Syslog Messages 400000 to 450001

This chapter contains the following sections:

Messages 400000 to 409128

This chapter includes messages from 400000 to 409128.

4000nn

Error Message `%ASA-4-4000nn: IPS:`*`number string`* `from` *`IP_address`* `to` *`IP_address`* `on interface` *`interface_name`*

Explanation Messages 400000 through 400051 are Cisco Intrusion Prevention Service signature messages.

Recommended Action See the Cisco Intrusion Prevention Service User Guide on Cisco.com.

Not all signature messages are supported by the ASA in this release. IPS messages all start with 4-4000nn and have the following format:

number	The signature number. For more information, see the Cisco Intrusion Prevention Service User Guide on Cisco.com.
string	The signature message—approximately the same as the NetRanger signature message.
IP_address	The local to remote address to which the signature applies.
interface_name	The name of the interface on which the signature originated.

For example:

```
%ASA-4-400013 IPS:2003 ICMP redirect from 10.4.1.2 to 10.2.1.1 on interface dmz
%ASA-4-400032 IPS:4051 UDP Snork attack from 10.1.1.1 to 192.168.1.1 on interface outside
```

The following table lists the supported signature messages.

Table 1: IPS Syslog Messages

Message Number	Signature ID	Signature Title	Signature Type
400000	1000	IP options-Bad Option List	Informational
400001	1001	IP options-Record Packet Route	Informational
400002	1002	IP options-Timestamp	Informational
400003	1003	IP options-Security	Informational
400004	1004	IP options-Loose Source Route	Informational
400005	1005	IP options-SATNET ID	Informational
400006	1006	IP options-Strict Source Route	Informational
400007	1100	IP Fragment Attack	Attack
400008	1102	IP Impossible Packet	Attack
400009	1103	IP Fragments Overlap	Attack
400010	2000	ICMP Echo Reply	Informational
400011	2001	ICMP Host Unreachable	Informational
400012	2002	ICMP Source Quench	Informational
400013	2003	ICMP Redirect	Informational
400014	2004	ICMP Echo Request	Informational
400015	2005	ICMP Time Exceeded for a Datagram	Informational
400016	2006	ICMP Parameter Problem on Datagram	Informational
400017	2007	ICMP Timestamp Request	Informational
400018	2008	ICMP Timestamp Reply	Informational
400019	2009	ICMP Information Request	Informational
400020	2010	ICMP Information Reply	Informational
400021	2011	ICMP Address Mask Request	Informational
400022	2012	ICMP Address Mask Reply	Informational
400023	2150	Fragmented ICMP Traffic	Attack
400024	2151	Large ICMP Traffic	Attack
400025	2154	Ping of Death Attack	Attack
400026	3040	TCP NULL flags	Attack

Message Number	Signature ID	Signature Title	Signature Type
400027	3041	TCP SYN+FIN flags	Attack
400028	3042	TCP FIN only flags	Attack
400029	3153	FTP Improper Address Specified	Attack
400030	3154	FTP Improper Port Specified	Attack
400031	4050	UDP Bomb attack	Attack
400032	4051	UDP Snork attack	Attack
400033	4052	UDP Chargen DoS attack	Attack
400034	6050	DNS HINFO Request	Informational
400035	6051	DNS Zone Transfer	Informational
400036	6052	DNS Zone Transfer from High Port	Informational
400037	6053	DNS Request for All Records	Informational
400038	6100	RPC Port Registration	Informational
400039	6101	RPC Port Unregistration	Informational
400040	6102	RPC Dump	Informational
400041	6103	Proxied RPC Request	Attack
400042	6150	ypserv (YP server daemon) Portmap Request	Informational
400043	6151	ypbind (YP bind daemon) Portmap Request	Informational
400044	6152	yppasswdd (YP password daemon) Portmap Request	Informational
400045	6153	ypupdated (YP update daemon) Portmap Request	Informational
400046	6154	ypxfrd (YP transfer daemon) Portmap Request	Informational
400047	6155	mountd (mount daemon) Portmap Request	Informational
400048	6175	rexd (remote execution daemon) Portmap Request	Informational
400049	6180	rexd (remote execution daemon) Attempt	Informational
400050	6190	statd Buffer Overflow	Attack

401001

Error Message `%ASA-4-401001: Shuns cleared`

Explanation The **clear shun** command was entered to remove existing shuns from memory. An institution to keep a record of shunning activity was allowed.

Recommended Action None required.

401002

Error Message `%ASA-4-401002: Shun added: IP_address IP_address port port`

Explanation A **shun** command was entered, where the first IP address is the shunned host. The other addresses and ports are optional and are used to terminate the connection if available. An institution to keep a record of shunning activity was allowed.

Recommended Action None required.

401003

Error Message `%ASA-4-401003: Shun deleted: IP_address`

ExplanationA single shunned host was removed from the shun database. An institution to keep a record of shunning activity was allowed.

Recommended Action None required.

401004

Error Message `%ASA-4-401004: Shunned packet: IP_address ==> IP_address on interface interface_name`

ExplanationA packet was dropped because the host defined by IP SRC is a host in the shun database. A shunned host cannot pass traffic on the interface on which it is shunned. For example, an external host on the Internet can be shunned on the outside interface. A record of the activity of shunned hosts was provided. This message and message %ASA-4-401005 can be used to evaluate further risk concerning this host.

Recommended Action None required.

401005

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

ExplanationThe Secure Firewall ASA is out of memory; a shun cannot be applied.

Recommended Action The Cisco IPS should continue to attempt to apply this rule. Try to reclaim memory and reapply a shun manually, or wait for the Cisco IPS to do this.

402114

Error Message `%ASA-4-402114: IPSEC: Received an protocol packet (SPI= spi, sequence number= seq_num) from remote_IP to local_IP with an invalid SPI.`

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index

- seq_num>— IPsec sequence number
- remote_IP>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local_IP>— IP address of the local endpoint of the tunnel

ExplanationAn IPsec packet was received that specifies an SPI that does not exist in the SA database. This may be a temporary condition caused by slight differences in aging of SAs between the IPsec peers, or it may be because the local SAs have been cleared. It may also indicate incorrect packets sent by the IPsec peer, which may be part of an attack. This message is rate limited to no more than one message every five seconds.

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

402115

Error Message `%ASA-4-402115: IPSEC: Received a packet from remote_IP to local_IP containing act_prot data instead of exp_prot data.`

Explanation An IPsec packet was received that is missing the expected ESP header. The peer is sending packets that do not match the negotiated security policy, which may indicate an attack. This message is rate limited to no more than one message every five seconds.

- remote_IP>— IP address of the remote endpoint of the tunnel
- local_IP>— IP address of the local endpoint of the tunnel
- >*act_prot*— Received IPsec protocol
- >*exp_prot*— Expected IPsec protocol

Recommended Action Contact the administrator of the peer.

402116

Error Message `%ASA-4-402116: IPSEC: Received an protocol packet (SPI=spi , sequence number=seq_num) from remote_IP (username) to local_IP . The decapsulated inner packet doesn't match the negotiated policy in the SA. The packet specifies its destination as pkt_daddr , its source as pkt_saddr , and its protocol as pkt_prot . The SA specifies its local proxy as id_daddr /id_dmask /id_dprot /id_dport and its remote proxy as id_saddr /id_smask /id_sprot /id_sport .`

ExplanationA decapsulated IPsec packet does not match the negotiated identity. The peer is sending other traffic through this security association, which may be caused by a security association selection error by the peer, or it may be part of an attack. This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq_num>— IPsec sequence number
- remote_IP>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local_IP>— IP address of the local endpoint of the tunnel
- pkt_daddr>— Destination address from the decapsulated packet

- pkt_saddr>— Source address from the decapsulated packet
- pkt_prot>— Transport protocol from the decapsulated packet
- id_daddr>— Local proxy IP address
- id_dmask>— Local proxy IP subnet mask
- id_dprot>— Local proxy transport protocol
- id_dport>— Local proxy port
- id_saddr>— Remote proxy IP address
- id_smask>— Remote proxy IP subnet mask
- id_sprot>— Remote proxy transport protocol
- id_sport>— Remote proxy port

Recommended Action Contact the administrator of the peer and compare policy settings.

402117

Error Message `%ASA-4-402117: IPSEC: Received a non-IPSec packet (protocol= protocol) from remote_IP to local_IP.`

ExplanationThe received packet matched the crypto map ACL, but it is not IPsec-encapsulated. The IPsec peer is sending unencapsulated packets. This error can occur because of a policy setup error on the peer. For example, the firewall may be configured to only accept encrypted Telnet traffic to the outside interface port 23. If you attempt to use Telnet without IPsec encryption to access the outside interface on port 23, this message appears, but not with Telnet or traffic to the outside interface on ports other than 23. This error can also indicate an attack. This message is not generated except under these conditions (for example, it is not generated for traffic to the Secure Firewall ASA interfaces themselves). See messages 710001, 710002, and 710003, which track TCP and UDP requests. This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- remote_IP>— IP address of the remote endpoint of the tunnel
- local_IP>— IP address of the local endpoint of the tunnel

Recommended Action Contact the administrator of the peer to compare policy settings.

402118

Error Message `%ASA-4-402118: IPSEC: Received an protocol packet (SPI= spi, sequence number= seq_num) from remote_IP (user= username) to local_IP containing an illegal IP fragment of length frag_len with offset frag_offset.`

Explanation A decapsulatd IPsec packet included an IP fragment with an offset less than or equal to 128 bytes. The latest version of the security architecture for IP RFC recommends 128 bytes as the minimum IP fragment offset to prevent reassembly attacks. This may be part of an attack. This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq_num>— IPsec sequence number
- remote_IP>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local_IP>— IP address of the local endpoint of the tunnel

- frag_len>— IP fragment length
- frag_offset>— IP fragment offset in bytes

Recommended Action Contact the administrator of the remote peer to compare policy settings.

402119

Error Message `%ASA-4-402119: IPSEC: Received an protocol packet (SPI= spi, sequence number= seq_num) from remote_IP (user= username) to local_IP that failed anti-replay checking.`

ExplanationAn IPsec packet was received with an invalid sequence number. The peer is sending packets including sequence numbers that may have been previously used. This message indicates that an IPsec packet has been received with a sequence number outside of the acceptable window. This packet will be dropped by IPsec as part of a possible attack. This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq_num>— IPsec sequence number
- remote_IP>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local_IP>— IP address of the local endpoint of the tunnel

Recommended Action Contact the administrator of the peer.

402120

Error Message `%ASA-4-402120: IPSEC: Received an protocol packet (SPI= spi, sequence number= seq_num) from remote_IP (user= username) to local_IP that failed authentication.`

Explanation An IPsec packet was received and failed authentication. The packet is dropped. The packet may have been corrupted in transit, or the peer may be sending invalid IPsec packets, which may indicate an attack if many of these packets were received from the same peer. This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq_num>— IPsec sequence number
- remote_IP>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local_IP>— IP address of the local endpoint of the tunnel

Recommended Action Contact the administrator of the remote peer if many failed packets were received.

402121

Error Message `%ASA-4-402121: IPSEC: Received an protocol packet (SPI= spi, sequence number= seq_num) from peer_addr (user= username) to lcl_addr that was dropped by IPSec (drop_reason).`

Explanation An IPsec packet to be decapsulated was received and subsequently dropped by the IPsec subsystem. This may indicate a problem with the Secure Firewall ASA configuration or with the Secure Firewall ASA itself.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq_num>— IPsec sequence number
- peer_addr>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- lcl_addr>— IP address of the local endpoint of the tunnel
- drop_reason>— Reason that the packet was dropped

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

402122

Error Message `%ASA-4-402122: IPSEC: Received a cleartext packet from src_addr to dest_addr that was to be encapsulated in IPSec that was dropped by IPSec (drop_reason).`

Explanation A packet to be encapsulated in IPsec was received and subsequently dropped by the IPsec subsystem. This may indicate a problem with the Secure Firewall ASA configuration or with the Secure Firewall ASA itself.

- *src_addr* >— Source IP address
- *dest_addr* >— Destination> IP address
- drop_reason>— Reason that the packet was dropped

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

402123

Error Message `%ASA-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (eror_type, code= error_string) while executing the command command_name (command).`

Explanation An error was detected while running a crypto command with a hardware accelerator, which may indicate a problem with the accelerator. This type of error may occur for a variety of reasons, and this message supplements the crypto accelerator counters to help determine the cause.

- accel_type—Hardware accelerator type
- >*error_string*— Code indicating the type of error
- command—Crypto command that generated the error

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

402124

Error Message-1 `%ASA-4-402124: CRYPTO: The platform hardware accelerator encountered an error (HWErrAddr= 0xerror_address, Core= error_core, HwErrCode= error_code, IstatReg= 0xIstat, PciErrReg= 0xPCI, CoreErrStat= 0xcore_error_stat, CoreErrAddr= 0xcore_err_address, Doorbell Size[0]= size, DoorBell Outstanding[0]= outstanding, Doorbell Size[1]= size, DoorBell Outstanding[1]= outstanding, SWReset= Reset_code)`

Error Message-2 `%ASA-4-402124: CRYPTO: The platform hardware accelerator encountered an error (HWErrAddr= 0xerror_address, Core= error_core, HwErrCode= error_code, Queue= queue_string (0), IstatReg= 0xIstat, Station= core_station, CoreRptr= 0xcore_pointer, CoreConfig= 0xcore_config_pointer, SWReset= Reset_code)`

Explanation The crypto hardware chip has reported a fatal error, indicating that the chip is inoperable. The information from this message captures the details to allow further analysis of the problem. The crypto chip is reset when this condition is detected to unobtrusively allow the Secure Firewall ASA to continue functioning. Also, the crypto environment at the time this issue is detected is written to a crypto archive directory on flash to provide further debugging information. Various parameters related to the crypto hardware are included in this message, as follows:

- HWErrAddr>— Hardware address (set by crypto chip)
- Core>— Crypto core experiencing the error
- HwErrCode>— Hardware error code (set by crypto chip)
- IstatReg>— Interrupt status register (set by crypto chip)
- PciErrReg>— PCI error register (set by crypto chip)
- CoreErrStat>— Core error status (set by crypto chip)
- CoreErrAddr>— Core error address (set by crypto chip)
- Doorbell Size>— Maximum crypto commands allowed
- DoorBell Outstanding>— Crypto commands outstanding
- SWReset>— Number of crypto chip resets since boot

Note The %ASA-vpn-4-402124: CRYPTO: The ASA hardware accelerator encountered an error (HWErrAddr= 0x40EE9800, Core= 0, HwErrCode= 23, IstatReg= 0x8, PciErrReg= 0x0, CoreErrStat= 0x41, CoreErrAddr= 0x844E9800, Doorbell Size[0]= 2048, DoorBell Outstanding[0]= 0, Doorbell Size[1]= 0, DoorBell Outstanding[1]= 0, SWReset= 99) error message indicates a AnyConnect problem and the workaround for this to upgrade to AnyConnect 3.1.x.

Recommended Action Forward the message information to the Cisco TAC for further analysis.

402125

Error Message-1 `%ASA-4-402125: CRYPTO: The platform hardware accelerator ring_string ring timed out (Desc= 0xdescriptor_address, CtrlStat= 0xcontrol_or_status value, ResultP= 0xsuccess_pointer, ResultVal= success_value, Cmd= 0xcrypto_command, CmdSize= command_size, Param= 0xcommand_parameters, Dlen= Data_length, DataP= 0xData_pointer, CtxtP= 0xVPN_context_pointer, SWReset= reset_number)`

Explanation The crypto driver has detected that either the IPSEC descriptor ring or SSL/Admin descriptor ring is no longer progressing, meaning the crypto chip no longer appears to be functioning. The crypto chip is reset when this condition is detected to unobtrusively allow the Secure Firewall ASA to continue functioning. Also, the crypto environment at the time this issue was detected was written to a crypto archive directory on flash to provide further debugging information.

- >*ring*— IPSEC or Admin ring
- *parameters* >— Include the following:

- Desc>— Descriptor address

- CtrlStat>— Control/status value

- ResultP>— Success pointer

- ResultVal>— Success value

- Cmd>— Crypto command

- CmdSize>— Command size

- Param>— Command parameters

- Dlen>— Data length

- DataP>— Data pointer

- CtxtP>— VPN context pointer

- SWReset>— Number of crypto chip resets since boot

Recommended Action Forward the message information to the Cisco TAC for further analysis.

402126

Error Message `%ASA-4-402126: CRYPTO: The platform created Crypto Archive File <Archive_Filename> as a Soft Reset was necessary. Please forward this archived information to Cisco`

Explanation A functional problem with the hardware crypto chip was detected (see syslog messages 402124 and 402125). To further debug the crypto problem, a crypto archive file was generated that included the current crypto hardware environment (hardware registers and crypto description entries). At boot time, a crypto_archive directory was automatically created on the flash file system (if it did not exist previously). A maximum of two crypto archive files are allowed to exist in this directory.

- >*Archive Filename*— The name of the crypto archive file name. The crypto archive file names are of the form, crypto_arch_x.bin, where x = (1 or 2).

Recommended Action Forward the crypto archive files to the Cisco TAC for further analysis.

402127

Error Message `%ASA-4-402127: CRYPTO: The platform is skipping the writing of latest Crypto Archive File as the maximum # of files ( max_number ) allowed have been written to <archive_directory>. Please archive remove files from < Archive Directory > if you want more Crypto Archive Files saved`

Explanation A functional problem with the hardware crypto chip was detected (see messages 4402124 and 4402125). This message indicates a crypto archive file was not written, because the maximum number of crypto archive files already existed.

- *max_number* >— Maximum number of files allowed in the archive directory; currently set to two
- >*archive_directory*— Name of the archive directory

Recommended Action Forward previously generated crypto archive files to the Cisco TAC. Remove the previously generated archive file(s) so that more can be written (if deemed necessary).

402128

Error Message `%ASA-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: size, limit: limit.`

Explanation An SSL connection is attempting to use more memory than allowed. The request has been denied.

- *size* —The size of the memory block being allocated
- *limit* —The maximum size of allocated memory permitted

Recommended Action If this message persists, an SSL denial of service attack may be in progress. Contact the remote peer administrator or upstream provider.

402129

Error Message `%ASA-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: address.`

Explanation An internal software error has occurred.

- *address* —The address being freed

Recommended Action Contact the Cisco TAC for assistance.

402130

Error Message `%ASA-6-402130: CRYPTO: Received an ESP packet (SPI = xxxxxxxxxx, sequence number=xxxx) from 172.16.0.1 (user=user) to 192.168.0.2 with incorrect IPsec padding.`

Explanation The Secure Firewall ASA crypto hardware accelerator detected an IPsec packet with invalid padding. The ATT VPN client sometimes pads IPsec packets incorrectly.

- *SPI* —The SPI associated with the packet
- *sequence number* —The sequence number associated with the packet
- *user* —Username string
- *padding* —Padding data from the packet

Recommended Action While this message is None required and does not indicate a problem with the Secure Firewall ASA, customers using the ATT VPN client may wish to upgrade their VPN client software.

402131

Error Message `%ASA-4-402131: CRYPTO: status changing the accel_instance hardware accelerator's configuration bias from old_config_bias to new_config_bias.`

Explanation The hardware accelerator configuration has been changed on the Secure Firewall ASA. Some Secure Firewall ASA platforms have multiple hardware accelerators. One syslog message is generated for each hardware accelerator change.

- *status* —Indicates success or failure
- *accel_instance* —The instance of the hardware accelerator
- *old_config_bias* —The old configuration
- *new_config_bias* —The new configuration

Recommended Action If any of the accelerators fails when attempting to change its configuration, collect logging information and contact the Cisco TAC. If a failure occurs, the software will retry the configuration

change multiple times. The software will fall back to the original configuration bias if the retry attempts fail. If multiple attempts to reconfigure the hardware accelerator fail, it may indicate a hardware failure.

402140

Error Message `%ASA-3-402140: CRYPTO: RSA key generation error: modulus len len`

Explanation An error occurred during an RSA public key pair generation.

- *len* —The prime modulus length in bits

Recommended Action Contact the Cisco TAC for assistance.

402141

Error Message `%ASA-3-402141: CRYPTO: Key zeroization error: key set 'type', reason 'reason'`

Explanation An error occurred during an RSA public key pair generation.

- *type* —The key set type, which can be any of the following: DH, RSA, DSA, or unknown
- *reason* —The unexpected crypto session type

Recommended Action Contact the Cisco TAC for assistance.

402142

Error Message `%ASA-3-402142: CRYPTO: Bulk data op error: algorithm 'alg', mode 'mode'`

Explanation An error occurred during a symmetric key operation.

- *op* —The operation, which can be either encryption or decryption
- *alg* —The encryption algorithm, which can be any of the following: DES, 3DES, AES, or RC4
- *mode* —The mode, which can be any of the following: CBC, CTR, CFB, ECB, stateful-RC4, or stateless-RC4

Recommended Action Contact the Cisco TAC for assistance.

402143

Error Message `%ASA-3-402143: CRYPTO: alg type key op error`

Explanation An error occurred during an asymmetric key operation.

- *alg* —The encryption algorithm, which can be either RSA or DSA
- *type* —The key type, which can be either public or private
- *op* —The operation, which can be either encryption or decryption

Recommended Action Contact the Cisco TAC for assistance.

402144

Error Message `%ASA-3-402144: CRYPTO: Digital signature error: signature algorithm 'sig', hash algorithm 'hash'`

Explanation An error occurred during digital signature generation.

- *sig* —The signature algorithm, which can be either RSA or DSA
- *hash* —The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512

Recommended Action Contact the Cisco TAC for assistance.

402145

Error Message `%ASA-3-402145: CRYPTO: Hash generation error: algorithm 'hash'`

Explanation A hash generation error occurred.

- *hash* —The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512

Recommended Action Contact the Cisco TAC for assistance.

402146

Error Message `%ASA-3-402146: CRYPTO: Keyed hash generation error: algorithm 'hash', key len len`

Explanation A keyed hash generation error occurred.

- *hash* —The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512
- *len* —The key length in bits

Recommended Action Contact the Cisco TAC for assistance.

402147

Error Message `%ASA-3-402147: CRYPTO: HMAC generation error: algorithm 'alg'`

Explanation An HMAC generation error occurred.

- *alg* —The HMAC algorithm, which can be any of the following: HMAC-MD5, HMAC-SHA1, HMAC-SHA2, or AES-XCBC

Recommended Action Contact the Cisco TAC for assistance.

402148

Error Message `%ASA-3-402148: CRYPTO: Random Number Generator error`

Explanation A random number generator error occurred.

Recommended Action Contact the Cisco TAC for assistance.

402149

Error Message `%ASA-3-402149: CRYPTO: Weak encryption_type (length) provided. Operation disallowed. Not FIPS 140-2 compliant`

Explanation The Secure Firewall ASA tried to use an RSA key that is less than 2048 bits or DH groups 1, 2, or 5.

- *encryption type* —The encryption type
- *length* —The RSA key length or DH group number

Recommended Action Configure the Secure Firewall ASA or external application to use an RSA key that is at least 2048 bits, or to configure a DH group that is not 1, 2, or 5.

402150

Error Message `%ASA-3-402150: CRYPTO: Deprecated hash algorithm used for RSA operation (hash_alg). Operation disallowed. Not FIPS 140-2 compliant`

Explanation An unacceptable hashing algorithm has been used for digital certificate signing or verification for FIPS 140-2 certification.

- *operation* —Sign or verify
- *hash alg* —The name of the unacceptable hashing algorithm

Recommended Action Make sure that you use the minimum acceptable hashing algorithm for digital certificate signing or verification for FIPS 140-2 certification. These include SHA-256, SHA-384, and SHA-512.

403101

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

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

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

403102

Error Message `%ASA-4-403102: PPP virtual interface interface_name rcvd pkt with invalid protocol: protocol, reason: reason`

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

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

403103

Error Message `%ASA-4-403103: PPP virtual interface max connections reached`

Explanation The module cannot accept additional PPTP connections.Connections are allocated as soon as they are available.

Recommended Action None required.

403104

Error Message `%ASA-4-403104: PPP virtual interface interface_name requires mschap for MPPE`

Explanation The MPPE was configured, but MS-CHAP authentication was not.

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

403106

Error Message `%ASA-4-403106: PPP virtual interface interface_name requires RADIUS aaa server for MPPE`

Explanation The MPPE was configured, but RADIUS authentication was not.

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

403107

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

Explanation The AAA server configuration information cannot be found.

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

403108

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

Explanation The client IP address pool information is missing.

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

403109

Error Message `%ASA-4-403109: Rec'd packet not a PPTP packet. (ip) dest_addr= ip, src_addr= dest_address, data: source_address`

Explanation The module received a spoofed PPTP packet, which may indicate a hostile event.

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

403110

Error Message `%ASA-4-403110: PPP virtual interface interface_name, user: user missing MPPE key from aaa server`

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

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

403500

Error Message `%ASA-6-403500: PPPoE - Service name 'any' not received in interface_name. AC:ac_name.`

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

Recommended Action None required.

403501

Error Message `%ASA-3-403501: PPPoE - Bad host-unique in PADO - packet dropped. AC:interface_name.`

Explanation The Secure Firewall ASA sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The Secure Firewall ASA was unable to identify the corresponding connection request for this response. The packet was dropped, and connection negotiations were discontinued.

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

403502

Error Message `%ASA-3-403502: PPPoE - Bad host-unique in PADS - packet dropped. AC:interface_name.`

Explanation The Secure Firewall ASA sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The Secure Firewall ASA was unable to identify the corresponding connection request for this response. The packet was dropped, and connection negotiations were discontinued.

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

403503

Error Message `%ASA-3-403503: Header_string:PPP link down[:reason string]`

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

Recommended Action Check the network link to ensure that the link is connected. The access concentrator may be down. Make sure that your authentication protocol matches the access concentrator and that your name and password are correct. Verify this information with your ISP or network support person.

403504

Error Message `%ASA-3-403504: group_name:No 'vpdn group' for PPPoE has been created!`

Explanation PPPoE requires a dial-out configuration before starting a PPPoE session. In general, the configuration should specify a dialing policy, the PPP authentication, the username, and a password. The following example configures the Secure Firewall ASA for PPPoE dialout. The my-username and my-password commands are used to authenticate the access concentrator, using PAP if necessary.

For example:

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

Recommended Action Configure a VPDN group for PPPoE.

403505

Error Message `%ASA-4-403505: PPPoE:PPP - Unable to set default route to IP_address at interface_name. interface`

Explanation This message is usually followed by the message, default route already exists.

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

403506

Error Message `%ASA-4-403506: PPPoE: failed to assign PPP address IP_address netmask netmask at interface interface_name`

Explanation This message is followed by one of the followings messages: subnet is the same as interface, or on failover channel.

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

403507

Error Message `%ASA-3-403507: PPPoE:PPPoE client on interface interface failed to locate PPPoE vpdn group group_name`

Explanation You can configure the PPPoE client on an interface to use a particular VPDN group by entering the **pppoe client vpdn group group_name** command. If a PPPoE VPDN group of the configured name was not located during system startup, this message is generated.

- *interface* —The interface on which the PPPoE client failed

- *group_name* —The VPDN group name of the PPPoe client on the interface

Recommended Action Perform the following steps:

1. Add the required VPDN group by entering the **vpdn group group_name** command. Request dialout PPPoE in global configuration mode, and add all the group properties.
2. Remove the **pppoe client vpdn group** *group_name* command from the interface indicated. In this case, the PPPoE client will attempt to use the first PPPoE VPDN group defined.

Note All changes take effect only after the PPPoE client on the interface is restarted by entering the **ip address pppoe** command.

405001

Error Message `%ASA-4-405001: Received ARP {request | response} collision from IP_address /MAC_address on interface interface_name with existing ARP entry IP_address /MAC_address`

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

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

405002

Error Message `%ASA-4-405002: Received mac mismatch packet from IP_address/{MAC_bytes|MAC_address} for authenticated host`

Explanation This packet appears for one of the following conditions:

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

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

405003

Error Message `%ASA-4-405003: IP address collision detected between host IP_address at MAC_address and interface interface_name , MAC_address .`

Explanation A client IP address in the network is the same as the Secure Firewall ASA interface IP address.

Recommended Action Change the IP address of the client.

405101

Error Message-1 `%ASA-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for faddr foreign_ip_address to laddr local_ip_address/local_port`

Error Message-2 `%ASA-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for faddr foreign_ip_address/foreign_port to laddr local_ip_address`

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

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

405102

Error Message-1 `%ASA-4-405102: Unable to Pre-allocate H245 Connection for faddr foreign_ip_address to laddr local_ip_address/local_port`

Error Message-2 `%ASA-4-405102: Unable to Pre-allocate H245 Connection for faddr foreign_ip_address/foreign_port to laddr local_ip_address`

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

Recommended Action Check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of translations and connections. In addition, reduce the amount of memory usage, or purchase additional memory. If this message occurs periodically, it can be ignored. If the problem persists, contact the Cisco TAC.

405103

Error Message `%ASA-4-405103: H225 message from source_address/source_port to dest_address/dest_port contains bad protocol discriminator hex`

Explanation The Secure Firewall ASA is expecting the protocol discriminator, 0x08, but it received something other than 0x08. The endpoint may be sending a bad packet, or received a message segment other than the first segment. The packet is allowed through.

Recommended Action None required.

405104

Error Message `%ASA-4-405104: H225 message string received from outside_address/outside_port to inside_address/inside_port before SETUP`

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

Recommended Action None required.

405105

Error Message `%ASA-4-405105: H323 RAS message AdmissionConfirm received from source_address/source_port to dest_address/dest_port without an AdmissionRequest`

Explanation A gatekeeper has sent an ACF, but the Secure Firewall ASA did not send an ARQ to the gatekeeper.

Recommended Action Check the gatekeeper with the specified **source_address** to determine why it sent an ACF without receiving an ARQ from the Secure Firewall ASA.

405106

Error Message `%ASA-4-405106: H323 num channel is not created from %I/%d to %I/%d %s`

Explanation The ASA tried to create a match condition on the H.323 media-type channel. See the **match media-type** command for more information.

Recommended Action None required.

405107

Error Message `%ASA-4-405107: H245 Tunnel is detected and connection dropped from %I/%d to %I/%d %s`

Explanation An H.323 connection has been dropped because of an attempted H.245 tunnel control during call setup. See the **h245-tunnel-block** command for more information.

Recommended Action None required.

405201

Error Message `%ASA-4-405201: ILS ILS_message_type from inside_interface:source_IP_address/port to outside_interface:destination_IP_address/port has wrong embedded address embedded_IP_address`

Explanation The embedded address in the ILS packet payload was not the same as the source IP address of the IP packet header.

Recommended Action Check the host specified with the **source_IP_address** to determine why it sent an ILS packet with an incorrect embedded IP address.

405300

Error Message `%ASA-4-405300: Radius Accounting Request received from from_addr is not allowed`

Explanation The accounting request came from a host that was not configured in the policy map. The message is logged and processing stops.

- *from_addr* —The IP address of the host sending the request

Recommended Action If the host was configured to send RADIUS accounting messages to the ASA, make sure that it was configured in the correct policy map that was applied to the service policy. If the host was not

configured to send RADIUS accounting messages to the ASA, then check to see why the messages are being sent. If the messages are illegitimate, then create the proper ACLs to drop the packets.

405301

Error Message `%ASA-4-405301: Attribute attribute_number does not match for user user_ip`

Explanation When the **validate-attribute** command was entered, the attribute values stored in the accounting request start received do not match those stored in the entry, if it exists.

- *attribute_number* —The RADIUS attribute to be validated with RADIUS accounting. Values range from 1 to 191. Vendor-specific attributes are not supported.
- *user_ip* —The IP address (framed IP attribute) of the user.

Recommended Action None required.

406001

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

Explanation A client entered an FTP port command and supplied a port less than 1024 (in the well-known port range usually devoted to server ports). This is indicative of an attempt to avert the site security policy. The Secure Firewall ASA drops the packet, terminates the connection, and logs the event.

Recommended Action None required.

406002

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

Explanation A client entered an FTP port command and supplied an address other than the address used in the connection. An attempt to avert the site security policy occurred. For example, an attacker might attempt to hijack an FTP session by changing the packet on the way, and putting different source information instead of the correct source information. The Secure Firewall ASA drops the packet, terminates the connection, and logs the event. The address in parentheses is the address from the port command.

Recommended Action None required.

407001

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

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

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

Recommended Action The host limit is enforced on the low-end platforms. Use the **show version** command to view the host limit. Use the **show local-host** command to view the current active hosts and the inside users that have sessions at the Secure Firewall ASA. To forcefully disconnect one or more users, use the **clear**

local-host command. To expire the inside users more quickly from the limit, set the xlate, connection, and uauth timeouts to the recommended values or lower as given in the table below:

Table 2: Timeouts and Recommended Values

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

407002

Error Message `%ASA-4-407002: Embryonic limit for through connections exceeded` *`nconns/elimit. outside_address/outside_port`* `to` *`global_address`*`(`*`inside_address`*`)/`*`inside_port`* `on interface` *`interface_name`*

Explanation The number of connections from a specified foreign address over a specified global address to the specified local address exceeded the maximum embryonic limit for that static. The Secure Firewall ASA tries to accept the connection if it can allocate memory for that connection. It proxies on behalf of the local host and sends a SYN_ACK packet to the foreign host. The Secure Firewall ASA retains pertinent state information, drops the packet, and waits for the acknowledgment from the client. The message might indicate legitimate traffic or that a DoS attack is in progress.

Recommended Action Check the source address to determine where the packets are coming from and whether or not a valid host is sending them.

407003

Error Message `%ASA-4-407003: Established limit for RPC services exceeded`

Explanation The Secure Firewall ASA tried to open a new hole for a pair of RPC servers or services that have already been configured after the maximum number of holes has been met.

Recommended Action Wait for other holes to be closed (through associated timeout expiration), or limit the number of active pairs of servers or services.

408001

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

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

Recommended Action Enter the **clear ip route** command to reset the route counter. If the problem persists, contact the Cisco TAC.

408002

Error Message `%ASA-4-408002: ospf process id route type update address1 netmask1 [distance1/metric1 ] via source IP :interface1 address2 netmask2 [distance2 /metric2 ] interface2`

Explanation A network update was received from a different interface with the same distance and a better metric than the existing route. The new route overrides the existing route that was installed through another interface. The new route is for redundancy purposes only and means that a path has shifted in the network. This change must be controlled through topology and redistribution. Any existing connections affected by this change are probably disabled and will time out. This path shift only occurs if the network topology has been specifically designed to support path redundancy, in which case it is expected.

Recommended Action None required.

408003

Error Message `%ASA-4-408003: can't track this type of object hex`

Explanation A component of the tracking system has encountered an object type that is not supported by the component. A STATE object was expected.

- *hex* —A hexidecimal value(s) depicting variable value(s) or addresses in memory

Recommended Action Reconfigure the track object to make it a STATE object.

408101

Error Message `%ASA-4-408101: KEYMAN : Type encrption_type encryption unknown. Interpreting keystring as literal.`

Explanation The format type was not recognized by the system. A keystring format type value of 0 (unencrypted keystring) or 7 (hidden keystring), followed by a space, can precede the actual keystring to indicate its format. An unknown type value will be accepted, but the system will consider the keystring as being unencrypted.

Recommended Action Use the correct format for the value type or remove the space following the value type.

408102

Error Message `%ASA-4-408102: KEYMAN : Bad encrypted keystring for key id key_id.`

Explanation The system could not successfully decrypt an encrypted keystring. The keystring may have been corrupted during system configuration.

Recommended Action Re-enter the key-string command, and reconfigure the key string.

409001

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

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

Recommended Action None required.

409002

Error Message `%ASA-4-409002: db_free: external LSA IP_address netmask`

Explanation An internal software error occurred.

Recommended Action None required.

409003

Error Message `%ASA-4-409003: Received invalid packet: reason from IP_address , interface_name`

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

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

409004

Error Message `%ASA-4-409004: Received reason from unknown neighbor IP_address`

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

Recommended Action None required.

409005

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

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

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

409006

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

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

Recommended Action From a neighboring address, locate the problem router and reboot it. If the problem persists, contact the Cisco TAC.

409007

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

Explanation An internal software error occurred.

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

409008

Error Message `%ASA-4-409008: Found generating default LSA with non-zero mask LSA type: number Mask: netmask metric: number area: string`

Explanation The router tried to generate a default LSA with an incorrect mask and possibly incorrect metric because an internal software error occurred.

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

409009

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

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

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

409010

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

Explanation An internal error occurred.

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

409011

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

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

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

409012

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

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

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

409013

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

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

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

409014

Error Message `%ASA-4-409014: No valid authentication send key is available on interface nameif.`

Explanation The authentication key configured on the interface is not valid.

Recommended Action Configure a new key.

409015

Error Message `%ASA-4-409015: Key ID key-id received on interface nameif.`

Explanation The ID is not found in the configured key chain.

Recommended Action Configure a new security association with the Key ID.

409016

Error Message `%ASA-4-409016: Key chain name key-chain-name on nameif is invalid.`

Explanation The key-chain name configured under OSPF interface does not match global key chain configuration.

Recommended Action Fix configuration. Either remove OSPF authentication command or configure key chain in global configuration mode.

409017

Error Message `%ASA-4-409017: Key ID key-id in key chain key-chain-name is invalid.`

Explanation The Key ID configured in the key chain is out of range for OSPF. This may happen because the key chain allows Key ID values of the range which is not acceptable for OSPF.

Recommended Action Configure a new security association with a Key ID that is in the range 1-255.

409023

Error Message `%ASA-4-409023: Attempting AAA Fallback method method_name for request_type request for user user : Auth-server group Auth-server unreachable`

Explanation An authentication or authorization attempt to an external server has failed and will be performed using the local user database.

- **aaa_operation**—Either authentication or authorization
- **username**—The user associated with the connection
- **server_group**—The name of the AAA server whose servers were unreachable

Recommended Action Investigate any connectivity problems with the AAA servers configured in the first method. Ping the authentication servers from the Secure Firewall ASA. Make sure that the daemons are running on the AAA server.

409101

Error Message `%ASA-4-409101: Received invalid packet: s from P , s`

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

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

409102

Error Message `%ASA-4-409102: Received packet with incorrect area from P , s , area AREA_ID_STR , packet area AREA_ID_STR`

Explanation An OSPF packet was received with an area ID in its header that does not match the area of this interface.

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

409103

Error Message `%ASA-4-409103: Received s from unknown neighbor i`

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

Recommended Action None required.

409104

Error Message `%ASA-4-409104: Invalid length d in OSPF packet type d from P (ID i ), s`

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

Recommended Action None required.

409105

Error Message `%ASA-4-409105: Invalid lsa: s : Type 0x x , Length 0x x , LSID u from i`

Explanation The router received an LSA with invalid data. The LSA includes an invalid LSA type, incorrect checksum, or incorrect length, which is caused by either memory corruption or unexpected behavior on a router.

Recommended Action From a neighboring address, locate the problem router and do the following:

- Collect a running configuration of the router by entering the **show running-config** command.
- Enter the **show ipv6 ospf database** command to gather data that may help identify the nature of the error.
- Enter the **show ipv6 ospf database** *link-state-id* command. The *link-state-id* argument is the IP address of the invalid LSA.
- Enter the **show logging** command to gather data that may help identify the nature of the error.
- Reboot the router.

If you cannot determine the nature of the error from the collected information, contact the Cisco TAC and provide the gathered information.

409106

Error Message `%ASA-4-409106: Found generating default LSA with non-zero mask LSA type: 0x x Mask: i metric: lu area: AREA_ID_STR`

Explanation The router tried to generate the default LSA with the incorrect mask and possibly an incorrect metric because of an internal software error.

Recommended Action None required.

409107

Error Message `%ASA-4-409107: OSPFv3 process d could not pick a router-id, please configure manually`

Explanation OSPFv3 failed while attempting to allocate a router ID from the IP address of one of its interfaces.

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

409108

Error Message `%ASA-4-409108: Virtual link information found in non-backbone area: AREA_ID_STR`

Explanation An internal error has occurred.

Recommended Action None required.

409109

Error Message `%ASA-4-409109: OSPF detected duplicate router-id i from P on interface IF_NAME`

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

Recommended Action Change the neighbor router ID.

409110

Error Message `%ASA-4-409110: Detected router with duplicate router ID` *`i`* `in area` *`AREA_ID_STR`*

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

Recommended Action Change the neighbor router ID.

409111

Error Message `%ASA-4-409111: Multiple interfaces (`*`IF_NAME`* `/`*`IF_NAME`* `) on a single link detected.`

Explanation OSPFv3 enabled on multiple interfaces that are on the same link is not supported.

Recommended Action OSPFv3 should be disabled or made passive on all except one of the interfaces.

409112

Error Message `%ASA-4-409112: Packet not written to the output queue`

Explanation An internal error has occurred.

Recommended Action None required.

409113

Error Message `%ASA-4-409113: Doubly linked list linkage is NULL`

Explanation An internal error has occurred.

Recommended Action None required.

409114

Error Message `%ASA-4-409114: Doubly linked list prev linkage is NULL` *`x`*

Explanation An internal error has occurred.

Recommended Action None required.

409115

Error Message `%ASA-4-409115: Unrecognized timer` *`d`* `in OSPF` *`s`*

Explanation An internal error has occurred.

Recommended Action None required.

409116

Error Message `%ASA-4-409116: Error for timer d in OSPF process s`

Explanation An internal error has occurred.

Recommended Action None required.

409117

Error Message `%ASA-4-409117: Can't find LSA database type x , area AREA_ID_STR , interface x`

ExplanationAn internal error has occurred.

Recommended Action None required.

409118

Error Message `%ASA-4-409118: Could not allocate DBD packet`

ExplanationAn internal error has occurred.

Recommended Action None required.

409119

Error Message `%ASA-4-409119: Invalid build flag x for LSA i , type 0x x`

ExplanationAn internal error has occurred.

Recommended Action None required.

409120

Error Message `%ASA-4-409120: Router-ID i is in use by ospf process d`

Explanation The Secure Firewall ASA attempted to assign a router ID that is in use by another process.

Recommended Action Configure another router ID for one of the processes.

409121

Error Message `%ASA-4-409121: Router is currently an ASBR while having only one area which is a stub area`

Explanation An ASBR must be attached to an area that can carry AS External or NSSA LSAs.

Recommended Action Make the area to which the router is attached into an NSSA or regular area.

409122

Error Message `%ASA-4-409122: Could not select a global IPv6 address. Virtual links require at least one global IPv6 address.`

ExplanationA virtual link was configured. For the virtual link to function, a global IPv6 address must be available. However, no global IPv6 address could be found on the router.

Recommended Action Configure a global IPv6 address on an interface on this router.

409123

Error Message `%ASA-4-409123: Neighbor command allowed only on NBMA networks`

ExplanationThe **neighbor** command is allowed only on NBMA networks.

Recommended Action Check the configuration options for the **neighbor** command, and correct the options or the network type for the neighbor interface.

409125

Error Message `%ASA-4-409125: Can not use configured neighbor: poll and priority options are allowed only for a NBMA network`

ExplanationThe configured neighbor was found on a point-to-multipoint network and either the poll or priority option was configured. These options are only allowed on NBMA type networks.

Recommended Action Check the configuration options for the **neighbor** command, and correct the options or the network type for the neighbor interface.

409128

Error Message `%ASA-4-409128: OSPFv3-`*`d`* `Area` *`AREA_ID_STR`* `: Router` *`i`* `originating invalid type 0x` *`x`* `LSA, ID` *`u`* `, Metric` *`d`* `on Link ID` *`d`* `Link Type` *`d`*

ExplanationThe router indicated in this message has originated an LSA with an invalid metric. If this is a router LSA and the link metric is zero, a risk of routing loops and traffic loss exists in the network.

Recommended Action Configure a valid metric for the given LSA type and link type on the router that originated the reported LSA.

Messages 410001 to 450001

This chapter includes messages from 410001 to 450001.

410001

Error Message `%ASA-4-410001: Dropped UDP DNS` *`request`* `from` *`source_interface`*`:`*`source_address`*`/`*`source_port`* `to` *`dest_interface`*`:`*`dest_address`*`/`*`dest_port`*`;` *`label|domain-name`* `length` *`number`* `bytes exceeds` *`remaining_packet_length`* `limit of` *`number`* `bytes`

Explanation The label length exceeds bytes in a UDP DNS packet. See RFC 1035, section 2.3.4 for more information. .

Recommended Action Create the policy-map and add a custom DNS class-map to match traffic and exclude it from inspection to allow packets exceeding the label length.

410002

Error Message `%ASA-2-410002: Dropped num DNS responses with mis-matched id in the past sec second(s): from src_ifc:sip/sport to dest_ifc:dip/dport`

Explanation The ASA detects an excess number of DNS responses with a mismatched DNS identifier. A high rate of mismatched DNS identifiers might indicate an attack on the cache. The threshold is set by the **id-mismatch** DNS policy-map parameter submode command.

- *num* —The number of ID mismatch instances as configured by the **id-mismatch** command
- *sec* —The duration in seconds as configured by the **id-mismatch** command
- *src_ifc* —The source interface name at which the DNS message is received with a mismatched DNS identifier
- *sip* —The source IP address
- *sport* —The source port
- *dest_ifc* —The destination interface name
- *dip* —The destination IP address
- *dport* —The destination port

Recommended Action Check the IP address and port in the message to trace the source of the attack. You can configure ACLs to block traffic permanently from the source.

410003

Error Message `%ASA-4-410003: action_class DNS action from query_response:src_ifc/sip to sport:dest_ifc/dip; dport`

Explanation A DNS classification was performed on a DNS message and the specified criteria were satisfied. As a result, the configured action occurs.

- *action_class* —The DNS Classification action class
- *action* —The action taken: Dropped, Dropped (no TSIG), or Masked header flags for
- *query_response* —Either query or response
- *src_ifc* —The source interface name
- *sip* —The source IP address
- *sport* —The source port
- *dest_ifc* —The destination interface name
- *dip* —The destination IP address
- *dport* —The destination port
- *further_info* —One of the following: matched Class id: *class_name* , matched Class id: *match_command* (for a standalone **match** command), or TSIG resource record not present (for messages generated by the **tsig enforced** command)

Recommended Action None required.

410004

Error Message `%ASA-6-410004: action_class DNS action from query_response:src_ifc/sip to sport:dest_ifc/dip; dport`

Explanation A DNS classification was performed on a DNS message and the specified criteria were satisfied.

- *action_class* —The DNS Classification action class
- *action* —The action taken: Received or Received (no TSIG)
- *query_response* —Either query or response
- *src_ifc* —The source interface name
- *sip* —The source IP address
- *sport* —The source port
- *dest_ifc* —The destination interface name
- *dip* —The destination IP address
- *dport* —The destination port
- *further_info* —One of the following: matched Class id: *class_name* , matched Class id: *match_command* (for a standalone **match** command), or TSIG resource record not present (for messages generated by the **tsig enforced** command)

Recommended Action None required.

411001

Error Message `%ASA-4-411001: Line protocol on Interface interface_name, changed state to up`

Explanation The status of the line protocol has changed from down to up . If **interface_name** is a logical interface name such as inside and outside, this message indicates that the logical interface line protocol has changed from down to up . If **interface_name** is a physical interface name such as Ethernet0 and GigabitEthernet0/1, this message indicates that the physical interface line protocol has changed from down to up .

Recommended Action None required.

411002

Error Message `%ASA-4-411002: Line protocol on Interface interface_name, changed state to down`

Explanation The status of the line protocol has changed from up to down. If **interface_name** is a logical interface name such as inside and outside, this message indicates that the logical interface line protocol has changed from up to down. In this case, the physical interface line protocol status is not affected. If **interface_name** is a physical interface name such as Ethernet0 and GigabitEthernet0/1, this message indicates that the physical interface line protocol has changed from up to down.

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

411003

Error Message `%ASA-4-411003: Interface interface_name, changed state to administratively up`

Explanation The configuration status of the interface has changed from down to up.

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

411004

Error Message `%ASA-4-411004: Interface interface_name, changed state to administratively down`

Explanation The configuration status of the interface has changed from down to up.

Recommended Action None required.

411005

Error Message `%ASA-4-411005: Interface variable_1 experienced a hardware transmit hang. A software reset has been performed.`

Explanation The interface experienced a hardware transmit freeze that required a reset of the Ethernet controller to restore the interface to full operation.

- *variable 1* —The interface name, such as GigabitEthernet0/0

Recommended Action None required.

412001

Error Message `%ASA-4-412001: MAC MAC_address moved from interface_1 to interface_2`

Explanation A host move was detected from one module interface to another. In a transparent Secure Firewall ASA, mapping between the host (MAC) and Secure Firewall ASA port is maintained in a Layer 2 forwarding table. The table dynamically binds packet source MAC addresses to an Secure Firewall ASA port. In this process, whenever movement of a host from one interface to another interface is detected, this message is generated.

Recommended Action The host move might be valid or might be an attempt to spoof host MACs on other interfaces. If it is a MAC spoof attempt, you can either locate vulnerable hosts on your network and remove them or configure static MAC entries, which will not allow MAC address and port binding to change. If it is a genuine host move, no action is required.

412002

Error Message `%ASA-4-412002: Detected bridge table full while inserting MAC MAC_address on interface interface. Number of entries = num`

Explanation The bridge table was full and an attempt was made to add one more entry. The Secure Firewall ASA maintains a separate Layer 2 forwarding table per context and the message is generated whenever a context exceeds its size limit. The MAC address will be added, but it will replace the oldest existing dynamic entry (if available) in the table. This might be an attempted attack.

Recommended Action Make sure that the new bridge table entries are valid. In case of attack, use EtherType ACLs to control access to vulnerable hosts.

413001

Error Message `%ASA-4-413001: Module module_id is not able to shut down. Module Error: errnum message`

Explanation The module identified by *module_id* was not able to comply with a request from the Secure Firewall ASA system module to shut down. It may be performing a task that cannot be interrupted, such as a software upgrade. The **errnum** and **message** text describes the reason why the module cannot shut down, and the recommended corrective action.

Recommended Action Wait for the task on the module to complete before shutting down the module, or use the **session** command to access the CLI on the module, and stop the task that is preventing the module from shutting down.

413002

Error Message `%ASA-4-413002: Module module_id is not able to reload. Module Error: errnum message`

Explanation The module identified by *module_id* was not able to comply with a request from the Secure Firewall ASA module to reload. It may be performing a task that cannot be interrupted, such as a software upgrade. The **errnum** and **message** text describes the reason why the module cannot reload, and the recommended corrective action.

Recommended Action Wait for the task on the module to complete before reloading the module, or use the **session** command to access the CLI on the module and stop the task that is preventing the module from reloading.

413003

Error Message `%ASA-4-413003: Module string_one is not a recognized type.`

Explanation A module was detected that is not recognized as a valid module type.

Recommended Action Upgrade to a version of Secure Firewall ASA software that supports the module type installed.

413004

Error Message `%ASA-4-413004: Module in slot string_one failed to write software vnewver (currently vver), reason. Trying again.`

Explanation The module failed to accept a software version, and will be transitioned to an UNRESPONSIVE state. Another attempt will be made to update the module software.

- >*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 None required. Subsequent attempts will either generate a message indicating a successful update or failure. You may verify the module transitions to UP after a subsequent update attempt by using the **show module** command.

413005

Error Message `%ASA-4-413005: Module module_id, application is not supported "app_name" version "app_vers" type app_type.`

Error Message `%ASA-4-413005: Module prod_id in slot slot_num , application is not supported app_name version app_vers type app_type`

Explanation The module installed in slot *slot_num* was running an unsupported application version or type.

- *module_id*— The name of the software services module
- *prod_id* —Product ID string
- *slot_num* —The slot number in which the module is installed. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- *app_name* —Application name (string)
- *app_vers* —Application version (string)
- *app_type* —Application type (decimal)

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

413006

Error Message `%ASA-4-413006: prod-id Module software version mismatch; slot slot is "prod-id" version "running-vers". Slot slot "prod-id" requires version "required-vers"`

Explanation The version of software running on the module in slot *slot* was not the version required by another module.

- *slot* —Slot 0 indicates the system main board. Slot 1 indicates the module installed in the expansion slot.
- *prod_id* —Product ID string for the device installed in slot *slot*
- *running_vers* —Version of software currently running on the module installed in slot *slot*
- *required_vers* —Version of software required by the module in slot *slot*

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

413007

Error Message `%ASA-1-413007: An unsupported configuration is detected. The combination of an mpc_description with ips_description is not supported.`

Explanation An unsupported Secure Firewall ASA and IPS configuration has been detected during IPS SSP setup for slot 1. The Secure Firewall ASA should continue to function normally with an unsupported configuration.

- *mpc_description* —A description string for the ASA model, which can be one of the following: ASA5585-SSP-10, ASA5585-SSP-20, ASA5585-SSP-40, ASA5585-SSP-60, ASA5585-SSP-10-K7, ASA5585-SSP-20-K7, ASA5585-SSP-40-K7, ASA5585-SSP-60-K7.

- *ips_description* —A description string for the IPS SSP model, which can be one of the following: ASA5585-SSP-IPS10, ASA5585-SSP-IPS20, ASA5585-SSP-IPS40, ASA5585-SSP-IPS60, ASA5585-SSP-P10K7, ASA5585-SSP-P20K7, ASA5585-SSP-P40K7, ASA5585-SSP-P60K7.

Recommended Action None required.

413008

Error Message `%ASA-1-413008: An unsupported configuration is detected.`

Explanation Only one power supply and one fan module are inserted when an ASA 10G SSP and IPS 10G SSP are present.

Recommended Action When using an ASA 10G SSP and IPS 10G SSP, insert two power supplies instead of one fan module and one power supply module.

413009

Error Message `%ASA-4-413009: internal_interface =current value`

Explanation The firewall checks the current value of an internal interface or a data ring every one minute. When the current value of the ring falls below 10, this message is generated.

```
%ASA-4-413009: Internal-Data0/1:RX[1]=[2]
```

In the above example, Internal-Data0/1 RX1 value went to 2, which is less than 10.

Recommended Action None.

414001

Error Message `%ASA-3-414001: Failed to save logging buffer to FTP server filename using filename ftp_server_address on interface interface_name: fail_reason`

Explanation The logging module failed to save the logging buffer to an external FTP server.

Recommended Action Take applicable actions based on the failed reason:

- Protocol error—Make sure no connectivity issue exists between the FTP server and Secure Firewall ASA, and that the FTP sever can accept the FTP port command and PUT requests.
- Invalid username or password—Make sure that the configured FTP client username and password are correct.
- All other errors—If the problem persists, contact the Cisco TAC.

414002

Error Message `%ASA-3-414002: Failed to save logging buffer to flash:/syslog directory using filename filename: fail_reason`

Explanation The logging module failed to save the logging buffer to system flash.

Recommended Action If the failed reason is caused by insufficient space, check the flash free space, and make sure that the configured limits of the **logging flash-size** command are set correctly. If the error is a flash file system I/O error, then contact the Cisco TAC for assistance.

414003

Error Message `%ASA-3-414003: TCP Syslog Server intf:IP_Address/port not responding, New connections are [permitted|denied] based on logging permit-hostdown policy`

Explanation The TCP syslog server for remote host logging was successful, is connected to the server, and new connections are permitted or denied based on the logging permit-hostdown policy. If the logging permit-hostdown policy is configured, a new connection is permitted. If not configured, a new connection is denied.

- *intf* —Interface of the Secure Firewall ASA to which the server is connected
- *IP_Address* —IP address of the remote TCP syslog server
- *port* —Port of the remote TCP syslog server

Recommended Action Validate that the configured TCP syslog server is up. To permit new connections, configure the logging permit-hostdown policy. To deny new connections, do not configure the logging permit-hostdown policy.

414004

Error Message `%ASA-6-414004: TCP Syslog Server intf:IP_Address/port - Connection restored`

Explanation The TCP syslog setup involves 4 channels connecting to the server. This message is generated only when one of the TCP syslog server channels become unreachable and the server is restored. This message is the first to reach the syslog server after a successful connection. This message is generated only on TCP syslog server.

Note This message does not appear every time when the TCP syslog server is restored. It appears only when the server is restored after one of its channels became unreachable.

- *intf* —Interface of the ASA to which the server is connected
- *IP_Address* —IP address of the remote TCP syslog server
- *port* —Port of the remote TCP syslog server

Recommended Action None required.

414005

Error Message `%ASA-3-414005: TCP Syslog Server intf : IP_Address /port connected, New connections are permitted based on logging permit-hostdown policy`

Explanation The TCP syslog server for remote host logging was successful, is connected to the server, and new connections are permitted based on the logging permit-hostdown policy. If the logging permit-hostdown policy is configured, a new connection is permitted.

- *intf* —Interface of the Secure Firewall ASA to which the server is connected
- *IP_Address* —IP address of the remote TCP syslog server
- *port* —Port of the remote TCP syslog server

Recommended Action None required.

414006

Error Message `%ASA-3-414006: TCP syslog server configured and logging queue is full. New connections denied based on logging permit-hostdown policy.`

Explanation The logging queue is close to reaching the configured limit, so there is a risk that syslog messages will be discarded.

Recommended Action See the "Configuring the Logging Queue" section in the CLI configuration guide for information about how to tune the queue size to avoid this situation. If you want to deny new connections in this case, use the **no logging permit-hostdown** command. If you want to allow new connections in this case, use the **logging permit-hostdown** command.

414007

Error Message `%ASA-6-414007: TCP syslog server connection restored. New connections allowed.`

Explanation The TCP syslog server for remote host logging was successfully connected and new connections are permitted.

Recommended Action None required.

414008

Error Message `%ASA-6-414008: New connections are now allowed due to change of logging permit-hostdown policy.`

Explanation An administrator changed the logging permit-hostdown policy by entering the **logging permit-hostdown** command at a time when new connections are being denied. Due to this change of policy, new connections will be allowed.

Recommended Action None required.

415001

Error Message `%ASA-6-415001: HTTP - matched` *`matched_string`* `in policy-map` *`map_name`*`, header field count exceeded` *`connection_action int_type`*`:`*`IP_address/port_num`* `to` *`int_type`*`:`*`IP_address/port_num`*

Explanation This message is generated when one of the following occurs:

- The total number of fields in the HTTP header exceeds the user-configured number of header fields. The relevant command is: **match** {**request** | **response**} **header count num**.
- The appearance of a specified field in the HTTP header exceeds the user-configured number for this header field. The relevant command is: **match** {**request** | **response**} **header header-name count num**.
- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection

- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **match** {**request** | **response**} **header** command to reconfigure the HTTP header field value.

415002

Error Message `%ASA-6-415002: HTTP - matched matched_string in policy-map map_name, header field length exceeded connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The specified HTTP header field length exceeded the user-configured length.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping connection or Resetting connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **match** {**request** | **response**} **header header_name length gt num** command to change the HTTP header field length.

415003

Error Message `%ASA-6-415003: HTTP - matched matched_string in policy-map map_name, body length exceeded connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The length of the message body exceeded the user-configured length.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **match** {**request** | **response**} **body length gt num** command to change the length of the message body.

415004

Error Message `%ASA-5-415004: HTTP - matched matched_string in policy-map map_name, content-type verification failed connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The magic number in the body of the HTTP message is not the correct magic number for the MIME-type specified in the content-type field in the HTTP message header.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **match {request | response} header content-type violation** command to correct the error.

415005

Error Message `%ASA-5-415005: HTTP - matched matched_string in policy-map map_name, URI length exceeded connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The length of the URI exceeded the user-configured length.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **match request uri length gt num** command to change the length of the URI.

415006

Error Message `%ASA-5-415006: HTTP - matched matched_string in policy-map map_name, URI matched connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The URI matched the regular expression that the user configured. See the **match request uri regex** {**regex-name** | **class class-name**} command for more information.

• **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

• *map_name* —The name of the policy map
• *connection_action* —Dropping the connection or resetting the connection
• *interface_type* —The type of interface (for example, DMZ or outside)
• *IP_address* —The IP address of the interface
• *port_num* —The port number

Recommended Action None required.

415007

Error Message `%ASA-5-415007: HTTP - matched matched_string in policy-map map_name, Body matched connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The message body matched the regular expression that the user configured. See the **match** {**request** | **response**} **body regex** {**regex-name** | **class class-name**} command for more information.

• **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

• *map_name* —The name of the policy map
• *connection_action* —Dropping the connection or resetting the connection
• *interface_type* —The type of interface (for example, DMZ or outside)
• *IP_address* —The IP address of the interface
• *port_num* —The port number

Recommended Action None required.

415008

Error Message `%ASA-5-415008: HTTP - matched matched_string in policy-map map_name, header matched connection_action int_type:IP_address/port_num to int_type: IP_address/port_num`

Explanation A value in a user-specified field in the message header matched the regular expression that the user configured. See the **match** {**request** | **response** } **header header-field-name** {**regex-name** | **class class-name**} command for more information.

• **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

• *map_name* —The name of the policy map
• *connection_action* —Dropping the connection or resetting the connection

- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action None required.

415009

Error Message `%ASA-5-415009: HTTP - matched matched_string in policy-map map_name, method matched connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The HTTP method matched the user-configured regular expression. See the **match request method** {**regex-name** | **class class-name**} command for more information.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action None required.

415010

Error Message `%ASA-5-415010: matched matched_string in policy-map map_name , transfer encoding matched connection_action from int_type :IP_address /port_num to int_type :IP_address /port_num`

Explanation The value in the transfer encoding field matched the user-configured regular expression or keyword. See the **match** {**request** | **response**} **header transfer-encoding** {{**regex-name** | **class class-name**} | **keyword**} command for more information.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action None required.

415011

Error Message `%ASA-5-415011: HTTP - policy-map map_name:Protocol violation connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The HTTP parser cannot detect a valid HTTP message in the first few bytes of an HTTP message.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **protocol-violation action** {**drop** | **reset**} **log** command to correct the problem.

415012

Error Message `%ASA-5-415012: HTTP - matched matched_string in policy-map map_name, content-type unknown connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The content-type field did not contain a MIME type that matches a built-in MIME type.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **match** {**request** | **response**} **header content-type unknown** command to correct the problem.

415013

Error Message `%ASA-5-415013: HTTP - policy-map map-name:Malformed chunked encoding connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation A chunked encoding was malformed, and the HTTP message cannot be parsed. In addition, logging for the **protocol-violation** command was configured.

- **map-name**— The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **protocol-violation action** {**drop** | **reset**} **log** command to correct the problem.

415014

Error Message `%ASA-5-415014: HTTP - matched matched_string in policy-map map_name, Mime-type in response wasn't found in the accept-types of the request connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The MIME type in an HTTP response was not in the accept field of the request.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **match req-resp content-type mismatch** command to correct the problem.

415015

Error Message `%ASA-5-415015: HTTP - matched matched_string in policy-map map_name, transfer-encoding unknown connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation An empty transfer encoding occurred.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **match** {**request** | **response**} **header transfer-encoding empty** command to correct the problem.

415016

Error Message `%ASA-4-415016: policy-map map_name:Maximum number of unanswered HTTP requests exceeded connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The number of unanswered HTTP requests exceeded the internal number of requests allowed.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **protocol-violation action** {**drop** | **reset**} **log** command to correct the problem.

415017

Error Message `%ASA-6-415017: HTTP - matched matched_string in policy-map map_name, arguments matched connection_actionint_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation A pattern in the arguments matches the user-configured regular expression or keyword. See the **match request args regex** {**regex-name** | **class class-name**} command for more information.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action None required.

415018

Error Message `%ASA-5-415018: HTTP - matched matched_string in policy-map map_name, Header length exceeded connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The total header length exceeded the user-configured length for the header.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **match** {**request** | **response**} **header length gt num** command to reduce the length of the header.

415019

Error Message `%ASA-5-415019: HTTP - matched matched_string in policy-map map_name, status line matched connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation The status line in a response matched a user-configured regular expression. See the **match response status-line regex** {**regex-name** | **class class-name** } command for more information.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action None required.

415020

Error Message `%ASA-5-415020: HTTP - matched matched_string in policy-map map_name, a non-ASCII character was matched connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation A non-ASCII character was found.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface
- *port_num* —The port number

Recommended Action Enter the **match** {**request** | **response**} **header non-ascii** command to correct the problem.

416001

Error Message `%ASA-4-416001: Dropped UDP SNMP packet from source_interface:source_IP/source_port to dest_interface:dest_address/dest_port; prot_version`

Explanation An SNMP packet was denied passage through the ASA because of a bad packet format or because the **prot_version** is not allowed through the ASA. The **prot_version** parameter can be one of the following values: 1, 2, 2c, or 3.

Recommended Action Change the settings for SNMP inspection using the **snmp-map** command, which allows the user to permit or deny specific protocol versions.

417001

Error Message `%ASA-4-417001: Unexpected event received: number`

Explanation A process received a signal, but no handler was found for the event.

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

417004

Error Message `%ASA-4-417004: Filter violation error: conn number (string :string ) in string`

Explanation A client tried to modify a route attribute that the client does not own.

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

417006

Error Message `%ASA-4-417006: No memory for string ) in string . Handling: string`

Explanation An operation failed because of low memory, but will be handled with another mechanism.

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

418001

Error Message `%ASA-4-418001: Through-the-device packet to/from management-only network is denied: protocol_string`

Explanation A packet from the specified source to the destination was dropped because it is traversing the Secure Firewall ASA to and from the management-only network.

- **protocol_string**—TCP, UDP, ICMP, or protocol ID as a number in decimal
- **interface_name**— Interface name
- **IP_address**—IP address
- **port**—Port number
- *sg_info* —Security group name or tag for the specified IP address

Recommended Action Determine who is generating this packet and why.

418018

Error Message `%ASA-3-418018: neighbor IP_Address Down User reset` OR `%ASA-3-418018: neighbor IP_Address IPv4 Unicast topology base removed from session User reset` OR `%ASA-3-418018: neighbor IP_Address Up` OR `%ASA-3-418018: neighbor IP_Address IPv4 Unicast topology base removed from session BGP Notification sent`

Explanation The different states of BGP peering and notification of changes on the topology DB as a result of the peering state transitions.

Recommended Action None required.

418019

Error Message `%ASA-3-418019: sent to neighbor IP_Address, Reason: reason, Bytes: count`

Explanation An indication of why BGP peering was terminated.

- **Reason**—Reason for termination. The reason could be invalid or corrupt AS path, or expiry of hold time, and so on.
- **Bytes**—Number of bytes transmitted

Recommended Action None required.

418040

Error Message `%ASA-3-418040: unsupported or mal-formatted message received from IP_Address`

Explanation Indication of unsupported or mal-formed messages received during the BGP handshake, not necessarily only related to Graceful restart specifically.

Recommended Action None required.

418044

Error Message `%ASA-3-418044:IP_Address connection timed out - has not accepted a message from us for hold_time in ms (hold time), 0 messages pending transmmission.`

Explanation Indication of hold time for a BGP neighbor has expired.

- IP_Address—IPv4 or IPv6 address of the BGP neighbor.
- hold_time—The hold time in milliseconds.

Recommended Action None required.

419001

Error Message `%ASA-4-419001: Dropping TCP packet from src_ifc:src_IP/src_port to dest_ifc:dest_IP/dest_port, reason: reason, MSS size, data size`

Explanation The length of the TCP packet exceeded the MSS advertised in the three-way handshake.

- >*src_ifc*— Input interface name
- >*src_IP*— The source IP address of the packet
- >*src_port*— The source port of the packet
- >*dest_ifc*— The output interface name
- >*dest_IP*— The destination IP address of the packet
- >*dest_port*— The destination port of the packet

Recommended Action If there is a need to allow packets that exceed the MSS, create a TCP map using the **exceed-mss** command, as in the following example:

```
ciscoasa# access-list http-list permit tcp any host server_ip eq 80
ciscoasa# class-map http
 ciscoasa# match access-list http-list
 ciscoasa# tcp-map tmap
ciscoasa# exceed-mss allow
ciscoasa# policy-map global_policy
ciscoasa# class http
ciscoasa# set connection advanced-options tmap
```

419002

Error Message `%ASA-4-419002: Duplicate TCP SYN from` *`in_interface`*`:`*`src_address`*`/`*`src_port`* `to` *`out_interface`*`:`*`dest_address`*`/`*`dest_port`* `with different initial sequence number`

Explanation A duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number from the SYN that opened the embryonic connection. This may indicate that SYNs are being spoofed. This message occurs in Release 7.0.4.1 and later.

- **in_interface**—The input interface
- **src_address**—The source IP address of the packet
- **src_port**—The source port of the packet
- **out_interface**—The output interface
- **dest_address**—The destination IP address of the packet
- **dest_port**—The destination port of the packet

Recommended Action None required.

419003

Error Message `%ASA-4-419003: Cleared TCP urgent flag from` *`out_ifc`* `:`*`src_ip`* `/`*`src_port`* `to` *`in_ifc`* `:`*`dest_ip`* `/`*`dest_port`*`.`

Explanation A duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number from the SYN that opened the embryonic connection. This may indicate that SYNs are being spoofed. This message occurs in Release 7.0.4.1 and later.

- **in_ifc**—The input interface
- **src_ip**—The source IP address of the packet
- **src_port**—The source port of the packet
- **out_ifc**—The output interface
- **dest_ip**—The destination IP address of the packet
- **dest_port**—The destination port of the packet

Recommended Action If you need to keep the urgent flag in TCP headers, use the **urgent-flag allow** command in TCP map configuration mode.

Error Message `%ASA-7-419003: Cleared TCP urgent flag.`

Explanation This syslog is displayed when urgent flag or urgent pointer of tcp packet is cleared. This could be due to user configuration (tcp-map) or having some value for the urgent pointer in a tcp packet but the urgent flag is not set.

Recommended Action Verify if the tcp-map configurations whether the urget flag is set to clear.

419004

Error Message `%ASA-6-419004: TCP connection ID from src_ifc:src_ip/src_port (src_ip/src_port) to dst_ifc:dst_ip/dst_port (dst_ip/dst_port) is probed by DCD`

Explanation

A TCP connection was probed by Dead Connection Detection (DCD) to determine if connection was still valid.

Recommended Action None.

419005

Error Message `%ASA-6-419005: TCP connection ID from src_ifc:src_ip/src_port (src_ip/src_port) to dest_ifc:des_ip/des_port (des_ip/des_port) duration hh:mm:ss data bytes, is kept open by DCD as valid connection`

Explanation

A TCP connection was kept open by Dead Connection Detection (DCD) as a valid connection.

Recommended Action None.

419006

Error Message `%ASA-6-419006: Teardown TCP connection ID from src_ifc:src_ip/src_port (src_ip/src_port) to dst_ifc:dst_ip/dst_port (dst_ip/dst_port) duration hh:mm:ss data bytes, DCD probe was not responded from client/server interface ifc_name`

Explanation

A TCP connection was closed by Dead Connection Detection (DCD) as it is no longer required.

Recommended Action None.

420001

Error Message `%ASA-3-420001: IPS card not up and fail-close mode used, dropping ICMP packet from ifc_in:SIP/port to ifc_out:DIP/port`

For example:

```
%ASA-3-420001: IPS card not up and fail-close mode used, dropping TCP packet from >ifc_in
:>SIP
/>SPORT
 to >ifc_out
:>DIP
/>DPORT
%ASA-3-420001: IPS card not up and fail-close mode used, dropping UDP packet from >ifc_in
:>SIP
/>SPORT
 to >ifc_out
:>DIP
```

```
/>DPORT
%ASA-3-420001: IPS card not up and fail-close mode used, dropping protocol >protocol
 packet from >ifc_in
:>SIP
 to >ifc_out
:>DIP
```

Explanation Packets are dropped when the IPS fail-close mode is used, and the IPS card is not up. This message is rate limited.

- *ifc_in* —Input interface name
- *ifc_out* —Output interface name
- *SIP* —Source IP of the packet
- *SPORT* —Source port of the packet
- *DIP* —Destination IP of the packet
- *DPORT* —Destination port of the packet
- *ICMP_TYPE* —Type of the ICMP packet
- *ICMP_CODE* —Code of the ICMP packet

Recommended Action Bring up the IPS card.

420002

Error Message `%ASA-4-420002: IPS requested to drop ICMP packet from ifc_in:SIP/port to ifc_out:DIP/port`

For example:

```
%ASA-4-420002: IPS requested to drop TCP packet from ifc_in:SIP/SPORT to ifc_out:DIP/DPORT
%ASA-4-420002: IPS requested to drop UDP packet from ifc_in:SIP/SPORT to ifc_out:DIP/DPORT
%ASA-4-420002: IPS requested to drop protocol packet from ifc_in:SIP to ifc_out:DIP
```

Explanation IPS requested that the packet be dropped.

- *ifc_in* —Input interface name
- *ifc_out* —Output interface name
- *SIP* —Source IP of the packet
- *SPORT* —Source port of the packet
- *DIP* —Destination IP of the packet
- *DPORT* —Destination port of the packet
- *ICMP_TYPE* —Type of the ICMP packet
- *ICMP_CODE* —Code of the ICMP packet

Recommended Action None required.

420003

Error Message `%ASA-4-420003: IPS requested to reset TCP connection from ifc_in:SIP/SPORT to ifc_out:DIP/DPORT`

Explanation IPS requested a reset of a TCP connection.

- *ifc_in* —Input interface name
- *ifc_out* —Output interface name

- *SIP* —Source IP of the packet
- *SPORT* —Source port of the packet
- *DIP* —Destination IP of the packet
- *DPORT* —Destination port of the packet

Recommended Action None required.

420004

Error Message `%ASA-6-420004: Virtual Sensor sensor_name was added on the AIP SSM`

Explanation A virtual sensor was added on the AIP SSM card.

- *n* —Card number

Recommended Action None required.

420005

Error Message `%ASA-6-420005: Virtual Sensor sensor_name was deleted from the AIP SSM`

Explanation A virtual sensor was deleted from the AIP SSM card.

- *n* —Card number

Recommended Action None required.

420006

Error Message `%ASA-3-420006: Virtual sensor not present and fail-close mode used, dropping protocol packet from ifc_in:SIP/SPORT to ifc_out:DIP/DPORT`

Explanation Packets are dropped when the IPS fail-close mode is used, and the virtual sensor used for the packet is not present.

- *protocol*— Protocol used to send the packet
- *ifc_in* —Input interface name
- *ifc_out* —Output interface name
- *SIP* —Source IP address of the packet
- *SPORT* —Source port of the packet
- *DIP* —Destination IP address of the packet
- *DPORT* —Destination port of the packet

Recommended Action Add the virtual sensor.

420007

Error Message `%ASA-4-420007: application-string cannot be enabled for the Module in slot slot_id. The module's current software version does not support this feature. Please upgrade the software on the module in slot slot_id to support this feature.`

Explanation This message is generated by any new feature in the ASA that needs a corresponding software version in the SSM or SSC hardware module. The message is sent each time that the ASA module manager detects state changes in the SSM or SSC hardware module.

- *application-string* —The name of the application (for example, Promiscuous IDS)
- *slot_id* —The module identifier, which is 1 for the current ASA
- *version_number* —The version number of the message header between the ASA and the IPS application

Recommended Action Load the SSM or SSC hardware module with the correct software images that support the designated application.

420008

Error Message `%ASA-3-420008: IPS module license disabled and fail-close mode used, dropping packet.`

Explanation The IPS module license has been disabled and when the fail-close mode is configured, all traffic destined for the IPS module will be dropped. You can check the status of the license by using the **show activation-key** command.

Recommended Action Use the **activation-key** command to apply an activation key that has the IPS license enabled.

421001

Error Message 1 `%ASA-3-421001: {TCP|UDP} flow from interface_name:IP_address/port to interface_name:IP_address/port is dropped because application_id has failed.`

Error Message 2 `%ASA-3-421001: {TCP|UDP} flow from interface_name:IP_address/port to interface_name:IP_address/port is skipped because application_id has failed.`

Explanation A packet was dropped (Error Message 1) or skipped (Error Message 2) because the CSC SSM application failed. By default, this message is rate limited to 1 message every 10 seconds.

- **interface_name**—The interface name
- **IP_address**—The IP address
- **port**—The port number
- **application**—The CSC SSM is the only application supported in the current release

Recommended Action Determine the problem with the service module.

421002

Error Message `%ASA-6-421002: TCP|UDP flow from interface_name :IP_address /port to interface_name :IP_address /port bypassed application checking because the protocol is not supported.`

Explanation The connection bypassed service module security checking because the protocol that it is using cannot be scanned by the service module. For example, the CSC SSM is not capable of scanning Telnet traffic. If the user configures Telnet traffic to be scanned, the traffic will bypass the scanning service. By default, this message is rate limited to 1 message every 10 seconds.

- **IP_address**—The IP address
- **port**—The port number

- **interface_name**—The name of the interface on which the policy is applied
- **application**—The CSC SSM is the only application supported in the current release

Recommended Action The configuration should be modified to only include protocols that are supported by the service module.

421003

Error Message `%ASA-3-421003: Invalid data plane encapsulation`

Explanation A packet injected by the service module did not have the correct data plane header. Packets exchanged on the data backplane adhere to a Cisco proprietary protocol called ASDP. Any packet that does not have the proper ASDP header is dropped.

Recommended Action Use the **capture name type asp-drop** [**ssm-asdp-invalid-encap**] command to capture the offending packets and contact the Cisco TAC.

421004

Error Message `%ASA-7-421004: Failed to inject {TCP|UDP} packet from IP_address/port to IP_address/port`

Explanation The ASA has failed to inject a packet as instructed by the service module. This may happen if the ASA tries to inject a packet into a flow that has already been released or when the ASA maintains its connection table independently from the service module. Normally it will not cause any problem.

- **IP_address**—The IP address
- **port**—The port number

Recommended Action If ASA performance is affected, or if the problem persists, contact the Cisco TAC.

421005

Error Message `%ASA-6-421005: interface_name:IP_address is counted as a user for application`

Explanation A host has been counted toward the license limit. The specified host was counted as a user of **application**. The total number of users in 24 hours is calculated at midnight for license validation.

- **interface_name**—The interface name
- **IP_address**—The IP address
- **application**—The CSC SSM

Recommended Action None required. However, if the overall count exceeds the user license that you have purchased, contact the Cisco TAC to upgrade your license.

421006

Error Message `%ASA-6-421006: There are number users of application accounted during the past 24 hours`

Explanation The total number of users who have used an application for the past 24 hours have been identified. This message is generated every 24 hours to give the total number of hosts that have used services provided by the service module.

- **application**—The CSC SSM

Recommended Action None required. However, if the overall count exceeds the user license that you have purchased, contact the Cisco TAC to upgrade your license.

421007

Error Message `%ASA-3-421007: TCP|UDP flow from interface_name :IP_address /port to interface_name :IP_address /port is skipped because application has failed.`

Explanation A flow was skipped because the service module application has failed. By default, this message is rate limited to 1 message every 10 seconds.

- **IP_address**—The IP address
- **port**—The port number
- **interface_name**—The name of the interface on which the policy is applied
- **application**—The CSC SSM

Recommended Action Determine the problem with the service module.

422004

Error Message `%ASA-4-422004: IP SLA Monitor number0 : Duplicate event received. Event number number1`

Explanation The IP SLA monitor process has received a duplicate event. Currently, this message applies to destroy events. Only one destroy request will be applied. This is only a warning message.

- *number0* —The SLA operation number
- *number1* —The SLA operation event ID

Recommended Action If this recurs, enter the **show sla monitor configuration SLA_operation_id** command and copy the output of the command. Copy the message as it appears on the console or in the system log. Then contact the Cisco TAC and provide the representative with the information that you have, along with information about the application that is configuring and polling the SLA probes.

422005

Error Message `%ASA-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.`

Explanation One or more IP SLA monitor probes cannot be scheduled because the system clock was not set.

Recommended Action Make sure that the system clock is functional by using NTP or another mechanism.

422006

Error Message `%ASA-4-422006: IP SLA Monitor Probe number : string`

Explanation The IP SLA monitor probe cannot be scheduled. Either the configured starting time has already occurred or the starting time is invalid.

- *number* —The SLA operation ID

• *string* —A string describing the error

Recommended Action Reschedule the failed probe with a valid start time.

423001

Error Message `%ASA-4-423001: {Allowed|Dropped} invalid NBNS pkt_type_name with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port.`

Explanation The NBNS packet format is incorrect.

Recommended Action None required.

423002

Error Message `%ASA-4-423002: {Allowed|Dropped} mismatched NBNS pkt_type_name with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port`

Explanation An NBNS ID mismatch occurred.

Recommended Action None required.

423003

Error Message `%ASA-4-423003: {Allowed|Dropped} invalid NBDGM pkt_type_name with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port.`

Explanation The NBDGM packet format is incorrect.

Recommended Action None required.

423004

Error Message `%ASA-4-423004: {Allowed|Dropped} mismatched NBDGM pkt_type_name with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port`

Explanation An NBDGM ID mismatch occurred.

Recommended Action None required.

423005

Error Message `%ASA-4-423005: {Allowed|Dropped} NBDGM pkt_type_name fragment with error_reason_str from ifc_name:ip_address/port to ifc_name:ip_address/port.`

Explanation The NBDGM fragment format is incorrect.

Recommended Action None required.

424001

Error Message `%ASA-4-424001: Packet denied: protocol_string. intf_in interface is in a backup state`

Explanation A packet was dropped because it was traversing the Secure Firewall ASA to or from a redundant interface. Interface functionality is limited on low-end platforms. The interface specified by the **backup interface** command can only be a backup for the primary interface configured. If the default route to the primary interface is up, any traffic through the Secure Firewall ASA from the backup interface will be denied. Conversely, if the default route to the primary interface is down, traffic through the Secure Firewall ASA from the primary interface will be denied.

- *protocol_string* —The protocol string; for example, TCP or protocol ID (a decimal number)
- *intf_in* —The input interface name
- *src_ip* —The source IP address of the packet
- *src_port* —The source port of the packet
- *intf_out* —The output interface name
- *dst_ip* —The destination IP address of the packet
- *dst_port* —The destination port of the packet
- *sg_info* —The security group name or tag for the specified IP address

Recommended Action Determine the source of the denied packet.

424002

Error Message `%ASA-4-424002: Connection to the backup interface is denied: protocol_string`

Explanation A connection was dropped because it is in a backup state. Interface functionality is limited on low-end platforms. The backup interface can only be a backup for the primary interface specified by the **backup interface** command. If the default route to the primary interface is up, any connection to the Secure Firewall ASA through the backup interface will be denied. Conversely, if the default route to the primary interface is down, connections to the Secure Firewall ASA through the primary interface will be denied.

- *protocol_string* —The protocol string; for example, TCP or protocol ID (a decimal number)
- *intf_in* —The input interface name
- *src_ip* —The source IP address of the packet
- *src_port* —The source port of the packet
- *intf_out* —The output interface name
- *dst_ip* —The destination IP address of the packet
- *dst_port* —The destination port of the packet

Recommended Action Determine the source of the denied packet.

425001

Error Message `%ASA-6-425001 Redundant interface redundant _interface_name created.`

Explanation The specified redundant interface was created in the configuration.

- *redundant_interface_name* —Redundant interface name

Recommended Action None required.

425002

Error Message `%ASA-6-425002 Redundant interface redundant _interface_name removed.`

Explanation The specified redundant interface was removed from the configuration.

- *redundant_interface_name* —Redundant interface name

Recommended Action None required.

425003

Error Message `%ASA-6-425003 Interface interface_name added into redundant interface redundant _interface_name .`

Explanation The specified physical interface was added to the specified redundant interface as a member interface.

- *interface_name* —An interface name
- *redundant_interface_name* —Redundant interface name

Recommended Action None required.

425004

Error Message `%ASA-6-425004 Interface interface_name removed from redundant interface redundant _interface_name .`

Explanation The specified redundant interface was removed from the specified redundant interface.

- *interface_name* —An interface name
- *redundant_interface_name* —Redundant interface name

Recommended Action None required.

425005

Error Message `%ASA-5-425005 Interface interface_name become active in redundant interface redundant _interface_name`

Explanation Within a redundant interface, one member interface is the active member. Traffic only passes through the active member interface. The specified physical interface became the active member of the specified redundant interface. Member interface switchover occurs when one of the following is true:

-
  - The **redundant-interface interface-name active-member interface-name** command was executed.
  - The active member interface is down, while the standby member interface is up.
  - The standby member interface comes up (from down), while the active member interface remains down.
- *interface_name* —An interface name
- *redundant_interface_name* —Redundant interface name

Recommended Action Check the status of the member interfaces.

425006

Error Message `%ASA-3-425006 Redundant interface redundant _interface_name switch active member to interface_name failed.`

Explanation An error occurred when member interface switchover was attempted.

- *redundant_interface_name* —Redundant interface name
- *interface_name* —An interface name

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

426001

Error Message `%ASA-6-426001: PORT-CHANNEL:Interface ifc_name bundled into EtherChannel interface num`

Explanation The **interface port-channel** *num* or the **channel-group** *num* **mode** *mode* command has been used on a nonexistent port channel.

- *ifc_name* —The EtherChannel interface name
- *num* —The port channel number

Recommended Action None required.

426002

Error Message `%ASA-6-426002: PORT-CHANNEL:Interface ifc_name unbundled from EtherChannel interface num`

Explanation The **no interface port-channel** *num* command has been used.

- *ifc_name* —The EtherChannel interface name
- *num*— The port channel number

Recommended Action None required.

426003

Error Message `%ASA-6-426003: PORT-CHANNEL:Interface ifc_name1 has become standby in EtherChannel interface num`

Explanation The **channel-group** *num* **mode** *mode* command has been used.

- *ifc_name1* —The EtherChannel interface name
- *num* —The port channel number

Recommended Action None required.

426004

Error Message `%ASA-4-426004: PORT-CHANNEL:Interface ifc_name1 is not compatible with ifc_name and will be suspended (speed_of ifc_name1 is X_Mbps, Y is 1000_Mbps)`

Error Message `%ASA-4-426004: Interface ifc_name1 is not compatible with ifc_name1 and will be suspended (ifc_name1 is Full-duplex, ifc_name1 is Half-duplex)`

Explanation The **channel-group** *num* **mode** *mode* command is executed on a physical interface and there is a speed or duplex mismatch of this physical interface with that of the port channel.

- *ifc_name* —The interface that is being added to the port channel
- *ifc_name1* —The interface that is already in the port channel and in a bundled state

Recommended Action Do one of the following:

- Change the speed of the physical interface to that of the port channel and execute the **channel-group** *num* **mode** *mode* command again.
- Leave the member interface in a suspended state. When the last active member is removed, then that member will try to reestablish LACP on the suspended member.

426101

Error Message `%ASA-6-426101: PORT-CHANNEL:Interface ifc_name is allowed to bundle into EtherChannel interface port-channel_id by CLACP.`

Explanation A port has been bundled in a span-cluster channel group.

Recommended Action None required.

426102

Error Message `%ASA-6-426102: PORT-CHANNEL:Interface ifc_name is moved to standby in EtherChannel interface port-channel_id by CLACP.`

Explanation A port has been moved to hot-standby state in a span-cluster channel group.

Recommended Action None required.

426103

Error Message `%ASA-6-426103: PORT-CHANNEL:Interface ifc_name is selected to move from standby to bundle in EtherChannel interface port-channel_id by CLACP.`

Explanation A standby port has been selected to move to bundled state in a span-cluster channel group.

Recommended Action None required.

426104

Error Message `%ASA-6-426104: PORT-CHANNEL:Interface ifc_name is unselected in EtherChannel interface port-channel_id by CLACP.`

Explanation A bundled port has been unbundled in a span-cluster channel group to obtain space for other ports to be bundled.

Recommended Action None required.

428002

Error Message `%ASA-6-428002: WAAS confirmed from in_interface :src_ip_addr/src_port to out_interface :dest_ip_addr/dest_port , inspection services bypassed on this connection.`

Explanation WAAS optimization was detected on a connection. All layer 7 inspection services, including IPS, are bypassed on WAAS-optimized connections.

Recommended Action No action is required if the network includes WAE devices; otherwise, the network administrator should investigate the use of the WAAS option on this connection.

429001

Error Message `%ASA-3-429001: CX card not up and fail-close mode used, dropping protocol packet from interface_name:ip_address/port to interface_name:ip_address/port`

Explanation Data has been dropped because an SSP is down and a fail-close policy exists.

Recommended Action Check the status of the service module and contact the Cisco TAC for assistance, if necessary.

429002

Error Message `%ASA-4-429002: CX requested to drop protocol packet from interface_name:ip_address/port to interface_name:ip_address/port`

Explanation The CXSC SSP requested that the ASA drop a packet of a connection.

Recommended Action None.

429003

Error Message `%ASA-4-429003: CX requested to reset TCP connection from interface_name:ip_addr/port to interface_name:ip_addr/port`

Explanation The CXSC SSP requested that the ASA reset a TCP connection.

Recommended Action None required.

429004

Error Message `%ASA-3-429004: Unable to set up rule_name authentication-proxy rule for the cxsc action on interface interface_name for policy_type service-policy.`

Explanation The ASA could not set up to-the-box rules for authentication proxy with the CXSC action because of some internal errors, such as insufficient memory.

Recommended Action This error should not occur. Contact the Cisco TAC.for assistance.

429005

Error Message `%ASA-6-429005: Set up protocol_type authentication-proxy rule for the cxsc action on interface interface_name for traffic destined to ip_address/port for policy_type service-policy`

Explanation The ASA successfully set up to-the-box rules for authentication proxy with the CXSC action.

Recommended Action None.

429006

Error Message `%ASA-6-429006: Cleaned up authentication-proxy rule for the cxsc action on interface interface_name for traffic destined to ip_address for policy_type service-policy`

Explanation The ASA successfully cleaned up to-the-box rules for authentication proxy with the CXSC action.

Recommended Action None.

429007

Error Message `%ASA-4-429007: CXSC redirect will override Scansafe redirect for flow from interface_name:ip_address/port to interface_name:ip_address/port [(username)]`

Explanation A flow matches both CXSC and Scansafe redirects. The message indicates that the CXSC redirect overrides the Scansafe redirect for the displayed flow.

Recommended Action If this is unwanted behavior, then reconfigure the policy to ensure that no overlap of CXSC and Scansafe redirection occurs for the same flow.

429008

Error Message `%ASA-4-429008: Unable to respond to VPN query from CX for session 0x%x . Reason %s`

Explanation The CX sent a VPN session query to the Secure Firewall ASA, but it did not respond either because of an invalid session ID or another reason. Valid reasons can be any of the following:

- TLV length is invalid
- TLV memory allocation failed
- VPN session query message enqueue failed
- VPN session ID is invalid

Recommended Action None required.

431001

Error Message `%ASA-4-431001: RTP conformance: Dropping RTP packet from in_ifc :src_ip /src_port to out_ifc :dest_ip /dest_port , Drop reason: drop_reason value`

Explanation The RTP packet was dropped.

- **in_ifc**—The input interface
- **src_ip**—The source IP address of the packet
- **src_port**—The source port of the packet
- **out_ifc**—The output interface
- *dest_ip* —The destination IP address of the packet
- **dest_port**—The destination port of the packet
- **drop_reason**—One of the following drop reasons:

- Incorrect version *value* —The version number from the packet is incorrect.

- Invalid payload-type *value* —The payload type from the packet is invalid.

- Incorrect SSRC *value* —The SSRC from the packet is incorrect.

- Out-of-range sequence number *value* sequence number from the packet.

- Out of sequence in packet in probation *value* sequence number from the packet.

Recommended Action Examine the dropped RTP packets to determine which field the RTP source is setting incorrectly. Also examine the source to verify that it is legitimate and not an attacker trying to misuse an opening in the ASA.

431002

Error Message `%ASA-4-431002: RTCP conformance: Dropping RTCP packet from in_ifc :src_ip /src_port to out_ifc :dest_ip /dest_port , Drop reason: drop_reason value`

Explanation The RTCP packet was dropped.

- **in_ifc**—The input interface
- **src_ip**—The source IP address of the packet
- **src_port**—The source port of the packet
- **out_ifc**—The output interface
- **dest_ip**—The destination IP address of the packet
- **dest_port**—The destination port of the packet
- **drop_reason**—One of the following drop reasons:

- Incorrect version **value**—The version number from the packet is incorrect.

- Invalid payload-type **value**—The payload type from the packet is incorrect.

Recommended Action Examine the dropped RTP packets to determine which field the RTP source is setting incorrectly. Also examine the source to verify that it is legitimate and not an attacker trying to misuse an opening in the ASA.

434001

Error Message `%ASA-4-434001: SFR card not up and fail-close mode used, dropping protocol packet from ingress:source/IP_address to source_port:egress_interface/destination_IP_address`

Explanation A packet has been dropped because of a fail-close configuration for the module. Your loss of connectivity for all the flows is caused by redirecting them to the module, because the fail-close configuration is designed to drop all the flows if the module is down.

Recommended Action Try to understand the reason for failure and restore services. Alternatively, you can use the fail-open option even if the card does not recover immediately. Note that in the fail-open configuration, all packets to the module are bypassed if the card status is down.

434002

Error Message `%ASA-4-434002: SFR requested to drop protocol packet from ingress_interface:source_IP_address/source_port to egress_interface:destination_IP_address/destination_port`

Explanation A packet has been denied by the module. Your connection is not successful for a certain flow has been redirected to the module.

Recommended Action Try to identify the module policy that caused this flow or packet to be denied.

434003

Error Message `%ASA-4-434003: SFR requested to reset TCP connection from ingress_interface:source_IP_address/source_port to egress:interface/destination_IP_address`

Explanation A TCP flow has been reset by the ASA, as requested by the module. Your TCP connection is not successful for a certain flow because it was redirected to the module.

Recommended Action Try to identify the module policy that caused this flow or packet to be denied.

434004

Error Message `%ASA-5-434004: SFR requested device to bypass further packet redirection and process protocol flow from inside_ifc_name:src_ip/src_port to outside_ifc_name:dst_ip/dst_port locally`

Explanation SourceFire (SFR) has determined not to inspect more traffic of a flow and requests the Secure Firewall ASA to stop redirecting the flow of traffic to SFR.

Recommended Action None Required.

434007

Error Message `%ASA-4-434007: SFR redirect will override Scansafe redirect for flow from inside_interface:source_ip_address/source_port to outside_interface:destination_IP_address/destination_port [(user)]`

Explanation A flow that was inspected by Scansafe is now inspected by SourceFire (SFR) only. Scansafe and SFR cannot inspect a flow simultaneously.

Recommended Action Reconfigure the ASA inspect policy that caused this flow or packet to be inspected by either Scansafe or SFR.

444004

Error Message `%ASA-2-444004: Timebased activation key xxx xxx xxx xxx xxx has expired. Applying permanent_license activation key xxx xxx xxx xxx xxx.`

Explanation The temporary license that was installed has expired. The features that the license provided are no longer available.

- *key* —The temporary activation key
- *permkey* —The permanent activation key

Recommended Action A permanent license should be purchased and installed.

444005

Error Message `%ASA-4-444005: Timebased license key xxx xxx xxx xxx xxx will expire in num days.`

Explanation This message is generated every 24 hours, indicating that the temporary license will expire in the number of days specified. After that date, the features that the license provided will no longer be available.

- *activation-key* —The temporary activation key
- *num* —The number of days left until expiration

Recommended Action If the amount of time remaining is less than 30 days, you should purchase another time-based activation key before the temporary license runs out.

444007

Error Message `%ASA-2-444007: Timebased activation key xxx xxx xxx xxx xxx has expired.`

Explanation The time-based activation key has expired. The specified features that the license provided are no longer available.

- *activation-key* —The temporary activation key
- *feature* —The name of the licensed feature being affected

Recommended Action You must purchase another time-based activation key as soon as possible to prevent service disruption for the features specified.

444008

Error Message `%ASA-4-444008: license-type license has expired, and the system is scheduled to reload in number days. Apply a new activation key to enable license-type license and prevent the automatic reload.`

Explanation The specific license has expired, which will cause the system to reload in x days. Apply a new activation key to enable the specific license and prevent automatic reload.

Recommended Action Apply a new activation key to enable the specific license and prevent automatic reload.

444009

Error Message `%ASA-2-444009: license-type license has expired 30 days ago. The system will now reload.`

Explanation The specific license expired 30 days ago. The system will reload.

Recommended Action None required.

444100

Error Message `%ASA-5-444100: Shared license request request failed, Reason: reason.`

Explanation A shared license client request was unsuccessfully sent or processed by the server.

- *request* —Valid requests are:

- get AnyConnect Premium

- release AnyConnect Premium

- transfer AnyConnect Premium

• *reason* —The reason that the request failed. Valid reasons are:

- connection failed to server

- version not supported by server

- message signature invalid

- client ID unknown by server

- server is not active

- license capacity reached

Recommended Action None required.

444101

Error Message `%ASA-5-444101: Shared license service is active. License server address: address`

Explanation The shared license server has become active.

• *address* —The license server IPv4 or IPv6 address

Recommended Action None required.

444102

Error Message `%ASA-2-444102: Shared license service inactive. License server is not responding.`

Explanation The shared license service was inactive because the license server was not responding. The ASA failed to register with the shared license server.

Recommended Action Verify that the license server address, secret, and port are configured correctly.

444103

Error Message `%ASA-6-444103: Shared licensetype license usage is over 90% capacity.`

Explanation The shared license usage on the network is over 90 percent capacity.

• *licensetype* —AnyConnect Premium

Recommended Action None required.

444104

Error Message `%ASA-6-444104: Shared licensetype license availability: value.`

Explanation The shared license availability on the network appeared.

• *licensetype* —AnyConnect Premium
• *value* —The license availability

Recommended Action None required.

444105

Error Message `%ASA-2-444105: Released value shared licensetype license(s). License server has been unreachable for 24 hours.`

Explanation The shared license server has been unreachable for 24 hours, and all shared licenses that have been acquired by the ASA have been released. The ASA failed to register with the license server.

- *licensetype* —AnyConnect Premium
- *value* —The license availability

Recommended Action Verify the connectivity to the license server, and that the configuration has not been changed on the license server.

444106

Error Message `%ASA-4-444106: Shared license backup server address is not available`

Explanation The shared license backup server is not reachable. License server information is not synchronized with the backup device.

- *address* —The IPv4 or IPv6 address of the backup license server

Recommended Action None required.

444107

Error Message `%ASA-6-444107: Shared license service status on interface ifname.`

Explanation The shared license service has been enabled or disabled on the specified interface.

- *ifname* —The interface name.
- *status* —The status of the license server. Valid values are enabled or disabled.

Recommended Action None required.

444108

Error Message `%ASA-6-444108: Shared license state client id id.`

Explanation The multi-site license client ID has registered or expired with the server.

- *id* —The ID of the client
- *state* —The state of the license server. Valid values are registered or expired.

Recommended Action None required.

444109

Error Message `%ASA-4-444109: Shared license backup server role change to state..`

Explanation The shared backup license server role has changed.

- *state* —The state of the license server. Valid values are active or inactive.

Recommended Action None required.

444110

Error Message `%ASA-4-444110: Shared license server backup has days day(s) remaining as active license server.`

Explanation The shared backup license server is in an active role and remains active for a specified number of days. The ASA failed to register with the license server, and needs to register with the primary license server soon.

- *days* —The number of days left as the active license server

Recommended Action Verify that the license server is online and reachable by the ASA.

444111

Error Message `%ASA-2-444111: Shared license backup service has been terminated due to the primary license server address being unavailable for more than days days. The License server needs to be brought back on-line to continue using shared licensing.`

Explanation The shared backup license server active time has expired. The primary server needs to go online in order for the shared license service to continue.

- *address* —The IPv4 or IPv6 address of the license server
- *days* —The number of days that the license server has been unavailable

Recommended Action Register with the primary license server in order to continue using the shared license service.

444302

Error Message `%ASA-2-444302: %SMART_LIC-2-PLATFORM_ERROR: Platform error.`

Explanation Smart Licensing Agent has encountered a platform problem. This indicates that the platform team did not properly implement smart licensing on the device.

Recommended Action The platform team needs to address this problem before release.

444303

Error Message `%ASA-3-444303: %SMART_LIC-3-AGENT_REG_FAILED: Smart Agent for licensing registration with Cisco licensing cloud failed.`

Explanation Smart Licensing registration failed. This may have been caused due to an invalid ID token used during the registration or network connection failure to cisco.com.

Recommended Action Please check the Smart Agent syslog messages for additional information. Turn on the smart agent debug mode (CLI command: 'debug license agent all') and retry for more detailed information. Check your Smart Call Home configuration, your network connection with Cisco, and if the Identity token you used for registration is valid.

Error Message `%ASA-3-444303: %SMART_LIC-3-AGENT_DEREG_FAILED: Smart Agent for licensing deregistration with CSSM failed.`

Explanation Smart Licensing deregistration failed. This may have been caused due to a network connection failure to CSSM. The local registration information has been removed from the device.

Recommended Action Please check the Smart Agent syslog messages for additional information. Turn on the smart agent debug mode (CLI command: 'debug license agent all') and retry for more detailed information. Check your Smart Call Home configuration and your network connection with CSSM.

Error Message `%ASA-3-444303: %SMART_LIC-3-OUT_OF_COMPLIANCE: One or more entitlements are out of compliance.`

Explanation One or more requested entitlements from the customer are out of compliance.

Recommended Action Customer needs to go to the smart licensing portal to view their entitlements to understand the non-compliance.

Error Message `%ASA-3-444303: %SMART_LIC-3-EVAL_EXPIRED: Evaluation period expired.`

Explanation Your evaluation period has expired. Please obtain a new identity token from the smart agent portal and re-register the device.

Recommended Action Customer needs to obtain a new identity token from the smart agent portal and re-register the device with the Cisco licensing service.

Error Message `%ASA-3-444303: %SMART_LIC-3-BAD_MODE: An unknown mode was specified.`

Explanation An invalid entitlement enforcement mode was received by the smart agent in the process of logging a syslog message.

Recommended Action This is a smart call home internal error. Please report this to Cisco.

Error Message `%ASA-3-444303: %SMART_LIC-3-BAD_NOTIF: A bad notification type was specified.`

Explanation An invalid notification type was received by the smart agent in the process of logging a syslog message.

Recommended Action This is a smart call home internal error. Please report this to Cisco.

Error Message `%ASA-3-444303: %SMART_LIC-3-ID_CERT_EXPIRED: Identity certificate expired. Agent will transition to the unidentified (not registered) state.`

Explanation The device has not communicated with Cisco for an extended period of time and the device has not automatically renewed the device registration with Cisco.

Recommended Action Please check the smart call home settings and network connectivity to cisco.com.

Error Message `%ASA-3-444303: %SMART_LIC-3-ID_CERT_RENEW_NOT_STARTED: Identity certificate start date not reached yet.`

Explanation The device registration failed. The Identity certificate start date is later than the device current time.

Recommended Action Please adjust your device clock to be up-to-date and retry the registration again.

Error Message `%ASA-3-444303: %SMART_LIC-3-ID_CERT_RENEW_FAILED: Identity certificate renewal failed.`

Explanation The device has not communicated with Cisco for an extended period of time and the device has failed to automatically renew the device registration with Cisco.

Recommended Action Please check the smart call home settings and network connectivity to cisco.com.

Error Message `%ASA-3-444303: %SMART_LIC-3-ENTITLEMENT_RENEW_FAILED: Entitlement authorization with Cisco licensing cloud failed.`

Explanation The device has failed to communicate with Cisco to renew the entitlement authorization.

Recommended Action Please check the smart agent syslog messages for further information. Additionally, check for smart call home settings and network connectivity to cisco.com.

Error Message `%ASA-3-444303: %SMART_LIC-3-COMM_FAILED: Communications failure with Cisco licensing cloud.`

Explanation The device communication with the Cisco licensing service failed.

Recommended Action Please check the smart call home settings and network connectivity to cisco.com.

Error Message `%ASA-3-444303: %SMART_LIC-3-CERTIFICATE_VALIDATION: Certificate validation failed by smart agent.`

Explanation The identity certificate validation failed.

Recommended Action Please check the smart agent syslog file for more information. Turn on the smart agent debug mode (CLI command: license smart debug enable) and retry again for additional information. Additionally, check if the identity certificate expiration date has been reached.

Error Message `%ASA-3-444303: %SMART_LIC-3-AUTH_RENEW_FAILED: Authorization renewal with Cisco licensing cloud failed.`

Explanation The authorization renew request failed. This may have been caused due to wrong smart call home settings or network connectivity failure to cisco.com.

Recommended Action Please check the smart agent syslog file for more information. Turn on the smart agent debug mode and retry again for additional information. Additionally, check the smart call home settings and network connectivity to cisco.com.

Error Message `%ASA-3-444303: %SMART_LIC-3-INVALID_TAG: The entitlement tag is invalid.`

Explanation The tag is not defined in the Cisco Smart Software Manager.

Recommended Action Report this error to Cisco.

Error Message `%ASA-3-444303: %SMART_LIC-3-INVALID_ROLE_STATE: The current role is not allowed to move to the new role.`

Explanation From the last role event, we can only move to certain roles. The device has moved to a role to which the smart agent cannot follow.

Recommended Action Please check the smart agent syslog file for more information. Turn on the smart agent debug mode and retry again for additional information.

Error Message `%ASA-3-444303: %SMART_LIC-3-EVAL_WILL_EXPIRE_WARNING: Evaluation period will expire in time.`

Explanation The device is using the evaluation period which will expire in the specified time.

Recommended Action Use the 'license smart register ID token' CLI to register this device before the evaluation period expires.

Error Message `%ASA-3-444303: %SMART_LIC-3-EVAL_EXPIRED_WARNING: Evaluation period expired on time.`

Explanation The device evaluation period has expired.

Recommended Action Use the 'license smart register ID token' CLI to register this device.

Error Message `%ASA-3-444303: %SMART_LIC-3-ID_CERT_EXPIRED_WARNING: This device's registration will expire in time.`

Explanation The registration for this device will expire at the specified time. This usually indicates a communications failure with the Cisco licensing authority.

Recommended Action Please check the smart call home settings and network connectivity to cisco.com. Additionally, check if the identity certificate need to be renewed.

Error Message `%ASA-3-444303: %SMART_LIC-3-CONFIG_OUT_OF_SYNC: Trusted Store Enable flag not in sync with System Configuration, TS flag Config flag.`

Explanation Smart licensing configuration does not match the value of the enable flag in persistent storage. This can happen if a configuration is copied onto the system and a reload occurs. If the new configuration does not contain the Smart Licensing Enable command, the value in persistent storage will not match.

Recommended Action Apply the desired Smart Licensing Configuration Command and persist the configuration.

Error Message `%ASA-3-444303: %SMART_LIC-3-REG_EXPIRED_CLOCK_CHANGE: Smart Licensing registration has expired because the system time was changed outside the validity period of the registration period. The agent will transition to the un-registered state in 60 minutes.`

Explanation The system clock has been changed so that it is now outside the valid registration period. If the clock is reset to a value inside the registration validity period within one hour smart licensing will continue function normally. If the clock is not reset the device will become un-registered and a new identity token will need to be obtained to re-register the device. The registration validity period is defined by the start and end date in the identity certificate. Use 'show tech license' to get the id certificate information.

Error Message `%ASA-3-444303: %SMART_LIC-3-ROOT_CERT_MISMATCH_PROD: Certificate type mismatch.`

Explanation Smart Agent received incorrect certificate for validation. Please contact your product support team.

Error Message `%ASA-3-444303: %SMART_LIC-3-HOT_STANDBY_OUT_OF_SYNC: Smart Licensing agent on hot standby is out of sync with active Smart Licensing agent.`

Explanation Smart Licensing Agent on the hot standby failed to process the data necessary to stay in sync with the active agent. If a switchover occurs the new active agent will not be in the same state as the current active agent configuration does not match the value of the enable flag in persistent storage. This can happen if a configuration is copied onto the system and a reload occurs. If the new configuration does not contain the Smart Licensing Enable command, the value in persistent storage will not match.

444304

Error Message `%ASA-4-444304: %SMART_LIC-4-IN_OVERAGE: One or more entitlements are in overage.`

Explanation This is for information only. The customer is still in compliance and within the overage amount as specified in their contract.

Error Message `%ASA-4-444304: %SMART_LIC-4-CONFIG_NOT_SAVED: Smart Licensing configuration has not been saved.`

This is for information only. The customer remains in IN/OUT_OF compliance state.

Recommended Action None.

444305

Error Message %ASA-5-444305: %SMART_LIC-5-SYSTEM_CLOCK_CHANGED: Smart Agent for Licensing System clock has been changed.

Explanation System clock was manually reset.

Error Message `%ASA-5-444305: %SMART_LIC-5-IN_COMPLIANCE: All entitlements are authorized.`

Explanation All customer requested entitlements are authorized by Cisco licensing service.

Error Message `%ASA-5-444305: %SMART_LIC-5-EVAL_START: Entering evaluation period.`

Explanation Either customer allocate entitlement prior to registration or customer registration has expired. The device is now de-registered and is in evaluation mode.

Error Message `%ASA-5-444305: %SMART_LIC-5-AUTHORIZATION_EXPIRED: Authorization expired.`

Explanation The device has not communicated with Cisco for an extended period of time and the device has not automatically renewed the entitlement authorizations.

Error Message `%ASA-5-444305: %SMART_LIC-5-COMM_RESTORED: Communications with Cisco licensing cloud restored.`

Explanation Smart Agent communication with the Cisco licensing service is restored.

Error Message `%ASA-5-444305: %SMART_LIC-5-COMM_INIT_FAILED: Failed to initialize communications with the Cisco Licensing Cloud.`

Explanation Smart Agent could not initialize communication with the Cisco licensing service.

Recommended Action None.

444306

Error Message `%ASA-6-444306: %SMART_LIC-6-AGENT_READY: Smart Agent for Licensing is initialized.`

Explanation Smart Agent is initialized and ready for use.

Error Message `%ASA-6-444306: %SMART_LIC-6-AGENT_ENABLED: Smart Agent for Licensing is enabled.`

Explanation Smart Agent is enabled and ready for use.

Error Message `%ASA-6-444306: %SMART_LIC-6-AGENT_REG_SUCCESS: Smart Agent for Licensing Registration with Cisco licensing cloud successful.`

Explanation Smart Licensing registration was successful.

Error Message `%ASA-6-444306: %SMART_LIC-6-AGENT_DEREG_SUCCESS: Smart Agent for Licensing De-registration with Cisco licensing cloud successful.`

Explanation Smart Licensing deregistration was successful.

Error Message `%ASA-6-444306: %SMART_LIC-6-DISABLED: Smart Agent for Licensing disabled.`

Explanation Smart Agent has been disabled.

Error Message `%ASA-6-444306: %SMART_LIC-6-ID_CERT_RENEW_SUCCESS: Identity certificate renewal successful.`

Explanation Customer identity certificate has been renewed successfully and can continue to use the device.

Error Message `%ASA-6-444306: %SMART_LIC-6-ENTITLEMENT_RENEW_SUCCESS: Entitlement authorization renewal with Cisco licensing cloud successful.`

Explanation Authorization renewal request is successful.

Error Message `%ASA-6-444306: %SMART_LIC-6-AUTH_RENEW_SUCCESS: Authorization renewal with Cisco licensing cloud successful.`

Explanation Authorization of customer requested entitlements are successfully renewed.

Error Message `%ASA-6-444306: %SMART_LIC-6-HA_ROLE_CHANGED: Smart Agent HA role changed to role.`

Explanation Smart Agent role on HA RP has been changed to either active or standby.

Error Message `%ASA-6-444306: %SMART_LIC-6-HA_CHASSIS_ROLE_CHANGED: Smart Agent HA chassis role changed to role.`

Explanation Smart Agent chassis role on HA has been changed to either active or standby.

Error Message `%ASA-6-444306: %SMART_LIC-6-AGENT_ALREADY_REGISTER: Smart Agent is already registered with the Cisco licensing cloud.`

Explanation Smart Licensing has already registered with Cisco. Use the force option to register again.

Error Message `%ASA-6-444306: %SMART_LIC-6-AGENT_ALREADY_DEREGISTER: Smart Agent is already Deregistered with the CSSM.`

Explanation Smart Licensing has already de-registered with Cisco, use the force option to register again.

Error Message `%ASA-6-444306: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is status.`

Explanation Notification of whether the usage of export controlled features is allowed or not allowed. This message is generated following the registration with Cisco licensing cloud.

Recommended Action None.

444307

Error Message `%ASA-7-444307: %SMART_LIC-7-DAILY_JOB_TIMER_RESET: Daily job timer reset.`

Explanation This message is only used for testing purposes and does not indicate an error.

Recommended Action None.

446001

Error Message `%ASA-4-446001: Maximum TLS Proxy session limit of max_sess reached`

Explanation A configured maximum session limit for TLS proxy was reached. New sessions beyond the limit were denied.

- *max_sess* —The currently effective maximum session limit

Recommended Action If more TLS sessions are needed, use the **tls-proxy maximum-sessions max_sess** command to increase the limit. Alternatively, you can use the **tls-proxy proxy_name** and **tls-proxy maximum-sessions max_sess** commands, and then reboot for the commands to take effect.

446003

Error Message `%ASA-4-446003: Denied TLS Proxy session from src_int :src_ip /src_port to dst_int :dst_ip /dst_port , UC-IME license is disabled.`

Explanation The UC-IME license is either on or off. Once enabled, UC-IME can use any number of available TLS sessions, according to the Secure Firewall ASA limit and the K8 export limit.

- *src_int* —The source interface name (inside or outside)
- *src_ip* —The source IP address
- *src_port* —The source port
- *dst_int* —The destination interface name (inside or outside)
- *dst_ip* —The destination IP address
- *dst_port* —The destination port

Recommended Action Check to see if UC-IME is disabled. If so, activate it.

447001

Error Message `%ASA-4-447001: ASP DP to CP queue_name was full. Queue length length , limit limit`

Explanation This message indicates a particular data path (DP) to control point (CP) event queue is full, and one or more multiple enqueue actions have failed. If the event contains a packet block, such as for CP application inspection, the packet will be dropped by the DP, and a counter from the **show asp drop** command will increment. If the event is for punt to CP, a typical counter is the Punt no memory ASP-drop counter.

- *queue* —The name of the DP-CP event queue.
- *length* —The current number of events on the queue.
- *limit* —The maximum number of events that are allowed on the queue.

Recommended Action The queue-full condition reflects the fact that the load on the CP has exceeded the CP processing ability, which may or may not be a temporary condition. You should consider reducing the feature load on the CP if this message appears repeatedly. Use the **show asp event dp-cp** command to identify the features that contribute the most load on the event queue.

448001

Error Message `%ASA-4-448001: Denied SRTP crypto session setup on flow from src_int:src_ip/src_port to dst_int:dst_ip/dst_port, licensed K8 SRTP crypto session limit of limit exceeded`

Explanation For a K8 platform, the limit of 250 SRTP crypto sessions is enforced. Each pair of SRTP encrypt or decrypt sessions is counted as one SRTP crypto session. A call is counted toward this limit only when encryption or decryption is required for a medium, which means that if the pass-through is set for the call, even if both legs use SRTP, they are not counted toward this limit.

- *src_int* —The source interface name (inside or outside)
- *src_ip* —The source IP address
- *src_port* —The source port
- *dst_int* —The destination interface name (inside or outside)
- *dst_ip* —The destination IP address

- *dst_port* —The destination port
- *limit* —The K8 limit of SRTP crypto sessions (250)

Recommended Action None required. You can set up new SRTP crypto sessions only when existing SRTP crypto sessions have been released.

450001

Error Message `ASA-4-450001: Deny traffic for protocol protocol_id src interface_name :IP_address /port dst interface_name :IP_address /port , licensed host limit of num exceeded.`

Explanation The licensed host limit was exceeded. This message applies to the ASA 5505 ASA only.

- *protocol_id* —The protocol ID number
- *interface_name* —The interface associated with the sender or receiver of the packet
- *IP_address* —The IP address of the sender/receiver of the packet
- *port* —The port number of the packet transmitted
- *num* —The maximum host limit value

Recommended Action None required.