Syslog Messages 302003 to 342008

This chapter contains the following sections:

- Messages 302003 to 319004, on page 1
- Messages 320001 to 342008, on page 37

Messages 302003 to 319004

This chapter includes messages from 302003 to 319004.

302003

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

**Explanation** An H.245 connection has been started from the outside_address to the inside_address. The ASA has detected the use of an Intel Internet Phone. The foreign port (outside_port) only appears on connections from outside the ASA. The local port value (inside_port) only appears on connections that were 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** An H.323 UDP back connection has been preallocated to the foreign address (outside_address) from the local address (inside_address). The ASA has detected the use of an Intel Internet Phone. The foreign port (outside_port) only appears on connections from outside the ASA. The local port value (inside_port) only appears on connections that were started on an internal interface.

**Recommended Action** None required.

302010

**Error Message** %ASA-6-302010: connections in use, connections most used
Explanation Provides information on the number of connections that are in use and most used.
  
  • connections — 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) [idfw_user]} to interface
:real-address /real-port {mapped-address(mapped-port) [idfw_user]} [user]

Explanation A TCP connection slot between two hosts was created.
  
  • connection_id — A unique identifier
  • interface, real-address, real-port — The actual sockets
  • mapped-address, mapped-port — The mapped sockets
  • user — The AAA name of the user
  • idfw_user — The name of the identity firewall 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 [idfw_user]
to interface :real-address /real-port [idfw_user] duration hh:mm:ss bytes bytes [reason
[from teardown-initiator]] [(user)]

Explanation A TCP connection between two hosts was deleted. The following list describes the message values:
  
  • id — A unique identifier
  • interface, real-address, real-port — The actual socket
  • duration — The lifetime of the connection
  • bytes — The data transfer of the connection
  • user — The AAA name of the user
  • idfw_user — The name of the identity firewall user
• **reason**—The action that causes the connection to terminate. Set the **reason** variable to one of the TCP termination reasons listed in the following table.

• **teardown-initiator**—Interface name of the side that initiated the teardown.

**Table 1: TCP Termination Reasons**

<table>
<thead>
<tr>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conn-timeout</td>
<td>The connection ended when a flow is closed because of the expiration of its inactivity timer.</td>
</tr>
<tr>
<td>Deny Terminate</td>
<td>Flow was terminated by application inspection.</td>
</tr>
<tr>
<td>Failover primary closed</td>
<td>The standby unit in a failover pair deleted a connection because of a message received from the active unit.</td>
</tr>
<tr>
<td>FIN Timeout</td>
<td>Force termination after 10 minutes awaiting the last ACK or after half-closed timeout.</td>
</tr>
<tr>
<td>Flow closed by inspection</td>
<td>Flow was terminated by the inspection feature.</td>
</tr>
<tr>
<td>Flow terminated by IPS</td>
<td>Flow was terminated by IPS.</td>
</tr>
<tr>
<td>Flow reset by IPS</td>
<td>Flow was reset by IPS.</td>
</tr>
<tr>
<td>Flow terminated by TCP Intercept</td>
<td>Flow was terminated by TCP Intercept.</td>
</tr>
<tr>
<td>Flow timed out</td>
<td>Flow has timed out.</td>
</tr>
<tr>
<td>Flow timed out with reset</td>
<td>Flow has timed out, but was reset.</td>
</tr>
<tr>
<td>Flow is a loopback</td>
<td>Flow is a loopback.</td>
</tr>
<tr>
<td>Free the flow created as result of packet injection</td>
<td>The connection was built because the packet tracer feature sent a simulated packet through the ASA.</td>
</tr>
<tr>
<td>Invalid SYN</td>
<td>The SYN packet was not valid.</td>
</tr>
<tr>
<td>IPS fail-close</td>
<td>Flow was terminated because the IPS card is down.</td>
</tr>
<tr>
<td>No interfaces associated with zone</td>
<td>Flows were torn down after the “no nameif” or “no zone-member” leaves a zone with no interface members.</td>
</tr>
<tr>
<td>No valid adjacency</td>
<td>This counter is incremented when the ASA tried to obtain an adjacency and could not obtain the MAC address for the next hop. The packet is dropped.</td>
</tr>
<tr>
<td>Pinhole Timeout</td>
<td>The counter is incremented to report that the ASA opened a secondary flow, but no packets passed through this flow within the timeout interval, and so 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.</td>
</tr>
<tr>
<td>Reason</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Route change</td>
<td>When the ASA adds a lower cost (better metric) route, packets arriving that match the new route cause their existing connection to be torn down after the user-configured timeout (floating-conn) value. Subsequent packets rebuild the connection out of the interface with the better metric. To prevent the addition of lower cost routes from affecting active flows, you can set the floating-conn configuration timeout value to 0:0:0.</td>
</tr>
<tr>
<td>SYN Control</td>
<td>A back channel initiation occurred from the wrong side.</td>
</tr>
<tr>
<td>SYN Timeout</td>
<td>Force termination after 30 seconds, awaiting three-way handshake completion.</td>
</tr>
<tr>
<td>TCP bad retransmission</td>
<td>The connection was terminated because of a bad TCP retransmission.</td>
</tr>
<tr>
<td>TCP FINs</td>
<td>A normal close-down sequence occurred. The IP address follows the reason.</td>
</tr>
<tr>
<td>TCP Invalid SYN</td>
<td>Invalid TCP SYN packet.</td>
</tr>
<tr>
<td>TCP Reset - APPLIANCE</td>
<td>The flow is closed when a TCP reset is generated by the ASA.</td>
</tr>
<tr>
<td>TCP Reset - I</td>
<td>Reset was from the inside.</td>
</tr>
<tr>
<td>TCP Reset - O</td>
<td>Reset was from the outside.</td>
</tr>
<tr>
<td>TCP segment partial overlap</td>
<td>A partially overlapping segment was detected.</td>
</tr>
<tr>
<td>TCP unexpected window size variation</td>
<td>A connection was terminated due to variation in the TCP window size.</td>
</tr>
<tr>
<td>Tunnel has been torn down</td>
<td>Flow was terminated because the tunnel is down.</td>
</tr>
<tr>
<td>Unauth Deny</td>
<td>An authorization was denied by a URL filter.</td>
</tr>
<tr>
<td>Unknown</td>
<td>An unknown error has occurred.</td>
</tr>
<tr>
<td>Xlate Clear</td>
<td>A command line was removed.</td>
</tr>
</tbody>
</table>

**Recommended Action** None required.

---

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

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

- **number**—A unique identifier
- **interface, real_address, real_port**—The actual sockets
• **mapped_address and mapped_port**—The mapped sockets
• **user**—The AAA name of the user
• **idfw_user**—The name of the identity firewall 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 [((idfw_user))] to interface :real-address/real-port [((idfw_user))] duration hh:mm:ss bytes bytes [((user))]  

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

• **number**—A unique identifier  
• **interface, real_address, real_port**—The actual sockets  
• **time**—The lifetime of the connection  
• **bytes**—The data transfer of the connection  
• **id**—A unique identifier  
• **interface, real-address, real-port**—The actual sockets  
• **duration**—The lifetime of the connection  
• **bytes**—The data transfer of the connection  
• **user**—The AAA name of the user  
• **idfw_user**—The name of the identity firewall user  

**Recommended Action** None required.

### 302017

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

**Explanation** A GRE connection slot between two hosts was created. The **id** is an unique identifier. The **interface, real_address, real_cid** tuple identifies the one of the two simplex PPTP GRE streams. The parenthetical **translated_address, translated_cid** tuple identifies the translated value with NAT. If inbound is indicated, then the connection can only be used inbound. If outbound is indicated, then the connection can only be used for outbound. The following list describes the message values:

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

**Recommended Action** None required.

---

**302018**

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

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

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

**Recommended Action** None required.

---

**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 ASA uses for decoding the H.323 messages failed to initialize; the ASA cannot decode or inspect the arriving H.323 packet. The ASA allows the H.323 packet to pass through without any modification. When the next H.323 message arrives, the ASA tries 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 } [{idfw_user }] gaddr {gaddr | icmp_type } laddr laddr [{idfw_user }] type {type } code {code }`

**Explanation** An ICMP session was established in the fast-path when stateful ICMP was enabled using the inspect icmp command. The following list describes the message values:

• **faddr**—Specifies the IP address of the foreign host
• **gaddr**—Specifies the IP address of the global host
• **laddr**—Specifies the IP address of the local host
• `idfw_user` — The name of the identity firewall user
• `user` — The username associated with the host from where the connection was initiated
• `type` — Specifies the ICMP type
• `code` — Specifies the ICMP code

**Recommended Action** None required.

### 302021 Error Message

%ASA-6-302021: Teardown ICMP connection for `faddr {faddr | icmp_seq_num}`

```plaintext
| idfw_user | gaddr {gaddr | icmp_type} | laddr {laddr | idfw_user} |
|-----------|---------------------------|---------------------------|
```

**Explanation** An ICMP session is removed in the fast-path when stateful ICMP is enabled using the `inspect icmp` command. The following list describes the message values:

• `faddr` — Specifies the IP address of the foreign host
• `gaddr` — Specifies the IP address of the global host
• `laddr` — Specifies the IP address of the local host
• `idfw_user` — The name of the identity firewall user
• `user` — The username associated with the host from where the connection was initiated
• `type` — Specifies the ICMP type
• `code` — Specifies the ICMP code

**Recommended Action** None required.

### 302022 Error Message

%ASA-6-302022: Built role stub TCP connection for interface : real-address / real-port (mapped-address / mapped-port) to interface : real-address / real-port (mapped-address / mapped-port)

**Explanation** A TCP director/backup/forwarder flow has been created.

**Recommended Action** None required.

### 302023 Error Message

%ASA-6-302023: Teardown stub TCP connection for interface : real-address / real-port to interface : real-address / real-port duration hh:mm:ss forwarded bytes bytes reason

**Explanation** A TCP director/backup/forwarder flow has been torn down.

**Recommended Action** None required.

### 302024 Error Message

%ASA-6-302024: Built role stub UDP connection for interface : real-address / real-port (mapped-address / mapped-port) to interface : real-address / real-port (mapped-address / mapped-port)
**Explanation** A UDP director/backup/forwarder flow has been created.

**Recommended Action** None required.

**302025**

**Error Message** %ASA-6-302025: Teardown stub UDP connection for interface :real-address /real-port to interface :real-address /real-port duration hh:mm:ss forwarded bytes bytes reason

**Explanation** A UDP director/backup/forwarder flow has been torn down.

**Recommended Action** None required.

**302026**

**Error Message** %ASA-6-302026: Built role stub ICMP connection for interface :real-address /real-port (mapped-address ) to interface :real-address /real-port (mapped-address )

**Explanation** An ICMP director/backup/forwarder flow has been created.

**Recommended Action** None required.

**302027**

**Error Message** %ASA-6-302027: Teardown stub ICMP connection for interface :real-address /real-port to interface :real-address /real-port duration hh:mm:ss forwarded bytes bytes reason

**Explanation** An ICMP director/backup/forwarder flow has been torn down.

**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** A GUP connection was started from the foreign address to the local address. The foreign port (outside port) only appears 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 the 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 translations and connections. This message may also be caused by insufficient memory; try reducing the amount of memory usage, or purchasing additional memory.

302035

Error Message %ASA-6-302035: Built {inbound|outbound} SCTP connection conn_id for outside_interface :outside_ip /outside_port (mapped_outside_ip /mapped_outside_port )\{\{outside_idfw_user \},\{outside_sg_info \}\} to inside_interface :inside_ip /inside_port (mapped_inside_ip /mapped_inside_port )\{\{inside_idfw_user \},\{inside_sg_info \}\} \{\{user \}\}

Explanation SCTP flow creation is logged when SCTP-state-bypass is not configured.

- **conn_id** — The unique connection ID
- **outside_interface** — The interface with the lower security level
- **outside_ip** — The IP address of the host on the lower security level side of the ASA
- **outside_port** — The port number of the host on the lower security level side of the ASA
- **mapped_outside_ip** — The mapped IP address of the host on the lower security level side of the ASA
- **mapped_outside_port** — The mapped port number of the host on the lower security level side of the ASA
- **outside_idfw_user** — The IDFW username associated with the host on the lower security level side of the ASA
- **outside_sg_info** — The SGT and SG name associated with the host on the lower security level side of the ASA
- **inside_interface** — The interface with the higher security level
- **inside_ip** — The IP address of the host on the higher security level side of the ASA
- **inside_port** — The port number of the host on the higher security level side of the ASA
- **mapped_inside_ip** — The mapped IP address of the host on the higher security level side of the ASA
- **mapped_inside_port** — The mapped port number of the host on the higher security level side of the ASA
- **inside_idfw_user** — The IDFW username associated with the host on the higher security level side of the ASA
- **inside_sg_info** — The SGT and SG name associated with the host on the higher security level side of the ASA
- **user** — The username associated with the host from where the connection was initiated

Recommended Action None required.
951 complete topic

Error Message %ASA-6-302036: Teardown SCTP connection conn_id for outside_interface :outside_ip /outside_port [{[outside_idfw_user ],[outside_sg_info ]}] to inside_interface :inside_ip /inside_port [{[inside_idfw_user ],[inside_sg_info ]}] duration time bytes bytes reason {[user ]}

Explanation SCTP flow deletion is logged when SCTP-state-bypass is not configured.

- **conn_id** — The unique connection ID
- **outside_interface** — The interface with the lower security level
- **outside_ip** — The IP address of the host on the lower security level side of the ASA
- **outside_port** — The port number of the host on the lower security level side of the ASA
- **outside_idfw_user** — The IDFW username associated with the host on the lower security level side of the ASA
- **outside_sg_info** — The SGT and SG name associated with the host on the lower security level side of the ASA
- **inside_interface** — The interface with the higher security level
- **inside_ip** — The IP address of the host on the higher security level side of the ASA
- **inside_port** — The port number of the host on the higher security level side of the ASA
- **inside_idfw_user** — The IDFW username associated with the host on the higher security level side of the ASA
- **inside_sg_info** — The SGT and SG name associated with the host on the higher security level side of the ASA
- **user** — The username associated with the host from where the connection was initiated
- **time** — The amount of the flow stayed alive in hh:mm:ss
- **bytes** — The number of bytes passed on the flow
- **reason** — The reason the connection was torn down

Recommended Action None required.

302302

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

Explanation IPsec proxy mismatches have occurred. 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.

302303

Error Message %ASA-6-302303: Built TCP state-bypass connection conn_id from initiator_interface :real_ip /real_port (mapped_ip /mapped_port ) to responder_interface :real_ip /real_port (mapped_ip /mapped_port )

Explanation A new TCP connection has been created, and this connection is a TCP-state-bypass connection. This type of connection bypasses all the TCP state checks and additional security checks and inspections.
**Recommended Action** If you need to secure TCP traffic with all the normal TCP state checks as well as all other security checks and inspections, you can use the `no set connection advanced-options tcp-state-bypass` command to disable this feature for TCP traffic.

**302304**

**Error Message** %ASA-6-302304: Teardown TCP state-bypass connection conn_id from initiator_interface :ip/port to responder_interface :ip/port duration, bytes, teardown reason.

**Explanation** A new TCP connection has been torn down, and this connection is a TCP-state-bypass connection. This type of connection bypasses all the TCP state checks and additional security checks and inspections.

- **duration** — The duration of the TCP connection
- **bytes** — The total number of bytes transmitted over the TCP connection
- **teardown reason** — The reason for the teardown of the TCP connection

**Recommended Action** If you need to secure TCP traffic with all the normal TCP state checks as well as all other security checks and inspections, you can use the `no set connection advanced-options tcp-state-bypass` command to disable this feature for TCP traffic.

**302305**

**Error Message** %ASA-6-302305: Built SCTP state-bypass connection conn_id for outside_interface :outside_ip /outside_port (mapped_outside_ip /mapped_outside_port )(([outside_idfw_user ],[outside_sg_info ])) to inside_interface :inside_ip /inside_port (mapped_inside_ip /mapped_inside_port )(([inside_idfw_user ],[inside_sg_info ]))

**Explanation** SCTP flow creation is logged when SCTP-state-bypass is configured.

- **conn_id** — The unique connection ID
- **outside_interface** — The interface with the lower security level
- **outside_ip** — The IP address of the host on the lower security level side of the ASA
- **outside_port** — The port number of the host on the lower security level side of the ASA
- **mapped_outside_ip** — The mapped IP address of the host on the lower security level side of the ASA
- **mapped_outside_port** — The mapped port number of the host on the lower security level side of the ASA
- **outside_idfw_user** — The IDFW username associated with the host on the lower security level side of the ASA
- **outside_sg_info** — The SGT and SG name associated with the host on the lower security level side of the ASA
- **inside_interface** — The interface with the higher security level
- **inside_ip** — The IP address of the host on the higher security level side of the ASA
- **inside_port** — The port number of the host on the higher security level side of the ASA
- **mapped_inside_ip** — The mapped IP address of the host on the higher security level side of the ASA
- **mapped_inside_port** — The mapped port number of the host on the higher security level side of the ASA
- **inside_idfw_user** — The IDFW username associated with the host on the higher security level side of the ASA
- **inside_sg_info** — The SGT and SG name associated with the host on the higher security level side of the ASA

**Recommended Action** None required.
**302306**

**Error Message** %ASA-6-302306: Teardown SCTP state-bypass connection conn_id for outside_interface : outside_ip / outside_port [[outside_idfw_user ],[outside_sg_info ]] to inside_interface : inside_ip / inside_port [[inside_idfw_user ],[inside_sg_info ]] duration time bytes bytes reason

**Explanation** SCTP flow deletion is logged when SCTP-state-bypass is configured.

- **conn_id** — The unique connection ID
- **outside_interface** — The interface with the lower security level
- **outside_ip** — The IP address of the host on the lower security level side of the ASA
- **outside_port** — The port number of the host on the lower security level side of the ASA
- **outside_idfw_user** — The IDFW username associated with the host on the lower security level side of the ASA
- **outside_sg_info** — The SGT and SG name associated with the host on the lower security level side of the ASA
- **inside_interface** — The interface with the higher security level
- **inside_ip** — The IP address of the host on the higher security level side of the ASA
- **inside_port** — The port number of the host on the higher security level side of the ASA
- **inside_outside_ip** — The mapped IP address of the host on the higher security level side of the ASA
- **inside_idfw_user** — The IDFW username associated with the host on the higher security level side of the ASA
- **inside_sg_info** — The SGT and SG name associated with the host on the higher security level side of the ASA
- **time** — The amount of time that the flow stayed alive in hh:mm:ss
- **bytes** — The number of bytes passed on the flow
- **reason** — The reason the connection was torn down

**Recommended Action** None required.

---

**302311**

**Error Message** %ASA-4-302311: Failed to create a new protocol connection from ingress interface:source IP/source port to egress interface:destination IP/destination port due to application cache memory allocation failure. The app-cache memory threshold level is threshold% and threshold check is enabled/disabled.

**Explanation** A new connection could not be created due to app-cache memory allocation failure. The failure could be due to system running out of memory or exceeding app-cache memory threshold.

- **protocol** — The name of the protocol used to create the connection
- **ingress interface** — The interface name
- **source IP** — The source IP address
- **source port** — The source port number
- **egress interface** — The interface name
- **destination IP** — The destination address
- **destination port** — The destination port number
Recommended Action Disable memory intensive features on the device or reduce the number of through-the-box connections.

303002

Error Message %ASA-6-303002: FTP connection from src_ifc : src_ip / src_port to dst_ifc : dst_ip / dst_port, user username action file filename

Explanation A client has uploaded or downloaded a file from the FTP server.

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 Strict FTP inspection on FTP traffic has been used, and 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 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 message occurs.

Recommended Action None required.
- **dip**—The destination IP address
- **dport**—The destination port

**Recommended Action** None required.

### 304001

**Error Message** %ASA-5-304001: user@source_address [((idfw_user ))] Accessed URL dest_address : url .

**Explanation** The specified host tried to access the specified URL. If you enable the HTTP inspection with custom HTTP policy map, the following possibilities are seen. When the packet of GET request does not have the hostname parameter, instead of printing the URI, it prints the following message:%ASA-5-304001: client IP Accessed URL server ip: Hostname not present URI: URI If a large URI which cannot be printed in a single syslog, you can print partial wherever it is being chopped down. For instance, when the URL is to be divided into multiple chunks and logged, the following message is printed:%ASA-5-304001: client IP Accessed URL server ip: http://hostname/URI CHUNK1 partial%ASA-5-304001: client IP Accessed URL server ip: partial URI CHUNK1 partial.............%ASA-5-304001: client IP Accessed URL server ip: partial URI CHUNKnThe limit for URI is 1024 bytes. If the current packet contains partial URI at the beginning or end, use the same logic as explained above.

**Recommended Action** None required.

### 304002

**Error Message** %ASA-5-304002: Access denied URL chars SRC IP_address [((idfw_user ))] DEST IP_address : chars

**Explanation** Access from the source address to the specified URL or FTP site was 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** A Websense server request failed.

**Recommended Action** None required.

### 304005

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

**Explanation** A Websense server request is pending.
Recommended Action None required.

304006

Error Message %ASA-3-304006: URL Server IP_address not responding
Explanation The Websense server is unavailable for access, and the ASA 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 You used the allow option of the filter command, and the Websense servers are not responding. The ASA 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 You used the allow option of the filter command, and the ASA receives a response message from a Websense server that previously was not responding. With this response message, the ASA 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 [(idfw_user)] dst interface_name: dest_address /dest_port [(idfw_user)]
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, the 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 [(idfw_user)] dst interface_name:dest_address/dest_port [(idfw_user)]

**Explanation** A protocol (UDP, TCP, or ICMP) failed to create a translation through the ASA. The ASA does not allow packets through that are destined for network or broadcast addresses. The ASA provides this checking for addresses that are explicitly identified with static commands. For inbound traffic, the ASA denies translations for an IP address identified as a network or broadcast address.

The ASA 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 translation. As a result, when the other ICMP message types are dropped, this message is generated.

The ASA uses the global IP address and mask from configured static commands 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 ASA 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
```

The ASA responds to global address 10.2.2.128 as a network address and to 10.2.2.255 as the broadcast address. Without an existing translation, the ASA denies inbound packets destined for 10.2.2.128 or 10.2.2.255, and logs this message.

When the suspected IP address is a host IP address, configure a separate static command with a host mask in front of the subnet static command (the first match rule for static commands). The following static commands cause the ASA 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 from the inside host with the IP address in question. Because the ASA views a network or broadcast IP address as a host IP address with an overlapped subnet static configuration, the network address translation for both static commands 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 ASA has attempted to translate an address that it cannot find in any of its global pools. The ASA 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 ASA 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 ASA is running a Stateful Failover setup, and some of the internal states are momentarily out of sync between the active unit and the standby unit. This condition is not catastrophic, and the synchronization 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 [(idfw_user )] 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 [(idfw_user )] 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 [(idfw_user )] 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 } [(idfw_user )] 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 [(idfw_user )] dst interface_name :dst_address /dst_port [(idfw_user )] 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 actual address to connect to the host. In addition, enable the inspect command if the application embeds the IP address.

305014

**Error Message** %ASA-6-305014: %d: Allocated %s block of ports for translation from %s:%B to %s:%B/%d-%d\n.

**Explanation** When CGNAT “block-allocation” is configured, this syslog will be generated on allocation of a new port block.

**Recommended Action** None.

305016

**Error Message** %ASA-3-305016: Unable to create protocol connection from real_interface :real_host_ip /real_source_port to real_dest_interface :real_dest_ip /real_dest_port due to reason .

**Explanation** The maximum port blocks per host limit has been reached for a host or the port blocks have been exhausted.

- **reason** — May be one of the following:
  - reaching per-host PAT port block limit of value
  - port block exhaustion in PAT pool

**Recommended Action** For reaching the per-host PAT port block limit, review the maximum blocks per host limit by entering the following command:

```
xlate block-allocation maximum-per-host 4
```

For the port block exhaustion in the PAT pool, we recommend increasing the pool size. Also, review the block size by entering the following command:

```
xlate block-allocation size 512
```

305017

**Error Message** %ASA-3-305017: Pba-interim-logging: Active ICMP block of ports for translation from <source_device_IP> to <destination_device_IP>/<Active Port Block>

**Explanation** When CGNAT interim logging feature is turned on. This syslog specifies the Active Port Block from a particular source IP address to a destination IP address at that time.
**Recommended Action** None.

**305018**

**Error Message** %ASA-6-305018: MAP translation from
src_ifc:src_ip/src_port-dst_ifc:dst_ip/dst_port to
src_ifc:translated_src_ip/src_port-dst_ifc:translated_dst_ip/dst_port

**Explanation** MAP style address translation has been applied to a connection being established, their source and destination have been translated

Example:
%ASA-6-305018: MAP translation from

**Recommended Action** None.

**305019**

**Error Message** %ASA-3-305019: MAP node address ip/port has inconsistent Port Set ID encoding

**Explanation** A packet has an address that matches MAP basic mapping rules (meaning it is meant to be translated) but the Port Set ID encoded within the address is inconsistent (per RFC7599). This could be due to a software fault on the MAP node where this packet originates.

Example
%ASA-3-305019: MAP node address 2001:DB8:0000:FFFF:0000:0000:0000:0002/57964 has inconsistent Port Set ID encoding

**Recommended Action** None.

**305020**

**Error Message** %ASA-3-305020: MAP node with address ip is not allowed to use port port

**Explanation** A packet has an address that matches MAP basic mapping rules (meaning it is meant to be translated) but the associated port does not fall within the range allocated to that address. This likely means there is misconfiguration on the MAP node where this packet originates.

Example:
%ASA-3-305020: MAP node with address 2001:DB8:0000:0000:0000:0000:0000:0002 is not allowed to use port 37964

**Recommended Action** None.

**308001**

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

**Explanation** This is a ASA management message. This message appears after the specified number of times a user incorrectly types the password to enter privileged mode. The maximum is three attempts.
308002

**Recommended Action** Verify the password and try again.

**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.

308003

**Error Message** %ASA-4-308003: WARNING: The enable password is not configured

**Explanation** When entering enable mode (privilege level 2 or greater), you are forced to configure the enable password for privilege level 15 when the enable password is not already set.

**Recommended Action** Set the enable password. The permitted length of password is between 3 and 15.

308004

**Error Message** %ASA-4-308004: The enable password has been configured by user admin

**Explanation** You have configured the enable password for the first time. This message will not be displayed when you are modifying an existing enable password.

**Recommended Action** None.

311001

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

**Explanation** Stateful Failover update information was sent to the standby ASA when the standby ASA 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 ASA.

**Recommended Action** None required.

311003

**Error Message** %ASA-6-311003: LU recv thread up
**Explanation** An update acknowledgment was received from the standby ASA.

**Recommended Action** None required.

---

**311004**

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

**Explanation** A Stateful Failover update was transmitted to the standby ASA.

**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 ASA 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. Another RIP device may not be configured correctly to communicate with the ASA.

**Recommended Action** None required.

---

**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 ASA discards the ICMP packet and generates this message. The `icmp` command enables or disables pinging to an interface. With pinging disabled, the ASA 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 on interface interface_name to dest_address: no matching session

**Explanation** ICMP packets were dropped by the ASA 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 ASA or ICMP error messages not related to any TCP, UDP, or ICMP session already established in the ASA.

**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 [[idfw_user | FQDN_string ], sg_info ] dst dest_interface_name :dest_address [[idfw_user | FQDN_string ], sg_info ] (type icmp_type,
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 ASA discards the ICMPv6 packet and generates this message.

The icmp command enables or disables pinging to an interface. When pinging is disabled, the ASA is undetectable on the network. This feature is also referred to as “configurable proxy pinging.”

Recommended Action Contact the administrator of the peer device.

313009

Error Message  %ASA-4-313009: Denied invalid ICMP code icmp-code, for src-ifc : src-address / src-port (mapped-src-address/mapped-src-port) to dest-ifc : dest-address / dest-port (mapped-dest-address/mapped-dest-port) [user ], ICMP id icmp-id , ICMP type icmp-type

Explanation An ICMP echo request/reply packet was received with a malformed code(non-zero).

Recommended Action If it is an intermittent event, no action is required. If the cause is an attack, you can deny the host using the ACLs.

314001

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

Explanation The ASA opened a UDP media channel for the RTSP client that was receiving data from the 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 ASA 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 by running the show memory command, or the number of connections used by running the show conn command, because the ASA 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 — The reasons may be one of the following:
  - 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_URI

Explanation An RTSP client tried 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 An RTSP client tried to access a prohibited site.
**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 ASA cannot find the RSA host key, which is required for establishing an SSH session. The ASA host key may be absent because it was not generated or because the license for this ASA does not allow DES or 3DES encryption.

**Recommended Action**  
From the ASA 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**  
An SSH session has ended. If a user enters `quit` or `exit`, the `terminated normally` message appears. The username is hidden when invalid or unknown, but appears when valid or the `no logging hide username` command has been configured. If the session disconnected for another reason, the text describes the reason. The following table lists the possible reasons why a session is disconnected.

**Table 2: SSH Disconnect Reasons**

<table>
<thead>
<tr>
<th>Text String</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad checkbytes</td>
<td>A mismatch was detected in the check bytes during an SSH key exchange.</td>
<td>Restart the SSH session.</td>
</tr>
<tr>
<td>Text String</td>
<td>Explanation</td>
<td>Action</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CRC check failed</td>
<td>The CRC value computed for a particular packet does not match the CRC value embedded in the packet; the packet is bad.</td>
<td>None required. If this message persists, call Cisco TAC.</td>
</tr>
<tr>
<td>Decryption failure</td>
<td>Decryption of an SSH session key failed during an SSH key exchange.</td>
<td>Check the RSA host key and try again.</td>
</tr>
<tr>
<td>Format error</td>
<td>A nonprotocol version message was received during an SSH version exchange.</td>
<td>Check the SSH client, to ensure it is a supported version.</td>
</tr>
<tr>
<td>Internal error</td>
<td>This message indicates either an error internal to SSH on the ASA or an RSA key may not have been entered on the ASA or cannot be retrieved.</td>
<td>From the ASA console, enter the <code>show crypto key mypubkey rsa</code> command to verify that the RSA host key is present. If the host key is not present, enter the <code>show version</code> 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 <code>crypto key mypubkey rsa</code> command.</td>
</tr>
<tr>
<td>Invalid cipher type</td>
<td>The SSH client requested an unsupported cipher.</td>
<td>Enter the <code>show version</code> command to determine which features your license supports, then reconfigure the SSH client to use the supported cipher.</td>
</tr>
<tr>
<td>Invalid message length</td>
<td>The length of SSH message arriving at the ASA exceeds 262,144 bytes or is shorter than 4096 bytes. The data may be corrupted.</td>
<td>None required.</td>
</tr>
<tr>
<td>Invalid message type</td>
<td>The ASA received a non-SSH message, or an unsupported or unwanted SSH message.</td>
<td>Check whether the peer is an SSH client. If it is a client supporting SSHv1, and this message persists, from the ASA serial console enter the <code>debug ssh</code> command and capture the debugging messages. Then contact the Cisco TAC.</td>
</tr>
<tr>
<td>Out of memory</td>
<td>This message appears when the ASA cannot allocate memory for use by the SSH server, probably when the ASA is busy with high traffic.</td>
<td>Restart the SSH session later.</td>
</tr>
<tr>
<td>Rejected by server</td>
<td>User authentication failed.</td>
<td>Ask the user to verify username and password.</td>
</tr>
<tr>
<td>Reset by client</td>
<td>An SSH client sent the <code>SSH_MSG_DISCONNECT</code> message to the ASA.</td>
<td>None required.</td>
</tr>
<tr>
<td>status code: hex (hex)</td>
<td>Users closed the SSH client window (running on Windows) instead of entering <code>quit</code> or <code>exit</code> at the SSH console.</td>
<td>None required. Encourage users to exit the client gracefully instead of just exiting.</td>
</tr>
</tbody>
</table>
### 315012

**Error Message** %ASA-3-315012: Weak SSH type (alg) provided from client IP_address on interface Int. Connection failed. Not FIPS 140-2 compliant.

**Explanation** As part of the FIPS 140-2 certification, when FIPS is enabled, SSH connections can only be brought up using aes128-cbc or aes256-cbc as the cipher and SHA1 as the MAC. This syslog is generated when an unacceptable cipher or MAC is used. This syslog will not be seen if FIPS mode is disabled.

- **type** — cipher or MAC
- **alg** — The name of the unacceptable cipher or MAC
- **IP_address** — The IP address of the client
- **int** — The interface that the client is attempting to connect to

**Recommended Action** Provide an acceptable cipher or MAC

### 315013

**Error Message** %ASA-6-315013: SSH session from <SSH client address> on interface <interface name> for user "<user name>" rekeyed successfully.

**Explanation** This syslog is needed to indicate that an SSH rekey has successfully completed. This is a Common Criteria certification requirement.

- **SSH client address** — The IP address of the client
- **interface name** — The interface that the client is attempting to connect to
- **user_name** — The user name associated with the session

**Recommended Action** None

### 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 trying to be established than are 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** The ASA cannot 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:

```plaintext
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 a 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 collected information.

**317007**

**Error Message** %ASA-6-317007: Added route_type route dest_address netmask via gateway_address [distance /metric] on interface_name route_type

**Explanation** A new route has been added to the routing table.

Routing protocol type:

B – BGP, D – EIGRP, EX - EIGRP external, O - OSPF
IA - OSPF inter area, N1 - OSPF NSSA external type 1
N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
E2 - OSPF external type 2, E – EGP, i - IS-IS, L1 - IS-IS level-1
L2 - IS-IS level-2, ia - IS-IS inter area

- **dest_address** —The destination network for this route
- **netmask** —The netmask for the destination network
- **gateway_address** —The address of the gateway by which the destination network is reached
- **distance** —Administrative distance for this route
- **metric** —Metric for this route
- **interface_name** —Network interface name through which the traffic is routed

**Recommended Action** None required.
**317008**

**Error Message**%ASA-6-317008: Deleted route_type route dest_address netmask via gateway_address

[distance /metric ] on interface_name route_type

**Explanation** A new route has been deleted from the routing table.

Routing protocol type:

- B – BGP, D – EIGRP, EX - EIGRP external, O - OSPF
- IA - OSPF inter area, N1 - OSPF NSSA external type 1
- N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
- E2 - OSPF external type 2, E – EGP, i - IS-IS, L1 - IS-IS level-1
- L2 - IS-IS level-2, ia - IS-IS inter area

- dest_address —The destination network for this route
- netmask —The netmask for the destination network
- gateway_address —The address of the gateway by which the destination network is reached
- distance —Administrative distance for this route
- metric —Metric for this route
- interface_name —Network interface name through which the traffic is routed

**Recommended Action** None required.

**317012**

**Error Message**%ASA-3-317012: Interface IP route counter negative - nameif-string-value

**Explanation** Indicates that the interface route count is negative.

- nameif-string-value—The interface name as specified by the nameif command

**Recommended Action** None required.

**318001**

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

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

**Recommended Action** Copy the message exactly as it appears, and report it to 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 without a backbone area configured in the router. This message occurs at five-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** Copy the message exactly as it appears, and report it to the Cisco TAC.

318004

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

**Explanation** The OSPF process had a problem locating the link state advertisement, 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** Copy the message exactly as it appears, and report it to 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** Copy the message exactly as it appears, and report it to 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 the 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** OSPF is running and has tried 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.

318101

**Error Message** %ASA-3-318101: Internal error: REASON

**Explanation** An internal software error has occurred.

- **REASON** — The detailed cause of the event

**Recommended Action** None required.

318102

**Error Message** %ASA-3-318102: Flagged as being an ABR without a backbone area

**Explanation** The router was flagged as an Area Border Router (ABR) without a backbone area in the router.

**Recommended Action** Restart the OSPF process.

318103

**Error Message** %ASA-3-318103: Reached unknown state in neighbor state machine

**Explanation** An internal software error has occurred.

**Recommended Action** None required.

318104

**Error Message** %ASA-3-318104: DB already exist: area AREA_ID_STR lsid i adv i type 0x x

**Explanation** OSPF has a problem locating the LSA, which could lead to a memory leak.

- **AREA_ID_STR** — A string representing the area
- **i** — An integer value
- **x** — A hexadecimal representation of an integer value

**Recommended Action** None required.
**318105**

**Error Message**  %ASA-3-318105: lsid i adv i type 0x x gateway i metric d network i mask i protocol #x attr #x net-metric d

**Explanation** OSPF found an inconsistency between its database and the IP routing table.
- \( i \) — An integer value
- \( x \) — A hexadecimal representation of an integer value
- \( d \) — A number

**Recommended Action** None required.

**318106**

**Error Message**  %ASA-3-318106: if IF_NAME if_state d

**Explanation** An internal error has occurred.
- \( IF\_NAME \) — The name of the affected interface
- \( d \) — A number

**Recommended Action** None required.

**318107**

**Error Message**  %ASA-3-318107: OSPF is enabled on IF_NAME during idb initialization

**Explanation** An internal error has occurred.
- \( IF\_NAME \) — The name of the affected interface

**Recommended Action** None required.

**318108**

**Error Message**  %ASA-3-318108: OSPF process d 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, which brings down all virtual links. To make them work again, you need to change the virtual link configuration on all virtual link neighbors.
- \( d \) — A number representing the process ID

**Recommended Action** Change the virtual link configuration on all the virtual link neighbors to include the new router ID.

**318109**

**Error Message**  %ASA-3-318109: OSPFv3 has received an unexpected message: 0x x / 0x

**Explanation** OSPFv3 has received an unexpected interprocess message.
- \( x \) — A hexadecimal representation of an integer value
Recommended Action None required.

318110

Error Message %ASA-3-318110: Invalid encrypted key s.
Explanation The specified encrypted key is not valid.
  • s — A string representing the encrypted key

Recommended Action Either specify a clear text key and enter the service password-encryption command for encryption, or ensure that the specified encrypted key is valid. If the specified encrypted key is not valid, an error message appears during system configuration.

318111

Error Message %ASA-3-318111: SPI u is already in use with ospf process d.
Explanation An attempt was made to use a SPI that has already been used.
  • u — A number representing the SPI
  • d — A number representing the process ID

Recommended Action Choose a different SPI.

318112

Error Message %ASA-3-318112: SPI u is already in use by a process other than ospf process d.
Explanation An attempt was made to use a SPI that has already been used.
  • u — A number representing the SPI
  • d — A number representing the process ID

Recommended Action Choose a different SPI. Enter the show crypto ipv6 ipsec sa command to view a list of SPIs that are already being used.

318113

Error Message %ASA-3-318113: s s is already configured with SPI u.
Explanation An attempt was made to use a SPI that has already been used.
  • s — A string representing an interface
  • u — A number representing the SPI

Recommended Action Unconfigure the SPI first, or choose a different one.

318114

Error Message %ASA-3-318114: The key length used with SPI u is not valid
Explanation The key length was incorrect.
• u — A number representing the SPI

**Recommended Action** Choose a valid IPsec key. An IPsec authentication key must be 32 (MD5) or 40 (SHA-1) hexadecimal digits long.

### 318115

**Error Message** %ASA-3-318115: s error occurred when attempting to create an IPsec policy for SPI u

**Explanation** An IPsec API (internal) error has occurred.

- s — A string representing the error
- u — A number representing the SPI

**Recommended Action** None required.

### 318116

**Error Message** %ASA-3-318116: SPI u is not being used by ospf process d.

**Explanation** An attempt was made to unconfigure a SPI that is not being used with OSPFv3.

- u — A number representing the SPI
- d — A number representing the process ID

**Recommended Action** Enter a `show` command to see which SPIs are used by OSPFv3.

### 318117

**Error Message** %ASA-3-318117: The policy for SPI u could not be removed because it is in use.

**Explanation** An attempt was made to remove the policy for the indicated SPI, but the policy was still being used by a secure socket.

- u — A number representing the SPI

**Recommended Action** None required.

### 318118

**Error Message** %ASA-3-318118: s error occurred when attempting to remove the IPsec policy with SPI u

**Explanation** An IPsec API (internal) error has occurred.

- s — A string representing the specified error
- u — A number representing the SPI

**Recommended Action** None required.

### 318119

**Error Message** %ASA-3-318119: Unable to close secure socket with SPI u on interface s
Explanation An IPsec API (internal) error has occurred.

- **u** —A number representing the SPI
- **s** —A string representing the specified interface

**Recommended Action** None required.

### 318120

**Error Message** %ASA-3-318120: OSPFv3 was unable to register with IPsec

**Explanation** An internal error has occurred.

**Recommended Action** None required.

### 318121

**Error Message** %ASA-3-318121: IPsec reported a GENERAL ERROR: message **s**, count **d**

**Explanation** An internal error has occurred.

- **s** —A string representing the specified message
- **d** —A number representing the total number of generated messages

**Recommended Action** None required.

### 318122

**Error Message** %ASA-3-318122: IPsec sent a **s** message **s** to OSPFV3 for interface **s**. Recovery attempt **d**

**Explanation** An internal error has occurred. The system is trying to reopen the secure socket and to recover.

- **s** —A string representing the specified message and specified interface
- **d** —A number representing the total number of recovery attempts

**Recommended Action** None required.

### 318123

**Error Message** %ASA-3-318123: IPsec sent a **s** message **s** to OSPFV3 for interface **IF_NAME**. Recovery aborted

**Explanation** An internal error has occurred. The maximum number of recovery attempts has been exceeded.

- **s** —A string representing the specified message
- **IF_NAME** —The specified interface

**Recommended Action** None required.

### 318125

**Error Message** %ASA-3-318125: Init failed for interface **IF_NAME**

**Explanation** The interface initialization failed. Possible reasons include the following:
• The area to which the interface is being attached is being deleted.
• It was not possible to create the link scope database.
• It was not possible to create a neighbor datablock for the local router.

**Recommended Action** Remove the configuration command that initializes the interface and then try it again.

### 318126

**Error Message** %ASA-3-318126: Interface \texttt{IF\_NAME} is attached to more than one area

**Explanation** The interface is on the interface list for an area other than the one to which the interface links.

• \texttt{IF\_NAME} — The specified interface

**Recommended Action** None required.

### 318127

**Error Message** %ASA-3-318127: Could not allocate or find the neighbor

**Explanation** An internal error has occurred.

**Recommended Action** None required.

### 319001

**Error Message** %ASA-3-319001: Acknowledge for arp update for IP address \texttt{dest\_address} not received (\texttt{number}).

**Explanation** The ARP process in the ASA lost internal synchronization because the ASA was overloaded.

**Recommended Action** None required. The failure is only temporary. Check the average load of the ASA and make sure that it is not used beyond its capabilities.

### 319002

**Error Message** %ASA-3-319002: Acknowledge for route update for IP address \texttt{dest\_address} not received (\texttt{number}).

**Explanation** The routing module in the ASA lost internal synchronization because the ASA was overloaded.

**Recommended Action** None required. The failure is only temporary. Check the average load of the ASA and make sure that it is not used beyond its capabilities.

### 319003

**Error Message** %ASA-3-319003: Arp update for IP address \texttt{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 by reviewing 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 ASA lost internal synchronization because the system was overloaded.

**Recommended Action** None required. The failure is only temporary. Check the average load of the system and make sure that it is not used beyond its capabilities.

**Messages 320001 to 342008**

This chapter includes messages from 320001 to 342008.

**320001**

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

**Explanation** When the ASA is an easy VPN remote device or server, the peer certificate includes a subject name that does not match the output of the `ca verifycertdn` command. A man-in-the-middle attack might be occurring, where a device spoofs the peer IP address and tries to intercept a VPN connection from the ASA.

**Recommended Action** None required.

**321001**

**Error Message** \%ASA-5-321001: Resource \textit{var1} limit of \textit{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 \textit{var1} rate limit of \textit{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 \textit{var1} log level of \textit{var2} reached.

**Explanation** A configured resource usage or rate logging 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 logging level for the indicated resource was reached.
Recommended Action None required.

321005

Error Message %ASA-2-321005: System CPU utilization reached utilization %
Explanation The system CPU utilization has reached 95 percent or more and remains at this level for five minutes.
   • utilization %—The percentage of CPU being used
Recommended Action If this message occurs periodically, you can ignore it. If it repeats frequently, check the output of the `show cpu` command and verify the CPU usage. If it is high, contact the Cisco TAC.

321006

Error Message %ASA-2-321006: System memory usage reached utilization %
Explanation The system memory usage has reached 80 percent or more and remains at this level for five minutes.
   • utilization %—The percentage of memory being used
Recommended Action If this message occurs periodically, you can ignore it. If it repeats frequently, check the output of the `show memory` command and verify the memory usage. If it is high, contact the Cisco TAC.

321007

Error Message %ASA-3-321007: System is low on free memory blocks of size block_size (free_blocks CNT out of max_blocks MAX)
Explanation The system is low on free blocks of memory. Running out of blocks may result in traffic disruption.
   • block_size—The block size of memory (for example, 4, 1550, 8192)
   • free_blocks—The number of free blocks, as shown in the CNT column after using the `show blocks` command
   • max_blocks—The maximum number of blocks that the system can allocate, as shown in the MAX column after using the `show blocks` command
Recommended Action Use the `show blocks` command to monitor the amount of free blocks in the CNT column of the output for the indicated block size. If the CNT column remains zero, or very close to it for an extended period of time, then the ASA may be overloaded or running into another issue that needs additional investigation.
322001

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

**Explanation** The ASA 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 the configuration. Either a MAC-spoofing attack or a misconfiguration may be the cause.

**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 ASA. 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 ASA. 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 ASA 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 module_id experienced a control channel communications failure.

%ASA-3-323001: Module in slot slot_num experienced a control channel communications failure.

**Explanation** The ASA is unable to communicate via control channel with the module installed (in the specified slot).

• **module_id**—For a software services module, specifies the services module name.
• **slot_num**—For a hardware services module, specifies 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.

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

### 323002

**Error Message**  
%ASA-3-323002: Module module_id is not able to shut down, shut down request not answered.

%ASA-3-323002: Module in slot slot_num is not able to shut down, shut down request not answered.

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

• **module_id**—For a software services module, specifies the service module name.
• **slot_num**—For a hardware services module, specifies 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.

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

### 323003

**Error Message**  
%ASA-3-323003: Module module_id is not able to reload, reload request not answered.

%ASA-3-323003: Module in slot slot_num is not able to reload, reload request not answered.

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

• **module_id**—For a software services module, specifies the service module name.
• **slot_num**—For a hardware services module, specifies 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.
**Recommended Action** If the problem persists, contact the Cisco TAC.

### 323004

**Error Message** %ASA-3-323004: Module string one failed to write software newver (currently ver ), reason . Hw-module reset is required before further use.

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

- **string one**—The text string that specifies 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 cannot 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** If the module software cannot be updated, it will not be usable. If the problem persists, contact the Cisco TAC.

### 323005

**Error Message** %ASA-3-323005: Module module_id can not be started completely

%ASA-3-323005: Module in slot slot_num can not be started completely

**Explanation** This message indicates that the module cannot be started completely. The module will remain in the UNRESPONSIVE state until this condition is corrected. A module that is not fully seated in the slot is the most likely cause.

- **module_id**—For a software services module, specifies the service module name.
- **slot_num**—For a hardware services module, specifies the slot number that contains the module.

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

### 323006

**Error Message** %ASA-1-323006: Module ips experienced a data channel communication failure, data channel is DOWN.

**Explanation** A data channel communication failure occurred and the ASA was unable to forward traffic to the services module. This failure triggers a failover when the failure occurs on the active ASA 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 services module. This message is generated whenever a communication problem over the ASA dataplane occurs between the system module and the services module, which can be caused when the services module stops, resets, is removed or disabled.
**Recommended Action** For software services modules such as IPS, recover the module using the `sw-module module ips recover` command. For hardware services modules, if this message is not the result of the SSM reloading or resetting and the corresponding syslog message 505010 is not seen after the SSM returns to an UP state, reset the module using the `hw-module module 1 reset` command.

### 323007

**Error Message**  %ASA-3-323007: Module in slot slot experienced a firmware failure and the recovery is in progress.

**Explanation** An ASA with a 4GE-SSM installed experienced a short power surge, then rebooted. As a result, the 4GE-SSM may come online in an unresponsive state. The ASA has detected that the 4GE-SSM is unresponsive, and automatically restarts the 4GE-SSM.

**Recommended Action** None required.

### 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 may be 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 message 321100, memory allocation error, the message indicates that there were not enough resources to create the PDP context. If not, it was not preceded by message 321100. For version 0, it indicates that the corresponding PDP context cannot be found. For version 1, if this message was preceded by message 324001, then a packet processing error occurred, and the operation stopped.

**Recommended Action** If the problem persists, determine why the source is sending packets without a valid PDP context.

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 may be 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 transport protocol data units.

**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 GPRS support node 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_address /0 to dest_address /dest_port

**Explanation** An error occurred while trying to create the tunnel for the transport protocol data units for a different Servicing GPRS support node or gateway GPRS support node.

**Recommended Action** Check debugging messages to see why the connection was not created correctly. If the problem persists, contact the Cisco TAC.

**324008**

**Error Message** %ASA-3-324008: No PDP exists to update the data sgsn [ggsn] PDPMCB Info REID: teid_value, Request TEID; teid_value, Local GSN: IPaddress (VPIfNum), Remove GSN: IPaddress (VPIfNum)

**Explanation** When a GTP HA message is received on the standby unit to update the PDP with data sgsn/ggsn PDPMCB information, the PDP is not found because of a previous PDP update message that was not successfully delivered or successfully processed on the standby unit.

**Recommended Action** If this message occurs periodically, you can ignore it. If it occurs frequently, contact the Cisco TAC.

**324010**

**Error Message** %ASA-5-324010: Subscriber IMSI PDP Context activated on network MCC/MNC mccmnc (IE type[IE type]{CellID cellID})

**Explanation** This message appears when the PDP Context is activated. MCC is always 3 digits and MNC is 2 or 3 digits.

**Note**

The MCC, MNC, IE type, or Cell ID could be "Unknown" if the packet does not contain the location information IEs.

**Example:**

%ASA-5-324010: Subscriber ID PDP Context activated on network MCC/MNC 11122 (v1 RAI/v1 ULI)

CellID 1

%ASA-5-324010: Subscriber ID PDP Context activated on network Unknown

**Recommended Action** None
324011

Error Message %ASA-5-324011: Subscriber IMSI location changed during handoff from MCC/MNC mccmnc (IE type[IE type]) [CellID cellID] to MCC/MNC mccmnc (IE type[IE type]) [CellID cellID]

Explanation
A message appears when the location has changed. MCC is always 3 digits and MNC is 2 or 3 digits. This change could be triggered by handoff or a subsequent create request after the PDP is created and that the previous create request on ASA expired.

Note
The MCC, MNC, IE type, or Cell ID could be "Unknown" if the packet does not contain the location information IEs.

Example:
%ASA-5-324011: Subscriber ID location changed during v1 handoff from MCC/MNC 11122 (v1 RAI/v1 ULI-CGI) CellID 1 to MCC/MNC 111222 (v1 RAI/v1 ULI-CGI) CellID 2
%ASA-5-324011: Subscriber ID location changed during v1 handoff from MCC/MNC 11122 (v2 ULI) CellID 1 to Unknown
%ASA-5-324011: Subscriber ID location changed during v1 handoff from Unknown to MCC/MNC 11122 (v1 RAI) CellID 1

Recommended Action None

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 request authenticator is verified with that secret. If it fails, it is logged and packet processing stops.

• from_addr — The IP address of the host sending the RADIUS accounting request

Recommended Action Check to see that the correct shared secret was configured. If it is, double-check the source of the packet to make sure that it was 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 was not spoofed. If the packet is legitimate, then capture the packet and make sure the header length is incorrect, as indicated by the message. If the header length is correct, and if 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—IPv6 address of the other router
- interface—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—The IPv6 address of the other router
- MAC_address—The MAC address of the other system, if known; otherwise, it is considered unknown.
- interface—The interface name of the link with the other system

Recommended Action Change the IPv6 address of one of the two systems.

325004

Error Message %ASA-4-325004: IPv6 Extension Header hdr_type action configuration. protocol from src_int : src_ipv6_addr / src_port to dst_interface : dst_ipv6_addr / dst_port.

Explanation A user has configured one or multiple actions over the specified IPv6 header extension.

- hdr_type—Can be one of the following values:
  - ah—Configured action over the AH extension header
  - count—Configured action over the number of extension headers
  - destination-option—Configured action over the destination option extension header
  - esp—Configured action over the ESP extension header
  - fragment—Configured action over the fragment extension header
  - hop-by-hop—Configured action over the hop-by-hop extension header
  - routing-address count—Configured action over the number of addresses in the routing extension header
  - routing-type—Configured action over the routing type extension header

- action—Can be one of the following values:
  - denied—The packet is denied.
  - denied/logged—The packet is denied and logged.
  - logged—The packet is logged.
**Recommended Action** If the configured action is not expected, under the `policy-map` command, check the action in the `match header extension_header_type` command and the `parameters` command, and make the correct changes. For example:

```bash
ciscoasa (config)# policy-map type inspect ipv6 pname
ciscoasa (config-pmap)# parameters
   ! to remove the configuration
   ciscoasa (config-pmap-p)# no match header extension_header_type
   ! to remove the configuration
   ciscoasa (config-pmap-p)# no drop ! so packets with the specified extension_header_type are not dropped
   ciscoasa (config-pmap-p)# no log ! so packets with the specified extension_header_type are not logged
   ciscoasa (config-pmap-p)# no drop log ! so packets with the specified extension_header_type are not dropped or logged
```

**325005**

**Error Message** %ASA-4-325005: Invalid IPv6 Extension Header Content: *string*. *detail regarding protocol, ingress and egress interface*

**Explanation** An IPv6 packet with a bad extension header has been detected.

- *string* — Can be one of the following values:
  - wrong extension header order
  - duplicate extension header
  - routing extension header

**Recommended Action** Configure the `capture` command to record the dropped packet, then analyze the cause of the dropped packet. If the validity check of the IPv6 extension header can be ignored, disable the validity check in the IPv6 policy map by entering the following commands:

```bash
ciscoasa (config)# policy-map type inspect ipv6 policy_name
ciscoasa (config-pmap)# parameters
ciscoasa (config-pmap-p)# no verify-header type
```

**325006**

**Error Message** %ASA-4-325006: IPv6 Extension Header not in order: Type *hdr_type* occurs after Type *hdr_type*. TCP *prot* from inside *src_int*: *src_ipv6_addr*/*src_port* to *dst_interface*: *dst_ipv6_addr*/*dst_port*

**Explanation** An IPv6 packet with out-of-order extension headers has been detected.

**Recommended Action** Configure the `capture` command to record the dropped packet, then analyze the extension header order of the dropped packet. If out-of-order header extensions are allowed, disable the out-of-order check in the IPv6 type policy map by entering the following commands:

```bash
ciscoasa (config)# policy-map type inspect ipv6 policy_name
ciscoasa (config-pmap)# parameters
ciscoasa (config-pmap-p)# no verify-header order
```
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. Alternatively, if the number of events queued exceeds a system limit, an attempt to process them will occur at a later time.

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

326002

**Error Message**  %ASA-3-326002: Error in error_message

**Explanation** The IGMP process failed to shut down upon request. Events that are performed in preparation for this shutdown may be out-of-sync.

**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. The probable cause is 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 probable cause 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 specified 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

**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 cannot be found, or because of an 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.
<table>
<thead>
<tr>
<th>Error Message</th>
<th>Explanation</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>%ASA-3-326022: Error in string : string</td>
<td>The PIM process failed to shut down upon request. Events that are performed in preparation for this shutdown may be out-of-sync.</td>
<td>If the problem persists, contact the Cisco TAC.</td>
</tr>
<tr>
<td>%ASA-3-326023: string = IP_address : string</td>
<td>An error occurred while processing a PIM group range.</td>
<td>If the problem persists, contact the Cisco TAC.</td>
</tr>
<tr>
<td>%ASA-3-326024: An internal error occurred while processing a packet queue.</td>
<td>The PIM packet queue received a signal without a packet.</td>
<td>If the problem persists, contact the Cisco TAC.</td>
</tr>
<tr>
<td>%ASA-3-326025: string</td>
<td>An internal error occurred while trying to send a message. Events scheduled to occur on the receipt of a message, such as deletion of the PIM tunnel IDB, may not occur.</td>
<td>If the problem persists, contact the Cisco TAC.</td>
</tr>
<tr>
<td>%ASA-3-326026: Server unexpected error: error_message</td>
<td>The MRIB failed to register a client.</td>
<td>If the problem persists, contact the Cisco TAC.</td>
</tr>
<tr>
<td>%ASA-3-326027: Corrupted update: error_message</td>
<td>The MRIB received a corrupt update.</td>
<td>If the problem persists, contact the Cisco TAC.</td>
</tr>
<tr>
<td>%ASA-3-326028: Asynchronous error: error_message</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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: The IP SLA monitor was unable to start a new process.

Recommended Action: Check the system memory. If memory is low, then this is probably the 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: The IP SLA monitor failed to initialize. This condition is caused by either the timer wheel function failing to initialize or a process not being created. Sufficient memory is probably not available to complete the task.

Recommended Action: Check the system memory. If memory is low, then this is probably the 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: The IP SLA monitor cannot initialize the timer wheel.

Recommended Action: Check the system memory. If memory is low, then the timer wheel function 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 with a check registry is invoked. 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.

328002

Error Message: %ASA-3-328002: Attempt made in string to register with out of bounds key

Explanation: In the FASTCASE registry, the key has to be smaller than the size specified when the registry was created. An attempt was made to register with a key out-of-bounds.
**Recommended Action** Copy the error message exactly as it appears, and report it to the Cisco TAC.

---

### 329001

**Error Message** %ASA-3-329001: The string0 subblock named string1 was not removed

**Explanation** A software error has occurred. 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** The dynamic DNS subsystem failed to update the resource records on the DNS server. This failure might occur if the ASA is unable to contact the DNS server or the 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 that a DNS server is configured and reachable by the ASA. 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) successfully updated in DNS server dns_server_ip

**Explanation** A dynamic DNS update succeeded in the DNS server.

- **type** — The type of resource record, which may 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 has been 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 enough memory is 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 ASA 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 ASA was lost.

- **IP_address**—The IP address of the web cache
- **service_ID**—The WCCP service identifier

**Recommended Action** Verify operation of the 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 includes 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 includes 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 includes a MAC that 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 includes 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 the configuration of the 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** 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 and is therefore not subject to posture validation.

- **host-address** — The IP address of the host in dotted decimal format (for example, 10.1.1.1)
- **oper-sys** — The operating system (for example, 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, 10.1.1.1)

**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, 10.1.1.1)

**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, 10.1.1.1)
Recommended Action Verify the configuration of the Cisco Secure Access Control Server.

335006

Error Message  %ASA-6-335006: NAC Applying ACL: ACL-name - host-address
Explanation The name of the ACL that is 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, 10.1.1.1)
Recommended Action None required.

335007

Error Message  %ASA-7-335007: NAC Default ACL not configured - host-address
Explanation A NAC default ACL has not been configured.
  • host-address —The IP address of the host in dotted decimal format (for example, 10.1.1.1)
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 requires 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, 10.1.1.1)
Recommended Action None required.

335009

Error Message  %ASA-6-335009: NAC Revalidate request by administrative action - host-address
Explanation A NAC Revalidate action was requested by the administrator.
  • host-address —The IP address of the host in dotted decimal format (for example, 10.1.1.1)
Recommended Action None required.
335010

**Error Message**  %ASA-6-335010: NAC Revalidate All request by administrative action - num sessions

**Explanation**  A NAC Revalidate All action 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**  A NAC Revalidate Group action 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**  A NAC Initialize action was requested by the administrator.

* host-address — The IP address of the host in dotted decimal format (for example, 10.1.1.1)

**Recommended Action**  None required.

335013

**Error Message**  %ASA-6-335013: NAC Initialize All request by administrative action - num sessions

**Explanation**  A NAC Initialize All action 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**  A NAC Initialize Group action 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 destination_network stuck-in-active state in EIGRP-\( ddb\_name \) as_num. Cleaning up

**Explanation** The 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 became active.

- destination_network — The route that became 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.

**336002**

**Error Message** %ASA-3-336002: Handle handle_id is not allocated in pool.

**Explanation** The EIGRP router is unable to find the handle for the next hop.

- handle_id — The identity of the missing 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** The DUAL software was unable to allocate a packet buffer. The ASA may be out of memory.

- bytes — Number of bytes in the packet

**Recommended Action** Check to see if the ASA is out of memory by entering the `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** The reference count packet count became 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** The interface is flow blocked for multicast. Qelm is the queue element, and 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 cleanup 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** 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** 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** — 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** 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 may occur 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.

### 336012

**Error Message** %ASA-3-336012: Interface interface_names going down and neighbor_links links exist

**Explanation** An interface is going down or is being removed from routing through IGRP, but not all links (neighbors) have been removed from the topology table.

**Recommended Action** If the problem persists, contact the Cisco TAC.
336013

**Error Message**  %ASA-3-336013: Route iproute, iproute_successors successors, db_successors rdbs

**Explanation**  A hardware or software error occurred.

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

336014

**Error Message**  %ASA-3-336014: “EIGRP_PDM_Process_name, event_log”

**Explanation**  A hardware or software error occurred.

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

336015

**Error Message**  %ASA-3-336015: “Unable to open socket for AS as_number”

**Explanation**  A hardware or software error occurred.

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

336016

**Error Message**  %ASA-3-336016: Unknown timer type timer_type expiration

**Explanation**  A hardware or software error occurred.

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

336019

**Error Message**  %ASA-6-336019: process_name as_number: prefix_source threshold prefix level (prefix_threshold) reached

**Explanation**  The number of prefixes in the topology database has reached the configured or default threshold level. The prefix source may be any of the following:

- Neighbor
- Redistributed
- Aggregate

**Recommended Action**  Use the `show eigrp accounting` command to obtain details about the source of the prefixes and take corrective action.

337000

**Error Message**  %ASA-6-337000: Created BFD session with local discriminator <id> on <real_interface> with neighbor <real_host_ip>

**Explanation**  This syslog message indicates that a BFD active session has been created.
• id— A numerical field that denotes the local discriminator value for a particular BFD session
• real_interface— The interface name if on which the BFD session is running
• real_host_ip— The IP address of the neighbor with which the BFD session has come up

Recommended Action None.

337001

Error Message %ASA-6-337001: Terminated BFD session with local discriminator <id> on <real_interface> with neighbor <real_host_ip> due to <failure_reason>

Explanation This syslog message indicates that an active BFD session has been terminated.

• id— A numerical field that denotes the local discriminator value for a particular BFD session
• real_interface— The interface name if on which the BFD session is running
• real_host_ip— The IP address of the neighbor with which the BFD session has come up
• failure_reason— One of the following failure reasons: BFD going down on peer’s side, BFD configuration removal on peer’s side, Detection timer expiration, Echo function failure, Path to peer going down, Local BFD configuration removal, BFD client configuration removal

Recommended Action None.

337005

Error Message %ASA-4-337005: Phone Proxy SRTP: Media session not found for media_term_ip/media_term_port for packet from in_ifc:src_ip/src_port to out_ifc:dest_ip/dest_port

Explanation The adaptive security appliance received an SRTP or RTP packet that was destined to go to the media termination IP address and port, but the corresponding media session to process this packet was not found.

• 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 this message occurs at the end of the call, it is considered normal because the signaling messages may have released the media session, but the endpoint is continuing to send a few SRTP or RTP packets. If this message occurs for an odd-numbered media termination port, the endpoint is sending RTCP, which must be disabled from the CUCM. If this message happens continuously for a call, debug the signaling message transaction either using phone proxy debug commands or capture commands to determine if the signaling messages are being modified with the media termination IP address and port.

338001

Error Message %ASA-4-338001: Dynamic filter monitored blacklisted protocol traffic from in_interface :src_ip_addr /src_port (mapped-ip /mapped-port) to out_interface :dest_ip_addr /dest_port , (mapped-ip /mapped-port), source malicious address resolved from local or dynamic list: domain name, threat-level: level_value, category: category_name
**Explanation** Traffic from a blacklisted domain in the dynamic filter database has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the `dynamic-filter drop blacklist` command to automatically drop such traffic.

**Error Message** %ASA-4-338002: Dynamic filter monitored blacklisted protocol traffic from in_interface : src_ip_addr / src_port (mapped-ip / mapped-port) to out_interface : dest_ip_addr / dest_port (mapped-ip / mapped-port), destination malicious address resolved from local or dynamic list: domain name, threat-level: level_value, category: category_name

**Explanation** Traffic to a blacklisted domain name in the dynamic filter database has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the `dynamic-filter drop blacklist` command to automatically drop such traffic.

**Error Message** %ASA-4-338003: Dynamic filter monitored blacklisted protocol traffic from in_interface : src_ip_addr / src_port (mapped-ip / mapped-port) to out_interface : dest_ip_addr / dest_port (mapped-ip / mapped-port), source malicious address resolved from local or dynamic list: ip address/netmask, threat-level: level_value, category: category_name

**Explanation** Traffic from a blacklisted IP address in the dynamic filter database has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the `dynamic-filter drop blacklist` command to automatically drop such traffic.

**Error Message** %ASA-4-338004: Dynamic filter monitored blacklisted protocol traffic from in_interface : src_ip_addr / src_port (mapped-ip / mapped-port) to out_interface : dest_ip_addr / dest_port (mapped-ip / mapped-port), destination malicious address resolved from local or dynamic list: ip address/netmask, threat-level: level_value, category: category_name

**Explanation** Traffic to a blacklisted IP address in the dynamic filter database has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the `dynamic-filter drop blacklist` command to automatically drop such traffic.
**338005**

**Error Message** %ASA-4-338005: Dynamic filter dropped blacklisted protocol traffic from
in_interface : src_ip_addr / src_port (mapped-ip / mapped-port ) to out_interface : dest_ip_addr / dest_port (mapped-ip / mapped-port ), source malicious address resolved from local or dynamic list: domain name, threat-level: level_value, category: category_name

**Explanation** Traffic from a black-listed domain name in the dynamic filter database was denied. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).

**Recommended Action** None required.

**338006**

**Error Message** %ASA-4-338006: Dynamic filter dropped blacklisted protocol traffic from
in_interface : src_ip_addr / src_port (mapped-ip / mapped-port ) to out_interface : dest_ip_addr / dest_port (mapped-ip / mapped-port ), destination malicious address resolved from local or dynamic list: domain name, threat-level: level_value, category: category_name

**Explanation** Traffic to a blacklisted domain name in the dynamic filter database was denied. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).

**Recommended Action** None required.

**338007**

**Error Message** %ASA-4-338007: Dynamic filter dropped blacklisted protocol traffic from
in_interface : src_ip_addr / src_port (mapped-ip / mapped-port ) to out_interface : dest_ip_addr / dest_port (mapped-ip / mapped-port ), source malicious address resolved from local or dynamic list: ip address/netmask, threat-level: level_value, category: category_name

**Explanation** Traffic from a blacklisted IP address in the dynamic filter database was denied. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).

**Recommended Action** None required.

**338008**

**Error Message** %ASA-4-338008: Dynamic filter dropped blacklisted protocol traffic from
in_interface : src_ip_addr / src_port (mapped-ip / mapped-port ) to out_interface : dest_ip_addr / dest_port (mapped-ip / mapped-port ), destination malicious address resolved from local or dynamic list: ip address/netmask, threat-level: level_value, category: category_name

**Explanation** Traffic to a blacklisted IP address in the dynamic filter database was denied. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).
Recommended Action None required.

Error Message %ASA-4-338101: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port, (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: domain name

Explanation Traffic from a whitelisted domain in the dynamic filter database has appeared.

Recommended Action None required.

Error Message %ASA-4-338102: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: domain name

Explanation Traffic to a whitelisted domain name in the dynamic filter database has appeared.

Recommended Action None required.

Error Message %ASA-4-338103: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port, (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: ip address/netmask

Explanation Traffic from a whitelisted IP address in the dynamic filter database has appeared.

Recommended Action None required.

Error Message %ASA-4-338104: Dynamic filter action whitelisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port, (mapped-ip/mapped-port), destination malicious address resolved from local or dynamic list: ip address/netmask

Explanation Traffic to a whitelisted IP address in the dynamic filter database has appeared.

Recommended Action None required.

Error Message %ASA-4-338201: Dynamic filter monitored greylisted protocol traffic from in_interface:src_ip_addr/src_port (mapped-ip/mapped-port) to out_interface:dest_ip_addr/dest_port, (mapped-ip/mapped-port), source malicious address resolved from local or dynamic list: domain name, threat-level: level_value, category: category_name
Explanation Traffic from a greylisted domain in the dynamic filter database has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).

Recommended Action Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the `dynamic-filter drop blacklist` command and the `dynamic-filter ambiguous-is-black` command to automatically drop such traffic.

338202

Error Message %ASA-4-338202: Dynamic filter monitored greylisted protocol traffic from in_interface:src_ip_addr /src_port (mapped-ip /mapped-port ) to out_interface:dest_ip_addr /dest_port (mapped-ip /mapped-port ), destination malicious address resolved from local or dynamic list: domain name, threat-level: level_value, category: category_name

Explanation Traffic to a greylisted domain name in the dynamic filter database has appeared. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).

Recommended Action Access to a malicious site has been logged. Use the internal IP address to trace the infected machine, or enter the `dynamic-filter drop blacklist` command and the `dynamic-filter ambiguous-is-black` command to automatically drop such traffic.

338203

Error Message %ASA-4-338203: Dynamic filter dropped greylisted protocol traffic from in_interface:src_ip_addr /src_port (mapped-ip /mapped-port ) to out_interface:dest_ip_addr /dest_port (mapped-ip /mapped-port ), source malicious address resolved from local or dynamic list: domain name, threat-level: level_value, category: category_name

Explanation Traffic from a greylisted domain name in the dynamic filter database was denied; however, the malicious IP address was also resolved to domain names that are unknown to the dynamic filter database. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).

Recommended Action Access to a malicious site was dropped. If you do not want to automatically drop greylisted traffic whose IP address matches both blacklisted domain names and unknown domain names, disable the `dynamic-filter ambiguous-is-black` command.

338204

Error Message %ASA-4-338204: Dynamic filter dropped greylisted protocol traffic from in_interface:src_ip_addr /src_port (mapped-ip /mapped-port ) to out_interface:dest_ip_addr /dest_port (mapped-ip /mapped-port ), destination malicious address resolved from local or dynamic list: domain name, threat-level: level_value, category: category_name

Explanation Traffic to a greylisted domain name in the dynamic filter database was denied; however, the malicious IP address was also resolved to domain names that are unknown to the dynamic filter database. The threat level is a string that shows one of the following values: none, very-low, low, moderate, high, and
very-high. The category is a string that shows the reason why a domain name is blacklisted (for example, botnet, Trojan, and spyware).

**Recommended Action** Access to a malicious site was dropped. If you do not want to automatically drop greylisted traffic whose IP address matches both blacklisted domain names and unknown domain names, disable the `dynamic-filter ambiguous-is-black` command.

### 338301

**Error Message** %ASA-4-338301: Intercepted DNS reply for domain name from in_interface :src_ip_addr /src_port to out_interface :dest_ip_addr /dest_port , matched list

**Explanation** A DNS reply that was present in an administrator whitelist, blacklist, or IronPort list was intercepted.

- **name** — The domain name
- **list** — The list that includes the domain name, administrator whitelist, blacklist, or IronPort list

**Recommended Action** None required.

### 338302

**Error Message** %ASA-5-338302: Address ipaddr discovered for domain name from list , Adding rule

**Explanation** An IP address that was discovered from a DNS reply to the dynamic filter rule table was added.

- **ipaddr** — The IP address from the DNS reply
- **name** — The domain name
- **list** — The list that includes the domain name, administrator blacklist, blacklist, or IronPort list

**Recommended Action** None required.

### 338303

**Error Message** %ASA-5-338303: Address ipaddr (name) timed out, Removing rule

**Explanation** An IP address that was discovered from the dynamic filter rule table was removed.

- **ipaddr** — The IP address from the DNS reply
- **name** — The domain name

**Recommended Action** None required.

### 338304

**Error Message** %ASA-6-338304: Successfully downloaded dynamic filter data file from updater server url

**Explanation** A new version of the data file has been downloaded.

- **url** — The URL of the updater server

**Recommended Action** None required.
338305

Error Message  %ASA-3-338305: Failed to download dynamic filter data file from updater server

url

Explanation The dynamic filter database has failed to download.

  • url —The URL of the updater server

Recommended Action Make sure that you have a DNS configuration on the ASA so that the updater server URL can be resolved. If you cannot ping the server from the ASA, check with your network administrator for the correct network connection and routing configuration. If you are still having problems, contact the Cisco TAC.

338306

Error Message  %ASA-3-338306: Failed to authenticate with dynamic filter updater server

url

Explanation The ASA failed to authenticate with the dynamic filter updater server.

  • url —The URL of the updater server

Recommended Action Contact the Cisco TAC.

338307

Error Message  %ASA-3-338307: Failed to decrypt downloaded dynamic filter database file

Explanation The downloaded dynamic filter database file failed to decrypt.

Recommended Action Contact the Cisco TAC.

338308

Error Message  %ASA-5-338308: Dynamic filter updater server dynamically changed from

old_server_host : old_server_port to new_server_host : new_server_port

Explanation The ASA was directed to a new updater server host or port.

  • old_server_host : old_server_port —The previous updater server host and port
  • new_server_host : new_server_port —The new updater server host and port

Recommended Action None required.

338309

Error Message  %ASA-3-338309: The license on this ASA does not support dynamic filter updater feature.

Explanation The dynamic filter updater is a licensed feature; however, the license on the ASA does not support this feature.

Recommended Action None required.
**338310**

**Error Message** %ASA-3-338310: Failed to update from dynamic filter updater server url, reason: reason string

**Explanation** The ASA failed to receive an update from the dynamic filter updater server.

- `url` — The URL of the updater server
- `reason string` — The reason for the failure, which can be one of the following:
  - Failed to connect to updater server
  - Received invalid server response
  - Received invalid server manifest
  - Error in stored update file information
  - Script error
  - Function call error
  - Out of memory

**Recommended Action** Check the network connection to the server. Try to ping the server URL, which is shown in the output of the `show dynamic-filter updater-client` command. Make sure that the port is allowed through your network. If the network connection is not the problem, contact your network administrator.

---

**339001**

**Error Message** %ASA-3-339001: DNSCrypt certificate update failed for <num_tries> tries

**Explanation** The DNSCrypt failed to receive a certificate update.

- `num_tries` — The number of times DNSCrypt failed to get a certificate update

**Recommended Action** Check for the following:

- If the route is setup for the Umbrella server.
- If the Umbrella server egress interface is up.
- If the correct Provider public key is used.

---

**339002**

**Error Message** %ASA-3-339002: Umbrella device registration failed with error code <err_code>

**Explanation** The umbrella device registration failed.

- `err_code` — The error code returned from the Umbrella Server.

**Recommended Action** If the error code is:

- 400 – There is a problem with the request format or content. The token is probably too short or corrupted. Verify if the token matches what is on the Umbrella Dashboard.

- 401 – The token is not authorized. If the token was refreshed on the Umbrella Dashboard, then the new token should be updated on ASA.
• 409 – The device id is conflicting with another organization. Contact the Umbrella Server Administrator.
• 500 – There is an internal server error. Contact the Umbrella Server Administrator.

339003

**Error Message** %ASA-3-339003: Umbrella device registration was successful

**Explanation** Successful message for the umbrella device registration.

**Recommended Action** None.

339004

**Error Message** %ASA-3-339004: Umbrella device registration failed due to missing token

**Explanation** Umbrella device registration failed due to missing token.

**Recommended Action** Make sure the token is configured under the global “umbrella” submode.

339005

**Error Message** %ASA-3-339005: Umbrella device registration failed after <num_tries> retries

**Explanation** Umbrella device registration failed.

- **num_tries**— The number of times the device failed to register with the Umbrella Server.

**Recommended Action** Locate the error code in the syslog 339002 message. Refer the workaround for the 339002 syslog message and fix.

339006

**Error Message** %ASA-3-339006: Umbrella resolver current resolver ipv46 is reachable, resuming Umbrella redirect.

**Explanation** Umbrella had failed to open, and the resolver was unreachable. The resolver is now reachable and service is resumed.

**Recommended Action** None.

339007

**Error Message** %ASA-3-339007: Umbrella resolver current resolver ipv46 is unreachable, moving to fail-open. Starting probe to resolver.

**Explanation** Umbrella fail-open has been configured and a resolver unreachability has been detected.

**Recommended Action** Check the network settings for reachability to the Umbrella resolvers.
**339008**

**Error Message** %ASA-3-339008: Umbrella resolver current resolver ipv46 is unreachable, moving to fail-close.

**Explanation** Umbrella fail-open has NOT been configured and a resolver unreachableity has been detected.

**Recommended Action** Check the network settings for reachability to the Umbrella resolvers.

---

**340001**

**Error Message** %ASA-3-340001: Loopback-proxy error: error_string context id context_id, context_type = version / request_type / address_type client socket (internal)= client_address_internal / client_port_internal server socket (internal)= server_address_internal / server_port_internal server socket (external)= server_address_external / server_port_external remote socket (external)= remote_address_external / remote_port_external

**Explanation** Loopback proxy allows third-party applications running on the ASA to access the network. The loopback proxy encountered an error.

- **context_id**—A unique, 32-bit context ID that is generated for each loopback client proxy request
- **version**—The protocol version
- **request_type**—The type of request, which can be one of the following: TC (TCP connection), TB (TCP bind), or UA (UDP association)
- **address_type**—The types of addresses, which can be one of the following: IP4 (IPv4), IP6 (IPv6), or DNS (domain name service)
- **client_address_internal/server_address_internal**—The addresses that the loopback client and the loopback server used for communication
- **client_port_internal/server_port_internal**—The ports that the loopback client and the loopback server used for communication
- **server_address_external/remote_address_external**—The addresses that the loopback server and the remote host used for communication
- **server_port_external/remote_port_external**—The ports that the loopback server and the remote host used for communication
- **error_string**—The error string that may help troubleshoot the problem

**Recommended Action** Copy the syslog message and contact the Cisco TAC.

---

**340002**

**Error Message** %ASA-6-340002: Loopback-proxy info: error_string context id context_id, context_type = version / request_type / address_type client socket (internal)= client_address_internal / client_port_internal server socket (internal)= server_address_internal / server_port_internal server socket (external)= server_address_external / server_port_external remote socket (external)= remote_address_external / remote_port_external

**Explanation** Loopback proxy allows third-party applications running on the ASA to access the network. The loopback proxy generated debugging information for use in troubleshooting.

- **context_id**—A unique, 32-bit context ID that is generated for each loopback client proxy request
• version — The protocol version
• request_type — The type of request, which can be one of the following: TC (TCP connection), TB (TCP bind), or UA (UDP association)
• address_type — The types of addresses, which can be one of the following: IP4 (IPv4), IP6 (IPv6), or DNS (domain name service)
• client_address_internal/server_address_internal — The addresses that the loopback client and the loopback server used for communication
• client_port_internal/server_port_internal — The ports that the loopback client and the loopback server used for communication
• server_address_external/remote_address_external — The addresses that the loopback server and the remote host used for communication
• server_port_external/remote_port_external — The ports that the loopback server and the remote host used for communication
• error_string — The error string that may help troubleshoot the problem

Recommended Action Copy the syslog message and contact the Cisco TAC.

341001

Error Message %ASA-6-341001: Policy Agent started successfully for VNMC vnmc_ip_addr
Explanation The policy agent processes (DME, ducatiAG, and commonAG) started successfully.
• vnmc_ip_addr — The IP address of the VNMC server

Recommended Action None.

341002

Error Message %ASA-6-341002: Policy Agent stopped successfully for VNMC vnmc_ip_addr
Explanation The policy agent processes (DME, ducatiAG, and commonAG) were stopped.
• vnmc_ip_addr — The IP address of the VNMC server

Recommended Action None.

341003

Error Message %ASA-3-341003: Policy Agent failed to start for VNMC vnmc_ip_addr
Explanation The policy agent failed to start.
• vnmc_ip_addr — The IP address of the VNMC server

Recommended Action Check for console history and the disk0:/pa/log/vnm_pa_error_status for error messages. To retry starting the policy agent, issue the registration host command again.

341004

Error Message %ASA-3-341004: Storage device not available: Attempt to shutdown module $s failed.
**Explanation** All SSDs have failed or been removed with the system in Up state. The system has attempted to shut down the software module, but that attempt has failed.

- %s — The software module (for example, cxsc)

**Recommended Action** Replace the removed or failed drive and reload the ASA.

---

**341005**

**Error Message** %ASA-3-341005: Storage device not available. Shutdown issued for module %s.

**Explanation** All SSDs have failed or been removed with the system in Up state. The system is shutting down the software module.

- %s — The software module (for example, cxsc)

**Recommended Action** Replace the removed or failed drive and reload the software module.

---

**341006**

**Error Message** %ASA-3-341006: Storage device not available. Failed to stop recovery of module %s.

**Explanation** All SSDs have failed or been removed with the system in recovery state. The system attempted to stop the recovery, but that attempt failed.

- %s — The software module (for example, cxsc)

**Recommended Action** Replace the removed or failed drive and reload the ASA.

---

**341007**

**Error Message** %ASA-3-341007: Storage device not available. Further recovery of module %s was stopped. This may take several minutes to complete.

**Explanation** All SSDs have failed or been removed with the system in recovery state. The system is stopping the recovery of the software module.

- %s — The software module (for example, cxsc)

**Recommended Action** Replace the removed or failed drive and reload the software module.

---

**341008**

**Error Message** %ASA-3-341008: Storage device not found. Auto-boot of module %s cancelled. Install drive and reload to try again.

**Explanation** After getting the system into Up state, all SSDs have failed or been removed before reloading the system. Because the default action during boot is to auto-boot the software module, that action is blocked because there is no storage device available.

**Recommended Action** Replace the removed or failed drive and reload the software module.
**341010**

**Error Message** %ASA-6-341010: Storage device with serial number `ser_no` [inserted into | removed from] bay `bay_no`

**Explanation** The ASA has detected insertion or removal events and generates this syslog message immediately.

**Recommended Action** None required.

**341011**

**Error Message** %ASA-3-341011: Storage device with serial number `ser_no` in bay `bay_no` faulty.

**Explanation** The ASA polls the hard disk drive (HDD) health status every 10 minutes and generates this syslog message if the HDD is in a failed state.

**Recommended Action** None required.

**342001**

**Error Message** %ASA-7-342001: REST API Agent started successfully.

**Explanation** The REST API Agent must be successfully started before a REST API Client can configure the ASA.

**Recommended Action** None.

**342002**

**Error Message** %ASA-3-342002: REST API Agent failed, reason: `reason`

**Explanation** The REST API Agent could fail to start or crash for various reasons, and the reason is specified.

- `reason` — The cause for the REST API failure

**Recommended Action** The actions taken to resolve the issue vary depending on the reason logged. For example, the REST API Agent crashes when the Java process runs out of memory. If this occurs, you need to restart the REST API Agent. If the restart is not successful, contact the Cisco TAC to identify the root cause fix.

**342003**

**Error Message** %ASA-3-342003: REST API Agent failure notification received. Agent will be restarted automatically.

**Explanation** A failure notification from the REST API Agent has been received and a restart of the Agent is being attempted.

**Recommended Action** None.
### 342004

**Error Message** %ASA-3-342004: Failed to automatically restart the REST API Agent after 5 unsuccessful attempts. Use the 'no rest-api agent' and 'rest-api agent' commands to manually restart the Agent.

**Explanation** The REST API Agent has failed to start after many attempts.

**Recommended Action** See syslog %ASA-3-342002 (if logged) to better understand the reason behind the failure. Try to disable the REST API Agent by entering the **no rest-api agent** command and re-enable the REST API Agent using the **rest-api agent** command.

---

### 342005

**Error Message** %ASA-7-342005: REST API image has been installed successfully.

**Explanation** The REST API image must be successfully installed before starting the REST API Agent.

**Recommended Action** None.

---

### 342006

**Error Message** %ASA-3-342006: Failed to install REST API image, reason: <reason>.

**Explanation** The REST API image installation may fail, for one of the following reasons: version check failed, image verification failed, image file not found, out of space on flash or mount failed.

**Recommended Action** The administrator should fix the failure and try to install the image again using 'rest-api image <image>'.

---

### 342007

**Error Message** %ASA-7-342007: REST API image has been uninstalled successfully.

**Explanation** The old REST API image must be successfully uninstalled before a new one can be installed.

**Recommended Action** None.

---

### 342008

**Error Message** %ASA-3-342008: Failed to uninstall REST API image, reason: <reason>.

**Explanation** The REST API image could not be uninstalled for the following reasons- unmount failed or REST Agent is enabled.

**Recommended Action** The administrator should disable the REST Agent, before trying to uninstall the REST API image.