ACL.

713225

Error Message `%ASA-7-713225: [IKEv1], Static Crypto Map check, map map_name, seq = sequence_number is a successful match`

Explanation This message indicates that the security appliance found a valid matching crypto map for this VPN tunnel.

Recommended Action None required.

713226

Error Message `%ASA-3-713226: Connection failed with peer IP_address, no trust-point defined in tunnel-group tunnel_group`

Explanation When the device is configured to use digital certificates, a trust point must be specified in the configuration. When the trust point is missing from the config, this message is generated to flag an error.

- *IP_address*—IP address of the peer.
- *tunnel_group*—Tunnel group for which trust point was missing in the configuration.

Recommended Action The administrator of the device has to specify a trust point in the configuration.

713227

Error Message `%ASA-3-713227: Rejecting new IPSec SA negotiation for peer Peer_address. A negotiation was already in progress for local Proxy Local_address/Local_netmask, remote Proxy Remote_address/Remote_netmask`

Explanation When establishing a Phase 2 SA, the security appliance will reject a new Phase SA that matches this proxy.

Recommended Action None required. The security appliance should recover automatically.

713228

Error Message `%ASA-6-713228: Group = group, Username = uname, IP = remote_IP_address Assigned private IP address assigned_private_IP to remote user`

- *group*—The name of the group.
- *uname*—The name of the user.
- *remote_IP_address*—The IP address of the remote client.
- *assigned_private_IP*—The client IP assigned by DHCP or from the local address pool.

Explanation This message is generated when IKE obtains an address for the client private IP address from DHCP or from the address pool. The message specifies the IP address assigned to the client.

Recommended Action None required.

713229

Error Message `%ASA-5-713229: Auto Update - Notification to client client_ip of update string: message_string.`

Explanation This message is displayed when a VPN remote access client is notified that updated software is available for download. The remote client user is responsible for choosing to update the client access software.

- *client_ip*—The IP address of the remote client.
- *message_string*—The message text sent to the remote client.

Recommended Action None required.

713230

Error Message `%ASA-3-713230 Internal Error, ike_lock trying to lock bit that is already locked for type type`

- *type*—String that describes the type of semaphore that had a locking issue.

Explanation This message is displayed due to an internal error, which is reporting that the IKE subsystem is attempting to lock memory that has already been locked. This indicates errors on semaphores used to protect memory violations for IKE SAs. This message does not indicate that anything is seriously wrong. However, an unexpected event has happened and steps are automatically being taken for recovery.

Recommended Action If the problem persists, contact the Cisco TAC.

713231

Error Message `%ASA-3-713231 Internal Error, ike_lock trying to unlock bit that is not locked for type` *`type`*

Explanation This message is displayed due to an internal error, which is reporting that the IKE subsystem is attempting to unlock memory that is not currently locked. This indicates errors on semaphores used to protect memory violations for IKE SAs. This message does not indicate that anything is seriously wrong. However, an unexpected event has happened and steps are automatically being taken for recovery.

- *type*—String that describes the type of semaphore that had a locking issue.

Recommended Action If the problem persists, contact the Cisco TAC.

713232

Error Message `%ASA-3-713232 SA lock refCnt =` *`value`*`, bitmask =` *`hexvalue`*`, p1_decrypt_cb =` *`value`*`, qm_decrypt_cb =` *`value`*`, qm_hash_cb =` *`value`*`, qm_spi_ok_cb =` *`value`*`, qm_dh_cb =` *`value`*`, qm_secret_key_cb =` *`value`*`, qm_encrypt_cb =` *`value`*

Explanation This message displays all the IKE SA locks and is displayed when a possible error has been detected. This message reports errors on semaphores used to protect memory violations for IKE SAs.

- *value*—Decimal value.
- *hexvalue*—Hexadecimal value.

Recommended Action If the problem persists, contact the Cisco TAC.

713233

Error Message `%ASA-7-713233: (VPN-unit) Remote network (remote network) validated for network extension mode.`

Explanation This message is displayed when the remote network received during the Phase 2 negotiation is validated. This message indicates the results of the remote network check during Phase 2 negotiations for Network Extension Mode clients. This is part of an existing feature that prevents users from misconfiguring their HW client network (for example, configuring overlapping networks or the same network on multiple clients).

- *remote network*—Subnet address and subnet mask from Phase 2 proxy.

Recommended Action None required.

713234

Error Message `%ASA-7-713234: (VPN-unit) Remote network (remote network) from network extension mode client mismatches AAA configuration (aaa network).`

Explanation This message is displayed when the remote network received during the Phase 2 negotiation does not match the framed-ip-address and framed-subnet-mask returned from the AAA server for this session.

- *remote network*—Subnet address and subnet mask from Phase 2 proxy.
- *aaa network*—Subnet address and subnet mask configured through AAA.

Recommended Action Do one of the following:

- Check the address assignment for this user and group, check the network configuration on the hardware client, and fix any inconsistencies.
- Disable address assignment for this user and group.

713235

Error Message `%ASA-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!`

Explanation Normally, IKE packets should never be sent from the standby unit to the remote peer. This message is displayed if such an attempt is made due to an internal logic error. The packet never leaves the standby unit because of protective code. This message is mainly to facilitate debugging.

Recommended Action None required by the user. Developers should look into the condition causing the IKE packet to be sent from the standby unit.

713236

Error Message `%ASA-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1_len) + payload2 (payload2_len)...total length: tlen`

Explanation This message is displayed when IKE sends or receives various messages.

The following example shows the output when IKE receives a message with an 8-byte hash payload, an 11-byte notify payload and two 13-byte vendor-specific payloads:

```
%ASA-7-713236: IKE_DECODE RECEIVED Message msgid=0) with payloads: HDR + HASH (8) +
NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0)
```

Recommended Action None required.

713237

Error Message `%ASA-5-713237: ACL update (access_list) received during re-key re-authentication will not be applied to the tunnel.`

Explanation This message is displayed during the Phase 1 rekey of a remote access IPsec tunnel under the following conditions:

- The tunnel is configured to reauthenticate the user when the tunnel is rekeyed.
- The RADIUS server returns an access list or a reference to a locally configured access list that is different from the one that was returned when the tunnel was first established.

Under these conditions, the security appliance ignores the new access list and this message is generated.

- *access_list*—Name associated with the static or dynamic access-list, as displayed in the output of the **show access-list** command

Recommended Action IPsec users must reconnect for new user-specific access lists to take effect.

713238

Error Message `%ASA-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client`

Explanation The private side address of a network extension mode client came across as 0.0.0.0. This usually indicates that no IP address was set on the private interface of the hardware client.

Recommended Action Verify the configuration of the remote client.

713239

Error Message `%ASA-4-713239: IP_Address: Tunnel Rejected: The maximum tunnel count allowed has been reached`

Explanation An attempt to create a tunnel has occurred after the maximum number of tunnels allowed has been reached.

- *IP_Address*—The IP address of the peer.

Recommended Action None required.

713240

Error Message `%ASA-4-713240: Received DH key with bad length: received length=rlength expected length=elength`

Explanation A Diffie-Hellman key with the incorrect length was received from the peer.

- *rlength*—The length of the DH key that was received.
- *elength*—The expected length (based on DH key size).

Recommended Action None required.

713241

Error Message `%ASA-4-713241: IE Browser Proxy Method setting_number is Invalid`

Explanation An invalid proxy setting was found during ModeCfg processing. P1 negotiation will fail.

Recommended Action Check the **msie-proxy method** command settings (a subcommand of the **group-policy** command), which should conform to one of the following: [**auto-detect** | **no-modify** | **no-proxy** | **use-server**]. Any other value or no value is incorrect. Try resetting the "msie-proxy method" settings. If the problem persists, contact the Cisco TAC.

713242

Error Message `%ASA-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.`

Explanation The security appliance has detected a request to start an IKE rekey for a tunnel configured to use Hybrid Xauth, but the rekey was not started. The security appliance will wait for the client to detect and initiate an IKE rekey.

Recommended Action None required.

713243

Error Message `%ASA-4-713243: META-DATA Unable to find the requested certificate`

Explanation The IKE peer requested a certificate from the cert-req payload. However, no valid identity certificate was issued by the requested DN was found.

Recommended Action Perform the following steps:

1. Check the identity certificates.
2. Enroll or import the desired certificate.
3. Enable certificate debugging for more details.

713244

Error Message `%ASA-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type.`

- *type*—The LAM type.

Explanation The LAM attribute type received differs from the last type received. The type must be consistent throughout the user authentication process. The user authentication process cannot proceed and the VPN connection will not be established.

Recommended Action If the problem persists, contact the Cisco TAC.

713245

Error Message `%ASA-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.`

Explanation An unsupported LAM type was received during the CRACK challenge/response user authentication process. The user authentication process cannot proceed, and the VPN connection will not be established.

- *type*—The LAM type

Recommended Action If the problem persists, contact the Cisco TAC.

713246

Error Message `%ASA-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.`

Explanation The device received an unknown LAM attribute type, which should not cause connectivity problems but might affect the functionality of the peer.

- *type*—The LAM attribute type.

Recommended Action None required.

713247

Error Message `%ASA-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.`

Explanation An unexpected error occurred during state processing.

Recommended Action If the problem persists, contact the Cisco TAC.

713248

Error Message `%ASA-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.`

Explanation When an IKE SA is negotiated using the CRACK authentication method, Phase 1 SA rekey timer at the headend expired before a successful rekey. Because the remote client is always the initiator of the exchange when using the CRACK authentication method, the headend will not initiate the rekey. Unless the remote peer initiates a successful rekey before the IKE SA expires, the connection will come down upon IKE SA expiration.

Recommended Action None required.

713249

Error Message `%ASA-4-713249: META-DATA Received unsupported authentication results: result`

Explanation While negotiating an IKE SA using the CRACK authentication method, the IKE subsystem received a result that is not supported during CRACK authentication from the authentication subsystem. The user authentication fails and the VPN connection is torn down.

- *result*—The result returned from the authentication subsystem.

Recommended Action If the problem persists, contact the Cisco TAC.

713250

Error Message `%ASA-5-713250: META-DATA Received unknown Internal Address attribute: attribute`

Explanation The device received a request for an Internal Address attribute that is not recognizable. The attribute might be valid, but not currently supported or the peer might be sending an illegal value. This should not cause connectivity problems but might affect the functionality of the peer.

Recommended Action None required.

713251

Error Message `%ASA-4-713251: META-DATA Received authentication failure message`

Explanation The device received a notify message indicating authentication failure while an IKE SA is negotiated using the CRACK authentication method. The connection is torn down.

Recommended Action None required.

713252

Error Message `%ASA-5-713252: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.`

Explanation When the group policy is configured to require the client to authenticate with a Zonelab Integrity Server, the server might need to be connected to the concentrator depending on the fail policy configured. If the fail policy is to reject the client connection, this syslog message is generated when a Zonelab Integrity Server is not connected to the security appliance at the time the client is connecting.

- *group*—The tunnel group to which the remote access user is connecting.
- *user*—The remote access user.
- *ip*—The IP address of the remote access user.

Recommended Action Check that the configurations on the concentrator and the Zonelab Integrity Server match. Then verify communication between the concentrator and the Zonelab Integrity Server.

713253

Error Message `%ASA-5-713253: Group = group, Username = user, IP = ip, Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.`

Explanation When the group policy is configured to require a client to authenticate with a Zonelab Integrity Server, the server might need to be connected to the concentrator, depending on the fail policy configured. If the fail policy is to accept the client connection, and provides unrestricted network access, this syslog message is generated when a Zonelab Integrity Server is not connected to the security appliance at the time the client is connecting.

- *group*—The tunnel group to which the remote access user is connecting.
- *user*—The remote access user.
- *ip*—The IP address of the remote access user.

Recommended Action Check that the configurations on the security device and the Zonelab Integrity Server match, and verify communication between the security appliance and the Zonelab Integrity Server.

713254

Error Message `%ASA-3-713254: Group = groupname, Username = username, IP = peerip, Invalid IPsec/UDP port = portnum, valid range is minport - maxport, except port 4500, which is reserved for IPsec/NAT-T`

Explanation You cannot use UDP port 4500 for IPsec/UDP connections, because it is reserved for IPsec/NAT-T connections. The CLI does not allow this configuration for local groups. This message should only occur for externally defined groups.

- *groupname*—The name of the user group.
- *usernamae*—The name of the user.
- *peerip*—The IP address of the client.
- *portnum*—The IPsec/UDP port number on the external server.
- *minport*—The minimum valid port number for a user-configurable port, which is 4001.
- *maxport*—The maximum valid port number for a user-configurable port, which is 49151.

Recommended Action Change the IPsec/UDP port number on the external server to another port number. Valid port numbers are 4001 to 49151.

713255

Error Message `%ASA-4-713255: IP = peer-IP, Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name 'group-name'`

Explanation An unknown tunnel group was specified in ISAKMP Aggressive Mode message 1.

- *peer-ip*—The address of the peer.
- *group-name*—The group name specified by the peer.

Recommended Action Check the tunnel group and client configurations to make sure they are valid.

713256

Error Message `%ASA-6-713256: IP = peer-IP, Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.`

Explanation When the peer specifies an invalid tunnel group, the ASA will still send message 2 to prevent the peer from gleaning tunnel group information.

- *peer-ip*—The address of the peer.

Recommended Action None required.

713257

Error Message `%ASA-5-713257: Phase var1 failure: Mismatched attribute types for class var2: Rcv'd: var3 Cfg'd: var4`

Explanation This syslog will be seen on an ASA acting as the responder in a LAN-to-LAN connection. It indicates that the ASA's crypto configuration does not match that of the initiator's. The syslog specifies during what phase the mismatch happened, and what attributes both the responder and the initiator had that were different.

- *var1*—The phase the mismatch happened during
- *var2*—The class the attributes that do not match belong to
- *var3*—The attribute received from the initiator
- *var4*—The attribute configured

Recommended Action Check the crypto configuration on both of the LAN-to-LAN devices for inconsistencies. In particular, if a mismatch between UDP-Tunnel(NAT-T) and something else is reported, check the crypto maps. If one configuration has NAT-T disabled on the matched crypto map and the other does not, this will cause a failure.

713258

Error Message `%ASA-3-713258: IP = var1, Attempting to establish a phase2 tunnel on var2 interface but phase1 tunnel is on var3 interface. Tearing down old phase1 tunnel due to a potential routing change.`

Explanation This message appears when the adaptive security appliance tries to establish a phase 2 tunnel on an interface, and a phase 1 tunnel already exists on a different interface. The existing phase 1 tunnel is torn down to allow the establishment of a new tunnel on the new interface.

- *var1*—The IP address of the peer.
- *var2*—The interface on which the adaptive security appliance is trying to establish a phase 2 tunnel.
- *var3*—The interface on which the phase 1 tunnel exists.

Recommended Action Check whether or not the route of the peer has changed. If the route has not changed, a possible misconfiguration may exist.

713259

Error Message `%ASA-5-713259: Group = groupname, Username = username, IP = peerIP, Session is being torn down. Reason: reason`

Explanation This message is generated when an ISAKMP session is torn down through session management.

- *groupname*—The tunnel group of the session being terminated.
- *username*—Theusername of the session being terminated.
- *peerIP*—The peer IP address of the session being terminated.
- *reason*—The RADIUS termination reason of the session being terminated, which can be one of the following:

  - Port Preempted, because of simultaneous login
  - Idle Timeout
  - Max Time Exceeded
  - Administrator Reset

Recommended Action None required.

713900

Error Message `%ASA-7-713900: Descriptive_event_string.`

Explanation A message with several possible text strings describing a serious event or failure.

Recommended Action If the problem persists, contact the Cisco TAC.

713901

Error Message %ASA-7-713901: *Descriptive_event_string*.

Explanation Message with several possible text strings describing an error which has occurred. This may be the result of configuration error on the headend or remote access client. The event string provides details about the error that occurred.

Recommended Action You may need to troubleshoot the to determine what caused the error. Check the **isakmp** and **crypto map** configuration on both peers.

713902

Error Message %ASA-3-713902 *descriptive_event_string*

Explanation This syslog message could have several possible text strings describing an error. This may be the result of a configuration error either on the headend or remote access client.

Recommended Action It might be necessary to troubleshoot the configuration to determine the cause of the error. Check the ISAKMP and crypto map configuration on both peers.

713903

Error Message %ASA-4-713903: *descriptive_event_string*.

Explanation This may be the result of unexpected behavior of a peer (for example, a loss of connectivity).

For example, %ASA-4-713903: Group = IPSecGroup. IP = 70.172.17.23, Error: Unable to remove PeerTblEntry. This message usally occurs when an IPsec connection attempt fails (for example, in an authentication failure) that was caused by an incorrectly typed password or the inadventent disconnection of an IPSec client during authentication.

Recommended Action Informational only.

713904

Error Message %ASA-5-713904: *descriptive_event_string*.

Explanation Syslog message with several possible text strings describing some general status information. These messages are used to keep track of events that have occurred.

Recommended Action Informational only.

714001

Error Message `%ASA-7-714001: description_of_event_or_packet`

Explanation Description of IKE protocol event or packet.

Recommended Action Informational only.

714002

Error Message `%ASA-7-714002: IKE Initiator starting QM: msg id = message_number`

Explanation The security appliance has sent the first packet of the Quick mode exchange as the Phase 2 initiator.

Recommended Action Informational only.

714003

Error Message `%ASA-7-714003: IKE Responder starting QM: msg id = message_number`

Explanation The security appliance has received the first packet of the Quick mode exchange as the Phase 2 responder.

Recommended Action Informational only.

714004

Error Message `%ASA-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number`

Explanation Protocol decode of the first Quick Mode packet.

Recommended Action Informational only.

714005

Error Message `%ASA-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number`

Explanation Protocol decode of the second Quick Mode packet.

Recommended Action Informational only.

714006

Error Message `%ASA-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number`

Explanation Protocol decode of the third Quick Mode packet.

Recommended Action Informational only.

714007

Error Message `%ASA-7-714007: IKE Initiator sending Initial Contact`

Explanation The security appliance is building and sending the initial contact payload.

Recommended Action Informational only.

714011

Error Message `%ASA-7-714011: Description of received ID values`

Explanation The security appliance received the displayed ID information during the negotiation.

Recommended Action Informational only.

715001

Error Message `%ASA-7-715001: Descriptive statement`

Explanation This message provides a description of an event or problem encountered by the security appliance.

Recommended Action The action depends on the description.

715004

Error Message `%ASA-7-715004: subroutine name() Q Send failure: RetCode (return_code)`

Explanation This message indicates that there was an internal error when attempting to put messages in a queue.

Recommended Action This is often a benign condition. If the problem persists, contact the Cisco TAC.

715005

Error Message %ASA-7-715005: subroutine *name*() Bad message code: Code (*message_code*)

Explanation This message indicates that an internal subroutine received a bad message code.

Recommended Action This is often a benign condition. If the problem persists, contact the Cisco TAC.

715006

Error Message %ASA-7-715006: IKE got SPI from key engine: SPI = *SPI_value*

Explanation This message indicates that the IKE subsystem received an SPI value from IPsec.

Recommended Action None required.

715007

Error Message %ASA-7-715007: IKE got a KEY_ADD msg for SA: SPI = *SPI_value*

Explanation This message indicates that IKE has completed tunnel negotiation and has successfully loaded the appropriate encryption and hashing keys for IPsec use.

Recommended Action None required.

715008

Error Message %ASA-7-715008: Could not delete SA *SA_address*, refCnt = *number*, caller = *calling_subroutine_address*

Explanation This message indicates that the calling subroutine could not delete the IPsec SA. This could indicate a reference count problem.

Recommended Action If the number of stale SAs grows as a result of this event, contact the Cisco TAC.

715009

Error Message %ASA-7-715009: IKE Deleting SA: Remote Proxy *IP_address*, Local Proxy *IP_address*

Explanation This message indicates that SA is being deleted with the listed proxy addresses.

Recommended Action None required.

715013

Error Message %ASA-7-715013: Tunnel negotiation in progress for destination *IP_address*, discarding data

Explanation This message indicates that IKE is in the process of establishing a tunnel for this data. All packets to be protected by this tunnel will be dropped until the tunnel is fully established.

Recommended Action None required.

715019

Error Message %ASA-7-715019: IKEGetUserAttributes: Attribute name = *name*

Explanation This message displays the *modecfg* attribute name and value pair being processed by the security appliance.

Recommended Action None required.

715020

Error Message %ASA-7-715020: construct_cfg_set: Attribute name = *name*

Explanation This message displays the *modecfg* attribute name and value pair being transmitted by the security appliance.

Recommended Action None required.

715021

Error Message %ASA-7-715021: Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress

Explanation This message indicates that quick mode processing is being delayed until all Phase 1 processing has been completed (transaction mode, and so on).

Recommended Action None required.

715022

Error Message %ASA-7-715022: Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed

Explanation This message indicates that Phase 1 processing has completed and quick mode is being resumed.

Recommended Action None required.

715027

Error Message %ASA-7-715027: IPsec SA Proposal # *chosen_proposal*, Transform # *chosen_transform* acceptable Matches global IPsec SA entry # *crypto_map_index*

Explanation This message appears when the indicated IPsec SA proposal and transform were selected from the payloads that the responder received. This data can be useful when attempting to debug IKE negotiation issues.

Recommended Action None required.

715028

Error Message %ASA-7-715028: IKE SA Proposal # 1, Transform # *chosen_transform* acceptable Matches global IKE entry # *crypto_map_index*

Explanation This message appears when the indicated IKE SA transform was selected from the payloads that the responder received. This data can be useful when attempting to debug IKE negotiation issues.

Recommended Action None required.

715033

Error Message %ASA-7-715033: Processing CONNECTED notify (MsgId *message_number*)

Explanation This message indicates that the security appliance is processing a message containing a notify payload with notify type CONNECTED (16384). The CONNECTED notify is used to complete the commit bit processing and should be included in the fourth overall quick mode packet, which is sent from the responder to the initiator.

Recommended Action None required.

715034

Error Message %ASA-7-715034: *action* IOS keep alive payload: proposal=*time 1/time 2* sec.

Explanation This message indicates that processing for sending/receiving a keepalive payload message is being performed.

Recommended Action None required.

715035

Error Message %ASA-7-715035: Starting IOS keepalive monitor: *seconds* sec.

Explanation This message indicates that the keepalive timer will monitor for a variable number of seconds for keepalive messages.

Recommended Action None required.

715036

Error Message %ASA-7-715036: Sending keep-alive of type *notify_type* (seq number *number*)

Explanation This message indicates that processing for sending a keepalive notify message is being performed.

Recommended Action None required.

715037

Error Message %ASA-7-715037: Unknown IOS Vendor ID version: *major.minor.variance*

Explanation This message indicates that we do not know the capabilities of this version of IOS.

Recommended Action There may be interoperability issues with features like IKE keepalives. If the problem persists, contact the Cisco TAC

715038

Error Message %ASA-7-715038: *action Spoofing_information* Vendor ID payload (version: *major.minor.variance*, capabilities: *value*)

Explanation This message indicates that processing for the IOS Vendor ID payload has been performed. The message being performed could be Altiga spoofing IOS.

Recommended Action None required.

715039

Error Message %ASA-7-715039: Unexpected cleanup of tunnel table entry during SA delete.

Explanation This message indicates that there was an entry in the IKE tunnel table that was never removed when the SA was freed. This indicates a bug in the state machine.

Recommended Action If the problem persists, contact the Cisco TAC.

715040

Error Message %ASA--7-715040: Deleting active auth handle during SA deletion: handle = *internal_authentication_handle*

Explanation This message indicates that the auth handle was still active during SA deletion. This is part of cleanup recovery during the error condition.

Recommended Action None required.

715041

Error Message %ASA-7-715041: Received keep-alive of type *keepalive_type*, not the negotiated type

Explanation This indicates that a keep-alive of the type indicated in the message was received unexpectedly.

Recommended Action Check the keepalive configuration on both peers.

715042

Error Message `%ASA-7-715042: IKE received response of type failure_type to a request from the IP_address utility`

Explanation This indicates that a request for an IP address for a remote access client from the internal utility that provides these addresses could not be satisfied. Variable text in the message string indicates more specifically what went wrong.

Recommended Action Check the IP address assignment configuration and adjust it accordingly.

715044

Error Message `%ASA-7-715044: Ignoring Keepalive payload from vendor not support KeepAlive capability`

Explanation The security appliance received an IOS keepalive payload from a vendor without KA capabilities set. The payload is ignored.

Recommended Action None required.

715045

Error Message `%ASA-7-715045: ERROR: malformed Keepalive payload`

Explanation The security appliance received a malformed Keepalive payload. The payload is ignored.

Recommended Action None required.

715046

Error Message `%ASA-7-715046: Group = groupname, Username = username, IP = IP_address, constructing payload_description payload`

Explanation This message indicates that an IP address from a remote client for a specific group and user displays details about the IKE payload being constructed.

Recommended Action None required.

715047

Error Message `%ASA-7-715047: processing payload_description payload`

Explanation Details about the IKE payload received and being processed appear.

Recommended Action None required.

715048

Error Message `%ASA-7-715048: Send VID_type VID`

Explanation Displays type of Vendor ID payload being sent.

Recommended Action None required.

715049

Error Message `%ASA-7-715049: Received VID_type VID`

Explanation The type of Vendor ID payload received appears.

Recommended Action None required.

715050

Error Message `%ASA-7-715050: Claims to be IOS but failed authentication`

Explanation The number looks like the IOS Vendor ID, but does not match the *hmac_sha* argument.

Recommended Action Check the Vendor ID configuration on both peers. If this issue affects interoperability and the problem persists, contact the Cisco TAC.

715051

Error Message `%ASA-7-715051: Received unexpected TLV type TLV_type while processing FWTYPE ModeCfg Reply`

Explanation An unknown TLV was received in a security appliance record while a FWTYPE ModeCfg Reply was being processed. This will be discarded. This could occur either because of packet corruption or because the connecting client supports a later version of the security appliance protocol.

Recommended Action Check the personal FW installed on the Cisco VPN Client and the Personal FW configuration on the security appliance. This may also indicate a version mismatch between the VPN Client and the security appliance.

715052

Error Message `%ASA-7-715052: Old P1 SA is being deleted but new SA is DEAD, cannot transition centries`

Explanation The old P1 SA is being deleted, but it has no new SA to transition to because it was also marked for deletion. This generally indicates that the two IKE peers are out of synchronization and may be using different rekey times. The problem should correct itself, but there may be some small amount of data loss until a fresh P1 SA is reestablished.

Recommended Action None required.

715053

Error Message `%ASA-7-715053: MODE_CFG: Received request for attribute_info!`

Explanation The security appliance received a mode configuration message requesting the specified attribute.

Recommended Action None required.

715054

Error Message `%ASA-7-715054: MODE_CFG: Received attribute_name reply: value`

Explanation The security appliance received a mode configuration reply message from the remote peer.

Recommended Action None required.

715055

Error Message `%ASA-7-715055: Send attribute_name`

Explanation The security appliance sent a mode configuration message to the remote peer.

Recommended Action None required.

715056

Error Message `%ASA-7-715056: Client is configured for TCP_transparency`

Explanation Since the remote end (client) is configured for IPsec Over TCP, the headend security appliance must not negotiate IPsec over UDP or IPsec over NAT-T with the client.

Recommended Action May require adjustment to the NAT transparency configuration of one of the peers if the tunnel does not come up. Otherwise, this is an informational message.

715057

Error Message `%ASA-7-715057: Auto-detected a NAT device with NAT-Traversal. Ignoring IPsec-over-UDP configuration.`

Explanation IPsec-over-UDP Mode Config information will not be exchanged because NAT-Traversal was detected.

Recommended Action None required.

715058

Error Message `%ASA-7-715058: NAT-Discovery payloads missing. Aborting NAT-Traversal.`

Explanation The remote end didn't provide NAT-D payloads required for NAT-Traversal after exchanging NAT-Traversal VIDs. At least two NAT-D payloads must be received.

Recommended Action This may indicate a non-conforming NAT-T implementation. If the offending peer is a Cisco product, and the problem persists, contact the Cisco TAC. If the offending peer is not a Cisco product, then contact the manufacturer support team.

715059

Error Message `%ASA-7-715059: Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal`

Explanation You must use these modes instead of the usual Transport and Tunnel modes defined in the SA to successfully negotiate NAT-Traversal.

Recommended Action None required.

715060

Error Message `%ASA-7-715060: Dropped received IKE fragment. Reason:` *reason*

Explanation The reason for dropping the fragment appears. The drop reason could indicate a problem with an intervening NAT device or a non-conforming peer.

Recommended Action The resolution depends on the drop reason.

715061

Error Message `%ASA-7-715061: Rcv'd fragment from a new fragmentation set. Deleting any old fragments.`

Explanation This could be either a retransmission of the same packet (but fragmented to a different MTU), or another packet altogether.

Recommended Action None required.

715062

Error Message `%ASA-7-715062: Error assembling fragments! Fragment numbers are non-continuous.`

Explanation There is a gap in fragment numbers.

Recommended Action This could indicate a network problem. If the condition persists and results in dropped tunnels or prevents certain peers from negotiating with the security appliance, contact the Cisco TAC.

715063

Error Message `%ASA-7-715063: Successfully assembled an encrypted pkt from rcv'd fragments!`

Explanation Assembly for a fragmented packet that was received was successful.

Recommended Action None required.

715064

Error Message `%ASA-7-715064 -- IKE Peer included IKE fragmentation capability flags: Main Mode: true/false Aggressive Mode: true/false`

Explanation The peer supports IKE fragmentation based on the information provided in the message.

Recommended Action None required.

715065

Error Message `%ASA-7-715065: IKE state_machine subtype FSM error history (struct data_structure_address) state, event: state/event pairs`

Explanation A phase 1 error occurred and the *state/event* history pairs will be displayed in reverse chronological order.

Recommended Action Most of these errors are benign. If the problem persists, contact the Cisco TAC.

715066

Error Message `%ASA-7-715066: Can't load an IPsec SA! The corresponding IKE SA contains an invalid logical ID.`

Explanation The logical ID in the IKE SA is NULL. The phase II negotiation will be torn down.

Recommended Action An internal error has occurred. If the problem persists, contact the Cisco TAC.

715067

Error Message `%ASA-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa`

Explanation The LAN-TO-LAN SA that is being established already exists, in other words, an SA with the same remote network, but is sourced from a different peer. This new SA will be deleted because this is not a legal configuration.

Recommended Action Check the LAN-TO-LAN configuration on all associated peers. Specifically, multiple peers should not be sharing private networks.

715068

Error Message `%ASA-7-715068: QM IsRekeyed: duplicate sa found by address, deleting old sa`

Explanation The remote access SA that is being established already exists, in other words, an SA with the same remote network, but is sourced from a different peer. The old SA will be deleted, because the peer may simply have changed its IP address.

Recommended Action This may be a benign condition, especially if a client tunnel was terminated abruptly. If the problem persists, contact the Cisco TAC.

715069

Error Message `%ASA-7-715069: Invalid ESP SPI size of SPI_size`

Explanation The security appliance received an IPsec SA proposal with an invalid ESP SPI size. This proposal will be skipped.

Recommended Action Generally, this is a benign condition, but could indicate that a peer may be non-conforming. If the problem persists, contact the Cisco TAC.

715070

Error Message `%ASA-7-715070: Invalid IPComp SPI size of SPI_size`

Explanation The security appliance received an IPsec SA proposal with an invalid IPComp SPI size. This proposal will be skipped.

Recommended Action Generally, this is a benign condition, but it could indicate that a peer is non-conforming. If the problem persists, contact the Cisco TAC.

715071

Error Message `%ASA-7-715071: AH proposal not supported`

Explanation The IPsec AH proposal is not supported. This proposal will be skipped.

Recommended Action None required.

715072

Error Message `%ASA-7-715072: Received proposal with unknown protocol ID` *`protocol_ID`*

Explanation The security appliance received an IPsec SA proposal with unknown protocol ID. This proposal will be skipped.

Recommended Action Generally, this is a benign condition, but could indicate that a peer is non-conforming. If the problem persists, contact the Cisco TAC.

715074

Error Message `%ASA-7-715074: Could not retrieve authentication attributes for peer` *IP_address*

Explanation The security appliance could not get authorization information for the remote user.

Recommended Action Ensure that all authentication and authorization configuration is set correctly. If the problem persists, contact the Cisco TAC.

715075

Error Message `%ASA-7-715075: Group =` *`group_name`*`, Username =` *`client`*`, IP =` *`IP_address`* `Received keep-alive of type` *`message_type`* `(seq number` *`number`*`)`

Explanation This new message is paired with syslog message 715036, a "DPD R-U-THERE" message, which logs the DPD messages being sent.

The two possible scenarios are:

1) A received peer sending a "DPD R-U-THERE" message.

2) A received peer replying with a "DPD R-U-THERE-ACK" message.

You should observe the following:

Scenario 1—The "DPD R-U-THERE" message is received and its sequence number matches the outgoing DPD reply message.

If f1 sends a "DPD R-U-THERE-ACK" message before receiving a "DPD R-U-THERE" message from the peer, f1 may be experiencing a security breech.

Scenario 2—The received "DPD R-U-THERE-ACK" message sequence number matched the DPD message previously sent.

If f1 did not receive a "DPD R-U-THERE-ACK" message in a reasonable amount of time after sending a "DPD R-U-THERE" message to the peer, the tunnel is most likely down.

- *group_name*—The group name of the VPN peer.
- *client*—The username of the peer.
- *IP_address*—IP address of the VPN peer.
- *message_type*—The message type ("DPD R-U-THERE" or "DPD R-U-THERE-ACK").
- *number*—The DPD sequence number.

Recommended Action None required.

715076

Error Message `%ASA-7-715076: Computing hash for ISAKMP`

Explanation This message is displayed when IKE computes various hash values.

This object will be prepended as follows:

Group = *groupname*, Username = *username*, IP = *ip_address*...

Recommended Action None required.

715077

Error Message `%ASA-7-715077: Pitcher: msg string, spi spi`

Explanation This message is displayed when various messages are sent to IKE.

msg_string can be one of the following:

- received a key acquire message
- received SPI for non-existent SA
- received key delete msg
- received KEY_UPDATE
- received KEY_REKEY_IB
- received KEY_REKEY_OB
- received KEY_SA_ACTIVE
- could not find IKE SA to activate IPsec (OB)
- could not find IKE SA to rekey IPsec (OB)
- KEY_SA_ACTIVE no centry found
- KEY_ADD centry not found
- KEY_UPDATE centry not found

Like other ISAKMP messages, the following statement applies:

This object will be prepended as follows:

Group = *groupname*, Username = *username*, IP = *ip_address*, ...

Recommended Action None required.

715080

Error Message `%ASA-7-715080: Starting P2 rekey timer: 28800 seconds.`

Explanation The IKE (P1) Phase 1 or IPsec (P2) Phase 2 rekeying timers have been started or restarted. When an IKE (P1) or IPsec (P2) tunnel is connected, timers are created to determine when the next rekeying will occur. These messages show what the timers are set to.

Recommended Action None required.

716001

Error Message `%ASA-6-716001: Group group User user IP ip WebVPN session started.`

Explanation The WebVPN session has started for the *user* in this *group* at the specified IP address. When the user logs in via the WebVPN login page, the WebVPN session starts.

Recommended Action None required.

716002

Error Message `%ASA-6-716002: Group group User user IP ip WebVPN session terminated: User requested.`

Explanation The WebVPN session has terminated because of a user request. Possible reasons include:

- Lost Carrier
- Lost Service
- Idle Timeout
- Max time exceeded
- Administrator Reset
- Administrator Reboot
- Administrator Shutdown
- Port Error
- NAS Error
- NAS Request

- NAS Reboot
- Port unneeded
- Port Preempted. This reason indicates that the allowed number of simultaneous (same user) logins has been exceeded. To resolve this problem, increase the number of simultaneous logins or have users only log in once with a given username and password.
- Port Suspended
- Service Unavailable
- Callback
- User error
- Host Requested
- Bandwidth Management Error
- ACL parse error
- Unknown

Recommended Action Unless the reason indicates a problem, none required.

716003

Error Message `%ASA-6-716003: Group group User user IP ip WebVPN access "GRANTED: url"`

Explanation The WebVPN *user* in this *group* with the specified IP address has been granted access to this *url*. The user access to various locations can be controlled using WebVPN-specific access control lists.

Recommended Action None required.

716004

Error Message `%ASA-6-716004: Group group User user WebVPN access DENIED to specified location: url`

Explanation The WebVPN *user* in this *group* has been denied access to this *url*. The WebVPN user access to various locations can be controlled using WebVPN-specific access control lists. In this case, a particular access control list entry is denying access to this *url*.

Recommended Action None required.

716005

Error Message `%ASA-6-716005: Group group User user WebVPN ACL Parse Error: reason`

Explanation The ACL for the WebVPN user in the specified group failed to parse correctly. The reason for the error is reported.

The WebVPN access control list for the *user* in this *group* did not parse correctly. The reason for the error is reported.

Recommended Action Fix the WebVPN ACL.

716006

Error Message `%ASA-6-716006: Group name User user WebVPN session terminated. Idle timeout.`

Explanation The WebVPN session was not created for this user in the specified group because the VPN tunnel protocol is not set to WebVPN.

Recommended Action None required.

716007

Error Message `%ASA-4-716007: Group group User user WebVPN Unable to create session.`

Explanation The WebVPN session was not created for the in the specified group because of resource issues. For example, the user may have reached the maximum login limit.

Recommended Action None required.

716008

Error Message `%ASA-7-716008: WebVPN ACL: action`

Explanation The WebVPN ACL has begun performing an *action*. For example, the *action* could be "begin parsing." This is a debugging level message.

Recommended Action None required.

716009

Error Message `%ASA-6-716009: Group group User user WebVPN session not allowed. WebVPN ACL parse error.`

Explanation The WebVPN session for the specified user in this group is not allowed because the associated access control list did not parse. The user will not be allowed to log in via WebVPN until this error has been rectified.

Recommended Action Fix the WebVPN ACL.

716010

Error Message `%ASA-7-716010: Group group User user Browse network.`

Explanation The WebVPN user in the specified group browsed the network.

Recommended Action None required.

716011

Error Message `%ASA-7-716011: Group group User user Browse domain domain.`

Explanation The WebVPN specified user in this group browsed the specified domain.

Recommended Action None required.

716012

Error Message `%ASA-7-716012: Group group User user Browse directory directory.`

Explanation The specified WebVPN user browsed the specified directory.

Recommended Action None required.

716013

Error Message `%ASA-7-716013: Group group User user Close file filename.`

Explanation The specified WebVPN user closed the specified file.

Recommended Action None required.

716014

Error Message %ASA-7-716014: Group *group* User *user* View file *filename*.

Explanation The specified WebVPN user viewed the specified file.

Recommended Action None required.

716015

Error Message %ASA-7-716015: Group *group* User *user* Remove file *filename*.

Explanation The WebVPN user in the specified group removed the specified file.

Recommended Action None required.

716016

Error Message %ASA-7-716016: Group *group* User *user* Rename file *old_filename* to *new_filename*.

Explanation The specified WebVPN user renamed the specified file.

Recommended Action None required.

716017

Error Message %ASA-7-716017: Group *group* User *user* Modify file *filename*.

Explanation The specified WebVPN user modified the specified file.

Recommended Action None required.

716018

Error Message %ASA-7-716018: Group *group* User *user* Create file *filename*.

Explanation The specified WebVPN user created the specified file.

Recommended Action None required.

716019

Error Message %ASA-7-716019: Group *group* User *user* Create directory *filename*.

Explanation The specified WebVPN user created the specified directory.

Recommended Action None required.

716020

Error Message %ASA-7-716020: Group *group* User *user* Remove directory *directory*.

Explanation The specified WebVPN user removed the specified directory.

Recommended Action None required.

716021

Error Message %ASA-7-716021: File access DENIED, *filename*.

Explanation The specified WebVPN user was denied access to the specified file.

Recommended Action None required.

716022

Error Message %ASA-4-716022: Unable to connect to proxy server *reason*.

Explanation The WebVPN HTTP/HTTPS redirection failed for the specified reason.

Recommended Action Check the HTTP/HTTPS proxy configuration.

716023

Error Message %ASA-4-716023: Group *name* User *user* Session could not be established: session limit of *maximum_sessions* reached.

Explanation The user session cannot be established because the current number of sessions exceeds the maximum session load.

Recommended Action Increase the configured limit, if possible, to create a load-balanced cluster.

716024

Error Message `%ASA-7-716024: Group name User user Unable to browse the network.Error: description`

Explanation The user was unable to browse the Windows network via the CIFS protocol as indicated by the description. For example, "Unable to contact necessary server" indicates that the remote server is unavailable or unreachable. This could be a transient condition or may require further troubleshooting.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device.

716025

Error Message `%ASA-7-716025: Group name User user Unable to browse domain domain. Error: description`

Explanation The user was unable to browse the remote domain via the CIFS protocol.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device.

716026

Error Message `%ASA-7-716026: Group name User user Unable to browse directory directory. Error: description`

Explanation The user was unable to browse the remote directory via the CIFS protocol.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device.

716027

Error Message `%ASA-7-716027: Group name User user Unable to view file filename. Error: description`

Explanation The user was unable to view the remote file via the CIFS protocol.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device.

716028

Error Message `%ASA-7-716028: Group name User user Unable to remove file filename. Error: description`

Explanation The user was unable to remove the remote file via the CIFS protocol. This error is probably caused by lack of permissions.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device. Check the file permissions.

716029

Error Message `%ASA-7-716029: Group name User user Unable to rename file filename. Error: description`

Explanation The user was unable to rename the remote file via the CIFS protocol. This error was probably caused by lack of permissions.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device. Check the file permissions.

716030

Error Message `%ASA-7-716030: Group name User user Unable to modify file filename. Error: description`

Explanation A problem occurred when a user attempted to modify an existing file via the CIFS protocol. This error was probably caused by a lack of permissions.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device. Check the file permissions.

716031

Error Message `%ASA-7-716031: Group name User user Unable to create file filename. Error: description`

Explanation A problem occurred when a user attempted to create a file via the CIFS protocol. This error was probably caused by a permissions problem.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device. Check the file permissions.

716032

Error Message `%ASA-7-716032: Group name User user Unable to create folder folder. Error: description`

Explanation A problem occurred when a user attempted to create a folder via the CIFS protocol. This error was probably caused by a permissions problem.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device. Check file permissions.

716033

Error Message `%ASA-7-716033: Group name User user Unable to remove folder folder. Error: description`

Explanation A problem occurred when a user of the CIFS protocol attempted to remove a folder. This error probably occurred because of a permissions problem or a problem communicating with the server on which the file resides.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by CIFS. Check the NetBIOS name server (NBNS) configuration on the device.

716034

Error Message `%ASA-7-716034: Group name User user Unable to write to file filename.`

Explanation A problem occurred when a user attempted to write to a file via the CIFS protocol. This error was probably caused by a permissions problem or a problem communicating with the server on which the file resides.

Recommended Action None required.

716035

Error Message %ASA-7-716035: Group *name* User *user* Unable to read file *filename*.

Explanation A problem occurred when a user of the CIFS protocol attempted to read a file. This error was probably caused by a permissions problem.

Recommended Action Check the file permissions.

716036

Error Message %ASA-7-716036: Group *name* User *user* File Access: User *user* logged into the *server* server.

Explanation A user successfully logged into the server via the CIFS protocol.

Recommended Action None required.

716037

Error Message %ASA-7-716037: Group *name* User *user* File Access: User *user* failed to login into the *server* server.

Explanation A user attempted to log in to a server via the CIFS protocol, but was not successful.

Recommended Action Verify that the user entered the correct username and password.

716038

Error Message %ASA-6-716038: Group *group* User *user* IP *ip* Authentication: successful, Session Type: WebVPN.

Explanation Before a WebVPN session can begin, the user must be authenticated successfully by a local or remote server (for example, RADIUS or TACACS+).

Recommended Action None required.

716039

Error Message `%ASA-6-716039: Authentication: rejected, group = name user = user, Session Type: WebVPN`

Explanation Before a WebVPN session starts, the user must be authenticated successfully by a local or remote server (for example, RADIUS or TACACS+). In this case, the user credentials (username and password) either did not match or the user does not have permission to start a WebVPN session.

Recommended Action Verify the user credentials on the local or remote server. Verify that WebVPN is configured for the user.

716040

Error Message `%ASA-6-716040: Reboot pending, new sessions disabled. Denied user login.`

Explanation A user was unable to log in to WebVPN because the system is in the process of rebooting.

Recommended Action None required.

716041

Error Message `%ASA-6-716041: access-list acl_ID action url url hit_cnt count`

Explanation The WebVPN URL access control list named *acl_ID* has been hit *count* times for location *url* whose *action* is "permitted" or "denied."

Recommended Action None required.

716042

Error Message `%ASA-6-716042: access-list acl_ID action tcp source_interface/source_address (source_port) -> dest_interface/dest_address(dest_port) hit-cnt count`

Explanation The WebVPN TCP access control list named *acl_ID* has been hit *count* times for packet received on source interface *source_interface*/*source_address* port *source_port* forwarded to *dest_interface*/*dest_address* destination *dest_port* whose *action* is "permitted" or "denied."

Recommended Action None required.

716043

Error Message %ASA-6-716043 Group *group-name*, User *user-name*, IP *IP_address*: WebVPN Port Forwarding Java applet started. Created new hosts file mappings.

Explanation The user has launched a TCP port forwarding applet from a WebVPN session.

- *group-name*—Group name associated with this session.
- *user-name*—Username associated with this session.
- *IP_address*—Source IP address associated with this session.

Recommended Action None required.

716044

Error Message %ASA-4-716044: Group *group-name* User *user-name* IP *IP_address* AAA parameter *param-name* value *param-value* out of range.

Explanation The given parameter has a bad value.

- *group-name*—The name of the group.
- *user-name*—The name of the user.
- *IP_address*—The IP address.
- *param-name*—The name of the parameter.
- *param-value*—The value of the parameter.

Recommended Action Modify the configuration to correct the indicated parameter. If the parameter is "vlan" or "nac-settings," verify that they are correctly configured on the AAA server and adaptive security appliance.

716045

Error Message %ASA-4-716045: Group *group-name* User *user-name* IP *IP_address* AAA parameter *param-name* value invalid.

Explanation The given parameter has a bad value. The value is not shown as it might be very long.

- *group-name*—The name of the group.
- *user-name*—The name of the user.
- *IP_address*—The IP address.
- *param-name*—The name of the parameter.

Recommended Action Modify the configuration to correct the indicated parameter.

716046

Error Message %ASA-4-716046: Group *group-name-name* User *user-name* IP *IP_address* User ACL *access-list-name* from AAA doesn't exist on the device, terminating connection.

Explanation The specified access list was not found on the device.

- *group-name*—The name of the group.
- *user-name*—The name of the user.
- *IP_address*—The IP address.
- *access-list-name*—The name of the access list.

Recommended Action Modify the configuration to add the specified access list or to correct the access list name.

716047

Error Message %ASA-4-716047: Group *group-name* User *user-name* IP *IP_address* User ACL *access-list* from AAA ignored, AV-PAIR ACL used instead.

Explanation The specified access list was not used because a Cisco AV-PAIR access list was used.

- *group-name*—The name of the group.
- *user-name*—The name of the user.
- *IP_address*—The IP address.
- *access-list-name*—The name of the access list.

Recommended Action Determine the correct access list to use and correct the configuration.

716048

Error Message %ASA-4-716048: Group *group-name* User *user-name* IP *IP_address* No memory to parse ACL.

Explanation There was not enough memory to parse the access list.

- *group-name*—The name of the group.
- *user-name*—The name of the user.
- *IP_address*—The IP address.

Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

716049

Error Message `%ASA-6-716049: Group group-name User user-name IP IP_address Empty SVC ACL.`

Explanation The access list to be used by the client was empty.

- *group-name*—The name of the group.
- *user-name*—The name of the user.
- *IP_address*—The IP address.

Recommended Action Determine the correct access list to use and modify the configuration.

716050

Error Message `%ASA-6-716050: Error adding to ACL: ace_command_line`

Explanation The access control entry had a syntax error.

- *ace_command_line*—The access control entry that is causing the error.

Recommended Action Correct the downloadable access list configuration.

716051

Error Message `%ASA-6-716051: Group group-name User user-name IP IP_address Error adding dynamic ACL for user.`

Explanation There is not enough memory to perform the action.

- *group-name*—The name of the group.
- *user-name*—The name of the user.
- *IP_address*—The IP address.

Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

716052

Error Message `%ASA-4-716052: Group group-name User user-name IP IP_address Pending session terminated.`

Explanation A user did not complete login and the pending session was terminated.

- *group-name*—The name of the group.
- *user-name*—The name of the user.

- *IP_address*—The IP address.

Recommended Action This may be due to an SSL VPN client (SVC) that is unable to connect. Check the user PC for SVC compatibility.

716053

Error Message `%ASA-5-716053: New SSO Server added: name: name Type: type`

Explanation The Single Sign-On (SSO) server name of the specified type has been configured.

- *name*—The name of the server.
- *type*—The type of the server. Currently, the only available server type is SiteMinder.

Recommended Action None required.

716054

Error Message `%ASA-5-716054: SSO Server deleted: name: name Type: type`

Explanation The SSO server name of the specified type has been removed from the configuration.

- *name*—The name of the server.
- *type*—The type of the server. Currently, the only available server type is SiteMinder.

Recommended Action None required.

716055

Error Message `%ASA-6-716055: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type succeeded`

Explanation The WebVPN user has been successfully authenticated to the SSO server.

- *group-name*—The group name.
- *user-name*—The username.
- *IP_address*—The IP address of the server.
- *name*—The name of the server.
- *type*—The type of the server. Currently, the only available server type is SiteMinder.

Recommended Action None required.

716056

Error Message `%ASA-3-716056: Group group-name User user-name IP IP_address Authentication to SSO server name: name type type failed reason: reason`

Explanation The WebVPN user failed to authenticate to the SSO server.

- *group-name*—The group name.
- *user-name*—The username.
- *IP_address*—The IP address of the server.
- *name*—The name of the server.
- *type*—The type of the server. Currently, the only available server type is SiteMinder.
- *reason*—The reason for the authentication failure.

Recommended Action Either the user or the security appliance administrator need to correct the problem, depending on the reason for the failure.

716057

Error Message `%ASA-3-716057: Group group User user IP ip Session terminated, no type license available.`

Explanation A user has attempted to connect to the adaptive security appliance using an unlicensed client. This message may also be generated when a temporary license has expired.

- *group*—The group-policy that the user logged in with.
- *user*—The name of the user.
- *ip*—The IP address of the user.
- *type*—The type of license requested, which can be one of the following:
  - AnyConnect Mobile
  - LinkSys Phone
  - The type of license that the client requested (if not AnyConnect Mobile or LinkSys Phone)
  - Unknown (for example, in cases of low memory)

Recommended Action Purchase and install a permanent license with the required features.

716058

Error Message `%ASA-6-716058: Group group User user IP ip AnyConnect session lost connection. Waiting to resume.`

Explanation This message is generated when the SSL tunnel drops and the AnyConnect session enters the inactive state, which can be caused by a hibernating host, a standby host, or a loss of network connectivity.

- *group*—The tunnel group name associated with the AnyConnect session
- *user*—The name of the user associated with the session
- *ip*—The source IP address of the session

Recommended Action None required.

716059

Error Message `%ASA-6-716059: Group group User user IP ip AnyConnect session resumed from ip2.`

Explanation This message is generated when an AnyConnect session is resumed from the waiting-to-resume state.

- *group*—The tunnel group name associated with the AnyConnect session
- *user*—The name of the user associated with the session
- *ip*—The source IP address of the session
- *ip2*—The source IP address of the host from which the session resumed

Recommended Action None required.

716060

Error Message `%ASA-6-716060: Group group User user IP ip Terminated AnyConnect session in inactive state to accept a new connection: License limit reached.`

Explanation This message is generated when an AnyConnect session in the inactive state is logged out to allow a new incoming SSL VPN (AnyConnect or clientless) connection.

- *group*—The tunnel group name associated with the AnyConnect session
- *user*—The name of the user associated with the session
- *ip*—The source IP address of the session

Recommended Action None required.

716500

Error Message `%ASA-2-716500: internal error in: function: Fiber library cannot locate AK47 instance`

Explanation The fiber library cannot locate the application kernel layer 4 to 7 instance.

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

716501

Error Message `%ASA-2-716501: internal error in: function: Fiber library cannot attach AK47 instance`

Explanation The fiber library cannot attach the application kernel layer 4 to 7 instance.

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

716502

Error Message `%ASA-2-716502: internal error in: function: Fiber library cannot allocate default arena`

Explanation The fiber library cannot allocate the default arena.

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

716503

Error Message `%ASA-2-716503: internal error in: function: Fiber library cannot allocate fiber descriptors pool`

Explanation The fiber library cannot allocate the fiber descriptors pool.

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

716504

Error Message `%ASA-2-716504: internal error in: function: Fiber library cannot allocate fiber stacks pool`

Explanation The fiber library cannot allocate the fiber stack pool.

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

716505

Error Message %ASA-2-716505: internal error in: *function*: Fiber has joined fiber in unfinished state

Explanation The fiber has joined fiber in an unfinished state.

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

716506

Error Message %ASA-2-716506: UNICORN_SYSLOGID_JOINED_UNEXPECTED_FIBER

Explanation An internal fiber join has occurred.

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

716508

Error Message %ASA-2-716508: internal error in: *function*: Fiber scheduler is scheduling rotten fiber. Cannot continuing terminating

Explanation The fiber scheduler is scheduling rotten fiber, so it cannot continue terminating.

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

716509

Error Message %ASA-2-716509:internal error in: *function*: Fiber scheduler is scheduling alien fiber. Cannot continue terminating

Explanation The fiber scheduler is scheduling alien fiber, so it cannot continue terminating.

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

716510

Error Message %ASA-2-716510:internal error in: *function*: Fiber scheduler is scheduling finished fiber. Cannot continue terminating

Explanation The fiber scheduler is scheduling finished fiber, so it cannot continue terminating.

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

716512

Error Message %ASA-2-716512:internal error in: *function*: Fiber has joined fiber waited upon by someone else

Explanation The fiber has joined fiber that is waited upon by someone else.

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

716513

Error Message %ASA-2-716513: internal error in: *function*: Fiber in callback blocked on other channel

Explanation The fiber in the callback was blocked on the other channel.

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

716515

Error Message %ASA-2-716515:internal error in: *function*: OCCAM failed to allocate memory for AK47 instance

Explanation The OCCAM failed to allocate memory for the AK47 instance.

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

716516

Error Message %ASA-2-716516: internal error in: *function*: OCCAM has corrupted ROL array. Cannot continue terminating

Explanation The OCCAM has a corrupted ROL array, so it cannot continue terminating.

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

716517

Error Message %ASA-2-716517: internal error in: *function*: OCCAM cached block has no associated arena

Explanation The OCCAM cached block has no associated arena.

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

716518

Error Message `%ASWA-2-716518: internal error in: function: OCCAM pool has no associated arena`

Explanation The OCCAM pool has no associated arena.

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

716519

Error Message `%ASA-2-716519: internal error in: function: OCCAM has corrupted pool list. Cannot continue terminating`

Explanation The OCCAM has a corrupted pool list, so it cannot continue terminating.

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

716520

Error Message `%ASA-2-716520:internal error in: function: OCCAM pool has no block list`

Explanation The OCCAM pool has no block list.

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

716521

Error Message `%ASA-2-716521: internal error in: function: OCCAM no realloc allowed in named pool`

Explanation The OCCAM did not allow reallocation in the named pool.

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

716522

Error Message `%ASA-2-716522: internal error in: function: OCCAM corrupted standalone block`

Explanation The OCCAM has a corrupted standalone block.

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

716525

Error Message `%ASA-2-716525: UNICORN_SYSLOGID_SAL_CLOSE_PRIVDATA_CHANGED`

Explanation An internal SAL error has occurred.

Recommended Action Contact the Cisco TAC for assistance.

716526

Error Message `%ASA-2-716526: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_LOAD_FAIL`

Explanation A failure in mounting of the permanent storage server directory occurred.

Recommended Action Contact the Cisco TAC for assistance.

716527

Error Message `%ASA-2-716527: UNICORN_SYSLOGID_PERM_STORAGE_SERVER_STORE_FAIL`

Explanation A failure in mounting of the permanent storage file occurred.

Recommended Action Contact the Cisco TAC for assistance.

716528

Error Message `%ASA-2-716528: Unexpected fiber scheduler error; possible out-of-memory condition`

Explanation Customers and TAC seeing this error message do not have enough information to know what to look for based on the error message.

Recommended Action Check for memory leaks and troubleshoot.

717001

Error Message `%ASA-3-717001: Querying keypair failed.`

Explanation A required keypair was not found during an enrollment request.

Recommended Action Verify that a valid keypair exists in the trustpoint configuration and resubmit the enrollment request.

717002

Error Message `%ASA-3-717002: Certificate enrollment failed for trustpoint trustpoint_name. Reason: reason_string.`

Explanation An enrollment request for this *trustpoint_name* trustpoint has failed.

- *trustpoint name*—Trustpoint name that the enrollment request was for.
- *reason_string*—The reason the enrollment request failed.

Recommended Action Check the Certificate Authority server for the failure reason.

717003

Error Message `%ASA-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint_name.`

Explanation A certificate was successfully received from the Certificate Authority for this *trustpoint_name* trustpoint.

Recommended Action None required

717004

Error Message `%ASA-6-717004: PKCS #12 export failed for trustpoint trustpoint_name.`

Explanation Trustpoint *trustpoint_name* failed to export. It is likely that only a CA certificate exists and an identity certificate does not exist for the trustpoint, or a required keypair is missing.

Recommended Action Ensure that required certificates and keypairs are present for the given trustpoint.

717005

Error Message `%ASA-6-717005: PKCS #12 export succeeded for trustpoint trustpoint_name.`

Explanation The trustpoint *trustpoint_name* was successfully exported.

Recommended Action None required

717006

Error Message `%ASA-6-717006: PKCS #12 import failed for trustpoint trustpoint_name.`

Explanation Import of the requested trustpoint *trustpoint_name* failed to be processed.

Recommended Action Verify the integrity of the imported data, make sure that the entire **pkcs12** record is correctly pasted, and resubmit the import request.

717007

Error Message `%ASA-6-717007: PKCS #12 import succeeded for trustpoint trustpoint_name.`

Explanation Import of the requested trustpoint *trustpoint_name* was successfully completed.

Recommended Action None required.

717008

Error Message `%ASA-2-717008: Insufficient memory to process_requiring_memory.`

Explanation An internal error occurred while attempting to allocate memory for *process_requiring_memory*. Other processes may experience problems allocating memory and prevent further processing.

Recommended Action Collect memory statistics and logs for further debugging, and reload the system.

717009

Error Message `%ASA-3-717009: Certificate validation failed. Reason: reason_string.`

Explanation A certificate validation failed due to *reason_string*. The *reason_string* specifies the reason for the failure, which could be caused by a validation attempt of a revoked certificate, invalid certificate attributes, or configuration issues.

- *reason_string*—The reason that the certificate validation failed.

Recommended Action Ensure configuration has a valid trustpoint configured for validation if the *reason_string* indicates that no suitable trustpoints are found. Check the system time to ensure that it is accurate relative to the certificate authority time. Check the *reason_string* and correct any issues that are indicated.

717010

Error Message `%ASA-3-717010: CRL polling failed for trustpoint trustpoint_name.`

Explanation CRL polling has failed and may cause connections to be denied if CRL checking is required.

- *trustpoint_name*—The name of the trustpoint that requested the CRL.

Recommended Action Verify that connectivity with the configured CRL Distribution Point exists and ensure that the manual CRL retrieval functions correctly.

717011

Error Message `%ASA-2-717011: Unexpected event event event_ID`

Explanation This message indicates that an event that is not expected under normal conditions has occurred.

Recommended Action If the problem persists, contact the Cisco TAC.

717012

Error Message `%ASA-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint_name at time_of_failure`

Explanation This log message indicates that an attempt to refresh a cached CRL entry has failed for the specified trustpoint *trustpoint_name*, at the indicated *time_of_failure*. This may result in obsolete CRLs on the system that may cause connections that require a valid CRL to be denied.

Recommended Action Check connectivity issues to the server including network down, server down, and so on. Try to retrieve the CRL manually using the **crypto ca crl retrieve** command.

717013

Error Message `%ASA-5-717013: Removing a cached CRL to accommodate an incoming CRL. Issuer: issuer`

Explanation When the device is configured to authenticate IPsec tunnels using digital certificates, Certificate Revocation Lists (CRLs) may be cached in memory to avoid requiring a CRL download during each connection. If the cache fills to the point where an incoming CRL cannot be accommodated, older CRLs will be removed until the required space is made available. This message will be generated for each CRL that is purged.

Recommended Action None required.

717014

Error Message `%ASA-5-717014: Unable to cache a CRL received from CDP due to size limitations (CRL size = size, available cache space = space)`

Explanation When the device is configured to authenticate IPsec tunnels using digital certificates, Certificate Revocation Lists (CRLs) may be cached in memory to avoid requiring a CRL download during each connection. This message will be generated if a received CRL is too large to fit in the cache.

Recommended Action None required. The large CRLs are still supported even though they are not cached. This means that the CRL will be downloaded with each IPsec connection. This may impact performance during IPsec connection bursts.

717015

Error Message `%ASA-3-717015: CRL received from issuer is too large to process (CRL size = crl_size, maximum CRL size = max_crl_size)`

Explanation This message will be generated when an IPsec connection causes a CRL, that is larger than the maximum permitted CRL size, *max_crl_size*, to be downloaded. This is an error condition that will cause the connection to fail. This message is rate limited to one message every ten seconds.

Recommended Action Scalability is perhaps the most significant drawback to the CRL method of revocation checking. The only options to solve this problem are to investigate a Certificate Authority based solution to reduce the CRL size or configure the device not to require CRL validation.

717016

Error Message `%ASA-6-717016: Removing expired CRL from the CRL cache. Issuer: issuer`

Explanation When the device is configured to authenticate IPsec tunnels using digital certificates, Certificate Revocation Lists (CRLs) may be cached in memory to avoid requiring a CRL download during each connection. This message is generated when either the CA specified expiration time or the configured cache-time has lapsed and the CRL is removed from the cache.

Recommended Action None required. This is a routine occurrence.

717017

Error Message `%ASA-3-717017: Failed to query CA certificate for trustpoint trustpoint_name from enrollment_url`

Explanation This message may occur when an attempt is made to authenticate a trustpoint by requesting a CA certificate from a Certificate Authority.

Recommended Action Ensure that an enrollment URL is configured with this trustpoint, and that connectivity with the Certificate Authority server is achieved. Then retry the request.

717018

Error Message `%ASA-3-717018: CRL received from issuer has too many entries to process (number of entries = number_of_entries, maximum number allowed = max_allowed)`

Explanation This message will be generated when an IPsec connection causes a CRL, that contains more revocation entries than can be supported, to be downloaded. This is an error condition that will cause the connection to fail. This message is rate limited to one message every ten seconds.

- *issuer*—The X.500 name of the CRLs issuer.
- *number_of_entries*—The number of revocation entries in the received CRL.
- *max_allowed*—The maximum number of CRL entries that the device supports.

Recommended Action Scalability is perhaps the most significant drawback to the CRL method of revocation checking. The only options to solve this problem are to investigate a Certificate Authority based solution to reduce the CRL size or configure the device not to require CRL validation.

717019

Error Message `%ASA-3-717019: Failed to insert CRL for trustpoint trustpoint_name. Reason: failure_reason.`

Explanation This message will be generated when a CRL is retrieved but is found to be invalid and cannot be inserted into the cache because of the *failure_reason*.

- *trustpoint_name*—The name of the trustpoint that requested the CRL.
- *failure_reason*—The reason that the CRL failed to be inserted into cache.

Recommended Action Ensure the current system time is correct relative to the CA time. If the NextUpdate field is missing, configure the trustpoint to ignore the NextUpdate field.

717020

Error Message `%ASA-3-717020: Failed to install device certificate for trustpoint label. Reason: reason string.`

Explanation A failure occurred while trying to enroll or import an enrolled certificate into a trustpoint. The message indicates the trustpoint that was attempting an enrollment and a reason for the failure.

- *label*—Label of the trustpoint which failed to install the enrolled device certificate.
- *reason_string*—The reason that the certificate could not be verified.

Recommended Action Use the failure reason to remedy the cause of failure and reattempt the enrollment. Common failures are due to invalid certificates being imported into the device or a mismatch of the public key included in the enrolled certificate versus the keypair referenced in the trustpoint.

717021

Error Message `%ASA-3-717021: Certificate data could not be verified. Locate Reason: reason_string serial number: serial number, subject name: subject name, key length key length bits.`

Explanation This message is displayed when an attempt to verify the certificate that is identified by the serial number and subject name can not be verified for the specified reason. When verifying certificate data using the signature, several errors can occur that should be logged. These include invalid key types specified and unsupported key size.

- *reason_string*—The reason that the certificate could not be verified.
- *serial number*—Serial number of the certificate that is being verified.
- *subject name*—Subject name contained in the certificate that is being verified.
- *key length*—The number of bits in the key used to sign this certificate.

Recommended Action Check the specified certificate to ensure that it is valid, that it contains a valid key type, and that it does not exceed the maximum supported key size.

717022

Error Message `%ASA-6-717022: Certificate was successfully validated. certificate_identifiers`

Explanation This message is displayed when the identified certificate is successfully validated.

- *certificate_identifiers*—Information to identify the certificate that was validated successfully, which might include a reason, serial number, subject name, and additional information.

Recommended Action None required.

717023

Error Message `%ASA-3-717023: SSL failed to set device certificate for trustpoint` *`trustpoint name`*`. Reason:` *`reason_string`*`.`

Explanation This message is displayed when a failure occurs while trying to set a device certificate for the given trustpoint for authenticating the SSL connection. When bringing up an SSL connection, an attempt is made to set the device certificate that will be used. A failure occurring during this process is logged. The message includes the configured trustpoint that should be used to load the device certificate and the reason for the failure.

- *trustpoint name*—Name of the trustpoint for which SSL failed to set a device certificate.
- *reason_string*—Reason indicating why the device certificate could not be set.

Recommended Action Resolve the issue indicated by the reason reported for the failure:

- Ensure that the specified trustpoint is enrolled and has a device certificate.
- Make sure the device certificate is valid.
- Reenroll the trustpoint, if required.

717024

Error Message `%ASA-7-717024: Checking CRL from trustpoint:` *`trustpoint name`* `for` *`purpose`*

Explanation This message indicates that a CRL is being retrieved.

- *trustpoint name*—Name of the trustpoint for which the CRL is being retrieved.
- *purpose*—Reason that the CRL is being retrieved.

Recommended Action None required.

717025

Error Message `%ASA-7-717025: Validating certificate chain containing` *`number of certs`* `certificate(s).`

Explanation This message is displayed when a chain of certificate is being validated.

- *number of certs*—Number of certificates in the chain.

Recommended Action None required.

717026

Error Message `%ASA-4-717026: Name lookup failed for hostname hostname during PKI operation.`

Explanation This message is displayed when the given hostname cannot be resolved while attempting a PKI operation.

- *hostname*—The hostname that failed to resolve.

Recommended Action Check the configuration and the DNS server entries for the given hostname to make sure that it can be resolved. Then retry the operation.

717027

Error Message `%ASA-3-717027: Certificate chain failed validation. reason_string.`

Explanation This message is displayed when a certificate chain could not be validated. A reason is given to pinpoint the cause of the failure.

- *reason_string*—Reason for the failure to validate the certificate chain.

Recommended Action Resolve the issue noted by the reason and retry the validation attempt by performing any of the following actions:

- Make sure connectivity to a CA if CRL checking is required.
- Make sure a trustpoint is authenticated and available to validation.
- Make sure the identity certificate within the chain is valid based on the validity dates.
- Make sure the certificate is not revoked.

717028

Error Message `%ASA-6-717028: Certificate chain was successfully validated additional info.`

Explanation This message is displayed when a certificate chain was successfully validated.

- *additional info*—Gives additional information for how the certificate chain was validated, such as “with warning,” indicating that a CRL check was not performed.

Recommended Action None required.

717029

Error Message `%ASA-7-717029: Identified client certificate within certificate chain. serial number: serial_number, subject name: subject_name.`

Explanation This message identifies the certificate that is found to be the client certificate.

- *serial_number*—Serial number of the certificate that is identified as the client certificate.
- *subject_name*—Subject name contained in the certificate that is identified as the client certificate.

Recommended Action None required.

717030

Error Message `%ASA-7-717030: Found a suitable trustpoint trustpoint name to validate certificate.`

Explanation This message is displayed when a suitable/usable trustpoint is found that can be used to validate the certificate.

- *trustpoint name*—Trustpoint that will be used to validate the certificate

Recommended Action None required.

717031

Error Message `%ASA-4-717031: Failed to find a suitable trustpoint for the issuer: issuer Reason: reason_string`

Explanation This syslog message displays when a usable trustpoint cannot be found. This message identifies the issuer of the certificate for which no suitable trustpoint could be found and indicates the reason for the failure. During certificate validation, a suitable trustpoint must be available to validate a certificate.

- *issuer* —Issuer of the certificate that was being validated.
- *reason_string*—The reason that a suitable trustpoint could not be found.

Recommended Action Resolve the issue indicated in the reason by checking configuration to make sure a trustpoint is configured, authenticated, and enrolled. Also make sure the configuration allows for specific types of certificates, such as issued identity certificates.

717033

Error Message `%ASA-6-717033: OCSP response status - Successful.`

Explanation This syslog message indicates that an OCSP status check response was received successfully.

Recommended Action None required.

717034

Error Message `%ASA-7-717034: No-check extension found in certificate. OCSP check bypassed.`

Explanation This syslog message indicates that an OCSP responder certificate was received that contains an "id-pkix-ocsp-nocheck" extension, which allows this certificate to be validated without a OCSP status check.

Recommended Action None required.

717035

Error Message `%ASA-4-717035: OCSP status is being checked for certificate. certificate_identifier.`

Explanation This syslog message identifies the certificate for which an OCSP status check occurs.

- *certificate_identifier*—Information that identifies the certificate being processed by the certificate map rules.

Recommended Action None required.

717036

Error Message `ASA-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with certificate_identifier.`

Explanation This syslog message indicates that the peer certificate identified by *certificate_identifier* is being processed through the configured certificate maps to attempt a possible tunnel-group match.

- *certificate_identifier*—Information that identifies the certificate being processed by the certificate map rules.

Recommended Action None required.

717037

Error Message `%ASA-4-717037: Tunnel group search using certificate maps failed for peer certificate: certificate_identifier.`

Explanation This syslog message indicates that the peer certificate identified by *certificate_identifier* was processed through the configured certificate maps to attempt a possible tunnel-group match, but no match could be found.

- *certificate_identifier*—Information that identifies the certificate being processed by the certificate map rules.

Recommended Action Ensure that the warning is expected based on the received peer certificate and the configured crypto ca certificate map rules.

717038

Error Message `%ASA-7-717038: Tunnel group match found. Tunnel Group: tunnel_group_name, Peer certificate: certificate_identifier.`

Explanation This syslog message indicates that the peer certificate identified by *certificate_identifier* was processed by the configured certificate maps, and a match was found to the *tunnel_group_name* tunnel group.

- *certificate_identifier*—Information that identifies the certificate being processed by the certificate map rules.
- *tunnel_group_name*—The name of the tunnel group matched by the certificate map rules.

Recommended Action None required.

717039

Error Message `%ASA-3-717039: Local CA Server internal error detected: error.`

Explanation Logs an internal processing error that has occurred with the local CA server. The error string indicates the cause of the error, which requires administrator intervention to overcome.

- *error*—Error string.

Recommended Action Based on *error,* take the necessary steps to resolve the issue. Currently, the possible errors include:

- *CA key does not exist*—Ensure CA key is present, or restore key from backup if necessary.
- *Failed to rollover expired CA certificate*—Ensure clock is correct and that the CA certificate is indeed expired then restart the CA server to attempt to re-issue the certificate.
- *Failed to generate self-signed certificate for Local CA Server certificate rollover upon expiration*—Ensure clock is correct and that the CA certificate is indeed about to expire then restart the CA server to attempt to re-issue the certificate.

- *Failed to configure Local CA Server*—Turn on debugging and attempt to configure the CA server again to pin-point the cause of the failure.
- *Invalid issuer name configured*—Change the issuer name DN to a valid DN string.

717040

Error Message `%ASA-2-717040: Local CA Server has failed and is being disabled. Reason: reason.`

Explanation Indicates that the Local CA Server is being disabled due to an error. The reason for the failure is indicated by the *reason* string and administrator intervention may be required to resolve the issue encountered.

- *reason*—Reason string.

Recommended Action Based on *reason,* take the necessary steps to resolve the issue. Currently, the possible errors include:

- *Storage down*—Ensure storage is accessible and reenable CA server via the **no shut** command

717041

Error Message `%ASA-7-717041: Local CA Server event: event info.`

Explanation This message reports events that have occurred on the CA server to allow you to track or debug CA server health. Events include when the CA server is created, enabled, or disabled, when the CA server certificate is rolled over, and others.

- *event info*—Details of the event that occurred.

Recommended Action None required.

717042

Error Message `%ASA-3-717042: Failed to enable Local CA Server.Reason: reason.`

Explanation This message reports errors that occur when an attempt is made to enable the Local CA Server. The reason for the failure is indicated by the *reason*.

- *reason*—Reason that the Local CA server was not enabled.

Recommended Action Resolve the issue encountered that is reported via the *reason* string. Currently, the possible reasons include:

- Failed to create server trustpoint
- Failed to create server keypair
- Time has not been set
- Failed to init storage

- Storage not accessible
- Failed to validate selfsigned CA certificate
- Failed to generate selfsigned CA certificate
- CA Certificate has expired
- Failed to generate CRL
- Failed to archive CA key and certificate
- Failed to generate empty user or certificate database file
- Failed to load user or certificate database file

717043

Error Message `%ASA-6-717043: Local CA Server certificate enrollment related info for user: user. Info: info.`

Explanation This message allows monitoring of enrollment-related activities for a user. The username and specific enrollment information are reported so that enrollments, e-mail invitation generation, renewal reminder generation, and so on can be monitored.

- *user*—Username of the user about whom the enrollment information is being generated.
- info—Enrollment information string.

Recommended Action None required.

717044

Error Message `%ASA-3-717044: Local CA server certificate enrollment related error for user: user. Error: error.`

Explanation This message reports any errors that occur in the processing of certificate enrollment. This may include errors in notifying users via email for renewal reminders, errors during issuing of a certificate to complete enrollment, invalid username or OTP, expired enrollment attempts, and so on.

- *user*—Username of the user for whom the enrollment error is being generated.
- *error*—Enrollment error.

Recommended Action The *error* indicates the specific enrollment-related error that occurred for the *user*. If the *error* string does not provide enough information to diagnose and resolve the issue, turn on debugging, and attempt enrollment again.

717045

Error Message `%ASA-7-717045:Local CA Server CRL info: info`

Explanation This message allows monitoring of the CRL file, when it is generated and regenerated.

- *info*—Informational string of CRL event.

Recommended Action None required.

717046

Error Message `%ASA-3-717046: Local CA Server CRL error: error.`

Explanation This message indicates errors that are encountered while trying to generate and re-issue the local CA server CRL file.

- *error*—Error string.

Recommended Action The *error* string indicates the error that occurred. Take appropriate action to resolve the reported issue, which may include verifying that storage is accessible, that the CRL file is valid in storage and signed by the existing local CA server, and others.

717047

Error Message `%ASA-6-717047: Revoked certificate issued to user: username, with serial number serial number.`

Explanation This message allows monitoring of any certificates, issued by the local CA server, that have been revoked.

- *username*—Username of the owner of the certificate that is being revoked.
- *serial number*—Serial number of the certificate that has been revoked.

Recommended Action None required.

717048

Error Message `%ASA-6-717048: Unrevoked certificate issued to user: username, with serial number serial number.`

Explanation This message allows monitoring of any certificates that were issued by the local CA server, that were previously revoked, that are now being unrevoked and removed from the CRL.

- *username*—Username of the owner of the certificate that is being unrevoked.

- *serial number*—Serial number of the certificate that has been unrevoked.

Recommended Action None required.

717049

Error Message `%ASA-1-717049: Local CA Server certificate is due to expire in` *`number`* `days and a replacement certificate is available for export.`

Explanation This message alerts the administrator of an upcoming CA certificate expiration so that the administrator can take action to export the replacement certificate to all devices that will require it.

- *number*—The number of days before the Local CA Server certificate expires.

Recommended Action Action should be taken before the actual expiration of the current Local CA Server certificate, which is indicated by the *number* field, to avoid certificate validation failures on any devices that require the Local CA Server certificate. Note that the Local CA Server doesn't require any action because the CA certificate will be replaced automatically. Issue the **show crypto ca server certificate** CLI to view the replacement/rollover Local CA Server certificate and cut-and-paste it for import into any device that will require the new certificate upon expiration of the current Local CA Server certificate.

718001

Error Message `%ASA-7-718001: Internal interprocess communication queue send failure: code` *`error_code`*

Explanation An internal software error has occurred while attempting to enqueue a message on the VPNLB queue.

Recommended Action This is generally a benign condition. If the problem persists, contact the Cisco TAC.

718002

Error Message `%ASA-5-718002: Create peer` *`IP_address`* `failure, already at maximum of` *`number_of_peers`*

Explanation The maximum number of load balancing peers was exceeded. A new peer was ignored.

Recommended Action Check your load balancing and network configuration to ensure that the number of LB peers does not exceed the maximum allowed.

718003

Error Message `%ASA-6-718003: Got unknown peer message message_number from IP_address, local version version_number, remote version version_number`

Explanation An unrecognized load balancing message was received from one of the LB peers. This could indicate a version mismatch between peers, but is most likely caused by an internal software error.

Recommended Action Verify that all LB peers are compatible. If they are and this condition persists, or is linked to undesirable behavior, contact the Cisco TAC.

718004

Error Message `%ASA-6-718004: Got unknown internal message message_number`

Explanation Received an unknown internal message. This generally indicates an internal software error.

Recommended Action This is generally a benign condition. If the problem persists, contact the Cisco TAC.

718005

Error Message `%ASA-5-718005: Fail to send to IP_address, port port`

Explanation An internal software error has occurred while attempting to send a packet on the load balancing socket. This could indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, contact the Cisco TAC.

718006

Error Message `%ASA-5-718006: Invalid load balancing state transition [cur=state_number][event=event_number]`

Explanation A state machine error has occurred. This could indicate an internal software error.

Recommended Action This is generally a benign condition. If the problem persists, contact the Cisco TAC.

718007

Error Message `%ASA-5-718007: Socket open failure failure_code`

Explanation An error has occurred while attempting to open the load balancing socket. This could indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, contact the Cisco TAC.

718008

Error Message `%ASA-5-718008: Socket bind failure failure_code`

Explanation An error has occurred while attempting to bind to the load balancing socket. This could indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, contact the Cisco TAC.

718009

Error Message `%ASA-5-718009: Send HELLO response failure to IP_address`

Explanation An error has occurred while attempting to send a Hello Response message to one of the LB peers. This could indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, contact the Cisco TAC.

718010

Error Message `%ASA-5-718010: Sent HELLO response to IP_address`

Explanation The security appliance transmitted a Hello Response message to a LB peer.

Recommended Action Informational only.

718011

Error Message `%ASA-5-718011: Send HELLO request failure to IP_address`

Explanation An error has occurred while attempting to send a Hello Request message to one of the LB peers. This could indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, contact the Cisco TAC.

718012

Error Message `%ASA-5-718012: Sent HELLO request to IP_address`

Explanation The security appliance transmitted a Hello Request message to a LB peer.

Recommended Action None required.

718013

Error Message `%ASA-6-718013: Peer IP_address is not answering HELLO`

Explanation The LB peer is not answering HELLO.

Recommended Action Check the status of the LBSSF peer and the network connections.

718014

Error Message `%ASA-5-718014: Master peer IP_address is not answering HELLO`

Explanation The LB master peer is not answering HELLO.

Recommended Action Check the status of the LBSSF master peer and the network connections.

718015

Error Message `%ASA-5-718015: Received HELLO request from IP_address`

Explanation The security appliance received a Hello Request message from a LB peer.

Recommended Action None required.

718016

Error Message `%ASA-5-718016: Received HELLO response from IP_address`

Explanation The security appliance received a Hello Response packet from a LB peer.

Recommended Action None required.

718017

Error Message `%ASA-7-718017: Got timeout for unknown peer IP_address msg type message_type`

Explanation The security appliance processed a timeout for an unknown peer. The message was ignored because the peer may have already been removed from the active list.

Recommended Action If the message persists or is linked to undesirable behavior, check LB peers and verify that all are configured correctly.

718018

Error Message `%ASA-7-718018: Send KEEPALIVE request failure to IP_address`

Explanation An error has occurred while attempting to send a Keepalive Request message to one of the LB peers. This could indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the security appliance, and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, contact the Cisco TAC.

718019

Error Message `%ASA-7-718019: Sent KEEPALIVE request to IP_address`

Explanation The security appliance transmitted a Keepalive Request message to a LB peer.

Recommended Action None required.

718020

Error Message `%ASA-7-718020: Send KEEPALIVE response failure to IP_address`

Explanation An error has occurred while attempting to send a Keepalive Response message to one of the LB peers. This could indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the security appliance, and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, contact the Cisco TAC.

718021

Error Message `%ASA-7-718021: Sent KEEPALIVE response to IP_address`

Explanation The security appliance transmitted a Keepalive Response message to a LB peer.

Recommended Action None required.

718022

Error Message `%ASA-7-718022: Received KEEPALIVE request from IP_address`

Explanation The security appliance received a Keepalive Request message from a LB peer.

Recommended Action None required.

718023

Error Message `%ASA-7-718023: Received KEEPALIVE response from IP_address`

Explanation The security appliance received a Keepalive Response message from a LB peer.

Recommended Action None required.

718024

Error Message `%ASA-5-718024: Send CFG UPDATE failure to IP_address`

Explanation An error has occurred while attempting to send a Configuration Update message to one of the LB peers. This could indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the security appliance and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, contact the Cisco TAC.

718025

Error Message `%ASA-7-718025: Sent CFG UPDATE to IP_address`

Explanation The security appliance transmitted a Configuration Update message to a LB peer.

Recommended Action None required.

718026

Error Message `%ASA-7-718026: Received CFG UPDATE from IP_address`

Explanation The security appliance received a Configuration Update message from a LB peer.

Recommended Action None required.

718027

Error Message `%ASA-6-718027: Received unexpected KEEPALIVE request from IP_address`

Explanation Informational message.

Recommended Action If the problem persists or is linked to undesirable behavior, verify that all LB peers are configured and discovered correctly.

718028

Error Message `%ASA-5-718028: Send OOS indicator failure to IP_address`

Explanation An error has occurred while attempting to send an OOS Indicator message to one of the LB peers. This could indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the security appliance, and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, contact the Cisco TAC.

718029

Error Message `%ASA-7-718029: Sent OOS indicator to IP_address`

Explanation The security appliance transmitted an OOS Indicator message to a LB peer.

Recommended Action None required.

718030

Error Message `%ASA-6-718030: Received planned OOS from IP_address`

Explanation The security appliance received a planned OOS message from a LB peer.

Recommended Action None required.

718031

Error Message `%ASA-5-718031: Received OOS obituary for IP_address`

Explanation The security appliance received an OOS Obituary from a LB peer.

Recommended Action None required.

718032

Error Message `%ASA-5-718032: Received OOS indicator from IP_address`

Explanation The security appliance received an OOS Indicator from a LB peer.

Recommended Action None required.

718033

Error Message `%ASA-5-718033: Send TOPOLOGY indicator failure to IP_address`

Explanation An error has occurred while attempting to send a Topology Indicator message to one of the LB peers. This could indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the security appliance, and verify that interfaces are active and protocol data is flowing through the device. If the problem persists, contact the Cisco TAC.

718034

Error Message `%ASA-7-718034: Sent TOPOLOGY indicator to IP_address`

Explanation The security appliance sent a Topology Indicator message to a LB peer.

Recommended Action None required.

718035

Error Message `%ASA-7-718035: Received TOPOLOGY indicator from IP_address`

Explanation The security appliance received a Topology Indicator message from a LB peer.

Recommended Action None required.

718036

Error Message `%ASA-7-718036: Process timeout for req-type type_value, exid exchange_ID, peer IP_address`

Explanation The security appliance processed a peer timeout.

Recommended Action Verify that the peer should have been timed out. If not, check the peer LB configuration and the network connection between the peer and the security appliance.

718037

Error Message %ASA-6-718037: Master processed *number_of_timeouts* timeouts

Explanation The security appliance in the master role processed the specified number of peer timeouts.

Recommended Action Verify that the timeouts are legitimate. If not, check the peer LB configuration and the network connection between the peer and the security appliance.

718038

Error Message %ASA-6-718038: Slave processed *number_of_timeouts* timeouts

Explanation The security appliance in the slave role processed the specified number of peer timeouts.

Recommended Action Verify that the timeouts are legitimate. If not, check the peer LB configuration and the network connection between the peer and the security appliance.

718039

Error Message %ASA-6-718039: Process dead peer *IP_address*

Explanation The security appliance has detected a dead peer.

Recommended Action Verify that the dead peer detection is legitimate. If not, check the peer LB configuration and the network connection between the peer and the security appliance.

718040

Error Message %ASA-6-718040: Timed-out exchange ID *exchange_ID* not found

Explanation The security appliance has detected a dead peer, but the exchange ID is not recognized.

Recommended Action None required.

718041

Error Message `%ASA-7-718041: Timeout [msgType=type] processed with no callback`

Explanation The security appliance has detected a dead peer, but a call back was not used in the processing.

Recommended Action None required.

718042

Error Message `%ASA-5-718042: Unable to ARP for IP_address`

Explanation The security appliance experienced an ARP failure when attempting to contact a peer.

Recommended Action Verify that the network is operational and all peers can communicate with each other.

718043

Error Message `%ASA-5-718043: Updating/removing duplicate peer entry IP_address`

Explanation The security appliance found and is removing a duplicate peer entry.

Recommended Action None required.

718044

Error Message `%ASA-5-718044: Deleted peer IP_address`

Explanation The security appliance is deleting a LB peer.

Recommended Action None required.

718045

Error Message `%ASA-5-718045: Created peer IP_address`

Explanation The security appliance has detected a LB peer.

Recommended Action None required.

718046

Error Message `%ASA-7-718046: Create group policy policy_name`

Explanation The security appliance has created a group policy to securely communicate with the LB peers.

Recommended Action None required.

718047

Error Message `%ASA-7-718047: Fail to create group policy policy_name`

Explanation The security appliance experienced a failure when attempting to create a group policy for securing the communication between LB peers.

Recommended Action Verify that the LB configuration is correct.

718048

Error Message `%ASA-5-718048: Create of secure tunnel failure for peer IP_address`

Explanation The security appliance experienced a failure when attempting to establish an IPsec tunnel to a LB peer.

Recommended Action Verify that the LB configuration is correct and that the network is operational.

718049

Error Message `%ASA-7-718049: Created secure tunnel to peer IP_address`

Explanation The security appliance successfully established an IPsec tunnel to a LB peer.

Recommended Action None required.

718050

Error Message `%ASA-5-718050: Delete of secure tunnel failure for peer IP_address`

Explanation The security appliance experienced a failure when attempting to terminate an IPsec tunnel to a LB peer.

Recommended Action Verify that LB configuration is correct and that the network is operational.

718051

Error Message `%ASA-6-718051: Deleted secure tunnel to peer IP_address`

Explanation The security appliance successfully terminated an IPsec tunnel to a LB peer.

Recommended Action None required.

718052

Error Message `%ASA-5-718052: Received GRAT-ARP from duplicate master MAC_address`

Explanation The security appliance received a Gratuitous ARP from a duplicate master.

Recommended Action Check the LB configuration and verify that the network is operational.

718053

Error Message `%ASA-5-718053: Detected duplicate master, mastership stolen MAC_address`

Explanation The security appliance detected a duplicate master and a stolen mastership.

Recommended Action Check the LB configuration and verify that the network is operational.

718054

Error Message `%ASA-5-718054: Detected duplicate master MAC_address and going to SLAVE`

Explanation The security appliance detected a duplicate master and is switching to slave mode.

Recommended Action Check the LB configuration and verify that the network is operational.

718055

Error Message `%ASA-5-718055: Detected duplicate master MAC_address and staying MASTER`

Explanation The security appliance detected a duplicate master and is staying in slave mode.

Recommended Action Check the LB configuration and verify that the network is operational.

718056

Error Message %ASA-7-718056: Deleted Master peer, IP *IP_address*

Explanation The security appliance deleted the LB master from its internal tables.

Recommended Action None required.

718057

Error Message %ASA-5-718057: Queue send failure from ISR, msg type *failure_code*

Explanation An internal software error has occurred while attempting to enqueue a message on the VPNLB queue from an Interrupt Service Routing.

Recommended Action This is generally a benign condition. If the problem persists, contact the Cisco TAC.

718058

Error Message %ASA-7-718058: State machine return code: *action_routine*, *return_code*

Explanation This event traces the return codes of action routines belonging to the LB finite state machine.

Recommended Action None required.

718059

Error Message %ASA-7-718059: State machine function trace: state=*state_name*, event=*event_name*, func=*action_routine*

Explanation This event traces the events and states of the LB finite state machine.

Recommended Action None required.

718060

Error Message `%ASA-5-718060: Inbound socket select fail: context=context_ID.`

Explanation The socket select call returned an error and the socket could not be read. This could indicate an internal software error.

Recommended Action If the problem persists, contact the Cisco TAC.

718061

Error Message `%ASA-5-718061: Inbound socket read fail: context=context_ID.`

Explanation The socket read failed after data was detected through the select call. This could indicate an internal software error.

Recommended Action If the problem persists, contact the Cisco TAC.

718062

Error Message `%ASA-5-718062: Inbound thread is awake (context=context_ID).`

Explanation This message occurs every time the LB process is awakened and begins processing.

Recommended Action None required.

718063

Error Message `%ASA-5-718063: Interface interface_name is down.`

Explanation This message indicates that the LB process found the interface down.

Recommended Action Check the interface configuration to make sure that the interface is operational.

718064

Error Message `%ASA-5-718064: Admin. interface interface_name is down.`

Explanation This message indicates that the LB process found the administrative interface down.

Recommended Action Check the administrative interface configuration to make sure that the interface is operational.

718065

Error Message `%ASA-5-718065: Cannot continue to run (public=up/down, private=up/down, enable=LB_state, master=IP_address, session=Enable/Disable).`

Explanation This message indicates that the LB process can not run because all prerequisite conditions have not been met. The prerequisite conditions are two active interfaces and LB is enabled.

Recommended Action Check the interface configuration to make sure at least two interfaces are operational. Also check the LB configuration.

718066

Error Message `%ASA-5-718066: Cannot add secondary address to interface interface_name, ip IP_address.`

Explanation LB requires a secondary address to be added to the outside interface. This event indicates that there was a failure in adding that secondary address.

Recommended Action Check the address being used as the secondary address and ensure that it is valid and unique. Check the configuration of the outside interface.

718067

Error Message `%ASA-5-718067: Cannot delete secondary address to interface interface_name, ip IP_address.`

Explanation The deletion of the secondary address failed. This could indicate an addressing problem or an internal software error.

Recommended Action Check the addressing information of the outside interface and ensure that the secondary address is valid and unique. If the problem persists, contact the Cisco TAC.

718068

Error Message `%ASA-5-718068: Start VPN Load Balancing in context context_ID.`

Explanation The LB process has been started and initialized.

Recommended Action None required.

718069

Error Message `%ASA-5-718069: Stop VPN Load Balancing in context context_ID.`

Explanation The LB process has been stopped.

Recommended Action None required.

718070

Error Message `%ASA-5-718070: Reset VPN Load Balancing in context context_ID.`

Explanation The LB process has been reset.

Recommended Action None required.

718071

Error Message `%ASA-5-718071: Terminate VPN Load Balancing in context context_ID.`

Explanation The LB process has been terminated.

Recommended Action None required.

718072

Error Message `%ASA-5-718072: Becoming master of Load Balancing in context context_ID.`

Explanation The security appliance has become the LB master.

Recommended Action None required.

718073

Error Message `%ASA-5-718073: Becoming slave of Load Balancing in context context_ID.`

Explanation The security appliance has become the LB slave.

Recommended Action None required.

718074

Error Message %ASA-5-718074: Fail to create access list for peer *context_ID*.

Explanation ACLs are used to create secure tunnels over which the LB peers can communicate. The security appliance was unable to create one of these ACLs. This could indicate an addressing problem or an internal software problem.

Recommended Action Check the addressing information of the inside interface on all peers and ensure that all peers are discovered correctly. If the problem persists, contact the Cisco TAC.

718075

Error Message %ASA-5-718075: Peer *IP_address* access list not set.

Explanation While removing a secure tunnel, the security appliance detected a peer entry that did not have an associated ACL.

Recommended Action None required.

718076

Error Message %ASA-5-718076: Fail to create tunnel group for peer *IP_address*.

Explanation The security appliance experienced a failure when attempting to create a tunnel group for securing the communication between LB peers.

Recommended Action Verify that the LB configuration is correct.

718077

Error Message %ASA-5-718077: Fail to delete tunnel group for peer *IP_address*.

Explanation The security appliance experienced a failure when attempting to delete a tunnel group for securing the communication between LB peers.

Recommended Action None required.

718078

Error Message `%ASA-5-718078: Fail to create crypto map for peer IP_address.`

Explanation The security appliance experienced a failure when attempting to create a crypto map for securing the communication between LB peers.

Recommended Action Verify that the LB configuration is correct.

718079

Error Message `%ASA-5-718079: Fail to delete crypto map for peer IP_address.`

Explanation The security appliance experienced a failure when attempting to delete a crypto map for securing the communication between LB peers.

Recommended Action None required.

718080

Error Message `%ASA-5-718080: Fail to create crypto policy for peer IP_address.`

Explanation The security appliance experienced a failure when attempting to create a transform set to be used in securing the communication between LB peers. This could indicate an internal software problem.

Recommended Action If the problem persists, contact the Cisco TAC.

718081

Error Message `%ASA-5-718081: Fail to delete crypto policy for peer IP_address.`

Explanation The security appliance experienced a failure when attempting to delete a transform set used in securing the communication between LB peers.

Recommended Action None required.

718082

Error Message `%ASA-5-718082: Fail to create crypto IPsec for peer IP_address.`

Explanation When cluster encryption for VPN load balancing is enabled, the VPN load balancing device creates a set of site-to-site tunnels for every other device in the load balancing cluster. For each tunnel, a set of crypto parameters (access list, crypto maps, transform set, and so on) is created dynamically. This syslog message indicates that one or more of these crypto parameters failed to be created or configured.

- *IP_address*—The IP address of the remote peer.

Recommended Action Examine the syslog message for other entries specific to the type of crypto parameters that failed to be created.

718083

Error Message `%ASA-5-718083: Fail to delete crypto IPsec for peer IP_address.`

Explanation When the local VPN load balancing device is removed from the cluster, crypto parameters are removed. This system log entry indicates that one or more crypto parameters failed to be deleted.

- *IP_address*—The IP address of the remote peer.

Recommended Action Examine the syslog message for other entries specific to the type of crypto parameters that failed to be deleted.

718084

Error Message `%ASA-5-718084: Public/cluster IP not on the same subnet: public IP_address, mask netmask, cluster IP_address`

Explanation The cluster IP address must be on the same subnet as the outside interface of the security appliance. This even indicates that it is not on the same network.

Recommended Action Make sure that both the cluster (or virtual) IP address and the outside interface address are on the same network.

718085

Error Message `%ASA-5-718085: Interface interface_name has no IP address defined.`

Explanation The indicated interface does not have an IP address configured.

Recommended Action Configure an IP address for the interface.

718086

Error Message `%ASA-5-718086: Fail to install LB NP rules: type rule_type, dst interface_name, port port.`

Explanation The security appliance experienced a failure when attempting to create a SoftNP ACL rule to be used in securing the communication between LB peers. This could indicate an internal software problem.

Recommended Action If the problem persists, contact the Cisco TAC.

718087

Error Message `%ASA-5-718087: Fail to delete LB NP rules: type rule_type, rule rule_ID.`

Explanation The security appliance experienced a failure when attempting to delete SoftNP ACL rule used in securing the communication between LB peers.

Recommended Action None required.

718088

Error Message `%ASA-7-718088: Possible VPN LB misconfiguration. Offending device MAC MAC_address.`

Explanation The presence of a duplicate master indicates that one of the LB peers may be misconfigured.

Recommended Action Check the LB configuration on all peers, but pay special attention to the peer identified.

719001

Error Message `%ASA-6-719001: Email Proxy session could not be established: session limit of maximum_sessions has been reached.`

Explanation This message appears when the incoming e-mail proxy session could not be established because the maximum session limit has been reached. *maximum_sessions* is the maximum session number.

Recommended Action None required.

719002

Error Message `%ASA-3-719002: Email Proxy session pointer from source_address has been terminated due to reason error.`

Explanation This message appears when the session has been terminated due to an error. The possible errors are: adding a session to a session database failure; memory allocation failure; writing data to channel failure, and so on. The *pointer* is the pointer of the session structure, *source_address* is the e-mail proxy client IP address, and *reason* is the error type.

Recommended Action None required.

719003

Error Message `%ASA-6-719003: Email Proxy session pointer resources have been freed for source_address.`

Explanation This message appears when the dynamic allocated session structure has been freed and set to NULL after the session terminated. The *pointer* is the pointer of the session structure, and *source_address* is the e-mail proxy client IP address.

Recommended Action None required.

719004

Error Message `%ASA-6-719004: Email Proxy session pointer has been successfully established for source_address.`

Explanation A new incoming e-mail client session has been established.

Recommended Action None required.

719005

Error Message `%ASA-7-719005: FSM NAME has been created using protocol for session pointer from source_address.`

Explanation This message appears when an FSM has been created for an incoming new session.The *NAME* is the FSM instance name for the session, *protocol* is the e-mail protocol type (for example, POP3, IMAP, SMTP), *pointer* is the pointer of session structure, and *source_address* is the e-mail proxy client IP address.

Recommended Action None required.

719006

Error Message `%ASA-7-719006: Email Proxy session pointer has timed out for source_address because of network congestion.`

Explanation This message appears due to network congestion, and data cannot be sent to either an e-mail client or an e-mail sever. This starts the block timer. After the block timer is timed out, the session expires. The *pointer* is the pointer of session structure, and *source_address* is the e-mail proxy client IP address.

Recommended Action Retry the operation after a few minutes.

719007

Error Message `%ASA-7-719007: Email Proxy session pointer cannot be found for source_address.`

Explanation This message appears when a matching session cannot be found in the session database. The session pointer is bad. The *pointer* is the pointer of session structure, and *source_address* is the e-mail proxy client IP address.

Recommended Action None required.

719008

Error Message `%ASA-3-719008: Email Proxy service is shutting down.`

Explanation This message appears when the e-mail proxy service is disabled. All resources are cleaned up and all threads are terminated.

Recommended Action None required.

719009

Error Message `%ASA-7-719009: Email Proxy service is starting.`

Explanation This message appears when the e-mail proxy service is enabled.

Recommended Action None required.

719010

Error Message `%ASA-6-719010: protocol Email Proxy feature is disabled on interface interface_name.`

Explanation This message appears when the e-mail proxy feature is disabled on a specific entry point, invoked from the CLI. This is the main "off" switch for the user. When all protocols are turned off for all interfaces, the main shut down routine is invoked to clean up global resources, threads, and so on. The *protocol* is the e-mail proxy protocol type (for example, POP3, IMAP, and SMTP), and *interface_name* is the security appliance interface name.

Recommended Action None required.

719011

Error Message `%ASA-6-719011: Protocol Email Proxy feature is enabled on interface interface_name.`

Explanation This message appears when the e-mail proxy feature is enabled on a specific entry point, invoked from the CLI. This is the main "on" switch for the user. When it is first used, the main startup routine is invoked to allocate global resources, threads, and so on. Subsequent calls only need to start listen threads for the particular protocol. The *protocol* is the e-mail proxy protocol type (for example, POP3, IMAP, and SMTP), and *interface_name* is the security appliance interface name.

Recommended Action None required.

719012

Error Message `%ASA-6-719012: Email Proxy server listening on port port for mail protocol protocol.`

Explanation This message appears when a listen channel is opened for a specific protocol on a configured port and adds it to a TCP select group. The *port* is the configured port number, and *protocol* is the e-mail proxy protocol type (for example, POP3, IMAP, and SMTP).

Recommended Action None required.

719013

Error Message `%ASA-6-719013: Email Proxy server closing port port for mail protocol protocol.`

Explanation This message appears when a listen channel is closed for a specific protocol on a configured port and removes it from the TCP select group. The *port* is the configured port number, and *protocol* is the e-mail proxy protocol type (for example, POP3, IMAP, and SMTP).

Recommended Action None required.

719014

Error Message `%ASA-5-719014: Email Proxy is changing listen port from old_port to new_port for mail protocol protocol.`

Explanation This message appears when a change is signaled in the listen port for the specified protocol. All enabled interfaces for that port have their listen channels closed and restarted listening on the new port. This is invoked from the CLI. The *old_port* is the old configured port number, *new_port* is the new configured port number, and *protocol* is the e-mail proxy protocol type (for example, POP3, IMAP, and SMTP).

Recommended Action None required.

719015

Error Message `%ASA-7-719015: Parsed emailproxy session pointer from source_address username: mailuser = mail_user, vpnuser = VPN_user, mailserver = server`

Explanation This message appears when the username string is received from the client in the format vpnuser (name delimiter) mailuser (server delimiter) mailserver (for example: xxx:yyy@cisco.com). The name delimiter is optional. When the delimiter is not there, the VPN username and mail username is the same. The server delimiter is optional. When it is not present, this means the default configured mail server will be used. The *pointer* is the pointer for the session structure, *source_address* is the e-mail proxy client IP address, *mail_user* is the e-mail account username, *VPN_user* is the WebVPN username, and *server* is the e-mail server.

Recommended Action None required.

719016

Error Message `%ASA-7-719016: Parsed emailproxy session pointer from source_address password: mailpass = ******, vpnpass= ******`

Explanation This message appears when the password string is received from the client in the format, vpnpass (name delimiter) mailpass (for example: xxx:yyy). The name delimiter is optional. When it is not present, the VPN password and mail password are the same. The *pointer* is the pointer of the session structure, and *source_address* is the e-mail proxy client IP address.

Recommended Action None required.

719017

Error Message `%ASA-6-719017: WebVPN user: vpnuser invalid dynamic ACL.`

Explanation This message appears when the WebVPN session is aborted because the access control list has failed to parse for this user. The ACL determines what the user restrictions are on e-mail account accessing. The ACL is downloaded from the AAA server. Because of this error, it is unsafe to proceed with login. The *vpnuser* is the WebVPN username.

Recommended Action Check the AAA server and fix the dynamic ACL for this user.

719018

Error Message `%ASA-6-719018: WebVPN user: vpnuser ACL ID acl_ID not found`

Explanation This message appears when the access control list cannot be found at the local maintained ACL list. The ACL determines what the user restrictions are on e-mail account access. The ACL is configured locally. Because of this error, you cannot be authorized to proceed. The *vpnuser* is the WebVPN username, and *acl_ID* is the local configured ACL identification string.

Recommended Action Check the local ACL configuration.

719019

Error Message `%ASA-6-719019: WebVPN user: vpnuser authorization failed.`

Explanation This message appears when the ACL determines what the user restrictions are on e-mail account access. The user cannot access the e-mail account because the authorization check fails. The *vpnuser* is the WebVPN username.

Recommended Action None required.

719020

Error Message `%ASA-6-719020: WebVPN user vpnuser authorization completed successfully.`

Explanation This message appears when the ACL determines what the user restrictions are on e-mail account access. The user is authorized to access the e-mail account. The *vpnuser* is the WebVPN username.

Recommended Action None required.

719021

Error Message `%ASA-6-719021: WebVPN user: vpnuser is not checked against ACL.`

Explanation This message appears when the ACL determines what the user restrictions are on e-mail account access. The authorization checking using the ACL is not enabled. The *vpnuser* is the WebVPN username.

Recommended Action Enable the ACL checking feature if necessary.

719022

Error Message `%ASA-6-719022: WebVPN user vpnuser has been authenticated.`

Explanation This message appears when the username is authenticated by the AAA server. The *vpnuser* is the WebVPN username.

Recommended Action None required.

719023

Error Message `%ASA-6-719023: WebVPN user vpnuser has not been successfully authenticated. Access denied.`

Explanation This message appears when the username is denied by the AAA server. The session will be aborted. The user is not allowed to access the e-mail account. The *vpnuser* is the WebVPN username.

Recommended Action None required.

719024

Error Message `%ASA-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source_address`

Explanation This message appears when the Piggyback authentication is using an established WebVPN session to verify the username and IP address matching in the WebVPN session database. This is based on the assumption that the WebVPN session and e-mail proxy session are initiated by the same user and a WebVPN session is already established. Because the authentication has failed, the session will be aborted. The user is not allowed to access the e-mail account. The *pointer* is the pointer of session structure, *vpnuser* is the WebVPN username, and *source_address* is the client IP address.

Recommended Action None required.

719025

Error Message `%ASA-6-719025: Email Proxy DNS name resolution failed for hostname.`

Explanation This message appears when the hostname cannot be resolved with the IP address because it is not valid or there is no DNS server available. The *hostname* is the hostname that needs to be resolved.

Recommended Action Check DNS server availability and whether the configured mail server name is valid.

719026

Error Message `%ASA-6-719026: Email Proxy DNS name hostname resolved to IP_address.`

Explanation This message appears when the hostname has successfully been resolved with the IP address. The *hostname* is the hostname that needs to be resolved, and *IP_address* is the IP address resolved from the configured mail server name.

Recommended Action None required.

720001

Error Message `%ASA-4-720001: (VPN-unit) Failed to initialize with Chunk Manager.`

Explanation This message occurs when the VPN failover subsystem fails to initialize with the memory buffer management subsystem. The *unit* is either “Primary” or “Secondary.”

Recommended Action This message indicates a system-wide problem and the VPN failover subsystem cannot be started. Examine the system log messages for any sign of system-level initialization problems.

720002

Error Message `%ASA-6-720002: (VPN-unit) Starting VPN Stateful Failover Subsystem...`

Explanation This message appears when the VPN failover subsystem is starting and the system boots up. The *unit* is either “Primary” or “Secondary.”

Recommended Action None required.

720003

Error Message `%ASA-6-720003: (VPN-unit) Initialization of VPN Stateful Failover Component completed successfully`

Explanation This message appears when the VPN failover subsystem's initialization is completed at boot time. The *unit* is either “Primary” or “Secondary.”

Recommended Action None required.

720004

Error Message `%ASA-6-720004: (VPN-unit) VPN failover main thread started.`

Explanation This message appears when the VPN failover's main processing thread is started at boot time. The *unit* is either “Primary” or “Secondary.”

Recommended Action None required.

720005

Error Message `%ASA-6-720005: (VPN-unit) VPN failover timer thread started.`

Explanation This message appears when the VPN failover timer processing thread is started at boot time. The *unit* is either “Primary” or “Secondary.”

Recommended Action None required.

720006

Error Message `%ASA-6-720006: (VPN-unit) VPN failover sync thread started.`

Explanation This message appears when the system bulk synchronization processing thread is started at boot time. The *unit* is either "Primary" or "Secondary."

Recommended Action None required.

720007

Error Message `%ASA-4-720007: (VPN-unit) Failed to allocate chunk from Chunk Manager.`

Explanation This message appears when the set of preallocated memory buffers is running out. The *unit* is either "Primary" or "Secondary."

Recommended Action This message indicates a resource issue. The system may be under heavy load when too many messages are being processed. This condition may be improved later when the VPN failover subsystem processes outstanding messages and releases memory previously allocated.

720008

Error Message `%ASA-4-720008: (VPN-unit) Failed to register to High Availability Framework.`

Explanation This message appears when the VPN failover subsystem fails to register to the core failover subsystem. The *unit* is either "Primary" or "Secondary."

Recommended Action The VPN failover subsystem cannot be started. This may be caused by initialization problems of other subsystems. Search the system log messages for any sign of system-wide initialization problems.

720009

Error Message `%ASA-4-720009: (VPN-unit) Failed to create version control block.`

Explanation This message appears when the VPN failover subsystem fails to create a version control block. This step is required for VPN failover subsystem to find out the backward compatible firmware versions for the current release. The *unit* is either "Primary" or "Secondary."

Recommended Action The VPN failover subsystem cannot be started. This may be caused by initialization problems of other subsystems. Search the system log messages for any sign of system-wide initialization problems.

720010

Error Message `%ASA-6-720010: (VPN-unit) VPN failover client is being disabled`

Explanation This message appears when an operator enables failover without defining a failover key. To use a VPN failover, a failover key must be defined. The *unit* is either "Primary" or "Secondary."

Recommended Action Use the failover key command to define a shared secret key between the active and standby unit.

720011

Error Message `%ASA-4-720011: (VPN-unit) Failed to allocate memory`

Explanation This message appears when the VPN failover subsystem cannot allocate a memory buffer. This indicates a system-wide resource problem. The *unit* is either "Primary" or "Secondary."

Recommended Action The system may be under heavy load. This condition may be improved later when you reduce the load on the system by reducing incoming traffic. By reducing incoming traffic, memory allocated for processing the existing work load will be available and the system may return to normal operation.

720012

Error Message `%ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.`

Explanation This message appears when the VPN failover subsystem cannot update IPsec-related runtime data because the corresponding IPsec tunnel has been deleted on the standby unit. The *unit* is either "Primary" or "Secondary."

Recommended Action None required.

720013

Error Message `%ASA-4-720013: (VPN-unit) Failed to insert certificate in trust point trustpoint_name`

Explanation This message appears when the VPN failover subsystem attempts to insert a certificate in the trust point. The *unit* is either "Primary" or "Secondary" and *trustpoint_name* is the name of the trust point.

Recommended Action Check the certificate content to determine if it is invalid.

720014

Error Message `%ASA-6-720014: (VPN-unit) Phase 2 connection entry (msg_id=message_number, my cookie=mine, his cookie=his) contains no SA list.`

Explanation This message appears when there is no security association linked to the Phase 2 connection entry. The *unit* is either "Primary" or "Secondary," *message_number* is the message ID of the Phase 2 connection entry, *mine* is the My Phase 1 cookie, and *his* is the peer Phase 1 cookie.

Recommended Action None required.

720015

Error Message `%ASA-6-720015: (VPN-unit) Cannot found Phase 1 SA for Phase 2 connection entry (msg_id=message_number,my cookie=mine, his cookie=his).`

Explanation This message appears when the corresponding Phase 1 security association for the given Phase 2 connection entry cannot be found. The *unit* is either "Primary" or "Secondary," *message_number* is the message ID of the Phase 2 connection entry, *mine* is the My Phase 1 cookie, and *his* is the peer Phase 1 cookie.

Recommended Action None required.

720016

Error Message `%ASA-5-720016: (VPN-unit) Failed to initialize default timer #index.`

Explanation This message appears when the VPN failover subsystem fails to initialize the given timer event. The *unit* is either "Primary" or "Secondary" and *index* is the internal index of the timer event.

Recommended Action The VPN failover subsystem cannot be started at boot time. Search the syslog message for any sign of system-wide initialization problems.

720017

Error Message `%ASA-5-720017: (VPN-unit) Failed to update LB runtime data`

Explanation This message appears when the VPN failover subsystem fails to update the VPN load balancing runtime data. The *unit* is either "Primary" or "Secondary."

Recommended Action None required.

720018

Error Message `%ASA-5-720018: (VPN-unit) Failed to get a buffer from the underlying core high availability subsystem. Error code code.`

Explanation This message appears when the system may be under heavy load. The VPN failover subsystem fails to obtain a failover buffer. The *unit* is either "Primary" or "Secondary," and *code* is the error code returned by the high-availability subsystem.

Recommended Action Decrease the amount of incoming traffic to improve the current load condition. With decreased incoming traffic, the system will free up memory allocated for processing the incoming load.

720019

Error Message `%ASA-5-720019: (VPN-unit) Failed to update cTCP statistics.`

Explanation This message appears when the VPN failover subsystem fails to update the IPsec/cTCP-related statistics. The *unit* is either "Primary" or "Secondary."

Recommended Action None required. Updates are sent periodically, so the standby unit's IPsec/cTCP statistics should be updated with the next update message.

720020

Error Message `%ASA-5-720020: (VPN-unit) Failed to send type timer message.`

Explanation This message appears when the VPN failover subsystem fails to send a periodic timer message to the standby unit. The *unit* is either "Primary" or "Secondary," and *type* is the type of timer message.

Recommended Action None required. The periodic timer message will be resent during the next timeout.

720021

Error Message `%ASA-5-720021: (VPN-unit) HA non-block send failed for peer msg message_number. HA error code.`

Explanation The VPN failover subsystem fails to send a non-block message.

- *unit*—Either "Primary" or "Secondary."
- *message_number*—ID number of the peer message.

- *code*—Error return code.

Recommended Action This is a temporary condition causes by system under load or out of system resources. The system condition will improve as more system resources are freed up.

720022

Error Message `%ASA-4-720022: (VPN-unit) Cannot find trust point trustpoint`

Explanation An error is encountered when VPN failover subsystem attempts to look up a trust point by name.

- *unit*—Either "Primary" or "Secondary."
- *trustpoint*—Name of the trust point.

Recommended Action The trust point may be deleted by an operator.

720023

Error Message `%ASA-6-720023: (VPN-unit) HA status callback: Peer is not present.`

Explanation This is an informational message. The VPN failover subsystem is notified by the core failover subsystem when the local device detected that a peer is available or becomes unavailable.

- *unit*—Either "Primary" or "Secondary."
- *not*—Either "not" or "".

Recommended Action None required.

720024

Error Message `%ASA-6-720024: (VPN-unit) HA status callback: Control channel is status.`

Explanation This is an informational message indicating that the failover control channel is either "up" or "down." The failover control channel is defined by the **failover link** and **show failover** commands, which indicate whether the failover link channel is "up" or "down."

- *unit*—Either "Primary" or "Secondary."
- *status*— "Up" or "down."

Recommended Action None required.

720025

Error Message `%ASA-6-720025: (VPN-unit) HA status callback: Data channel is status.`

Explanation This is an informational message indicating whether the failover data channel is up or down.

- *unit*—Either "Primary" or "Secondary."
- *status*—"Up" or "down."

Recommended Action None required.

720026

Error Message `%ASA-6-720026: (VPN-unit) HA status callback: Current progression is being aborted.`

Explanation This message is generated only when an operator or other external condition applies and causes the current failover progression to abort before the failover peer agrees on the role (either active or standby). One example is when the **failover active** command is entered on the standby unit during the negotiation. Another example is the active unit being rebooted.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720027

Error Message `%ASA-6-720027: (VPN-unit) HA status callback: My state state.`

Explanation This informational message is generated whenever the state of the local failover device is changed.

- *unit*—Either "Primary" or "Secondary."
- *state*—Current state of the local failover device.

Recommended Action None required.

720028

Error Message `%ASA-6-720028: (VPN-unit) HA status callback: Peer state state.`

- *unit*—Either "Primary" or "Secondary."
- *state*—Current state of the failover peer.

Explanation This informational message is generated to report the current state of the failover peer.

Recommended Action None required.

720029

Error Message `%ASA-6-720029: (VPN-unit) HA status callback: Start VPN bulk sync state.`

- *unit* - Either “Primary” or “Secondary.”

Explanation This is an informational message generated when the active unit is ready to send all the state information to the standby unit.

Recommended Action None required.

720030

Error Message `%ASA-6-720030: (VPN-unit) HA status callback: Stop bulk sync state.`

- *unit*—Either “Primary” or “Secondary.”

Explanation This is an informational message generated when the active unit finishes sending all the state information to the standby unit.

Recommended Action None required.

720031

Error Message `%ASA-7-720031: (VPN-unit) HA status callback: Invalid event received. event=event_ID.`

Explanation This message is generated when VPN failover subsystem receives an invalid callback event from the underlying failover subsystem. This is a debug message.

- *unit*—Either “Primary” or “Secondary.”
- *event_ID*—Invalid event ID received.

Recommended Action None required.

720032

Error Message `%ASA-6-720032: (VPN-unit) HA status callback: id=ID, seq=sequence_#, grp=group, event=event, op=operand, my=my_state, peer=peer_state.`

Explanation This is an informational message generated by the VPN failover subsystem when a status update is notified by the underlying failover subsystem.

- *unit*—Either “Primary” or “Secondary.”
- *ID*—Client ID number.
- *sequence_#*—Sequence number.
- *group*—Group ID.
- *event*—Current event.
- *operand*—Current operand.
- *my_state*—The system current state.
- *peer_state*—The current state of the peer.

Recommended Action None required.

720033

Error Message `%ASA-4-720033: (VPN-unit) Failed to queue add to message queue.`

Explanation This message indicates that system resources may be running low. An error is encountered when the VPN failover subsystem attempts to queue an internal message.

- *unit*—Either “Primary” or “Secondary.”

Recommended Action This may be a temporary condition indicating that the system is under heavy load and the VPN failover subsystem cannot allocate resource to handle incoming traffic. This error condition may goes away if the current load of the system reduces and additional system resources become available for processing new messages again.

720034

Error Message `%ASA-7-720034: (VPN-unit) Invalid type (type) for message handler.`

Explanation An error is encountered when the VPN failover subsystem attempts to process an invalid message type.

- *unit*—Either “Primary” or “Secondary.”
- *type*—Message type.

Recommended Action This is a debugging message.

720035

Error Message `%ASA-5-720035: (VPN-unit) Fail to look up CTCP flow handle`

Explanation The cTCP flow may be deleted on the standby unit before the VPN failover subsystem attempts to do a lookup.

- *unit*—Either “Primary” or “Secondary.”

Recommended Action Look for any sign of cTCP flow deletion in the syslog message to determine the reason (for example, idle timeout) for why the flow is deleted.

720036

Error Message `%ASA-5-720036: (VPN-unit) Failed to process state update message from the active peer.`

Explanation An error is encountered when the VPN failover subsystem attempts to process a state update message received by the standby unit.

- *unit* - Either “Primary” or “Secondary.”

Recommended Action This may be a temporary condition due to current load or low system resources.

720037

Error Message `%ASA-6-720037: (VPN-unit) HA progression callback: id=id,seq=sequence_number,grp=group,event=event,op=operand, my=my_state,peer=peer_state.`

- *unit*—Either “Primary” or “Secondary.”
- *id*—Client ID.
- *sequence_number*—Sequence number.
- *group*—Group ID
- *event*—Current event.
- *operand*—Current operand.
- *my_state*—Current state of the system.
- *peer_state*—Current state of the peer.

Explanation This is an informational message reporting the status of the current failover progression.

Recommended Action None required.

720038

Error Message `%ASA-4-720038: (VPN-unit) Corrupted message from active unit.`

Explanation The standby unit receives a corrupted message from the active unit. Messages from active unit are corrupted. This may be caused by incompatible firmware running between the active and standby unit.

- *unit*—Either "Primary" or "Secondary."

Recommended Action This is an informational message indicating the local unit has become the active unit of the failover pair.

720039

Error Message `%ASA-6-720039: (VPN-unit) VPN failover client is transitioning to active state`

Explanation This is an informational message indicating the local unit has become the active unit of the failover pair.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720040

Error Message `%ASA-6-720040: (VPN-unit) VPN failover client is transitioning to standby state.`

Explanation This is an informational message indicating the local unit has become the standby unit of the failover pair.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720041

Error Message `%ASA-7-720041: (VPN-unit) Sending type message id to standby unit`

Explanation This is a debugging message indicating a message is sent from the active unit to the standby unit.

- *unit*—Either "Primary" or "Secondary."
- *type*—Message type.

- *id*—Identifier for the message.

Recommended Action None required.

720042

Error Message `%ASA-7-720042: (VPN-unit) Receiving type message id from active unit`

Explanation This is a debugging message indicating a message is received by the standby unit.

- *unit*—Either "Primary" or "Secondary."
- *type*—Message type.
- *id*—Identifier for the message.

Recommended Action None required.

720043

Error Message `%ASA-4-720043: (VPN-unit) Failed to send type message id to standby unit`

Explanation An error was encountered when the VPN failover subsystem attempts to send a message from the active unit to the standby unit. This may be caused by syslog message 720018, in which the core failover subsystem runs out of failover buffer or the failover LAN link is down.

- *unit*—Either "Primary" or "Secondary."
- *type*—Message type.
- *id*—Identifier for the message.

Recommended Action Use the **show failover** command to see if the failover pair is running correctly and the failover LAN link is "up."

720044

Error Message `%ASA-4-720044: (VPN-unit) Failed to receive message from active unit`

Explanation An error is encountered when the VPN failover subsystem attempts to receive a message on the standby unit. This may be caused by a corrupted message, or insufficient memory was being allocated for storing the incoming message.

- *unit*—Either "Primary" or "Secondary."

Recommended Action Use the **show failover** command and look for receive errors to determine if this is a VPN failover-specific problems or a general failover issue. Corrupted messages may be caused by incompatible firmware versions running on active and standby units. Use the **show memory** command to determine if there is a low memory condition.

720045

Error Message `%ASA-6-720045: (VPN-unit) Start bulk syncing of state information on standby unit.`

Explanation This is an informational message indicating the standby unit has been notified to start receiving bulk synchronization information from the active unit.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720046

Error Message `%ASA-6-720046: (VPN-unit) End bulk syncing of state information on standby unit`

Explanation This is an informational message indicating the standby unit has been notified that bulk synchronization from the active unit is completed.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720047

Error Message `%ASA-4-720047: (VPN-unit) Failed to sync SDI node secret file for server IP_address on the standby unit.`

Explanation An error was encountered when the VPN failover subsystem attempted to synchronize a node secret file for the SDI server on the standby unit. The SDI node secret file is stored in the flash file system. This error may indicate that the flash file system is full or corrupted.

- *unit*—Either "Primary" or "Secondary."
- *IP_address*—IP address of the server.

Recommended Action Use the **dir** command to display the flash file system contents. The node secret file is named "*ip*.sdi."

720048

Error Message `%ASA-7-720048: (VPN-unit) FSM action trace begin: state=state, last event=event, func=function.`

Explanation This is a debugging message indicating a VPN failover subsystem finite state machine function is started.

- *unit*—Either “Primary” or “Secondary.”
- *state*—Current state.
- *event*—Last event.
- *function*—Current executing function.

Recommended Action None required.

720049

Error Message `%ASA-7-720049: (VPN-unit) FSM action trace end: state=state, last event=event, return=return, func=function.`

Explanation This is a debugging message indicating a VPN failover subsystem finite state machine function is completed.

- *unit*—Either “Primary” or “Secondary.”
- *state*—Current state.
- *event*—Last event.
- *return*—Return code.
- *function*—Current executing function.

Recommended Action None required.

720050

Error Message `%ASA-7-720050: (VPN-unit) Failed to remove timer. ID = id.`

Explanation This is a debug message indicating that a timer cannot be removed from the timer processing thread.

- *unit*—Either “Primary” or “Secondary.”
- *id*—Timer ID.

Recommended Action None required.

720051

Error Message `%ASA-4-720051: (VPN-unit) Failed to add new SDI node secret file for server id on the standby unit.`

Explanation An error was encountered when the VPN failover subsystem attempted to add a node secret file for the SDI server on the standby unit. The SDI node secret file is stored in the flash file system. This error may indicate that the flash file system is full or corrupted.

- *unit*—Either "Primary" or "Secondary."
- *id*—IP address of the SDI server.

Recommended Action Enter the **dir** command to display the flash file system contents. The node secret file is named "*ip*.sdi."

720052

Error Message `%ASA-4-720052: (VPN-unit) Failed to delete SDI node secret file for server id on the standby unit.`

Explanation An error was encountered when the VPN failover subsystem attempted to delete a node secret file on the active unit. The node secret file being deleted may not exist in the flash file system, or there is a problem reading the flash file system.

- *unit*—Either "Primary" or "Secondary."
- *IP_address*—IP address of the SDI server.

Recommended Action Use the **dir** command to display the flash file system contents. The node secret file is named "*ip*.sdi."

720053

Error Message `%ASA-4-720053: (VPN-unit) Failed to add cTCP IKE rule during bulk sync, peer=IP_address, port=port`

Explanation An error is encountered when the VPN failover subsystem attempts to load an cTCP IKE rule on the standby unit during bulk synchronization.

- *unit*—Either "Primary" or "Secondary."
- *IP_address*—IP address of the peer.
- *port*—Port number of the peer.

Recommended Action The standby unit may be under heavy load, and the new IKE rule request times out before completion.

720054

Error Message `%ASA-4-720054: (VPN-unit) Failed to add new cTCP record, peer=IP_address, port=port.`

Explanation A cTCP record is replicated to the standby and cannot be updated. The corresponding IPsec over cTCP tunnel may not be functioning after failover.

- *unit*—Either "Primary" or "Secondary."
- *IP_address*—IP address of the peer.
- *port*—Port number of the peer.

Recommended Action The cTCP database may be full or a record with the same peer IP address and port number exists already. This may be a temporary condition.

720055

Error Message `%ASA-4-720055: (VPN-unit) VPN Stateful failover can only be run in single/non-transparent mode.`

Explanation This message will be displayed and the VPN subsystem will not be started if you are not running in single (non-transparent) mode.

- *unit*—Either "Primary" or "Secondary."

Recommended Action Configure the device for the appropriate mode to support VPN failover and restart the device.

720056

Error Message `%ASA-6-720056: (VPN-unit) VPN Stateful failover Message Thread is being disabled.`

Explanation This is an informational message indicating the VPN failover subsystem main message processing thread is disabled when a user attempts to enable failover, but the failover key is not defined. A failover key is required for VPN failover.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720057

Error Message `%ASA-6-720057: (VPN-unit) VPN Stateful failover Message Thread is enabled.`

Explanation This is an informational message that indicates the VPN failover subsystem main message processing thread is enabled when failover is enabled, and a failover key is defined.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720058

Error Message `%ASA-6-720058: (VPN-unit) VPN Stateful failover Timer Thread is disabled.`

Explanation This is an informational message that indicates the VPN failover subsystem main timer processing thread is disabled when the failover key is not defined, and failover is enabled.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720059

Error Message `%ASA-6-720059: (VPN-unit) VPN Stateful failover Timer Thread is enabled.`

Explanation This is an informational message that indicates the VPN failover subsystem main timer processing thread is enabled when the failover key is defined, and failover is enabled.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720060

Error Message `%ASA-6-720060: (VPN-unit) VPN Stateful failover Sync Thread is disabled.`

Explanation This is an informational message that indicates the VPN failover subsystem main bulk synchronization processing thread is disabled when failover is enabled, but the failover key is not defined.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720061

Error Message `%ASA-6-720061: (VPN-unit) VPN Stateful failover Sync Thread is enabled.`

Explanation This is an informational message that indicates the VPN failover subsystem main bulk synchronization processing thread is enabled when failover is enabled and the failover key is defined.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720062

Error Message `%ASA-6-720062: (VPN-unit) Active unit started bulk sync of state information to standby unit.`

Explanation This is an informational message indicating the VPN failover subsystem active unit has started bulk synchronization of state information to the standby unit.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720063

Error Message `%ASA-6-720063: (VPN-unit) Active unit completed bulk sync of state information to standby.`

Explanation This is an informational message that indicates the VPN failover subsystem active unit has performed bulk synchronization of state information to the standby unit.

- *unit*—Either "Primary" or "Secondary."

Recommended Action None required.

720064

Error Message `%ASA-4-720064: (VPN-unit) Failed to update cTCP database record for peer=IP_address, port=port during bulk sync.`

Explanation An error was encountered while the VPN failover subsystem attempted to update an existing cTCP record during bulk synchronization. The cTCP record may have been deleted from the cTCP database on the standby unit and cannot be found.

- *unit*—Either "Primary" or "Secondary."
- *IP_address*—IP address of the peer.
- *port*—Port number of the peer.

Recommended Action Search in the system log messages.

720065

Error Message `%ASA-4-720065: (VPN-unit) Failed to add new cTCP IKE rule, peer=peer, port=port.`

Explanation An error is encountered when the VPN failover subsystem attempts to add a new IKE rule for the cTCP database entry on the standby unit.

- *unit*—Either "Primary" or "Secondary."
- *IP_address*—IP address of the peer.
- *port*—Port number of the peer.

Recommended Action The system may be under heavy load, and the request for adding a cTCP IKE rule timeout never completed. This may be a temporary condition.

720066

Error Message `%ASA-4-720066: (VPN-unit) Failed to activate IKE database.`

Explanation An error was encountered when the VPN failover subsystem attempted to activate the IKE security association database while the standby unit was transitioning to the active state. There may be resource-related issues on the standby unit that prevent the IKE security association database from activating.

- *unit*—Either "Primary" or "Secondary."

Recommended Action Use the **show failover** command to see whether the failover pair is still operating correctly and/or look for other IKE-related errors in the system log messages.

720067

Error Message `%ASA-4-720067: (VPN-unit) Failed to deactivate IKE database.`

Explanation An error was encountered when the VPN failover subsystem attempted to deactivate the IKE security association database while the active unit was transitioning to the standby state. There may be resources-related issues on the active unit that prevent the IKE security association database from deactivating.

- *unit*—Either "Primary" or "Secondary."

Recommended Action Enter the **show failover** command to see if the failover pair is still operating correctly and/or look for IKE related errors in the system log messages.

720068

Error Message `%ASA-4-720068: (VPN-unit) Failed to parse peer message.`

Explanation An error is encountered when the VPN failover subsystem attempts to parse a peer message received on the standby unit.

- *unit*—Either "Primary" or "Secondary."

Recommended Action The peer message received on the standby unit cannot be parsed. Make sure both the active and standby units are running the same versions of firmware. Also, use the **show failover** command to ensure the failover pair is still operating correctly.

720069

Error Message `%ASA-4-720069: (VPN-unit) Failed to activate cTCP database.`

Explanation An error was encountered when the VPN failover subsystem attempted to activate the cTCP database while the standby unit was transitioning to the active state. There may be resource-related issues on the standby unit that prevent the cTCP database from activating.

- *unit*—Either "Primary" or "Secondary."

Recommended Action Enter the **show failover** command to see if the failover pair is still operating correctly and/or look for other cTCP related errors in the system log messages.

720070

Error Message `%ASA-4-720070: (VPN-unit) Failed to deactivate cTCP database.`

Explanation An error was encountered when the VPN failover subsystem attempted to deactivate the cTCP database while the active unit was transitioning to the standby state. There may be resource-related issues on the active unit that prevent the cTCP database from deactivating.

- *unit*—Either "Primary" or "Secondary."

Recommended Action Use the **show failover** command to see if the failover pair is still operating correctly and/or look for cTCP-related errors in the system log messages.

720071

Error Message `%ASA-5-720071: (VPN-unit) Failed to update cTCP dynamic data.`

Explanation An error was encountered while the VPN failover subsystem attempted to update cTCP dynamic data.

- *unit*—Either "Primary" or "Secondary."

Explanation This may be a temporary condition. Because this is a periodic update, wait to see whether the same error occurs. Also, look for other failover-related messages in the system log messages.

720072

Error Message `%ASA-5-720072: Timeout waiting for Integrity Firewall Server [interface,ip] to become available.`

Explanation In an active or standby failover setup, the SSL connection between a Zonelab Integrity Server and the security appliance needs to be reestablished after a failover. This syslog message is generated if the Zonelab Integrity Server cannot reestablish a connection before timeout.

- *interface*—The interface to which the Zonelab Integrity Server is connected.
- *ip*—The IP address of the Zonelab Integrity Server.

Recommended Action Check that the configuration on the security appliance and the Zonelab Integrity Server match, and verify communication between the security appliance and the Zonelab Integrity Server.

720073

Error Message `%ASA-4-720073: (VPN-unit) Fail to insert certificate in trust point trustpoint on the standby unit.`

Explanation An error is encountered when the VPN failover subsystem attempts to insert a certificate in the trust point. This error may be caused by invalid content of the certificate.

- *unit*—Either "Primary" or "Secondary."
- *trustpoint*—Name of the trust point.

Recommended Action Enter the **write standby** command on the active unit to replicate the certificate to the standby unit manually. Search in the syslog message to see if there are any failover or PKI-related errors.

721001

Error Message `%ASA-6-721001: (device) WebVPN Failover SubSystem started successfully.(device) either WebVPN-primary or WebVPN-secondary.`

Explanation The WebVPN Failover SubSystem in the current failover unit, either primary or secondary, has been started successfully.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.

Recommended Action None required.

721002

Error Message `%ASA-6-721002: (device) HA status change: event event, my state my_state, peer state peer.`

Explanation The WebVPN Failover SubSystem receives status notification from the core HA component periodically. This is an informational message reporting the incoming event, the new state of the local device, and the new state of the failover peer.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *event*—New HA event.
- *my_state*—My new state.
- *peer*—Peer new state.

Recommended Action None required.

721003

Error Message `%ASA-6-721003: (device) HA progression change: event event, my state my_state, peer state peer.`

Explanation The WebVPN Failover SubSystem transitions from one state to another state based on event notified by the core HA component. This is an informational message reporting the incoming event, the new state of the local device, and the new state of the failover peer.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *event*—New HA event.
- *my_state*—My new state.
- *peer*—Peer new state.

Recommended Action None required.

721004

Error Message `%ASA-6-721004: (device) Create access list list_name on standby unit.`

Explanation A WebVPN-specific access list is replicated from the active unit to the standby unit. This message reports a successful installation of the WebVPN access list on the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *list_name*—The access list name.

Recommended Action None required.

721005

Error Message `%ASA-6-721005: (device) Fail to create access list list_name on standby unit.`

Explanation When a WebVPN-specific access list is installed on the active unit, a copy is installed on the standby unit. This message indicates that the access list failed to be installed on the standby unit. One possibility is that the access list already existed on the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *list_name*—Name of access list that failed to install on the standby unit.

Recommended Action Issue a **show access-list** command on both the active and standby unit. Compare the content of the output and determine whether there is any discrepancy. Re-sync the standby unit, if needed, by entering the **write standby** command on the active unit.

721006

Error Message `%ASA-6-721006: (device) Update access list list_name on standby unit.`

Explanation An informational message indicating that the content of the access list has been updated on the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *list_name*—Name of the access list that was updated.

Recommended Action None required.

721007

Error Message `%ASA-4-721007: (device) Fail to update access list list_name on standby unit.`

Explanation This message indicates that an error condition is encountered while the standby unit attempts to update a WebVPN-specific access list. One possibility is that the access list cannot be located on the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *list_name*—Name of the access list that was not updated.

Recommended Action Issue a **show access-list** command on both the active and standby unit. Compare the content of the output and determine whether there is any discrepancy. Re-sync the standby unit if needed by entering the **write standby** command on the active unit.

721008

Error Message `%ASA-6-721008: (device) Delete access list list_name on standby unit.`

Explanation When a WebVPN-specific access list is removed from the active unit, a message is sent to the standby unit requesting the same access list be removed. This is an informational message indicating that a WebVPN-specific access list has been removed from the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *list_name*—Name of the access list that was deleted.

Recommended Action None required.

721009

Error Message `%ASA-6-721009: (device) Fail to delete access list list_name on standby unit.`

Explanation When a WebVPN-specific access list is removed on the active unit, a message is sent to the standby unit requesting the same access list be removed. This message indicates that an error condition was encountered when an attempt was made to remove the corresponding access list on the standby unit. One possibility may be that the access list did not exist on the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *list_name*—Name of the access list that was deleted.

Recommended Action Issue a **show access-list** command on both the active and standby unit. Compare the content of the output and determine whether there is any discrepancy. Re-sync the standby unit if needed by entering the **write standby** command on the active unit.

721010

Error Message `%ASA-6-721010: (device) Add access list rule list_name, line line_no on standby unit.`

Explanation When an access list rule is added to the active unit, the same rule is added on the standby unit. This is an informational message indicating that a new access list rule has been added successfully on the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *list_name*—Name of the access list that was deleted.
- *line_no*—Line number of the rule added to the access list.

Recommended Action None required.

721011

Error Message `%ASA-4-721011: (device) Fail to add access list rule list_name, line line_no on standby unit.`

Explanation When an access list rule is added to the active unit, an attempt is made to add the same access list rule to the standby unit. This message indicates an error condition is encountered when an attempt is made to add a new access list rule to the standby unit. One possible situation is that the same access list rule exists on the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *list_name*—Name of the access list that was deleted.

- *line_no*—Line number of the rule added to the access list.

Recommended Action Issue a **show access-list** command on both the active and standby unit. Compare the content of the output and determine if there is any discrepancy. Re-sync the standby unit if needs to through entering the **write standby** command on the active unit.

721012

Error Message `%ASA-6-721012: (device) Enable APCF XML file file_name on the standby unit.`

Explanation When an APCF XML file is installed on the active unit, an attempt is made to install the same file on the standby unit. This is an informational message indicating that an APCF XML file is installed successfully on the standby unit. Using the **dir** command on the standby unit will show that the XML file exists in the flash file system.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *file_name*—Name of the XML file on the flash file system.

Recommended Action None required.

721013

Error Message `%ASA-4-721013: (device) Fail to enable APCF XML file file_name on the standby unit.`

Explanation When an APCF XML file is installed on the active unit, an attempt is made to install the same file on the standby unit. This is an error message indicating that an APCF XML file failed to install on the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *file_name*—Name of the XML file on the flash file system.

Recommended Action Perform a **dir** command on both the active and standby units. Compare the directory listing and determine if there is any discrepancy. Re-sync the standby unit if needed by entering the **write standby** command on the active unit.

721014

Error Message `%ASA-6-721014: (device) Disable APCF XML file file_name on the standby unit.`

Explanation When an APCF XML file is removed on the active unit, an attempt is made to remove the same file on the standby unit. This is a message indicating that an APCF XML file has been removed from the standby unit successfully.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.

- *file_name*—Name of the XML file on the flash file system.

Recommended Action None required.

721015

Error Message `%ASA-4-721015: (device) Fail to disable APCF XML file file_name on the standby unit.`

Explanation When an APCF XML file is removed on the active unit, an attempt is made to remove the same file on the standby unit. This message indicates an error condition occurred when an attempt is made to remove an APCF XML file from the standby unit. One possible cause may be the file was not installed on the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *file_name*—Name of the XML file on the flash file system.

Recommended Action Perform a **show running-config webvpn** command to make sure the APCF XML file of interest is not enabled. As long as it is not enabled, you may ignore this message. Otherwise, try to disable the file by using the **no apcf** *file_name* command under the webvpn configuration submode.

721016

Error Message `%ASA-6-721016: (device) WebVPN session for client user user_name, IP ip_address has been created.`

Explanation Indicates that a remote WebVPN user has logged in successfully and the login information has been installed on the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *user_name*—Name of the user.
- *ip_address*—IP address of the remote user.

Recommended Action None required.

721017

Error Message `%ASA-4-721017: (device) Fail to create WebVPN session for user user_name, IP ip_address.`

Explanation When a WebVPN user logs in to the active unit, the login information is replicated to the standby unit. This message indicates an error condition occurred while replicating the login information to the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *user_name*—Name of the user.

- *ip_address*—IP address of the remote user.

Recommended Action Perform a **show vpn-sessiondb detail webvpn** command for a regular WebVPN user, or **show vpn-sessiondb detail svc** for a WebVPN SVC user on both the active and standby units. Compare the entries and determine whether the same user session record appears on both devices. Re-sync the standby unit if needed by entering the **write standby** command on the active unit.

721018

Error Message `%ASA-6-721018: (device) WebVPN session for client user user_name, IP ip_address has been deleted.`

Explanation When a WebVPN user logs out on the active unit, a logout message is sent to the standby unit to remove the user session from the standby unit. This is an informational message indicating that a WebVPN user record was successfully removed from the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *user_name*—Name of the user.
- *ip_address*—IP address of the remote user.

Recommended Action None required.

721019

Error Message `%ASA-4-721019: (device) Fail to delete WebVPN session for client user user_name, IP ip_address.`

Explanation When a WebVPN user logs out on the active unit, a logout message is sent to the standby unit to remove the user session from the standby unit. This message indicates that an error was encountered when an attempt was made to remove a WebVPN user record from the standby unit.

- *(device)*—Either the WebVPN-primary or the WebVPN-secondary.
- *user_name*—Name of the user.
- *ip_address*—IP address of the remote user.

Recommended Action Enter the **show vpn-sessiondb detail webvpn** command for a regular WebVPN user, or the **show vpn-sessiondb detail svc** command for a WebVPN SVC user on both the active and standby units. Check whether there is any discrepancy. Re-sync the standby unit if needed by entering the **write standby** command on the active unit.

722001

Error Message `%ASA-4-722001: IP IP_address Error parsing SVC connect request.`

Explanation The request from the SSL VPN client (SVC) was invalid.

Recommended Action Research as necessary to determine if this was caused by a defect in the SVC, an incompatible SVC version, or an attack against the device.

722002

Error Message `%ASA-4-722002: IP IP_address Error consolidating SVC connect request.`

Explanation There is not enough memory to perform the action.

Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

722003

Error Message `%ASA-4-722003: IP IP_address Error authenticating SVC connect request.`

Explanation The user took too long to download and connect.

Recommended Action Increase the timeouts for session idle and maximum connect times.

722004

Error Message `%ASA-4-722004: Group group User user-name IP IP_address Error responding to SVC connect request.`

Explanation There is not enough memory to perform the action.

Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

722005

Error Message `%ASA-5-722005: Group group User user-name IP IP_address Unable to update session information for SVC connection.`

Explanation There is not enough memory to perform the action.

Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

722006

Error Message %ASA-5-722006: Group *group* User *user-name* IP *IP_address* Invalid address *IP_address* assigned to SVC connection.

Explanation An invalid address was assigned to the user.

Recommended Action Verify and correct the address assignment.

722007

Error Message %ASA-3-722007: Group *group-name* User *user-name* IP *IP_address* SVC Message: *type-num*/ERROR: *message*

Explanation This is a message from the SSL VPN client (SVC).

- *type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused
- *message*—A text message from the SVC.

Recommended Action None required.

722008

Error Message %ASA-3-722008: Group *group-name* User *user-name* IP *IP_address* SVC Message: *type-num*/ERROR: *message*

Explanation This is a message from the SSL VPN client (SVC).

- *type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused
- *message*—A text message from the SVC.

Recommended Action None required.

722009

Error Message `%ASA-3-722009: Group group-name User user-name IP IP_address SVC Message: type-num/ERROR: message`

Explanation This is a message from the SVC client.

- *type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused
- *message*—A text message from the SVC.

Recommended Action None required.

722010

Error Message `%ASA-5-722010: Group group-name User user-name IP IP_address SVC Message: type-num/NOTICE: message`

Explanation This is a message from the SVC client.

- *type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused
- *message*—A text message from the SVC.

Recommended Action None required.

722011

Error Message `%ASA-5-722011: Group group-name User user-name IP IP_address SVC Message: type-num/NOTICE: message`

Explanation This is a message from the SVC client.

- *type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout

  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused
- *message*—A text message from the SVC.

Recommended Action None required.

722012

Error Message `%ASA-5-722012: Group group-name User user-name IP IP_address SVC Message: type-num/INFO: message`

Explanation This is a message from the SVC client.

- *type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused
- *message*—A text message from the SVC.

Recommended Action None required.

722013

Error Message `%ASA-6-722013: Group group-name User user-name IP IP_address SVC Message: type-num/INFO: message`

Explanation This is a message from the SVC client.

- *type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused
- *message*—A text message from the SVC.

Recommended Action None required.

722014

Error Message `%ASA-6-722014: Group` *group-name* `User` *user-name* `IP` *IP_address* `SVC Message:` *type-num*`/INFO:` *message*

Explanation This is a message from the SVC client.

- *type-num*— A number from 0 to 31 indicating a message type. Message types are as follows:
  - 0—Normal.
  - 16—Logout
  - 17—Closed due to error
  - 18—Closed due to rekey
  - 1-15, 19-31—Reserved and unused
- *message*—A text message from the SVC.

Recommended Action None required.

722015

Error Message `%ASA-4-722015: Group` *group-name* `User` *user-name* `IP` *IP_address* `Unknown SVC frame type:` *type-num*

Explanation The SSL VPN client (SVC) sent an invalid frame type to the device.

- *type-num*—The number identifier of the frame type.

Recommended Action This could be caused by an SVC version incompatibility. Verify the SVC version.

722016

Error Message `%ASA-4-722016: Group` *group-name* `User` *user-name* `IP` *IP_address* `Bad SVC frame length:` *length* `expected:` *expected-length*

Explanation The expected amount of data was not available from the SSL VPN client (SVC).

Recommended Action This could be caused by an SVC version incompatibility. Verify the SVC version.

722017

Error Message `%ASA-4-722017: Group group-name User user-name IP IP_address Bad SVC framing: 525446, reserved: 0`

Explanation The SSL VPN client (SVC) send a badly framed datagram.

Recommended Action This could be caused by an SVC version incompatibility. Verify the SVC version.

722018

Error Message `%ASA-4-722018: Group group-name User user-name IP IP_address Bad SVC protocol version: version, expected: expected-version`

Explanation The SSL VPN client (SVC) sent a version unknown to the device.

Recommended Action This could be caused by an SVC version incompatibility. Verify the SVC version.

722019

Error Message `%ASA-4-722019: Group group-name User user-name IP IP_address Not enough data for an SVC header: length`

Explanation The expected amount of data was not available from the SSL VPN client (SVC).

Recommended Action This could be caused by an SVC version incompatibility. Verify the SVC version.

722020

Error Message `%ASA-3-722020: TunnelGroup tunnel_group GroupPolicy group_policy User user-name IP IP_address No address available for SVC connection`

Explanation Address assignment failed for the AnyConnect session. No IP addresses are available.

- *tunnel_group*—The name of the tunnel group that the user was assigned to or used to log in
- *group_policy*—The name of the group policy that the user was assigned to
- *user-name*—The name of the user with which this message is associated

- *IP_address*—The public IP (Internet) address of the client machine

Recommended Action Check the configuration listed in the **ip local ip** command to see if enough addresses exist in the pools that have been assigned to the tunnel group and the group policy. Check the DHCP configuration and status. Check the address assignment configuration. Enable IPAA syslog messages to determine why the AnyConnect client cannot obtain an IP address.

722021

Error Message `%ASA-3-722021: Group group-name User user-name IP IP_address Unable to start compression due to lack of memory resources`

Explanation There is not enough memory to perform the action.

Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

722022

Error Message `%ASA-6-722022: Group group-name User user-name IP addr (TCP | UDP) connection established (with | without) compression`

Explanation The TCP or UDP connection was established with or without compression.

Recommended Action None required.

722023

Error Message `%ASA-6-722023: Group group-name User user-name IP IP_address SVC connection terminated {with|without} compression`

Explanation Informational message only.

Recommended Action None required.

722024

Error Message `%ASA-6-722024: SVC Global Compression Enabled`

Explanation Indicates that subsequent SSL VPN Client (SVC) connections will be allowed to perform tunnel compression if SVC compression is enabled in the corresponding user or group configuration.

Recommended Action None required.

722025

Error Message `%ASA-6-722025: SVC Global Compression Disabled`

Explanation Indicates that subsequent SSL VPN Client (SVC) connections will *not* be allowed to perform tunnel compression.

Recommended Action None required.

722026

Error Message `%ASA-6-722026: Group` *`group-name`* `User` *`user-name`* `IP` *`IP_address`* `SVC compression history reset`

Explanation A compression error occurred. The SSL VPN client (SVC) and device corrected it.

Recommended Action None required.

722027

Error Message `%ASA-6-722027: Group` *`group-name`* `User` *`user-name`* `IP` *`IP_address`* `SVC decompression history reset`

Explanation A decompression error occurred. The SSL VPN client (SVC) and device corrected it.

Recommended Action None required.

722028

Error Message `%ASA-5-722028: Group` *`group-name`* `User` *`user-name`* `IP` *`IP_address`* `Stale SVC connection closed.`

Explanation An unused SSL VPN client (SVC) connection was closed.

Recommended Action None required. However, the client may be having trouble connecting if multiple connections are established. The SVC log should be examined.

722029

Error Message `%ASA-7-722029: Group group-name User user-name IP IP_address SVC Session Termination: Conns: connections, DPD Conns: DPD_conns, Comp resets: compression_resets, Dcmp resets: decompression_resets`

Explanation This message lists the number of connections, reconnections, and resets that have occurred. If *connections* is greater than 1 or the number of *DPD_conns*, *compression_resets, or decompression_resets* is greater than 0, it may indicate network reliability problems, which may be beyond the control of the security appliance administrator.

- *connections*—The total number of connections during this session (1 is normal).
- *DPD_conns*—The number of reconnections due to DPD (Dead-Peer-Detection).
- *compression_resets*—The number of compression history resets.
- *decompression_resets*—The number of decompression history resets.

Recommended Action If there are many connections or DPD connections, the user may be having problems connecting and may experience poor performance. The SSL VPN client (SVC) log should be examined.You may want to research and take appropriate action to resolve possible network reliability problems.

722030

Error Message `%ASA-7-722030: Group group-name User user-name IP IP_address SVC Session Termination: In: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops`

Explanation End-of-session statistics are being recorded.

- *data_bytes*—The number of inbound (from SVC) data bytes.
- *ctrl_bytes*—The number of inbound control bytes.
- *data_pkts*—The number of inbound data packets.
- *ctrl_pkts*—The number of inbound control packets.
- *drop_pkts*—The number of inbound packets that were dropped.

Recommended Action None required.

722031

Error Message `%ASA-7-722031: Group group-name User user-name IP IP_address SVC Session Termination: Out: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops.`

Explanation End-of-session statistics are being recorded.

- *data_bytes*—The number of outbound (to SVC) data bytes.

- *ctrl_bytes*—The number of outbound control bytes.
- *data_pkts*—The number of outbound data packets.
- *ctrl_pkts*—The number of outbound control packets.
- *ctrl_pkts*—The number of outbound packets that were dropped.

Recommended Action None required.

722032

Error Message `%ASA-5-722032: Group group-name User user-name IP IP_address New SVC connection replacing old connection.`

Explanation A new SSL VPN client (SVC) connection is replacing an existing one.

Recommended Action Users may be having trouble connecting. The SVC log should be examined.

722033

Error Message `%ASA-5-722033: Group group-name User user-name IP IP_address First SVC connection established for SVC session.`

Explanation Informational message only.

Recommended Action None required.

722034

Error Message `%ASA-5-722034: Group group-name User user-name IP IP_address New SVC connection, no existing connection.`

Explanation This message occurs during a reconnection attempt. A new SSL VPN client (SVC) connection is replacing a previously closed connection. There is no existing connection for this session because the connection was already dropped by the SVC or the security appliance.

Recommended Action The user may be having trouble connecting. The device and SVC log should be examined.

722035

Error Message `%ASA-3-722035: Group group-name User user-name IP IP_address Transmitting large packet length threshold.`

Explanation A large packet was sent to the client. The source of the packet may not be aware of the MTU of the client.

- *length*—The length of the large packet.
- +*num*—The threshold.

Recommended Action None required.

722036

Error Message `%ASA-3-722036: Group group-name User user-name IP IP_address Received large packet length (threshold threshold).`

Explanation A large packet was received from the client.

- *length*—The length of the large packet.
- +*num*—The threshold.

Recommended Action Determine if the SVC is compatible with the security appliance and correct as necessary.

722037

Error Message `%ASA-5-722037: Group group-name User user-name IP IP_address SVC closing connection: reason.`

Explanation An SSL VPN client (SVC) connection was terminated for the given reason.

- *reason*—The reason the SVC connection was terminated.

Recommended Action This may be normal, or the user may be having trouble connecting. The SVC log should be examined.

722038

Error Message `%ASA-5-722038: Group group-name User user-name IP IP_address SVC terminating session: reason.`

Explanation An SSL VPN client (SVC) session was terminated for the given reason.

- *reason*—The reason the SVC session was terminated.

Recommended Action This may be normal, or the user may be having trouble connecting. The SVC log should be examined if the reason for termination is unexpected.

722039

Error Message `%ASA-4-722039: Group group, User user, IP ip, SVC 'vpn-filter acl' is an IPv6 ACL; ACL not applied.`

Explanation The type of ACL to be applied is incorrect. An IPv6 ACL has been configured as an IPv4 ACL (**vpn-filter** command).

- *group*—The group-policy name of the user.
- *user*—The username.
- *ip*—The public (not assigned) IP address of the user.
- *acl*—The name of the invalid ACL.

Recommended Action Validate the vpn-filter and ipv6-vpn-filter configuration on the security appliance and the filter parameters on the AAA (RADIUS) server. Ensure that the correct type of ACL is specified.

722040

Error Message `%ASA-4-722040: Group group, User user, IP ip, SVC 'ipv6-vpn-filter acl' is an IPv4 ACL; ACL not applied`

Explanation The type of ACL to be applied is incorrect. An IPv4 ACL has been configured as an IPv6 ACL (**ipv6-vpn-filter** command).

- *group*—The group-policy name of the user.
- *user*—The username.
- *ip*—The public (not assigned) IP address of the user.
- *acl*—The name of the invalid ACL.

Recommended Action Validate the vpn-filter and ipv6-vpn-filter configuration on the ASA and the filter parameters on the AAA (RADIUS) server. Ensure that the correct type of ACL is specified.

722041

Error Message `%ASA-4-722041: TunnelGroup tunnel_group GroupPolicy group_policy User username IP peer_address No IPv6 address available for SVC connection\n.`

Explanation An IPv6 address was not available for assignment to the remote SVC client.

- *n*—The SVC connection identifier.

Recommended Action Augment or create an IPv6 address pool, if needed.

722053

Error Message `%ASA-6-722053: Group g User u IP ip Unknown client user-agent connection.`

Explanation An unknown or unsupported SSL VPN client has connected to the security appliance. Older clients include the Cisco SSL VPN client (SVC) and the Cisco AnyConnect client earlier than Version 2.3.1.

- *g*—The group policy under which the user logged in
- *u*—The name of the user
- *ip*—The IP address of the client
- *user-agent*—The user agent (usually includes the version) received from the client

Recommended Action Upgrade to a supported Cisco SSL VPN client.

723001

Error Message `%ASA-6-723001: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is up.`

Explanation The Citrix connection is up.

- *group-name*—The name of the Citrix group.
- *user-name*—The name of the Citrix user.
- *IP_address*—The IP address of the Citrix user.
- *connection*—The Citrix connection identifier.

Recommended Action None required.

723002

Error Message `%ASA-6-723002: Group group-name, User user-name, IP IP_address: WebVPN Citrix ICA connection connection is down.`

Explanation The Citrix connection is down.

- *group-name*—The name of the Citrix group.
- *user-name*—The name of the Citrix user.
- *IP_address*—The IP address of the Citrix user.
- *connection*—The Citrix connection identifier.

Recommended Action None required when the Citrix ICA connection is terminated intentionally by the client, the server, or the security appliance administrator. However, if this is not the case, verify that the WebVPN session in which the Citrix ICA connection is set up is still active. If it is inactive, then receiving this message is normal. If the WebVPN session is still active, verify that the ICA client and Citrix server both work correctly and that there is no error displayed. If not, bring either or both up or respond to any error. If this message is still received, contact the Cisco TAC and provide the following information:

- Network topology.
- Delay and packet loss.
- Citrix server configuration.
- Citrix ICA client information.
- Steps to reproduce the problem.
- Complete text of all associated messages.

723003

Error Message `%ASA-7-723003: No memory for WebVPN Citrix ICA connection connection.`

Explanation The security appliance is running out of memory. The Citrix connection was rejected.

- *connection*—The Citrix connection identifier.

Recommended Action Verify that the security appliance is working correctly. Pay special attention to memory and buffer usage. If the security appliance is under heavy load, buy more memory, and upgrade the security appliance or reduce the load on the security appliance. If the problem persists, contact the Cisco TAC.

723004

Error Message `%ASA-7-723004: WebVPN Citrix encountered bad flow control flow.`

Explanation An ASA internal flow control mismatch has occurred.

Recommended Action This issue can be caused by massive data flow, such as might occur during stress testing or with a high volume of ICA connections. Reduce ICA connectivity to the security appliance. If the problem persists, contact the Cisco TAC.

723005

Error Message `%ASA-7-723005: No channel to set up WebVPN Citrix ICA connection.`

Explanation The security appliance was unable to create a new channel for Citrix.

Recommended Action Verify that the Citrix ICA client and the Citrix server are still alive. If not, bring them back up and retest. Check the security appliance load, paying special attention to memory and buffer usage. If the security appliance is under heavy load, upgrade the security appliance, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

723006

Error Message `%ASA-7-723006: WebVPN Citrix SOCKS errors.`

Explanation An internal Citrix SOCKS error has occurred on the security appliance.

Recommended Action Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the Citrix ICA client and the security appliance, paying attention to packet loss and so forth. Resolve any abnormal network conditions. If the problem persists, contact the Cisco TAC.

723007

Error Message `%ASA-7-723007: WebVPN Citrix ICA connection connection list is broken.`

Explanation The ASA internal Citrix connection list is broken.

- *connection*—The Citrix connection identifier.

Recommended Action Verify that the security appliance is working correctly, paying special attention to memory and buffer usage. If the security appliance is under heavy load, upgrade the security appliance, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

723008

Error Message `%ASA-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.`

Explanation An attempt was made to access a Citrix Socks server that does not exist.

- *server*—The Citrix server identifier.

Recommended Action Verify that the security appliance is working correctly. Notice if there is any memory/buffer leakage. If this issue happens frequently, capture information about memory usage, the network topology, and the conditions when this message is received. Send this information to Cisco TAC for review. Make sure the WebVPN session is still up while this message is being received. If not, determine the reason that the WebVPN session is down. If the security appliance is under heavy load, upgrade the security appliance, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

723009

Error Message `%ASA-7-723009: Group group-name, User user-name, IP IP_address: WebVPN Citrix received data on invalid connection connection.`

Explanation Data was received on a Citrix connection that does not exist.

- *group-name*—The name of the Citrix group.
- *user-name*—The name of the Citrix user.
- *IP_address*—The IP address of the Citrix user.
- *connection*—The Citrix connection identifier.

Recommended Action The original published Citrix application connection was probably terminated, and the remaining active published applications lost connectivity. Restart all published applications to generate a new Citrix ICA tunnel. If the security appliance is under heavy load, upgrade the security appliance, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

723010

Error Message `%ASA-7-723010: Group group-name, User user-name, IP IP_address: WebVPN Citrix received closing channel channel for invalid connection connection.`

Explanation An abort was received on a Citrix connection that does not exist.

- *group-name*—The name of the Citrix group.
- *user-name*—The name of the Citrix user.
- *IP_address*—The IP address of the Citrix user.
- *channel*—The Citrix channel identifier.

- *connection*—The Citrix connection identifier.

Recommended Action This can be caused by massive data flow (such as stress testing) or a high volume of ICA connections, especially during network delay or packet loss. To eliminate the message, reduce the number of ICA connections to the security appliance, obtain more memory for the security appliance, or resolve the network problems.

723011

Error Message `%ASA-7-723011: Group group-name, User user-name, IP IP_address: WebVPN Citrix receives bad SOCKS socks message length msg-length. Expected length is exp-msg-length.`

Explanation The Citrix SOCKS message length is incorrect.

- *group-name*—The name of the Citrix group.
- *user-name*—The name of the Citrix user.
- *IP_address*—The IP address of the Citrix user.

Recommended Action Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the ICA client and the security appliance, paying attention to packet loss and so forth. After resolving any abnormal network conditions, if the problem still exists, contact the Cisco TAC.

723012

Error Message `%ASA-7-723012: Group group-name, User user-name, IP IP_address: WebVPN Citrix received bad SOCKS socks message format.`

Explanation Citrix SOCKS message format is incorrect.

- *group-name*—The name of the Citrix group.
- *user-name*—The name of the Citrix user.
- *IP_address*—The IP address of the Citrix user.
- *socks*—The SOCKS message.

Recommended Action Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the ICA client and the security appliance, paying attention to packet loss and so forth. After resolving any abnormal network conditions, if the problem persists, contact the Cisco TAC.

723013

Error Message `%ASA-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.`

Explanation The ASA internal Citrix timer has expired and the Citrix connection is invalid.

- *connection*—The Citrix connection identifier.

Recommended Action Check the network connection between the Citrix ICA client and the security appliance, and between the security appliance and the Citrix server. Resolve any abnormal network conditions, especially delay and packet loss. Verify that the security appliance works correctly, paying special attention to memory or buffer problems. If the security appliance is under heavy load, obtain more memory, upgrade the security appliance, or reduce the load. If the problem persists, contact the Cisco TAC.

723014

Error Message `%ASA-7-723014: Group group-name, User user-name, IP IP_address: WebVPN Citrix TCP connection connection to server server on channel channel initiated.`

Explanation The security appliance internal Citrix Secure Gateway is connected to the Citrix server.

- *group-name*—The name of the Citrix group.
- *user-name*—The name of the Citrix user.
- *IP_address*—The IP address of the Citrix user.
- *connection*—The connection name.
- server—The Citrix server identifier.
- channel—The Citrix channel identifier (hexadecimal).

Recommended Action None required.

724001

Error Message `%ASA-4-724001: Group group-name User user-name IP IP_address WebVPN session not allowed. Unable to determine if Cisco Secure Desktop was running on the client's workstation.`

Explanation The session was not allowed as an error occurred when processing the CSD Host Integrity Check results on the security appliance.

- *group-name*—The name of the group.
- *user-name*—The name of the user.
- *IP_address*—The IP address.

Recommended Action Determine whether the client firewall is truncating long URLs. Uninstall CSD from the client and reconnect to the security appliance.

724002

Error Message `%ASA-4-724002: Group group-name User user-name IP IP_address WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.`

Explanation CSD is not running on the client machine.

- *group-name*—The name of the group.
- *user-name*—The name of the user.
- *IP_address*—The IP address.

Recommended Action Verify that the end user is able to correctly install and run CSD on the client machine.

725001

Error Message `%ASA-6-725001 Starting SSL handshake with remote_device interface_name:IP_address/port for SSL_version session.`

Explanation This message indicates that a SSL handshake has started with the remote device.

- *remote_device*—Either the server or the client, depending on the device that initiated the connection.
- *interface_name*—The interface that the SSL session is using.
- *IP_address*—The remote device IP address.
- *port*—The remote device IP port number.
- *SSL_version*—The SSL version for the SSL handshake (SSLv3 or TLSv1).

Recommended Action None required.

725002

Error Message `%ASA-6-725002 Device completed SSL handshake with remote_device interface_name:IP_address/port`

Explanation The SSL handshake has completed successfully with the remote device.

- *remote_device*—Either the server or the client, depending on the device that initiated the connection.
- *interface_name*—The interface that the SSL session is using.
- *IP_address*—The remote device IP address.
- *port*—The remote device IP port number.

Recommended Action None required.

725003

Error Message `%ASA-6-725003 SSL client interface_name:IP_address/port requesting to resume previous session.`

Explanation The remote device is trying to resume a previous SSL session.

- *interface_name*—The interface that the SSL session is using.
- *IP_address*—The remote device IP address.
- *port*—The remote device IP port number.

Recommended Action None required.

725004

Error Message `%ASA-6-725004 Device requesting certificate from SSL client interface_name:IP_address/port for authentication.`

Explanation The security appliance has requested a client certificate for authentication.

- *interface_name*—The interface that the SSL session is using.
- *IP_address*—The remote device IP address.
- *port*—The remote device IP port number.

Recommended Action None required.

725005

Error Message `%ASA-6-725005 SSL server interface_name:IP_address/port requesting our device certificate for authentication.`

Explanation The server has requested the certificate of the security appliance for authentication.

- *interface_name*—The interface that the SSL session is using.
- *IP_address*—The remote device IP address.
- *port*—The remote device IP port number.

Recommended Action None required.

725006

Error Message `%ASA-6-725006 Device failed SSL handshake with` *`remote_device interface_name:IP_address/port`*

Explanation The SSL handshake with the remote device has failed.

- *remote_device*—Either the server or the client, depending on the device that initiates the connection.
- *interface_name*—The interface that the SSL session is using.
- *IP_address*—The remote device IP address.
- *port*—The remote device IP port number.

Recommended Action Look for syslog message 725014, which indicates the reason for the failure.

725007

Error Message `%ASA-6-725007 SSL session with` *`remote_device interface_name:IP_address/port`* `terminated.`

Explanation The SSL session has terminated.

- *remote_device*—Either the server or the client, depending on the device that initiates the connection.
- *interface_name*—The interface that the SSL session is using.
- *IP_address*—The remote device IP address.
- *port*—The remote device IP port number.

Recommended Action None required.

725008

Error Message `%ASA-7-725008 SSL client` *`interface_name:IP_address/port`* `proposes the following` *`number`* `cipher(s).`

Explanation Lists the number of ciphers proposed by the remote SSL device.

- *interface_name*—The interface that the SSL session is using.
- *IP_address*—The remote device IP address.
- *port*—The remote device IP port number.
- *number*—The number of ciphers in the proposal.

Recommended Action None required.

725009

Error Message `%ASA-7-725009 Device proposes the following number cipher(s) to SSL server interface_name:IP_address/port.`

Explanation This message lists the number of ciphers proposed to the SSL server.

- *number*—The number of ciphers in the proposal.
- *interface_name*—The interface that the SSL session is using.
- *IP_address*—The remote device IP address.
- *port*—The remote device IP port number.

Recommended Action None required.

725010

Error Message `%ASA-7-725010 Device supports the following number cipher(s).`

Explanation This message identifies the number of ciphers supported by the security appliance for a SSL session.

- *number*—The number of supported ciphers.

Recommended Action None required.

725011

Error Message `%ASA-7-725011 Cipher[order]: cipher_name`

Explanation This message indicates the cipher name and its order of preference, and always follows system log messages 725008, 725009, and 725010.

- *order*—The order of the cipher in the cipher list.
- *cipher_name*—The name of the cipher from the cipher list.

725012

Error Message `%ASA-7-725012 Device chooses cipher: cipher_name for SSL session with client interface_name:IP_address/port`

Explanation This message identifies the cipher that was chosen by the Cisco device for the SSL session.

- *cipher_name*—The name of the cipher from the cipher list.
- *interface_name*—The interface that the SSL session is using.

- *IP_address*—The remote device IP address.
- *port*—The remote device IP port number.

Recommended Action None required.

725013

Error Message `%ASA-7-725013 SSL Server interface_name:IP_address/port chooses cipher: cipher_name`

Explanation This message identifies the cipher that was chosen by the server for the SSL session.

- *cipher_name*—The name of the cipher from the cipher list.
- *interface_name*—The interface that the SSL session is using.
- *IP_address*—The remote device IP address.
- *port*—The remote device IP port number.

Recommended Action None required.

725014

Error Message `%ASA-7-725014 SSL lib error. Function: function Reason: reason`

Explanation This message identifies the reason for failure of the SSL handshake.

- *function*—The function name where the failure is reported.
- *reason*—The description of the failure condition.

Recommended Action Include this message when reporting any SSL-related issue.

725015

Error Message `%ASA-3-725015 Error verifying client certificate. Public key size in client certificate exceeds the maximum supported key size.`

Explanation Notice that the verification of a SSL client certificate failed due to an unsupported (large) key size.

Recommended Action Use client certificates with key sizes less than or equal to 4096 bits.

726001

Error Message `%ASA-6-726001: Inspected im_protocol im_service Session between Client im_client_1 and im_client_2 Packet flow from src_ifc:/sip/sport to dest_ifc:/dip/dport Action: action Matched Class class_map_id class_map_name`

Explanation This message is generated when an inspection is performed on an IM message and the specified criteria are satisfied. The configured action is taken.

- *im_protocol*—MSN IM or Yahoo IM.
- *im_service*—The IM services, such as: chat, conference, file transfer, voice, video, games, or unknown.
- *im_client_1*, *im_client_2*—The client peers that are using the IM service in the session: *client_login_name* or "?".
- *src_ifc*—The source interface name.
- *sip*—The source IP address.
- *sport*—The source port.
- *dest_ifc*—The destination interface name.
- *dip*—The destination IP address.
- *dport*—The destination port.
- *action*—The action taken: reset connection, dropped connection, or received.
- *class_map_id*—The matched class-map ID.
- *class_map_name*—The matched class-map name.

Recommended Action None required.

730001

Error Message `%ASA-7-730001 Group groupname, User username, IP ipaddr: VLAN MAPPING to VLAN vlanid`

Explanation VLAN mapping succeeded.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.
- *vlanid*— The VLAN ID that is used for the VLAN mapping session.

Recommended Action None required.

730002

Error Message `%ASA-7-730002 Group groupname, User username, IP ipaddr: VLAN MAPPING to VLAN vlanid failed`

Explanation VLAN mapping failed.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.
- *vlanid*— The VLAN ID that is used for the VLAN mapping session.

Recommended Action Verify that all the VLAN mapping related configurations are correct, and that the VLAN ID is valid.

730003

Error Message `%ASA-7-730003 NACApp sets IP ipaddr VLAN to vlanid`

Explanation The security appliance receives a SNMP set message from NACApp to set the new VLAN ID for the session.

- *ipaddr*—The IP address of this session.
- *vlanid*— The VLAN ID that is used for the VLAN mapping session.

Recommended Action None required.

730004

Error Message `%ASA-6-730004 Group groupname User username IP ipaddr VLAN ID vlanid from AAA ignored.`

Explanation The VLAN ID received from AAA is different from the current one in use and it is ignored for the current session.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.
- *vlanid*— The VLAN ID that is used for the VLAN mapping session.

Recommended Action If the newly received VLAN ID must be used, then the current session needs to be torn down. Otherwise, none required.

730005

Error Message `%ASA-6-730005 Group groupname User username IP ipaddr VLAN ID vlanid from AAA is invalid.`

Explanation The VLAN ID received from AAA is invalid.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.
- *vlanid*— The VLAN ID that is used for the VLAN mapping session.

Recommended Action Verify the VLAN ID configurations on the AAA server and the security appliance are both correct.

730006

Error Message `%ASA-7-730006 Group groupname, User username, IP ipaddr: is on NACApp AUTH VLAN vlanid.`

Explanation The session is under NACApp posture assessment.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.
- *vlanid*— The VLAN ID that is used for the VLAN mapping session.

Recommended Action None required.

730007

Error Message `%ASA-7-730007 Group groupname, User username, IP ipaddr: changed VLAN to %s ID vlanid`

Explanation NACApp (Cisco NAC appliance) posture assessment is done with the session, and the VLAN is changed from AUTH VLAN to a new VLAN.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.
- `%s`—A string.
- *vlanid*— The VLAN ID that is used for the VLAN mapping session.

Recommended Action None required.

730008

Error Message `%ASA-6-730008 Group groupname, User username, IP ipaddr, VLAN MAPPING timeout waiting NACApp.`

Explanation NACApp (Cisco NAC appliance) posture assessment takes longer than the timeout value configured.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.

Recommended Action Check the status of the NACApp setup.

730009

Error Message `%ASA-5-730009 Group groupname, User username, IP ipaddr, CAS casaddr, capacity exceeded, terminating connection.`

Explanation The load capacity of the NACApp (Cisco NAC appliance) CAS is exceeded, and the new incoming session that uses it is terminating.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.
- *casaddr*—The IP address of CAS (Clean Access Server).

Recommended Action Review and revise planning for how many groups, and which groups, are associated with the CAS to ensure that its load capacity is not exceeded.

730010

Error Message `%ASA-7-730010 Group groupname, User username, IP ipaddr, VLAN Mapping is enabled on VLAN vlanid.`

Explanation VLAN mapping is enabled on the session.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.
- *vlanid*— The VLAN ID that is used for the VLAN mapping session.

Recommended Action None required.

731001

Error Message `%ASA-6-731001 NAC policy added: name: policyname Type: policytype.`

Explanation A new NAC policy is added on the security appliance.

- *policyname*—The NAC policy name.
- *policytype*—The type of NAC policy.

Recommended Action None required.

731002

Error Message `%ASA-6-731002 NAC policy deleted: name: policyname Type: policytype.`

Explanation A NAC policy is removed from the security appliance.

- *policyname*—The NAC policy name.
- *policytype*—The type of NAC policy.

Recommended Action None required.

731003

Error Message `%ASA-6-731003 nac-policy unused: name: policyname Type: policytype.`

Explanation The NAC policy is unused because there is an existing NAC policy with the same name, but a different type.

- *policyname*—The NAC policy name.
- *policytype*—The type of NAC policy.

Recommended Action If the new NAC policy must be used, the existing NAC policy must be removed first. Otherwise, none required.

732001

Error Message `%ASA-6-732001 Group groupname, User username, IP ipaddr, Fail to parse NAC-SETTINGS nac-settings-id, terminating connection.`

Explanation The security appliance cannot apply the NAC settings because of insufficient memory.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.

- *nac-settings-id*— The ID that is used for the NAC filter.

Recommended Action Upgrade the security appliance memory. Resolve any errors in the log before this problem occurs. If the problem persists, contact the Cisco TAC.

732002

Error Message `%ASA-6-732002 Group groupname, User username, IP ipaddr, NAC-SETTINGS settingsid from AAA ignored, existing NAC-SETTINGS settingsid_inuse used instead.`

Explanation The NAC settings cannot be applied because there is a different ID for the session.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.
- *settingsid*— The settings ID, which should be a NAC policy name.
- *settingsid_inuse*— The NAC settings ID that is currently in use.

Recommended Action If the new NAC settings must be applied, then all the active sessions that use it must be torn down first. Otherwise, none required.

732003

Error Message `%ASA-6-732003 Group groupname, User username, IP ipaddr, NAC-SETTINGS nac-settings-id from AAA is invalid, terminating connection.`

Explanation The NAC settings received from AAA are invalid.

- *groupname*—The group name.
- *username*—The username.
- *ipaddr*—The IP address of this session.
- *nac-settings-id*—The ID that is used for the NAC filter.

Recommended Action Verify that the NAC settings configurations on the AAA server and the security appliance are both correct.

733100

Error Message `%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt`

Explanation The specified object in the syslog message has exceeded the specified burst threshold rate or average threshold rate. The object can be the drop activity of a host, TCP/UDP port, IP protocol, or various drops caused by potential attacks. This message indicates the system is under potential attack.

- *Object*—The general or particular source of a drop rate count, which might include the following:

  - Firewall

  - Bad pkts

  - Rate limit

  - DoS attck

  - ACL drop

  - Conn limit

  - ICMP attk

  - Scanning

  - SYN attck

  - Inspect

  - Interface

  (A citation of a particular interface object might take a number of forms. For example, you might see "*80/HTTP*" that would signify port 80, using the Hypertext Transfer Protocol.)

- *rate_ID*—The configured rate that is being exceeded. Most objects can be configured with up to three different rates for different intervals.
- *rate_val*—A particular rate value.
- *total_cnt*—The total count since the object was created or cleared.

The following two examples depict how these variables occur:

For an interface drop because of a CPU or bus limitation:

```
%ASA-4-730100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per
second, max configured rate is 8000; Current average rate is 2030 per second, max
configured rate is 2000; Cumulative total count is 3930654.
```

For bad packets caused by potential attacks:

```
%ASA-4-730100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per
second, max configured rate is 400; Current average rate is 760 per second, max
configured rate is 100; Cumulative total count is 1938933
```

Recommended Action If the object in the syslog message is one of the following:

- Firewall
- Bad pkts

- Rate limit
- DoS attck
- ACL drop
- Conn limit
- ICMP attk
- Scanning
- SYN attck
- Inspect
- Interface

Check whether the drop rate is acceptable for the running environment. Adjust the threshold rate of the particular drop, via the **threat-detection rate** *xxx* command, to an appropriate value, where *xxx* is one of the following:

- acl-drop
- bad-packet-drop
- conn-limit-drop
- dos-drop
- fw-drop
- icmp-drop
- inspect-drop
- interface-drop
- scanning-threat
- syn-attack

Otherwise, if the object in the syslog message is a TCP/UDP port, an IP protocol, or a host drop, check whether the drop rate is acceptable for the running environment, and adjust the threshold rate of the particular drop via the **threat-detection rate bad-packet-drop** command to an appropriate value. If this drop rate exceed warning is not desirable, you can disable it by using the **no threat-detection basic-threat** command.

733101

Error Message `%ASA-4-733101: Object objectIP (is targeted|is attacking). Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt.`

Explanation Scanning has been detected. This syslog message is sent when the system detects that a specific host (or several hosts in the same 1024-node subnet) either is scanning the network (attacking), or is being scanned (targeted).

- *object*—Attacker or target. This may be a specific host.or several hosts in the same 1024-node subnet).
- *objectIP*—The IP address of the scanning attacker or scanned target.

- *rate_val*—A particular rate value.
- *total_cnt*—The total count.

The following two examples show how these variables occur:

```
%ASA-4-733101: Subnet 100.0.0.0 is targeted. Current burst rate is 200 per second, max
configured rate is 0; Current average rate is 0 per second, max configured rate is 0;
Cumulative total count is 2028.

%ASA-4-733101: Host 175.0.0.1 is attacking. Current burst rate is 200 per second, max
configured rate is 0; Current average rate is 0 per second, max configured rate is 0;
Cumulative total count is 2024
```

Recommended Action For the specific host or subnet, issue the **show threat-detection statistics host ip-address ip-mask** command to check the overall situation and then adjust the threshold rate of *scanning-threat* to appropriate value. After the appropriate value is determined, an optional action can be taken to shun those host attackers (not the subnet attacker) by configuring the **threat-detection scanning-threat shun-host** command. You may specify certain hosts or object groups in the *shun-host except* list. See the *Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide* for details. If scanning detection is not desirable, you can disable this feature by using the **no threat-detection scanning** command.

733102

Error Message `%ASA-4-733102:Threat-detection adds host %I to shun list`

Explanation This message indicates that a host has been shunned by the threat detection engine. When the **threat-detection scanning-threat shun** command is configured, the attacking hosts will be shunned by the threat detection engine.

- *%I*—A particular hostname.

The following example shows how to implement this message:

```
%ASA-4-733102: Threat-detection add host 11.1.1.40 to shun list
```

Recommended Action To investigate whether the shunned host is an actual attacker, enter the **threat-detection statistics host ip-address** command. If the shunned host is not an attacker, you can remove the shunned host from the threat detection engine by entering the **clear threat-detection shun ip address** command. To remove all shunned hosts from the threat detection engine, enter the **clear shun** command.

If you receive this syslog message because an inappropriate threshold rate has been set to trigger the threat detection engine, then adjust the threshold rate by entering the **threat-detection rate scanning-threat rate-interval x average-rate y burst-rate z** command.

733103

Error Message `%ASA-4-733103: Threat-detection removes host %I from shun list`

Explanation This message indicates that a host has been shunned by the threat detection engine. When you enter the **clear-threat-detection shun** command, the specified host will be removed from the shunned list.

- *%I*—A particular hostname.

The following example shows how to implement this message:

```
%ASA-4-733103: Threat-detection removes host 11.1.1.40 from shun list
```

Recommended Action None required.

733104

Error Message `%ASA-4-733104: TD_SYSLOG_TCP_INTERCEPT_AVERAGE_RATE_EXCEED`

Explanation This message is generated when the system is under Syn flood attacks and protected by TCP Intercept mechanism, if the average rate for attacks intercepted exceeds the configured threshold.

Recommended Action None required (The syslog is showing which server is under attacks and where the attacks are coming from. User can further write an ACL to filter out the attacks).

733105

Error Message `%ASA-4-733105: TD_SYSLOG_TCP_INTERCEPT_BURST_RATE_EXCEED`

Explanation This message is generated when the system is under Syn flood attacks and protected by TCP Intercept mechanism, if the burst rate for attacks intercepted exceeds the configured threshold.

Recommended Action None required (The syslog is showing which server is under attacks and where the attacks are coming from. User can further write an ACL to filter out the attacks).

734001

Error Message `%ASA-6-734001: DAP: User user, Addr ipaddr, Connection connection: The following DAP records were selected for this connection: DAP record names`

Explanation Displays the DAP records that were selected for the connection.

- *user*—The authenticated username.
- *ipaddr*—The IP address of the remote client.

- *connection*—The type of client connection, which can be one of the following:
  - IPsec
  - AnyConnect
  - Clientless (web browser)
  - Cut-Through-Proxy
  - L2TP
- *DAP record names*—The comma-separated list of the DAP record names.

Recommended Action None required.

734002

Error Message `%ASA-5-734002: DAP: User user, Addr ipaddr: Connection terminated by the following DAP records: DAP record names`

Explanation Displays the DAP records that terminated the connection.

- *user*—The authenticated username.
- *ipaddr*—The IP address of the remote client.
- *DAP record names*—The comma-separated list of the DAP record names.

Recommended Action None required.

734003

Error Message `%ASA-7-734003: DAP: User name, Addr ipaddr: Session Attribute: attr name/value`

Explanation Displays the AAA and endpoint session attributes that are associated with the connection.

- *user*—The authenticated username.
- *ipaddr*—The IP address of the remote client.
- *attr/value*—The AAA or endpoint attribute name and value.

Recommended Action None required.

734004

Error Message `%ASA-3-734004: DAP: Processing error: Code number`

Explanation Displays a DAP processing error.

- *number*—The internal error code.

Recommended Action Provide Cisco TAC with the syslog message and information about the conditions that generated this error.

735001

Error Message `%ASA-1-735001 IPMI: Cooling Fan var1: OK`

Explanation A cooling fan has been restored to normal operation.

- *var1*—The device number markings.

Recommended Action None required.

735002

Error Message `%ASA-1-735002 IPMI: Cooling Fan var1: Failure Detected`

Explanation A cooling fan has failed.

- *var1*—The device number markings.

Recommended Action Perform the following steps:

1. Check for obstructions that would prevent the fan from rotating.
2. Replace the cooling fan.
3. If the problem persists, record the message as it appears and contact Cisco TAC.

735003

Error Message `%ASA-1-735003 IPMI: Power Supply var1: OK`

Explanation A power supply has been restored to normal operation.

- *var1*—The device number markings.

Recommended Action None required.

735004

Error Message `%ASA-1-735004 IPMI: Power Supply var1: Failure Detected`

Explanation AC power has been lost or the power supply has failed.

- *var1*—The device number markings.

Recommended Action Perform the following steps:

1. Check for AC power failure.
2. Replace the power supply.
3. If the problem persists, record the message as it appears and contact Cisco TAC.

735005

Error Message `%ASA-1-735005 IPMI: Power Supply Unit Redundancy OK`

Explanation Power supply unit redundancy has been restored.

Recommended Action None required.

735006

Error Message `%ASA-1-735006 IPMI: Power Supply Unit Redundancy Lost`

Explanation This message is accompanied by a power supply failure. Power supply unit redundancy has been lost, but the system is functioning normally with minimum resources. Any further failures will result in a system shutdown.

Recommended Action To regain full redundancy, perform the following steps:

1. Check for AC power failure.
2. Replace the power supply.
3. If the problem persists, record the message as it appears and contact Cisco TAC.

735007

Error Message `%ASA-1-735007 IPMI: CPU var1: Temp: var2 var3, Critical`

Explanation The CPU has reached a critical temperature.

- *var1*—The device number markings.
- *var2*—The temperature value.

- *var3*—Temperature value units (C, F).

Recommended Action Record the message as it appears and contact Cisco TAC.

735008

Error Message `%ASA-1-735008 IPMI: Chassis Ambient var1: Temp: var2 var3, Critical`

Explanation A chassis ambient temperature sensor has reached a critical level.

- *var1*—The device number markings.
- *var2*—The temperature value.
- *var3*—Temperature value units (C, F).

Recommended Action Record the message as it appears and contact Cisco TAC.

735009

Error Message `%ASA-2-735009: IPMI: Environment Monitoring has failed initialization and configuration. Environment Monitoring is not running.`

Explanation Environment Monitoring has experienced a fatal error during initialization and was unable to continue.

Recommended Action Collect the output of the **show environment** and **debug ipmi** commands. Record the message as it appears and contact Cisco TAC.

735010

Error Message `%ASA-3-735010: IPMI: Environment Monitoring has failed to update one or more of its records.`

Explanation Environment Monitoring has experienced an error that temporarily prevented it from updating one or more of its records.

Recommended Action If this message appears repeatedly, collect the output from the **show environment driver** and **debug ipmi** commands. Record the message as it appears and contact Cisco TAC.

736001

Error Message `%ASA-2-736001: Unable to allocate enough memory at boot for jumbo-frame reservation. Jumbo-frame support has been disabled.`

Explanation Insufficient memory has been detected when jumbo-frame support was being configured. As a result, jumbo-frame support was disabled.

Recommended Action Try reenabling jumbo-frame support with the **jumbo-frame reservation** command. Save the running configuration and reboot the device. If the problem persists, contact Cisco TAC.

737001

Error Message `%ASA-7-737001: IPAA: Received message 'message-type'`

Explanation A message has been received by the IP address assignment process.

- *message-type*—The message received by the IP address assignment process.

Recommended Action None required.

737002

Error Message `%ASA-3-737002: IPAA: Received unknown message 'num' variables`

Explanation A message has been received by the IP address assignment process.

- *num*—The identifier of the message received by the IP address assignment process.

Recommended Action None required.

737003

Error Message `%ASA-5-737003: IPAA: DHCP configured, no viable servers found for tunnel-group 'tunnel-group'`

Explanation The DHCP server configuration for the given tunnel-group is not valid.

- *tunnel-group*—The tunnel-group that IP address assignment is using for configuration.

Recommended Action Validate the DHCP configuration for the tunnel-group. Make sure that the DHCP server is online.

737004

Error Message `%ASA-5-737004: IPAA: DHCP configured, request failed for tunnel-group 'tunnel-group'`

Explanation The DHCP server configuration for the given tunnel-group is not valid.

- *tunnel-group*—The tunnel-group that IP address assignment is using for configuration.

Recommended Action Validate the DHCP configuration for the tunnel-group. Make sure that the DHCP server is online.

737005

Error Message `%ASA-6-737005: IPAA: DHCP configured, request succeeded for tunnel-group 'tunnel-group'`

Explanation The DHCP server request has succeeded.

- *tunnel-group*—The tunnel-group that IP address assignment is using for configuration.

Recommended Action None required.

737006

Error Message `%ASA-6-737006: IPAA: Local pool request succeeded for tunnel-group 'tunnel-group'`

Explanation The local pool request has succeeded.

- *tunnel-group*—The tunnel group that IP address assignment is using for configuration.

Recommended Action None required.

737007

Error Message `%ASA-5-737007: IPAA: Local pool request failed for tunnel-group 'tunnel-group'`

Explanation The local pool request has failed. The pool(s) assigned to the tunnel-group may be exhausted.

- *tunnel-group*—The tunnel-group that IP address assignment is using for configuration.

Recommended Action Validate the IP local pool configuration by using the **show ip local pool** command.

737008

Error Message `%ASA-5-737008: IPAA: 'tunnel-group' not found`

Explanation The tunnel-group was not found when trying to acquire an IP address for configuration.

- *tunnel-group*—The tunnel-group that IP address assignment is using for configuration.

Recommended Action Check the tunnel-group configuration. A software defect could cause this message to be generated. Contact the Cisco TAC and report the issue.

737009

Error Message `%ASA-6-737009: IPAA: Client requested address ip-address, request failed`

Explanation The remote-access client software requested the use of a particular address. The request to the AAA server to use this address failed. The address may be in use.

- *ip-address*—The IP address that the client requested.

Recommended Action Check the AAA server status and the status of IP local pools.

737010

Error Message `%ASA-6-737010: IPAA: Client requested address ip-address, request succeeded`

Explanation The remote-access client software requested the use of a particular address and successfully received this address .

- *ip-address*—The IP address that the client requested.

Recommended Action None required.

737011

Error Message `%ASA-5-737011: IPAA: requested address ip-address, not permitted by AAA, retrying`

Explanation The remote-access client software requested the use of a particular address. The **vpn-addr-assign aaa** command is not configured. An alternatively configured address assignment method will be used.

- *ip-address*—The IP address that the client requested.

Recommended Action If you want to permit clients to specify their own address, enable the **vpn-addr-assign aaa** command.

737012

Error Message `%ASA-4-737012: IPAA: Address assignment failed`

- *ip-address*—The IP address that the client requested.

Recommended Action If using IP local pools, validate the local pool configuration. If using AAA, validate the configuration and status of the AAA server. If using DHCP, validate the configuration and status of the DHCP server. Increase the logging level (use notification or informational) to obtain additional syslog messages to identify the issue.

737013

Error Message `%ASA-4-737013: IPAA: Error freeing address ip-address, not found`

Explanation The ASA attempted to free an address, but it was not on the allocated list. It could be the result of a recent configuration change.

- *ip-address*—The IP address to be released.

Recommended Action Validate your address assignment configuration. If this continues, it could be due to a software defect. Contact the TAC and report the issue..

737014

Error Message `%ASA-6-737014: IPAA: Freeing AAA address ip-address`

Explanation The ASA successfully released the IP address assigned via AAA.

- *ip-address*—The IP address to be released.

Recommended Action None required.

737015

Error Message `%ASA-6-737015: IPAA: Freeing DHCP address ip-address`

Explanation The ASA successfully released the IP address assigned via DHCP.

- *ip-address*—The IP address to be released.

Recommended Action None required.

737016

Error Message `%ASA-6-737016: IPAA: Freeing local pool address ip-address`

Explanation The ASA successfully released the IP address assigned via local pools.

- *ip-address*—The IP address to be released.

Recommended Action None required.

737017

Error Message `%ASA-6-737017: IPAA: DHCP request attempt num succeeded`

Explanation The ASA successfully sent a request to a DHCP server.

- *num*—The attempt number.

Recommended Action None required.

737018

Error Message `%ASA-5-737018: IPAA: DHCP request attempt num failed`

Explanation The ASA failed to send a request to a DHCP server.

- *num*—The attempt number.

Recommended Action Validate the DHCP configuration and connectivity to the DHCP server..

737019

Error Message `%ASA-4-737019: IPAA: Unable to get address from group-policy or tunnel-group local pools`

Explanation The ASA failed to acquire an address from the local pools configured on the group-policy or tunnel-group. The local pools may be exhausted.

Recommended Action Validate the local pool configuration and status. Validate the group-policy and tunnel-group configuration of local pools.

737023

Error Message `%ASA-5-737023: IPAA: Unable to allocate memory to store local pool address ip-address`

Explanation The ASA is low on memory.

- *ip-address*—The IP address that was acquired.

Recommended Action The ASA may be overloaded and need more memory, or there may be a memory leakcaused by a software defect. Contact the Cisco TAC and report the issue.

737024

Error Message `%ASA-5-737024: IPAA: Client requested address ip-address, already in use, retrying`

Explanation The client requested an IP address that is already in use. The request will be attempted using a new IP address.

- *ip-address*—The IP address that the client requested.

Recommended Action None required.

737025

Error Message `%ASA-5-737025: IPAA: Duplicate local pool address found, ip-address in quarantine`

Explanation The IP address that was to be given to the client is already in use. The IP address has been removed from the pool and will not be reused.

- *ip-address*—The IP address that was acquired.

Recommended Action Validate the local pool configuration; there may be an overlap caused by a software defect. Contact the Cisco TAC and report the issue.

737026

Error Message `%ASA-6-737026: IPAA: Client assigned ip-address from local pool`

Explanation The client has assigned the given address from a local pool.

- *ip-address*—The IP address that was assigned to the client.

Recommended Action None required.

737027

Error Message `%ASA-3-737027: IPAA: No data for address request`

Explanation A software defect has been encountered.

Recommended Action Contact the Cisco TAC and report the issue.

737028

Error Message `%ASA-4-737028: IPAA: Unable to send ip-address to standby: communication failure`

Explanation The active ASA was unable to communicate with the standby ASA. The failover pair may be out of sync.

- *ip-address*—The IP address that was assigned to the client.

Recommended Action Validate the failover configuration and status.

737029

Error Message `%ASA-6-737029: IPAA: Added ip-address to standby`

Explanation The standby ASA accepted the IP address assignment.

- *ip-address*—The IP address that was assigned to the client.

Recommended Action None required.

737030

Error Message `%ASA-4-737030: IPAA: Unable to send ip-address to standby: address in use`

Explanation The standby ASA has the given address already in use when the active ASA attempted to acquire it. The failover pair may be out of sync.

- *ip-address*—The IP address that was assigned to the client.

Recommended Action Validate the failover configuration and status.

737031

Error Message `%ASA-6-737031: IPAA: Removed ip-address from standby`

Explanation The standby ASA cleared the IP address assignment.

- *ip-address*—The IP address that was assigned to the client.

Recommended Action None required.

737032

Error Message `%ASA-4-737032: IPAA: Unable to remove ip-address from standby: address not found`

Explanation The standby ASA did not have in use when the active ASA attempted to release it. The failover pair may be out of sync.

- *ip-address*—The IP address that was assigned to the client.

Recommended Action Validate the failover configuration and status.

737033

Error Message `%ASA-4-737033: IPAA: Unable to assign addr_allocator provided IP address ip_addr to client. This IP address has already been assigned by previous_addr_allocator`

Explanation This syslog is generated when the address assigned by AAA/DHCP /Local pool is already in use.

- *addr_allocator*—The DHCP/AAA/Local Pool.
- *ip_addr*—The IP address allocated by the DHCP/AAA/Local Pool.
- *previous_ addr_allocator*—The address allocater that already assigned the ip address(Local Pool, AAA or DHCP).

Recommended Action Validate the AAA/DHCP/Local pool address configurations. Overlap may occur.