

Syslog Messages 722001 to 776254

This chapter contains the following sections:

- Messages 722001 to 722056, on page 1
- Messages 723001 to 736001, on page 14
- Messages 737001 to 776254, on page 37

Messages 722001 to 722056

This section includes messages from 722001 to 722056.

722001

Error Message `%FTD-4-722001: IP IP_address Error parsing SVC connect request.`

Explanation The request from the SVC was invalid.

Recommended Action Research as necessary to determine if this error was caused by a defect in the SVC, an incompatible SVC version, or an attack against the device.

722002

Error Message `%FTD-4-722002: IP IP_address Error consolidating SVC connect request.`

Explanation There is not enough memory to perform the action.

Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

722003

Error Message `%FTD-4-722003: IP IP_address Error authenticating SVC connect request.`

Explanation The user took too long to download and connect.

Recommended Action Increase the timeouts for session idle and maximum connect time.

722004

Error Message `%FTD-4-722004: Group group User user-name IP IP_address Error responding to SVC connect request.`

Explanation There is not enough memory to perform the action.

Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

722005

Error Message `%FTD-5-722005: Group group User user-name IP IP_address Unable to update session information for SVC connection.`

Explanation There is not enough memory to perform the action.

Recommended Action Purchase more memory, upgrade the device, or reduce the load on the device.

722006

Error Message `%FTD-5-722006: Group group User user-name IP ip_address Invalid address ip_address assigned to SVC connection.`

Explanation An invalid address was assigned to the user.

Recommended Action Verify and correct the address assignment, if possible. Otherwise, notify your network administrator or escalate this issue according to your security policy. For additional assistance, contact the Cisco TAC.

722007

Error Message `%FTD-3-722007: Group group User user-name IP IP_address SVC Message: type-num/EMERGENCY: message.`

Explanation The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal

- 16—Logout

- 17—Closed due to error

- 18—Closed due to rekey

- 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

Recommended Action None required.

722008

Error Message `%FTD-3-722008: Group group User user-name IP IP_address SVC Message: type-num/ALERT: message.`

Explanation The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal

- 16—Logout

- 17—Closed due to error

- 18—Closed due to rekey

- 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

Recommended Action None required.

722009

Error Message `%FTD-3-722009: Group group User user-name IP IP_address SVC Message: type-num/CRITICAL: message.`

Explanation The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal

- 16—Logout

- 17—Closed due to error

- 18—Closed due to rekey

- 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

Recommended Action None required.

722010

Error Message `%FTD-5-722010: Group group User user-name IP IP_address SVC Message: type-num/ERROR: message.`

Explanation The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal

- 16—Logout

- 17—Closed due to error

- 18—Closed due to rekey

- 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

Recommended Action None required.

722011

Error Message `%FTD-5-722011: Group group User user-name IP IP_address SVC Message: type-num/WARNING: message.`

Explanation The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal

- 16—Logout

- 17—Closed due to error

- 18—Closed due to rekey

- 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

Recommended Action None required.

722012

Error Message `%FTD-5-722012: Group group User user-name IP IP_address SVC Message: type-num/NOTICE: message.`

Explanation The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal

- 16—Logout

- 17—Closed due to error

- 18—Closed due to rekey

- 1-15, 19-31—Reserved and unused

- **message**—A text message from the SVC

Recommended Action None required.

722013

Error Message `%FTD-6-722013: Group group User user-name IP IP_address SVC Message: type-num/INFO: message.`

Explanation The SVC issued a message.

- **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal

- 16—Logout

- 17—Closed due to error

- 18—Closed due to rekey

- 1-15, 19-31—Reserved and unused

• **message**—A text message from the SVC

Recommended Action None required.

722014

Error Message `%FTD-6-722014: Group group User user-name IP IP_address SVC Message: type-num/DEBUG: message.`

Explanation The SVC issued a message.

• **type-num**— A number from 0 to 31 indicating a message type. Message types are as follows:

- 0—Normal.

- 16—Logout

- 17—Closed due to error

- 18—Closed due to rekey

- 1-15, 19-31—Reserved and unused

• **message**—A text message from the SVC

Recommended Action None required.

722015

Error Message `%FTD-4-722015: Group group User user-name IP IP_address Unknown SVC frame type: type-num`

Explanation The SVC sent an invalid frame type to the device, which might be caused by an SVC version incompatibility.

• **type-num—**The number identifier of the frame type

Recommended Action Verify the SVC version.

722016

Error Message `%FTD-4-722016: Group group User user-name IP IP_address Bad SVC frame length: length expected: expected-length`

Explanation The expected amount of data was not available from the SVC, which might be caused by an SVC version incompatibility.

Recommended Action Verify the SVC version.

722017

Error Message `%FTD-4-722017: Group group User user-name IP ip_address Bad SVC framing: xx.2Xxx.2Xxx.2X>, reserved: xx`

Explanation The SVC sent a badly framed datagram, which might be caused by an SVC version incompatibility.

Recommended Action Verify the SVC version.

722018

Error Message `%FTD-4-722018: Group group User user-name IP IP_address Bad SVC protocol version: version, expected: expected`

Explanation The SVC sent a version unknown to the device, which might be caused by an SVC version incompatibility.

Recommended Action Verify the SVC version.

722019

Error Message `%FTD-4-722019: Group group User user-name IP IP_address Not enough data for an SVC header: length`

Explanation The expected amount of data was not available from the SVC, which might be caused by an SVC version incompatibility.

Recommended Action Verify the SVC version.

722020

Error Message `%FTD-3-722020: TunnelGroup tunnel_group GroupPolicy group_policy User user-name IP IP_address No address available for SVC connection`

Explanation Address assignment failed for the AnyConnect session. No IP addresses are available.

- **tunnel_group—**The name of the tunnel group that the user was assigned to or used to log in
- *group_policy* —The name of the group policy that the user was assigned to
- *user-name* —The name of the user with which this message is associated
- *IP_address* —The public IP (Internet) address of the client machine

Recommended Action Check the configuration listed in the **ip local ip** command to see if enough addresses exist in the pools that have been assigned to the tunnel group and the group policy. Check the DHCP configuration and status. Check the address assignment configuration. Enable IPAA syslog messages to determine why the AnyConnect client cannot obtain an IP address.

722028

Error Message `%FTD-5-722028: Group group User user-name IP IP_address Stale SVC connection closed.`

Explanation An unused SVC connection was closed.

Recommended Action None required. However, the client may be having trouble connecting if multiple connections are established. The SVC log should be examined.

722029

Error Message `%FTD-7-722029: Group group User user-name IP IP_address SVC Session Termination: Conns: connections, DPD Conns: DPD_conns, Comp resets: compression_resets, Dcmp resets: decompression_resets.`

Explanation The number of connections, reconnections, and resets that have occurred are reported. If **connections** is greater than 1 or the number of **DPD_conns**, **compression_resets,** or **decompression_resets** is greater than 0, it may indicate network reliability problems, which may be beyond the control of the Secure Firewall Threat Defense administrator. If there are many connections or DPD connections, the user may be having problems connecting and may experience poor performance.

- **connections—**The total number of connections during this session (one is normal)
- **DPD_conns—**The number of reconnections due to DPD
- **compression_resets—**The number of compression history resets
- **decompression_resets—**The number of decompression history resets

Recommended Action The SVC log should be examined. You may want to research and take appropriate action to resolve possible network reliability problems.

722030

Error Message `%FTD-7-722030: Group group User user-name IP IP_address SVC Session Termination: In: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops.`

Explanation End-of-session statistics are being recorded.

- **data_bytes—**The number of inbound (from SVC) data bytes
- **ctrl_bytes—**The number of inbound control bytes
- **data_pkts—**The number of inbound data packets
- **ctrl_pkts—**The number of inbound control packets
- **drop_pkts—**The number of inbound packets that were dropped

Recommended Action None required.

722031

Error Message `%FTD-7-722031: Group group User user-name IP IP_address SVC Session Termination: Out: data_bytes (+ctrl_bytes) bytes, data_pkts (+ctrl_pkts) packets, drop_pkts drops.`

Explanation End-of-session statistics are being recorded. The statistics include data bytes, control packet bytes, data packets, control packets, and dropped packets.

- **data_bytes—**The number of outbound (to SVC) data bytes
- **ctrl_bytes—**The number of outbound control bytes
- **data_pkts—**The number of outbound data packets
- **ctrl_pkts—**The number of outbound control packets
- **drop_pkts—**The number of outbound packets that were dropped

In some cases, the dropped packets count is more than the overall data and control packets because this syslog does not provide the break-down of the dropped packets. Few examples of such instances:

```
2020-09-30T09:06:09.254798+00:00 local4.err pg122d-vpn116 %FTD-3-722031: Group <GP_1> User
<xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 800808 (+32)
bytes, 1957 (+4) packets, 3358 drops.

2020-09-30T08:53:11.359833+00:00 local4.err srr10c-vpn103 %FTD-3-722031: Group <GP_2> User
<xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 413194 (+32)
bytes, 1540 (+4) packets, 2059 drops.

2020-09-30T08:37:59.287415+00:00 local4.err srr10c-vpn115 %FTD-3-722031: Group <GP_3> User
<xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 571473 (+48)
bytes, 1283 (+6) packets, 1323 drops.

2020-09-30T08:31:48.105943+00:00 local4.err srr10c-vpn114 %FTD-3-722031: Group <GP_4> User
<xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 131566 (+0)
bytes, 283 (+0) packets, 320 drops.

2020-09-30T08:28:38.053003+00:00 local4.err pg122d-vpn117 %FTD-3-722031: Group <GP_5> User
<xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 497446 (+23)
bytes, 1048 (+1) packets, 1128 drops.

2020-09-30T07:45:43.044373+00:00 local4.err srr10c-vpn114 %FTD-3-722031: Group <GP_6> User
<xxxxxxxxxxxx.xxxxxxxxxx@intel.com> IP <x.x.x.x> SVC Session Termination: Out: 153165 (+16)
bytes, 398 (+2) packets, 1045 drops.
```

Recommended Action None required.

722032

Error Message `%FTD-5-722032: Group <group> User <user_name> IP <ip_address> New TCP|UDP SVC connection replacing old connection.`

Explanation A new SVC connection is replacing an existing one. You may be having trouble connecting.

Recommended Action Examine the SVC log.

722033

Error Message `%FTD-5-722033: Group <group> User <user_name> IP <ip_address> First TCP|UDP SVC connection established for SVC session.`

Explanation The first SVC connection was established for the SVC session.

Recommended Action None required.

722034

Error Message `%FTD-5-722034: Group <group> User <user_name> IP <ip_address> New TCP|UDP SVC connection, no existing connection.`

Explanation A reconnection attempt has occurred. An SVC connection is replacing a previously closed connection. There is no existing connection for this session because the connection was already dropped by the SVC or the Secure Firewall Threat Defense device. You may be having trouble connecting.

Recommended Action Examine the Secure Firewall Threat Defense device log and SVC log.

722035

Error Message `%FTD-3-722035: Group group User user-name IP IP_address Received large packet length (threshold num).`

Explanation A large packet was received from the client.

- **length—**The length of the large packet
- **num—**The threshold

Recommended Action Enter the **anyconnect ssl df-bit-ignore enable** command under the group policy to allow the Secure Firewall Threat Defense device to fragment the packets arriving with the DF bit set.

722036

Error Message `%FTD-6-722036: Group group User user-name IP IP_address Transmitting large packet length (threshold num).`

Explanation A large packet was sent to the client. The source of the packet may not be aware of the MTU of the client. This could also be due to compression of non-compressible data.

- **length—**The length of the large packet
- **num—**The threshold

Recommended Action Turn off SVC compression, otherwise, none required.

722037

Error Message `%FTD-5-722037: Group group User user-name IP ip_address SVC closing connection: reason.`

Explanation An SVC connection was terminated for the given reason. This behavior may be normal, or you may be having trouble connecting.

- **reason—**The reason that the SVC connection was terminated

Recommended Action Examine the SVC log.

722038

Error Message `%FTD-5-722038: Group group User name IP user-name SVC terminating session: reason.`

Explanation An SVC session was terminated for the given reason. This behavior may be normal, or you may be having trouble connecting.

- **reason—**The reason that the SVC session was terminated

Recommended Action Examine the SVC log if the reason for termination was unexpected.

722041

Error Message `%FTD-4-722041: TunnelGroup tunnel_group GroupPolicy group_policy User username IP peer_address No IPv6 address available for SVC connection`

Explanation An IPv6 address was not available for assignment to the remote SVC client.

- *n* —The SVC connection identifier

Recommended Action Augment or create an IPv6 address pool, if desired.

722042

Error Message `%FTD-4-722042: Group group User user IP ip Invalid Cisco SSL Tunneling Protocol version`

Explanation An invalid SVC or AnyConnect client is trying to connect.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

Recommended Action Validate that the SVC or AnyConnect client is compatible with the Secure Firewall Threat Defense device.

722043

Error Message `%FTD-5-722043: Group group User user IP ip DTLS disabled: unable to negotiate cipher`

Explanation The DTLS (UDP transport) cannot be established. The SSL encryption configuration was probably changed.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

Recommended Action Revert the SSL encryption configuration. Make sure there is at least one block cipher (AES, DES, or 3DES) in the SSL encryption configuration.

722044

Error Message `%FTD-5-722044: Group group User user IP ip Unable to request IPvver address for SSL tunnel`

Explanation An IP address cannot be requested because of low memory on the Secure Firewall Threat Defense device.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect
- *ver* —Either IPv4 or IPv6, based on the IP address version being requested

Recommended Action Reduce the load on the Secure Firewall Threat Defense device or add more memory.

722045

Error Message `%FTD-3-722045: Connection terminated: no SSL tunnel initialization data`

Explanation Data to establish a connection is missing. This is a defect in the Secure Firewall Threat Defense software.

Recommended Action Contact the Cisco TAC for assistance.

722046

Error Message `%FTD-3-722046: Group group User user IP ip Session terminated: Unable to establish tunnel`

Explanation The Secure Firewall Threat Defense device cannot set up connection parameters. This is a defect in the Secure Firewall Threat Defense software.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

Recommended Action Contact the Cisco TAC for assistance.

722047

Error Message `%FTD-4-722047: Group group User user IP ip Tunnel terminated: SVC not enabled or invalid SVC image on the FTD`

Explanation The user logged in via the web browser and tried to start the SVC or AnyConnect client. The SVC service is not enabled globally, or the SVC image is invalid or corrupted. The tunnel connection has been terminated, but the clientless connection remains.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

Recommended Action Enable the SVC globally using the **svc enable** command. Validate the integrity of versions of the SVC images by reloading new images using the **svc image** command.

722048

Error Message `%FTD-4-722048: Group group User user IP ip Tunnel terminated: SVC not enabled for the user`

Explanation The user logged in via the web browser, and tried to start the SVC or AnyConnect client. The SVC service is not enabled for this user. The tunnel connection has been terminated, but the clientless connection remains.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

Recommended Action Enable the service for this user using the **group-policy** and **username** commands.

722049

Error Message `%FTD-4-722049: Group group User user IP ip Session terminated: SVC not enabled or invalid SVC image on the FTD`

Explanation The user logged in via the AnyConnect client. The SVC service is not enabled globally, or the SVC image is invalid or corrupted. The session connection has been terminated.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

Recommended Action Enable the SVC globally using the **svc-enable** command. Validate the integrity and versions of the SVC images by reloading new images using the **svc image** command.

722050

Error Message `%FTD-4-722050: Group group User user IP ip Session terminated: SVC not enabled for the user`

Explanation The user logged in through the AnyConnect client. The SVC service is not enabled for this user. The session connection has been terminated.

- *group* —The name of the group policy with which the user is trying to connect
- *user* —The name of the user who is trying to connect
- *ip* —The IP address of the user who is trying to connect

Recommended Action Enable the service for this user using the **group-policy** and **username** commands.

722051

Error Message `%FTD-6-722051: Group group-policy User username IP public-ip IPv4 Address assigned-ip IPv6 address assigned-ip assigned to session`

Explanation The specified address has been assigned to the given user.

- *group-policy* —The group policy that allowed the user to gain access
- *username* —The name of the user
- *public-ip* —The public IP address of the connected client
- *assigned-ip* —The IPv4 or IPv6 address that is assigned to the client

Recommended Action None required.

722053

Error Message `%FTD-6-722053: Group g User u IP ip Unknown client user-agent connection`

Explanation An unknown or unsupported SSL VPN client has connected to the Secure Firewall Threat Defense device. Older clients include the Cisco SVC and the Cisco AnyConnect client earlier than Version 2.3.1.

- *g* —The group policy under which the user logged in
- *u* —The name of the user
- *ip* —The IP address of the client

- *user-agent* —The user agent (usually includes the version) received from the client

Recommended Action Upgrade to a supported Cisco SSL VPN client.

722054

Error Message `%FTD-4-722054: Group group_policy User user_name IP remote_IP SVC terminating connection: Failed to install Redirect URL: redirect_URL Redirect ACL: non_exist for assigned_IP.`

Explanation An error occurred for an AnyConnect VPN connection when a redirect URL was installed, and the ACL was received from the ISE, but the redirect ACL does not exist on the Secure Firewall Threat Defense device.

- *group policy* —The group policy that allowed the user to gain access
- *user name* —Username of the requester for the remote access
- *remote IP* — Remote IP address that the connection request is coming from
- *redirect URL* —The URL for the HTTP traffic redirection
- *assigned IP* —The IP address that is assigned to the user

Recommended Action Configure the redirect ACL on the Secure Firewall Threat Defense device.

722055

Error Message `%FTD-6-722055: Group group-policy User username IP public-ip Client Type: user-agent`

Explanation The indicated user is attempting to connect with the given user-agent.

- *group-policy* —The group policy that allowed the user to gain access
- *username* —The name of the user
- *public-ip* —The public IP address of the connected client
- *user-agent* —The user-agent string provided by the connecting client. Usually includes the AnyConnect version and host operating system for AnyConnect clients.

Recommended Action None required.

722056

Error Message `%FTD-4-722056: Unsupported AnyConnect client connection rejected from ip address. Client info: user-agent string. Reason: reason`

Explanation This syslog indicates that an AnyConnect client connection is rejected. The reason for this is provided in the syslog along with the client information.

- *ip address* —IP address from which a connection with the old client is attempted,
- *user- agent string* —User-Agent header in the client request. Usually includes the AnyConnect version and host operating system for AnyConnect clients
- *reason* —Reason for rejection

Recommended Action Use the client information and reason provided in the syslog to resolve the issue.

722057

Error Message `%FTD-4-722057: Group group policy User username IP client IP SVC terminating connection: Failed to bind SGT tag with assigned IP: assigned IP.`

Explanation When the device fails to bind a Security Group Tag (SGT) to the assigned IP address during remote access VPN authentication, this message is generated. The syslog message provides information that helps to identify when an SGT binding error occurs, along with specific user, group, and IP information, making it much easier to diagnose and resolve related issues.

Recommended Action Use the client information and reason provided in the syslog to resolve the issue.

Messages 723001 to 736001

This section includes messages from 723001 to 736001.

723001

Error Message `%FTD-6-723001: Group group-name User user-name IP IP_address WebVPN Citrix ICA connection connection is up.`

Explanation The Citrix connection is up.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP_address**—The IP address of the Citrix user
- **connection—**The Citrix connection identifier

Recommended Action None required.

723002

Error Message `%FTD-6-723002: Group group-name User user-name IP IP_address WebVPN Citrix ICA connection connection is down.`

Explanation The Citrix connection is down.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP_address**—The IP address of the Citrix user
- **connection—**The Citrix connection identifier

Recommended Action No action is required when the Citrix ICA connection is terminated intentionally by the client, the server, or the Secure Firewall Threat Defense administrator. However, if this is not the case, verify that the WebVPN session in which the Citrix ICA connection is set up is still active. If it is inactive, then receiving this message is normal. If the WebVPN session is still active, verify that the ICA client and Citrix server both work correctly and that there is no error displayed. If not, bring either or both up or respond to any error. If this message is still received, contact the Cisco TAC and provide the following information:

- Network topology
- Delay and packet loss
- Citrix server configuration

- Citrix ICA client information
- Steps to reproduce the problem
- Complete text of all associated messages

723003

Error Message `%FTD-7-723003: No memory for WebVPN Citrix ICA connection` *`connection`*`.`

Explanation The Secure Firewall Threat Defense device is running out of memory. The Citrix connection was rejected.

- **connection—**The Citrix connection identifier

Recommended Action Verify that the Secure Firewall Threat Defense device is working correctly. Pay special attention to memory and buffer usage. If the Secure Firewall Threat Defense device is under heavy load, buy more memory and upgrade the Secure Firewall Threat Defense device or reduce the load on the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

723004

Error Message `%FTD-7-723004: WebVPN Citrix encountered bad flow control` *`flow`*`.`

Explanation The Secure Firewall Threat Defense device encountered an internal flow control mismatch, which can be caused by massive data flow, such as might occur during stress testing or with a high volume of ICA connections.

Recommended Action Reduce ICA connectivity to the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

723005

Error Message `%FTD-7-723005: No channel to set up WebVPN Citrix ICA connection.`

Explanation The Secure Firewall Threat Defense device was unable to create a new channel for Citrix.

Recommended Action Verify that the Citrix ICA client and the Citrix server are still alive. If not, bring them back up and retest. Check the Secure Firewall Threat Defense device load, paying special attention to memory and buffer usage. If the Secure Firewall Threat Defense device is under heavy load, upgrade the Secure Firewall Threat Defense device, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

723006

Error Message `%FTD-7-723006: WebVPN Citrix SOCKS errors.`

Explanation An internal Citrix SOCKS error has occurred on the Secure Firewall Threat Defense device.

Recommended Action Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the Citrix ICA client and the Secure Firewall Threat Defense device, paying attention to packet loss. Resolve any abnormal network conditions. If the problem persists, contact the Cisco TAC.

723007

Error Message `%FTD-7-723007: WebVPN Citrix ICA connection connection list is broken.`

Explanation The Secure Firewall Threat Defense device internal Citrix connection list is broken.

- **connection—**The Citrix connection identifier

Recommended Action Verify that the Secure Firewall Threat Defense device is working correctly, paying special attention to memory and buffer usage. If the Secure Firewall Threat Defense device is under heavy load, upgrade the Secure Firewall Threat Defense device, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

723008

Error Message `%FTD-7-723008: WebVPN Citrix ICA SOCKS Server server is invalid.`

Explanation An attempt was made to access a Citrix Socks server that does not exist.

- **server**—The Citrix server identifier

Recommended Action Verify that the Secure Firewall Threat Defense device is working correctly. Note whether or not there is any memory or buffer leakage. If this issue occurs frequently, capture information about memory usage, network topology, and the conditions during which this message is received. Send this information to the Cisco TAC for review. Make sure that the WebVPN session is still up while this message is being received. If not, determine the reason that the WebVPN session is down. If the Secure Firewall Threat Defense device is under heavy load, upgrade the Secure Firewall Threat Defense device, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

723009

Error Message `%FTD-7-723009: Group group-name User user-name IP IP_address WebVPN Citrix received data on invalid connection connection.`

Explanation Data was received on a Citrix connection that does not exist.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP_address**—The IP address of the Citrix user
- **connection—**The Citrix connection identifier

Recommended Action The original published Citrix application connection was probably terminated, and the remaining active published applications lost connectivity. Restart all published applications to generate a new Citrix ICA tunnel. If the Secure Firewall Threat Defense device is under heavy load, upgrade the Secure Firewall Threat Defense device, add memory, or reduce the load. If the problem persists, contact the Cisco TAC.

723010

Error Message `%FTD-7-723010: Group group-name User user-name IP IP_address WebVPN Citrix received data on invalid connection channel.`

Explanation An abort was received on a nonexistent Citrix connection, which can be caused by massive data flow (such as stress testing) or a high volume of ICA connections, especially during network delay or packet loss.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP_address**—The IP address of the Citrix user
- channel—The Citrix channel identifier
- **connection—**The Citrix connection identifier

Recommended Action Reduce the number of ICA connections to the Secure Firewall Threat Defense device, obtain more memory for the Secure Firewall Threat Defense device, or resolve the network problems.

723011

Error Message `%FTD-7-723011: Group group-name User user-name IP IP_address WebVPN Citrix received bad SOCKS socks message length msg-length. Expected length is exp-msg-length.`

Explanation The Citrix SOCKS message length is incorrect.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP_address**—The IP address of the Citrix user

Recommended Action Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the ICA client and the Secure Firewall Threat Defense device, paying attention to packet loss. After resolving any abnormal network conditions, if the problem still exists, contact the Cisco TAC.

723012

Error Message `%FTD-7-723012: Group group-name User user-name IP IP_address WebVPN Citrix received bad SOCKS socks message format.`

Explanation The Citrix SOCKS message format is incorrect.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP_address**—The IP address of the Citrix user

Recommended Action Verify that the Citrix ICA client is working correctly. In addition, check the network connection status between the ICA client and the Secure Firewall Threat Defense device, paying attention to packet loss. After resolving any abnormal network conditions, if the problem still exists, contact the Cisco TAC.

723013

Error Message `%FTD-7-723013: WebVPN Citrix encountered invalid connection connection during periodic timeout.`

Explanation The Secure Firewall Threat Defense internal Citrix timer has expired, and the Citrix connection is invalid.

- **connection—**The Citrix connection identifier

Recommended Action Check the network connection between the Citrix ICA client and the Secure Firewall Threat Defense device, and between the Secure Firewall Threat Defense device and the Citrix server. Resolve any abnormal network conditions, especially delay and packet loss. Verify that the Secure Firewall Threat Defense device works correctly, paying special attention to memory or buffer problems. If the Secure Firewall Threat Defense device is under heavy load, obtain more memory, upgrade the Secure Firewall Threat Defense device, or reduce the load. If the problem persists, contact the Cisco TAC.

723014

Error Message `%FTD-7-723014: Group group-name User user-name IP IP_address WebVPN Citrix TCP connection connection to server server on channel channel initiated.`

Explanation The Secure Firewall Threat Defense internal Citrix Secure Gateway is connected to the Citrix server.

- **group-name**—The name of the Citrix group
- **user-name**—The name of the Citrix user
- **IP_address**—The IP address of the Citrix user
- **connection—**The connection name
- server—The Citrix server identifier
- channel—The Citrix channel identifier (hexadecimal)

Recommended Action None required.

724001

Error Message `%FTD-4-724001: Group group-name User user-name IP IP_address WebVPN session not allowed. Unable to determine if Secure Desktop software was running on the client's workstation.`

Explanation The session was not allowed because an error occurred during processing of the CSD Host Integrity Check results on the Secure Firewall Threat Defense device.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP_address**—The IP address

Recommended Action Determine whether the client firewall is truncating long URLs. Uninstall CSD from the client and reconnect to the Secure Firewall Threat Defense device.

724002

Error Message `%FTD-4-724002: Group group-name User user-name IP IP_address WebVPN session not terminated. Secure Desktop was not running on the client's workstation.`

Explanation CSD is not running on the client machine.

- **group-name**—The name of the group
- **user-name**—The name of the user
- **IP_address**—The IP address

Recommended Action Verify that the end user can install and run CSD on the client machine.

725001

Error Message `%FTD-6-725001: Starting SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol session`

Explanation The SSL handshake has started with the remote device, which can be a client or server.

- **peer-type—**Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- **dst-ip**—The destination IP address
- **dst-port**—The destination port number
- **protocol**—The SSL version used for the SSL handshake

Recommended Action None required.

725002

Error Message `%FTD-6-725002: Device completed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port for protocol-version session`

Explanation The SSL handshake has completed successfully with the remote device.

- **peer-type—**Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number
- *protocol-version* —The version of the SSL protocol being used: SSLv3, TLSv1, DTLSv1, TLSv1.1 or TLSv1.2

Recommended Action None required.

725003

Error Message `%FTD-6-725003: SSL client peer-type:interface/src-ip to src-port/dst-ip request to resume previous session`

Explanation The remote device is trying to resume a previous SSL session.

- **peer-type—**Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

Recommended Action None required.

725004

Error Message `%FTD-6-725004: Device requesting certificate from SSL client peer-type:interface/src-ip to src-port/dst-ip for authentication`

Explanation The Secure Firewall Threat Defense device has requested a client certificate for authentication.

- **peer-type—**Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

Recommended Action None required.

725005

Error Message `%FTD-6-725005: SSL server peer-type:interface/src-ip to src-port/dst-ip requesting our device certificate for authentication`

Explanation The server has requested the certificate of the Secure Firewall Threat Defense device for authentication.

- **peer-type—**Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

Recommended Action None required.

725006

Error Message `%FTD-6-725006: Device failed SSL handshake with peer-type interface:src-ip/src-port to dst-ip/dst-port`

Explanation The SSL handshake with the remote device has failed.

- **peer-type—**Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

Recommended Action Look for syslog message 725014, which indicates the reason for the failure.

725007

Error Message `%FTD-6-725007: SSL session with peer-type interface:src-ip/src-port to dst-ip/dst-port terminated`

Explanation The SSL session has terminated.

- **peer-type—**Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

Recommended Action None required.

725008

Error Message `%FTD-7-725008: SSL client peer-type:interface/src-ip to src-port/dst-ip proposes the following dst-port cipher(s)`

Explanation The number of ciphers proposed by the remote SSL device are listed.

- **peer-type—**Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number
- *n* —The number of supported ciphers

Recommended Action None required.

725009

Error Message `%FTD-7-725009: Device proposes the following n cipher(s) to server interface:src-ip/src_port to dst_ip/dst_port`

Explanation The number of ciphers proposed to the SSL server are listed.

- **peer-type—**Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number
- *n* —The number of supported ciphers

Recommended Action None required.

725010

Error Message `%FTD-7-725010: Device supports the following n cipher(s)`

Explanation The number of ciphers supported by the Secure Firewall Threat Defense device for an SSL session are listed.

- **n**—The number of supported ciphers

Recommended Action None required.

725011

Error Message `%FTD-7-725011: Cipher[order] : cipher_name`

Explanation Always following messages 725008, 725009, and 725010, this message indicates the cipher name and its order of preference.

- **order**—The order of the cipher in the cipher list
- **cipher_name—**The name of the OpenSSL cipher from the cipher list

Recommended Action None required.

725012

Error Message `%FTD-7-725012: Device chooses cipher cipher for the SSL session with client peer-type:interface/src-ip to src-port/dst-ip`

Explanation The cipher that was chosen by the Cisco device for the SSL session is listed.

- **cipher—**The name of the OpenSSL cipher from the cipher list
- **peer-type—**Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

Recommended Action None required.

725013

Error Message `%FTD-7-725013: SSL server interface:src-ip/src-port to dst-ip/dst-port chooses cipher cipher`

Explanation The cipher that was chosen by the server for the SSL session is identified.

- **peer-type—**Either the server or the client, depending on the device that initiated the connection
- **interface**—The interface name that the SSL session is using
- **source-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- *dst-ip* —The destination IP address
- *dst-port* —The destination port number

- **cipher—**The name of the OpenSSL cipher from the cipher list

Recommended Action None required.

725014

Error Message `%FTD-7-725014: SSL lib error. Function: function Reason: reason`

Explanation The reason for failure of the SSL handshake is indicated.

- **function**—The function name where the failure is reported
- **reason**—The description of the failure condition

Recommended Action Include this message when reporting any SSL-related issue to the Cisco TAC.

725015

Error Message `%FTD-3-725015: Error verifying client certificate. Public key size in client certificate (actual_key_size bits) exceeds the maximum supported key size of ideal_key_size bits`

Explanation The verification of an SSL client certificate failed because of an unsupported (large) key size.

Recommended Action Use client certificates with key sizes that are less than or equal to 4096 bits.

725016

Error Message `%FTD-6-725016: Device selects trust-point trustpoint for peer-type interface:src-ip/src-port to dst-ip/dst-port`

Explanation With server-name indication (SNI), the certificate used for a given connection may not be the certificate configured on the interface. There is also no indication of which certificate trustpoint has been selected. This syslog gives an indication of the trustpoint used by the connection (given by *interface* :*src-ip* /*src-port*).

- *trustpoint* —The name of the configured trustpoint that is being used for the specified connection
- *interface* —The name of the interface on the Secure Firewall Threat Defense device
- *src-ip* —The IP address of the peer
- *src-port* —The port number of the peer
- *dst-ip* —The IP address of the destination
- *dst-port* —The port number of the destination

Recommended Action None required.

725017

Error Message `%FTD-7-725017: No certificates received during the handshake with s s:B/d to B/d for s session`

Explanation A remote client has not sent a valid certificate.

- *remote_device* —Identifies whether a handshake is performed with the client or server
- *ctm->interface* —The interface name on which the handshake is sent

- *ctm->src_ip* —The IP address of the SSL server, which will communicate with the client
- *ctm->src_port* —The port of the SSL server, which will communicate with the client
- *ctm->dst_ip* —The IP address of the client
- *ctm->dst_port* —The port of the client through which it responds
- *s->method->version* —The protocol version involved in the transaction (SSLv3, TLSv1, or DTLSv1)

Recommended Action None required.

725021

Error Message `%FTD-7-725021: Device preferring cipher-suite cipher(s). Connection info: interface :src-ip /src-port to dst-ip /dst-port`

Explanation The cipher suites being preferred when negotiating the handshake is listed in this message.

- **cipher-suite**—Preferred cipher suite string
- **interface**—The interface name that the SSL session is using
- **src-ip**—The source IPv4 or IPv6 address
- **src-port**—The source port number
- **dst-ip**—The destination IPv4 or IPv6 address
- **dst-port**—The destination port number

Following is a list of prefered cipher suite strings that are used when negotiating the handshake:

- server
- SUITE-B
- ChaCha20
- client
- SHA-256 hash

Recommended Action None required.

725022

Error Message `%FTD-7-725022: Device skipping cipher : cipher - reason. Connection info: interface :src-ip /src-port to dst-ip /dst-port`

Explanation This syslog displays the reason for skipping a particular cipher in a list of cipher suites when negotiating the handshake.

- **cipher-suite**—Preferred cipher suite string
- **reason**—Reason for skipping a cipher.
- **interface**—The interface name that the SSL session is using
- **src-ip**—The source IPv4 or IPv6 address

- **src-port**—The source port number
- **dst-ip**—The destination IPv4 or IPv6 address
- **dst-port**—The destination port number

Following list provides few example reason for skipping a particular cipher:

- Ephemeral EC key is not compatible with trust-point <trust point>
- Not supported by protocol version
- PSK server callback is not set
- Not permitted by security callbacks
- ECDHE-ECDSA is broken on Safari
- Cipher suite does not use SHA256
- Unknown cipher
- Wrong cipher
- Message digest changed
- Ciphersuite from previous session not selected

Recommended Action None required.

725025

Error Message `%FTD-6-725025: SSL Pre-auth connection rate limit hit s watermark`

Explanation When the device reaches the rate-limit threshold for the number of pre-authenticated SSL connections. This message appears when the number of pre-authenticated SSL connections is high (90% of the limit) or when it is low (70% of the limit). The syslog is rate-limited to one syslog for every 10 seconds. In this message, s denotes high or low of the threshold limit.

Recommended Action Contact Cisco TAC.

726001

Error Message `%FTD-6-726001: Inspected im_protocol im_service Session between Client im_client_1 Packet flow from im_client_2:/src_ifc/sip to sport:/dest_ifc/dip Action: dport action`

Explanation An IM inspection was performed on an IM message and the specified criteria were satisfied. The configured action is taken.

- *im_protocol* —MSN IM or Yahoo IM
- *im_service* —The IM services, such as chat, conference, file transfer, voice, video, games, or unknown
- *im_client_1* , *im_client_2* —The client peers that are using the IM service in the session: *client_login_name* or "?"
- *src_ifc* —The source interface name
- *sip* —The source IP address

- *sport* —The source port
- *dest_ifc* —The destination interface name
- *dip* —The destination IP address
- *dport* —The destination port
- *action* —The action taken: reset connection, dropped connection, or received
- *class_map_id* —The matched class-map ID
- *class_map_name* —The matched class-map name

Recommended Action None required.

733100

Error Message `%FTD-4-733100: [Object] drop rate-rate_ID exceeded. Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt`

Explanation The specified object in the message has exceeded the specified burst threshold rate or average threshold rate. The object can be a drop activity of a host, TCP/UDP port, IP protocol, or various drops caused by potential attacks. The Secure Firewall Threat Defense device may be under attack.

- *Object* —The general or particular source of a drop rate count, which might include the following:

- Firewall

- Bad pkts

- Rate limit

- DoS attck

- ACL drop

- Conn limit

- ICMP attk

- Scanning

- SYN attck

- Inspect

- Interface

(A citation of a particular interface object might take a number of forms. For example, you might see 80/HTTP**,** which would signify port 80, with the well-known protocol HTTP.)

- *rate_ID* —The configured rate that is being exceeded. Most objects can be configured with up to three different rates for different intervals.
- *rate_val* —A particular rate value.
- *total_cnt* —The total count since the object was created or cleared.

The following three examples show how these variables occur:

- For an interface drop caused by a CPU or bus limitation:

```
%Firewall Threat Defense-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is
 1 per second, max configured rate is 8000; Current average rate is 2030 per second, max
configured rate is 2000; Cumulative total count is 3930654.”
```

- For a scanning drop caused by potential attacks:

```
%Firewall Threat Defense-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is
10 per second_max configured rate is 10; Current average rate is 245 per second_max configured
 rate is 5; Cumulative total count is 147409 (35 instances received)
```

- For bad packets caused by potential attacks:

```
%Firewall Threat Defense-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is
0 per second, max configured rate is 400; Current average rate is 760 per second, max
configured rate is 100; Cumulative total count is 1938933
```

- Because of the scanning rate configured and the **threat-detection rate scanning-rate 3600 average-rate 15** command:

```
%Firewall Threat Defense-4-733100: [144.60.88.2] drop rate-2 exceeded. Current burst rate
is 0 per second, max configured rate is 8; Current average rate is 5 per second, max
configured rate is 4; Cumulative total count is 38086
```

Perform the following steps according to the specified object type that appears in the message:

1. If the object in the message is one of the following:
   - Firewall
   - Bad pkts
   - Rate limit
   - DoS attck
   - ACL drop
   - Conn limit
   - ICMP attck
   - Scanning
   - SYN attck
   - Inspect
   - Interface

Recommended Action Check whether the drop rate is acceptable for the running environment.

1. Adjust the threshold rate of the particular drop to an appropriate value by using the threat-detection rate xxx command, where *xxx* is one of the following:
   - acl-drop
   - bad-packet-drop
   - conn-limit-drop
   - dos-drop
   - fw-drop
   - icmp-drop
   - inspect-drop
   - interface-drop
   - scanning-threat
   - syn-attack
2. If the object in the message is a TCP or UDP port, an IP address, or a host drop, check whether or not the drop rate is acceptable for the running environment.

3. Adjust the threshold rate of the particular drop to an appropriate value by using the threat-detection rate bad-packet-drop command.



Note If you do not want the drop rate exceed warning to appear, you can disable it by using the no threat-detection basic-threat command.

733101

Error Message `%FTD-4-733101: Object_objectIP. Current burst rate is rate_val per second, max configured rate is rate_val; Current average rate is rate_val per second, max configured rate is rate_val; Cumulative total count is total_cnt.`

Explanation The Secure Firewall Threat Defense device detected that a specific host (or several hosts in the same 1024-node subnet) is either scanning the network (attacking), or is being scanned (targeted).

- *object* —Attacker or target (a specific host or several hosts in the same 1024-node subnet)
- *objectIP* —The IP address of the scanning attacker or scanned target
- *rate_val* —A particular rate value
- *total_cnt* —The total count

The following two examples show how these variables occur:

```
%Firewall Threat Defense-4-733101: Subnet 100.0.0.0 is targeted. Current burst rate is 200
 per second, max configured rate is 0; Current average rate is 0 per second, max configured
 rate is 0; Cumulative total count is 2028.
%Firewall Threat Defense-4-733101: Host 175.0.0.1 is attacking. Current burst rate is 200
per second, max configured rate is 0; Current average rate is 0 per second, max configured
 rate is 0; Cumulative total count is 2024
```

Recommended Action For the specific host or subnet, use the **show threat-detection statistics host ip-address ip-mask** command to check the overall situation and then adjust the threshold rate of the scanning threat to the appropriate value. After the appropriate value is determined, an optional action can be taken to shun those host attackers (not subnet attacker) by configuring the **threat-detection scanning-threat shun-host** command. You may specify certain hosts or object groups in the shun-host except list. For more information, see the CLI configuration guide. If scanning detection is not desirable, you can disable this feature by using the **no threat-detection scanning** command.

733102

Error Message `%FTD-4-733102: Threat-detection adds host host to shun list`

Explanation A host has been shunned by the threat detection engine. When the **threat-detection scanning-threat shun** command is configured, the attacking hosts will be shunned by the threat detection engine.

- *%I* —A particular hostname

The following message shows how this command was implemented:

```
%Firewall Threat Defense-4-733102: Threat-detection add host 11.1.1.40 to shun list
```

Recommended Action To investigate whether the shunned host is an actual attacker, use the **threat-detection statistics host ip-address** command. If the shunned host is not an attacker, you can remove the shunned host from the threat detection engine by using the **clear threat-detection shun ip address** command. To remove all shunned hosts from the threat detection engine, use the **clear shun** command.

If you receive this message because an inappropriate threshold rate has been set to trigger the threat detection engine, then adjust the threshold rate by using the **threat-detection rate scanning-threat rate-interval x average-rate y burst-rate z** command.

733103

Error Message `%FTD-4-733103: Threat-detection removes host host from shun list`

Explanation A host has been shunned by the threat detection engine. When you use the **clear-threat-detection shun** command, the specified host will be removed from the shunned list.

- *%I* —A particular hostname

The following message shows how this command is implemented:

```
%Firewall Threat Defense-4-733103: Threat-detection removes host 11.1.1.40 from shun list
```

Recommended Action None required.

733104

Error Message `%FTD-4-733104: TCP Intercept SYN flood attack detected to host_ip/host_port (real_ip/real_port). Average rate of avg_rate SYNs/sec exceeded the threshold of threshold_rate.`

Explanation The Secure Firewall Threat Defense device is under Syn flood attack and protected by the TCP intercept mechanism, if the average rate for intercepted attacks exceeds the configured threshold. The message is showing which server is under attack and where the attacks are coming from.

Recommended Action Write an ACL to filter out the attacks.

733105

Error Message `%FTD-4-733105: TCP Intercept SYN flood attack detected to host_ip/host_port (real_ip/real_port). Burst rate of burst_rate SYNs/sec exceeded the threshold of threshold_rate.`

Explanation The Secure Firewall Threat Defense device is under Syn flood attack and protected by the TCP intercept mechanism, if the burst rate for intercepted attacks exceeds the configured threshold. The message is showing which server is under attack and where the attacks are coming from.

Recommended Action Write an ACL to filter out the attacks.

733201

(For IKEv2 connection requests) **Error Message 1** `%FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] Peer[peer-ip]: failure threshold of threshold-value exceeded: adding shun to interface interface. IKEv2:RA_excessive_client_initiation_requests`

(For SSL connection requests) **Error Message 2** `%FTD-4-733201: Threat-detection: Service[remote-access-client-initiations] Peer[peer-ip]: failure threshold of value exceeded: adding shun to interface interface. SSL: RA excessive client initiation requests.`

Explanation This message appears when the threat-detection service shunned an IP address due to excessive number of remote access client initiation requests to the headend from that host.

Recommended Action An IP address is shunned because it met the configured service threshold for mischievous activity. If this IP address should not be blocked, remove the shun manually using the **shun** CLI

.

734001

Error Message `%FTD-6-734001: DAP: User user, Addr ipaddr, Connection connection: The following DAP records were selected for this connection: string`

Explanation The DAP records that were selected for the connection are listed.

- *user* —The authenticated username
- *ipaddr* —The IP address of the remote client
- *connection* —The type of client connection, which can be one of the following:

- IPsec

- AnyConnect

- Clientless (web browser)

- Cut-Through-Proxy

- L2TP

- *DAP record names* —The comma-separated list of the DAP record names

Recommended Action None required.

734002

Error Message `%FTD-5-734002: DAP: User user, Addr ipaddr: Connection terminated by the following DAP records: string`

Explanation The DAP records that terminated the connection are listed.

- *user* —The authenticated username
- *ipaddr* —The IP address of the remote client
- *DAP record names* —The comma-separated list of the DAP record names

Recommended Action None required.

734003

Error Message `%FTD-7-734003: DAP: User name, Addr ipaddr: Session Attribute attr_name/value`

Explanation The AAA and endpoint session attributes that are associated with the connection are listed.

- *user* —The authenticated username

- *ipaddr* —The IP address of the remote client
- *attr/value* —The AAA or endpoint attribute name and value

Recommended Action None required.

734004

Error Message `%FTD-3-734004: DAP: Processing error: Code internal`

Explanation A DAP processing error occurred.

- *internal error code* —The internal error string

Recommended Action Enable the **debug dap errors** command and re-run DAP processing for further debugging information. If this does not resolve the issue, contact the Cisco TAC and provide the internal error code and any information about the conditions that generated the error.

735001

Error Message `%FTD-1-735001: Cooling Fan var1: OK`

Explanation A cooling fan has been restored to normal operation.

- *var1* —The device number markings

Recommended Action None required.

735002

Error Message `%FTD-1-735002: Cooling Fan var1: Failure Detected`

Explanation A cooling fan has failed.

- *var1* —The device number markings

Recommended Action Perform the following steps:

1. Check for obstructions that would prevent the fan from rotating.
2. Replace the cooling fan.
3. If the problem persists, record the message as it appears and contact the Cisco TAC.

735003

Error Message `%FTD-1-735003: Power Supply var1: OK`

Explanation A power supply has been restored to normal operation.

- *var1* —The device number markings

Recommended Action None required.

735004

Error Message `%FTD-1-735004: Power Supply var1: Failure Detected`

Explanation AC power has been lost, or the power supply has failed.

- *var1* —The device number markings

Recommended Action Perform the following steps:

1. Check for AC power failure.
2. Replace the power supply.
3. If the problem persists, record the message as it appears and contact the Cisco TAC.

735005

Error Message `%FTD-1-735005: Power Supply Unit Redundancy OK`

Explanation Power supply unit redundancy has been restored.

Recommended Action None required.

735006

Error Message `%FTD-1-735006: Power Supply Unit Redundancy Lost`

Explanation A power supply failure occurred. Power supply unit redundancy has been lost, but the Secure Firewall Threat Defense device is functioning normally with minimum resources. Any further failures will result in an Secure Firewall Threat Defense device shutdown.

Recommended Action To regain full redundancy, perform the following steps:

1. Check for AC power failure.
2. Replace the power supply.
3. If the problem persists, record the message as it appears and contact the Cisco TAC.

735007

Error Message `%FTD-1-735007: CPU var1: Temp: var2 var3, Critical`

Explanation The CPU has reached a critical temperature.

- *var1* —The device number markings
- *var2* —The temperature value
- *var3* —Temperature value units (C, F)

Recommended Action Record the message as it appears and contact the Cisco TAC.

735008

Error Message `%FTD-1-735008: Chassis Ambient var1: Temp: var2 var3, Critical`

Explanation A chassis ambient temperature sensor has reached a critical level.

- *var1* —The device number markings
- *var2* —The temperature value
- *var3* —Temperature value units (C, F)

Recommended Action Record the message as it appears and contact the Cisco TAC.

735009

Error Message `%FTD-2-735009: Environment Monitoring has failed initialization and configuration. Environment Monitoring is not running.`

Explanation Environment monitoring has experienced a fatal error during initialization and was unable to continue.

Recommended Action Collect the output of the **show environment** and **debug ipmi** commands. Record the message as it appears and contact the Cisco TAC.

735010

Error Message `%FTD-3-735010: Environment Monitoring has failed to update one or more of its records.`

Explanation Environment monitoring has experienced an error that temporarily prevented it from updating one or more of its records.

Recommended Action If this message appears repeatedly, collect the output from the **show environment driver** and **debug ipmi** commands. Record the message as it appears and contact the Cisco TAC.

735011

Error Message `%FTD-1-735011: Power Supply var1: Fan OK`

Explanation The power supply fan has returned to a working operating state.

- *var1* — Fan number

Recommended Action None required.

735012

Error Message `%FTD-1-735012: Power Supply var1: Fan Failure Detected`

Explanation The power supply fan has failed.

- *var1* — Fan number

Recommended Action Contact Cisco TAC to troubleshoot the failure. Power down the unit until this failure is resolved.

735013

Error Message `%FTD-1-735013: Voltage Channel var1: Voltage OK`

Explanation A voltage channel has returned to a normal operating level.

- *var1* — Voltage channel number

Recommended Action None required.

735014

Error Message `%FTD-1-735014: Voltage Channel var1: Voltage Critical`

Explanation A voltage channel has changed to a critical level.

- *var1* — Voltage channel number

Recommended Action Contact Cisco TAC to troubleshoot the failure. Power down the unit until this failure is resolved.

735015

Error Message `%FTD-4-735015: CPU var1: Temp: var2 var3, Warm`

Explanation The CPU temperature is warmer than the normal operating range.

- *var1* —CPU Number
- *var2* —Temperature Value
- *var3* —Units

Recommended Action Continue to monitor this component to ensure that it does not reach a critical temperature.

735016

Error Message `%FTD-4-735016: Chassis Ambient var1: Temp: var2 var3, Warm`

Explanation The chassis temperature is warmer than the normal operating range.

- *var1* —Chassis Sensor Number
- *var2* —Temperature Value
- *var3* —Units

Recommended Action Continue to monitor this component to ensure that it does not reach a critical temperature.

735017

Error Message `%FTD-1-735017: Power Supply var1: Temp: var2 var3, OK`

Explanation The power supply temperature has returned to a normal operating temperature.

- *var1* —Power Supply Number
- *var2* —Temperature Value
- *var3* —Units

Recommended Action None required.

735018

Error Message `%FTD-4-735018: Power Supply var1: Temp: var2 var3, Critical`

Explanation The power supply has reached a critical operating temperature.

- *var1* —Power Supply Number
- *var2* —Temperature Value
- *var3* —Units

Recommended Action Contact Cisco TAC to troubleshoot the failure. Power down the unit until this failure is resolved.

735019

Error Message `%FTD-4-735019: Power Supply var1: Temp: var2 var3, Warm`

Explanation The power supply temperature is warmer than the normal operating range.

- *var1* —Power Supply Number
- *var2* —Temperature Value
- *var3* —Units

Recommended Action Continue to monitor this component to ensure that it does not reach a critical temperature.

735020

Error Message `%FTD-1-735020: CPU var1: Temp: var2 var3, OK`

Explanation The CPU temperature has returned to the normal operating temperature.

- *var1* —CPU Number
- *var2* —Temperature Value
- *var3* —Units

Recommended Action None required.

735021

Error Message `%FTD-1-735021: Chassis Ambient var1: Temp: var2 var3, OK`

Explanation The chassis temperature has returned to the normal operating temperature.

- *var1* —Chassis Sensor Number
- *var2* —Temperature Value
- *var3* —Units

Recommended Action None required.

735022

Error Message `%FTD-1-735022: CPUnum is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the CPU`

Explanation The Secure Firewall Threat Defense device has detected a CPU running beyond the maximum thermal operating temperature, and will shut down immediately after detection.

Recommended Action The chassis and CPU need to be inspected immediately for ventilation issues.

735023

Error Message `%FTD-2-735023: device was previously shutdown due to the CPU complex running beyond the max thermal operating temperature. The chassis needs to be inspected immediately for ventilation issues`

Explanation At boot time, the Secure Firewall Threat Defense device detected a shutdown that occurred because a CPU was running beyond the maximum safe operating temperature. Using the **show environment** command will indicate that this event has occurred.

Recommended Action The chassis need to be inspected immediately for ventilation issues.

735024

Error Message `%FTD-1-735024: CPUvar1 Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. The chassis and CPU need to be inspected immediately for ventilation issues`

Explanation The IO hub temperature has returned to the normal operating temperature.

- *ar1* - IO hub number
- *var2* - Temperature value
- *var3* – Units

Recommended Action None required.

735025

Error Message `%FTD-1-735025: var1 was previously shutdown due to a CPU Voltage Regulator running beyond the max thermal operating temperature. The chassis and CPU need to be inspected immediately for ventilation issues`

Explanation The IO hub temperature has a critical temperature.

- *ar1* - IO hub number
- *var2* - Temperature value
- *var3* – Units

Recommended Action Record the message as it appears and contact the Cisco TAC.

735026

Error Message `%FTD-4-735026: IO Hub var1: Temp: var2 var3, OK`

Explanation The IO hub temperature is warmer than the normal operating range.

- *ar1* - IO hub number
- *var2* - Temperature value
- *var3* – Units

Recommended Action Continue to monitor this component to ensure that it does not reach a critical temperature.

735027

Error Message `%FTD-1-735027: CPU cpu_num Voltage Regulator is running beyond the max thermal operating temperature and the device will be shutting down immediately. The chassis and CPU need to be inspected immediately for ventilation issues.`

Explanation The Secure Firewall Threat Defense device has detected a CPU voltage regulator running beyond the maximum thermal operating temperature, and shuts down immediately after detection.

- *cpu_num* —The number to identify which CPU voltage regulator experienced the thermal event

Recommended Action The chassis and CPU need to be inspected immediately for ventilation issues.

735028

Error Message `%FTD-2-735028: FTD was previously shutdown due to a CPU Voltage Regulator running beyond the max thermal operating temperature. The chassis and CPU need to be inspected immediately for ventilation issues.`

Explanation At boot time, the Secure Firewall Threat Defense device detected a shutdown that occurred because of a CPU voltage regulator running beyond the maximum safe operating temperature. Enter the **show environment** command to indicate that this event has occurred.

Recommended Action The chassis and CPU need to be inspected immediately for ventilation issues.

735029

Error Message `%FTD-1-735029: IO Hub is running beyond the max thermal operating temperature and the device will be shutting down immediately to prevent permanent damage to the circuit`

Explanation The Secure Firewall Threat Defense device has detected that the IO hub is running beyond the maximum thermal operating temperature, and will shut down immediately after detection.

Recommended Action The chassis and IO hub need to be inspected immediately for ventilation issues.

736001

Error Message `%FTD-2-736001: Unable to allocate enough memory at boot for jumbo-frame reservation. Jumbo-frame support has been disabled.`

Explanation Insufficient memory has been detected when jumbo frame support was being configured. As a result, jumbo-frame support was disabled.

Recommended Action Try reenabling jumbo frame support using the **jumbo-frame reservation** command. Save the running configuration and reboot the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

Messages 737001 to 776254

This section includes messages from 737001 to 776254.

737001

Error Message `%FTD-7-737001: IPAA: Session=session, Received message 'message-type'`

Explanation The IP address assignment process received a message.

- *message-type* —The message received by the IP address assignment process

Recommended Action None required.

737002

Error Message `%FTD-3-737002: IPAA: Session=session, Received unknown message 'num'`

Explanation The IP address assignment process received a message.

- *session* —The session is the VPN session ID in hexadecimal.
- *num* —The identifier of the message received by the IP address assignment process

Recommended Action None required.

737003

Error Message `%FTD-5-737003: IPAA: Session=session, DHCP configured, no viable servers found for tunnel-group 'tunnel-group'`

Explanation The DHCP server configuration for the given tunnel group is not valid.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

Recommended Action Validate the DHCP configuration for the tunnel group. Make sure that the DHCP server is online.

737004

Error Message `%FTD-5-737004: IPAA: Session=session, DHCP configured, request failed for tunnel-group ''tunnel-group''`

Explanation The DHCP server configuration for the given tunnel group is not valid.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

Recommended Action Validate the DHCP configuration for the tunnel group. Make sure that the DHCP server is online.

737005

Error Message `%FTD-6-737005: IPAA: Session=session, DHCP configured, request succeeded for tunnel-group 'tunnel-group'`

Explanation The DHCP server request has succeeded.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

Recommended Action None required.

737006

Error Message `%FTD-6-737006: IPAA: Session=session, Local pool request succeeded for tunnel-group 'tunnel-group'`

Explanation The local pool request has succeeded.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

Recommended Action None required.

737007

Error Message `%FTD-5-737007: IPAA: Session=session, Local pool request failed for tunnel-group 'tunnel-group'`

Explanation The local pool request has failed. The pool assigned to the tunnel group may be exhausted.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

Recommended Action Validate the IP local pool configuration by using the **show ip local pool** command.

737008

Error Message `%FTD-5-737008: IPAA: Session=session, tunnel-group ''tunnel-group'' not found`

Explanation The tunnel group was not found when trying to acquire an IP address for configuration. A software defect may cause this message to be generated.

- *session* —The session is the VPN session ID in hexadecimal.
- *tunnel-group* —The tunnel group that IP address assignment is using for configuration

Recommended Action Check the tunnel group configuration. Contact the Cisco TAC and report the issue.

737009

Error Message `%FTD-6-737009: IPAA: Session=session, AAA assigned address ip-address, request failed`

Explanation The remote access client software requested the use of a particular address. The request to the AAA server to use this address failed. The address may be in use.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address that the client requested

Recommended Action Check the AAA server status and the status of IP local pools.

737010

Error Message `%FTD-6-737010: IPAA: Session=session, AAA assigned address ip-address, succeeded`

Explanation The remote access client software requested the use of a particular address and successfully received this address.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address that the client requested

Recommended Action None required.

737011

Error Message `%FTD-5-737011: IPAA: Session=session, AAA assigned address ip-address, not permitted, retrying`

Explanation The remote access client software requested the use of a particular address. The **vpn-addr-assign aaa** command is not configured. An alternatively configured address assignment method will be used.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address that the client requested

Recommended Action If you want to permit clients to specify their own address, enable the **vpn-addr-assign aaa** command.

737012

Error Message `%FTD-4-737012: IPAA: Session=session, Address assignment failed`

Explanation The remote access client software request of a particular address failed.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that the client requested

Recommended Action If using IP local pools, validate the local pool configuration. If using AAA, validate the configuration and status of the AAA server. If using DHCP, validate the configuration and status of the DHCP server. Increase the logging level (use notification or informational) to obtain additional messages to identify the reason for the failure.

737013

Error Message `%FTD-4-737013: IPAA: Session=session, Error freeing address ip-address, not found`

Explanation The Secure Firewall Threat Defense device tried to free an address, but it was not on the allocated list because of a recent configuration change.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address to be released

Recommended Action Validate your address assignment configuration. If this message recurs, it might be due to a software defect. Contact the Cisco TAC and report the issue.

737014

Error Message `%FTD-6-737014: IPAA: Session=session, Freeing AAA address ip-address`

Explanation The Secure Firewall Threat Defense device successfully released the IP address assigned through AAA.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address to be released

Recommended Action None required.

737015

Error Message `%FTD-6-737015: IPAA: Session=session, Freeing DHCP address ip-address`

Explanation The Secure Firewall Threat Defense device successfully released the IP address assigned through DHCP.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address to be released

Recommended Action None required.

737016

Error Message `%FTD-6-737016: IPAA: Session=session, Freeing local pool pool-name address ip-address`

Explanation The Secure Firewall Threat Defense device successfully released the IP address assigned through local pools.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IPv4 or IPv6 address to be released
- *pool-name* —The pool to which the address is being returned to

Recommended Action None required.

737017

Error Message `%FTD-6-737017: IPAA: Session=session, DHCP request attempt num succeeded`

Explanation The Secure Firewall Threat Defense device successfully sent a request to a DHCP server.

- *session* —The session is the VPN session ID in hexadecimal.
- *num* —The attempt number

Recommended Action None required.

737018

Error Message `%FTD-5-737018: IPAA: Session=session, DHCP request attempt num failed`

Explanation The Secure Firewall Threat Defense device failed to send a request to a DHCP server.

- *session* —The session is the VPN session ID in hexadecimal.
- *num* —The attempt number

Recommended Action Validate the DHCP configuration and connectivity to the DHCP server.

737019

Error Message `%FTD-4-737019: IPAA: Session=session, Unable to get address from group-policy or tunnel-group local pools`

Explanation The Secure Firewall Threat Defense device failed to acquire an address from the local pools configured on the group policy or tunnel group. The local pools may be exhausted.

- *session* —The session is the VPN session ID in hexadecimal.

Recommended Action Validate the local pool configuration and status. Validate the group policy and tunnel group configuration of local pools.

737023

Error Message `%FTD-5-737023: IPAA: Session=session, Unable to allocate memory to store local pool address ip-address`

Explanation The Secure Firewall Threat Defense device is low on memory.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was acquired

Recommended Action The Secure Firewall Threat Defense device may be overloaded and need more memory, or there may be a memory leak caused by a software defect. Contact the Cisco TAC and report the issue.

737024

Error Message `%FTD-5-737024: IPAA: Session= , Client requested address : , already in use, retrying`

Explanation The client requested an IP address that is already in use. The request will be tried using a new IP address.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that the client requested

Recommended Action None required.

737025

Error Message `%FTD-5-737025: IPAA:Session=session, Duplicate local pool address found, {ip-address|(ipv6-address)} in quarantine`

Explanation The IP address that was to be given to the client is already in use. The IP address has been removed from the pool and will not be reused.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was acquired

Recommended Action Validate the local pool configuration; there may be an overlap caused by a software defect. Contact the Cisco TAC and report the issue.

737026

Error Message `%FTD-6-737026: IPAA: Session= , Client assigned session from local pool ip-address`

Explanation The client has assigned the given address from a local pool.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was assigned to the client
- *pool-name*—The pool from which the address was allocated

Recommended Action None required.

737027

Error Message `%FTD-3-737027: IPAA: Session= , No data for address request`

Explanation A software defect has been found.

- *session* —The session is the VPN session ID in hexadecimal.

Recommended Action Contact the Cisco TAC and report the issue.

737028

Error Message `%FTD-4-737028: IPAA: Session= , Unable to send session to standby: communication failure`

Explanation The active Secure Firewall Threat Defense device was unable to communicate with the standby Secure Firewall Threat Defense device. The failover pair may be out-of-sync.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was assigned to the client

Recommended Action Validate the failover configuration and status.

737029

Error Message `%FTD-6-737029: IPAA: Session=session, Added {ip_address | ipv6_address} to standby`

Explanation The standby Secure Firewall Threat Defense device accepted the IP address assignment.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip_address* —The IP address that was assigned to the client

Recommended Action None required.

737030

Error Message `%FTD-4-737030: IPAA: Session=session, Unable to send {ip_address | ipv6_address} to standby: address in use`

Explanation The standby Secure Firewall Threat Defense device has the given address already in use when the active Secure Firewall Threat Defense device attempted to acquire it. The failover pair may be out-of-sync.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address (IPv4 or IPv6) that was assigned to the client.

Recommended Action Validate the failover configuration and status.

737031

Error Message `%FTD-6-737031: IPAA: Session= , Removed session from standby`

Explanation The standby Secure Firewall Threat Defense device cleared the IP address assignment.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was assigned to the client

Recommended Action None required.

737032

Error Message `%FTD-4-737032: IPAA: Session= , Unable to remove session from standby: address not found`

Explanation The standby Secure Firewall Threat Defense device did not have an IP address in use when the active Secure Firewall Threat Defense device attempted to release it. The failover pair may be out-of-sync.

- *session* —The session is the VPN session ID in hexadecimal.
- *ip-address* —The IP address that was assigned to the client

Recommended Action Validate the failover configuration and status.

737033

Error Message `%FTD-4-737033: IPAA: Session=session , Unable to assign session provided IP address (addr_allocator) to Client. This IP address has already been assigned by ip_addr`

Explanation The address assigned by the AAA/DHCP/local pool is already in use.

- *session* —The session is the VPN session ID in hexadecimal.
- *addr_allocator* —The DHCP/AAA/local pool
- *ip_addr* —The IP address allocated by the DHCP/AAA/local pool
- *previous_ addr_allocator* —The address allocater that already assigned the IP address (local pool, AAA, or DHCP)

Recommended Action Validate the AAA/DHCP/local pool address configurations. Overlap may occur.

737034

Error Message 1 `%FTD-4-737030: IPAA:Session=session, IPv4 address: ip-address`

Error Message 2 `%FTD-4-737030: IPAA:Session=session, IPv6 address: ipv6-address`

Explanation The IP address assignment process is unable to provide an address.

- *session* —The session is the VPN session ID in hexadecimal.

Recommended Action Action will be based on explanation for the failure.

737035

Error Message `%FTD-7-737035: IPAA: Session=session, ''message_type'' message queued`

Explanation A message is queued to the IP address assignment. This corresponds with syslog 737001. This message is not rate limited.

- *session* —The session is the VPN session ID in hexadecimal.

Recommended Action No action required.

737036

Error Message `%FTD-6-737035: IPAA: Session=session, '<address>' message queued`

Explanation IP address assignment process has provided a DHCP provisioned address back to the VPN client. This message is not rate limited.

- *session* —The session is the VPN session ID in hexadecimal.

Recommended Action No action required.

737038

Error Message `%FTD7-737038: IPAA: Session=session, specified address ip_address was in-use, trying to get another.`

Explanation This log occurs when the AAA server (internal or external) has specified an address to assign to the user; but this address already in-use. The request is being re-queued without a specified address to fall back to DHCP or local pools.

- *session* —The VPN session ID of the requesting session.
- *ip-address* —The IPv4 or IPv6 address specified by AAA

Recommended Action None required

737200

Error Message `%FTD-7-737200: VPNFIP: Pool=pool, Allocated ip-address from pool`

Explanation This log occurs an address is allocated from a local pool.

- *pool* —The local pool name.
- *ip-address* —The IPv4 or IPv6 address specified by AAA

Recommended Action None required

737201

Error Message `%FTD-7-737201: VPNFIP: Pool=pool, Returned ip-address to pool (recycle=recycle)`

Explanation This log occurs when an address returned to a local pool. The recycle flag indicates whether this address should be re-used for the next request. For rare situation, the recycle flag will be FALSE. For example, when there is an address collision , the address has been assigned to a VPN session by other means such as by AAA or DHCP. In this case, we will not immediately try to reuse that address for the next request.

- *pool* —The local pool name.
- *ip-address* —The IPv4 or IPv6 address specified by AAA

Recommended Action None required

737202

Error Message `%FTD-3-737202: VPNFIP: Pool=pool, ERROR: message`

Explanation This log is generated when an error event is detected related to the VPN FIP database.

- *pool* —The local pool name.
- *message* —The details for the event.

Recommended Action If error is persistent, contact Cisco TAC.

737203

Error Message `%FTD-4-737203: VPNFIP: Pool=pool, WARN: message`

Explanation This log is generated to warn of an event related to the VPN FIP database.

- *pool* —The local pool name.

- *message* —The details for the event.

Recommended Action If warning is persistent, contact Cisco TAC.

737204

Error Message `%FTD-5-737204: VPNFIP: Pool=pool, NOTIFY: message`

Explanation This log is generated to notify of an event related to the VPN FIP database.

- *pool* —The local pool name.
- *message* —The details for the event.

Recommended Action None required

737205

Error Message `%FTD-6-737205: VPNFIP: Pool=pool, INFO: message`

Explanation This log is generated to inform of an event related to the VPN FIP database.

- *pool* —The local pool name.
- *message* —The details for the event.

Recommended Action None required

737206

Error Message `%FTD-7-737206: VPNFIP: Pool=pool, DEBUG: message`

Explanation This log is generated to debug an event related to the VPN FIP database.

- *pool* —The local pool name.
- *message* —The details for the event.

Recommended Action None required

737400

Error Message `%FTD-7-737400: POOLIP: Pool=pool, Allocated ip-address from pool`

Explanation This log occurs an address is allocated from a local pool.

- *pool* —The local pool name
- *ip-address* —The IPv4 or IPv6 address specified by AAA

Recommended Action None required

737401

Error Message `%FTD-7-737401: POOLIP: Pool=pool, Returned ip-address to pool (recycle=recycle)`

Explanation This log occurs an address returned to a local pool. The recycle flag indicates whether this address should be re-used for the next request. For rare situation, the recycle flag will be FALSE. For example, when there is an address collision—the address has been assigned to a VPN session by other means such as by AAA or DHCP. In this case, we will not immediately try to reuse that address for the next request.

- *pool* —The local pool name
- *ip-address* —The IPv4 or IPv6 address specified by AAA

Recommended Action None required

737402

Error Message `%FTD-4-737402: POOLIP: Pool=pool, Failed to return ip-address to pool (recycle=recycle). Reason: message`

Explanation This log occurs unable to return an address to an address pool.

- *pool* —The local pool name
- *ip-address* —The IPv4 or IPv6 address specified by AAA
- *message*—The details of the failure. (For example, address not in pool range)

Recommended Action None required

737403

Error Message `%FTD-3-737403: POOLIP: Pool=pool, ERROR: message`

Explanation This log is generated when an error event is detected related to an IP local pool database.

- *pool* —The local pool name
- *message* —The details for the event.

Recommended Action If error is persistent, contact Cisco TAC.

737404

Error Message `%FTD-4-737404: POOLIP: Pool=pool, WARN: message`

Explanation This log is generated to warn of an event related to an IP local pool database.

- *pool* —The local pool name
- *message* —The details for the event.

Recommended Action If warning is persistent, contact Cisco TAC.

737405

Error Message `%FTD-5-737405: POOLIP: Pool=pool, NOTIFY: message`

Explanation This log is generated to notify of an event related to an IP local pool database.

- *pool* —The local pool name
- *message* —The details for the event.

Recommended Action None required

737406

Error Message `%FTD-6-737406: POOLIP: Pool=pool, INFO: message`

Explanation This log is generated to inform of an event related to an IP local pool database.

- *pool* —The local pool name
- *message* —The details for the event.

Recommended Action None required

737407

Error Message `%FTD-7-737407: POOLIP: Pool=pool, DEBUG: message`

Explanation This log is generated to debug an event related to an IP local pool database.

- *pool* —The local pool name
- *message* —The details for the event.

Recommended Action None required

741000

Error Message `%FTD-6-741000: Coredump filesystem image created on variable_1 - size variable_2 MB`

Explanation A core dump file system was successfully created. The file system is used to manage core dumps by capping the amount of disk space that core dumps may use.

- *variable 1* —The file system on which the core dumps are placed (for example, disk0:, disk1:, and flash:)
- *variable 2* —The size of the created core dump file system in MB

Recommended Action Make sure that you save your configuration after creating the core dump file system.

741001

Error Message `%FTD-6-741001: Coredump filesystem image on variable - resized from variable MB to variable MB`

Explanation The core dump file system has been successfully resized.

- *variable 1* —The file system on which the core dumps are placed
- *variable 2* —The size of the previous core dump file system in MB
- *variable 3* —The size of the current, newly resized core dump file system in MB

Recommended Action Make sure that you save your configuration after resizing the core dump file system. Resizing the core dump file system deletes the contents of the existing core dump file system. As a result, make sure that you archive any information before you resize the core dump file system.

741002

Error Message `%FTD-6-741002: Coredump log and filesystem contents cleared on variable_1`

Explanation All core dumps have been deleted from the core dump file system, and the core dump log has been cleared. The core dump file system and coredump log are always synchronized with each other.

- *variable 1* —The file system on which the core dumps are placed (for example, disk0:, disk1:,and flash:)

Recommended Action None required. You can clear the core dump file system to reset it to a known state using the **clear coredump** command.

741003

Error Message `%FTD-6-741003: Coredump filesystem and it's contents removed on variable_1`

Explanation The core dump file system and its contents have been removed, and the core dump feature has been disabled.

- *variable 1* —The file system on which the core dumps are placed (for example, disk0:, disk1:,and flash:)

Recommended Action Make sure that you save your configuration after the core dump feature has been disabled.

741004

Error Message `%FTD-6-741004: Coredump configuration reset to default values`

Explanation The core dump configuration has been reset to its default value, which is disabled.

Recommended Action Make sure that you save your configuration after the core dump feature has been disabled.

741005

Error Message `%FTD-4-741005: Coredump operation 'variable_1' failed with error variable_2_variable_3`

Explanation An error occurred during the performance of a core dump-related operation.

- *variable 1* —This variable may have the following values:

- CREATE_FSYS—An error occurred when creating the core dump file system.

- CLEAR_LOG—An error occurred when clearing the core dump log.

- DELETE_FSYS—An error occurred when deleting the core dump file system.

- CLEAR_FSYS—An error occurred when removing the contents of the core dump file system.

- MOUNT_FSYS—An error occurred when mounting the core dump file system.

  - *variable 2* —The decimal number that provides additional information about the cause of the error specified in *variable 1* .
  - *variable 3* —The descriptive ASCII string associated with *variable 2*. The ASCII string can have the following values:

- coredump files already exist

- unable to create coredump filesystem

- unable to create loopback device

- filesystem type not supported

- unable to delete the coredump filesystem

- unable to delete loopback device

- unable to unmount coredump filesystem

- unable to mount coredump filesystem

- unable to mount loopback device

- unable to clear coredump filesystem

- coredump filesystem not found

- requested coredump filesystem too big

- coredump operation aborted by administrator

- coredump command execution failed

- coredump IFS error encountered

- coredump, unidentified error encountered

Recommended Action Make sure that the core dump feature is disabled in the configuration, and send the message to the Cisco TAC for further analysis.

741006

Error Message `%FTD-4-741006: Unable to write Coredump Helper configuration, reason` *`variable_1`*

Explanation An error occurred when writing to the coredump helper configuration file. This error occurs only if disk0: is full. The configuration file is located in disk0:.coredumpinfo/coredump.cfg.

- *variable 1* —This variable includes a basic file system-related string that indicates why the writing of the core dump helper configuration file failed.

Recommended Action Disable the core dump feature, remove unneeded items from disk0:, and then reenable core dumps, if desired.

742001

Error Message `%FTD-3-742001: failed to read master key for password encryption from persistent store`

Explanation An attempt to read the primary password encryption key from the nonvolatile memory after bootup failed. Encrypted passwords in the configuration are not decrypted unless the primary key is set to the correct value using the **key config-key password encryption** command.

Recommended Action If there are encrypted passwords in the configuration that must be used, set the primary key to the previous value used to encrypt the password using the **key config-key password encryption** command. If there are no encrypted passwords or they can be discarded, set a new primary key. If password encryption is not used, no action is required.

742002

Error Message `%FTD-3-742002: failed to set master key for password encryption`

Explanation An attempt to read the **key config-key password encryption** command failed. The error may be caused by the following reasons:

- Configuration from a nonsecure terminal (for example, over a Telnet connection) was made.
- Failover is enabled, but it does not use an encrypted link.
- Another user is setting the key at the same time.
- When trying to change the key, the old key is incorrect.
- The key is too small to be secure.

Other reasons for the error may be valid. In these cases, the actual error is printed in response to the command.

Recommended Action Correct the problem indicated in the command response.

742003

Error Message `%FTD-3-742003: failed to save master key for password encryption, reason=`*`reason_text`*

Explanation An attempt to save the primary key to nonvolatile memory failed. The actual reason is specified by the *reason_text* parameter. The reason can be an out-of-memory condition, or the nonvolatile store can be inconsistent.

Recommended Action If the problem persists, reformat the nonvolatile store that is used to save the key by using the **write erase** command. Before performing this step, make sure that you back up the out-of-the-box configuration. Then reenter the **write erase** command.

742004

Error Message `%FTD-3-742004: failed to sync master key for password encryption, reason=`*`reason_text`*

Explanation An attempt to synchronize the primary key to the peer failed. The actual reason is specified by the *reason_text* parameter.

Recommended Action Try to correct the problem specified in the *reason_text* parameter.

742005

Error Message `%FTD-3-742005: cipher text `*`enc_pass`*` is not compatible with the configured master key or the cipher text has been tampered`

Explanation An attempt to decrypt a password failed. The password may have been encrypted using a primary key that is different from the current primary key, or the encrypted password has been changed from its original form.

Recommended Action If the correct primary key is not being used, correct the problem. If the encrypted password has been modified, reapply the configuration in question with a new password.

742006

Error Message `%FTD-3-742006: password decryption failed due to unavailable memory`

Explanation An attempt to decrypt a password failed because no memory was available. Features using this password will not work as desired.

Recommended Action Correct the memory problem.

742007

Error Message `%FTD-3-742007: password encryption failed due to unavailable memory`

Explanation An attempt to encrypt a password failed because no memory was available. Passwords may be left in clear text form in the configuration.

Recommended Action Correct the memory problem, and reapply the configuration that failed password encryption.

742008

Error Message `%FTD-3-742008: password` *`enc_pass`* `decryption failed due to decoding error`

Explanation Password decryption failed because of decoding errors, which may occur if the encrypted password has been modified after being encrypted.

Recommended Action Reapply the configuration in question with a clear text password.

742009

Error Message `%FTD-3-742009: password encryption failed due to encoding error`

Explanation Password encryption failed because of decoding errors, which may be an internal software error.

Recommended Action Reapply the configuration in question with a clear text password. If the problem persists, contact the Cisco TAC.

742010

Error Message `%FTD-3-742010: encrypted password` *`enc_pass`* `is not well formed`

Explanation The encrypted password provided in the command is not well formed. The password may not be a valid, encrypted password, or it may have been modified since it was encrypted.

- *reason_text* —A string that represents the actual cause of the failure
- *enc_pass* —The encrypted password that is related to the issue

Recommended Action Reapply the configuration in question with a clear text password.

743000

Error Message `%FTD-1-743000: The PCI device with vendor ID: vendor_id device ID: device_id located at bus:device.function (hex) bus_num:dev_num.func_num has a link link_attr_name of actual_link_attr_val when it should have a link link_attr_name of expected_link_attr_val`

Explanation A PCI device in the system is not configured correctly, which may result in the system not performing at its optimum level.

Recommended Action Collect the output of the **show controller pci detail** command, and contact the Cisco TAC.

743001

Error Message `%FTD-1-743001: Backplane health monitoring detected link failure`

Explanation A hardware failure has probably occurred and has been detected on one of the links between the Secure Firewall Threat Defense Services Module and the switch chassis.

Recommended Action Contact the Cisco TAC.

743002

Error Message `%FTD-1-743002: Backplane health monitoring detected link OK`

Explanation A link has been restored between the Secure Firewall Threat Defense Services Module and the switch chassis. However, the failure and subsequent recovery probably indicates a hardware failure.

Recommended Action Contact the Cisco TAC.

743004

Error Message `%FTD-1-743004: System is not fully operational - The PCI device with vendor ID: vendor_id (vendor_name) device ID: device_id (device_name) could not be found in the system.`

Explanation A PCI device in the system that is needed for it to be fully operational was not found.

- *vendor_id* —Hexadecimal value that identifies the device vendor
- *vendor_name* —Text string that identifies the vendor name
- *device_id* —Hexadecimal value that identifies the vendor device
- *device_name* —Text string that identifies the device name

Recommended Action Collect the output of the **show controller pci detail** command and contact the Cisco TAC.

743010

Error Message `%FTD-3-743010: EOBC RPC server failed to start for client module client_name.`

Explanation The service failed to start for a particular client of the EOBC RPC service on the server.

Recommended Action Call the Cisco TAC.

743011

Error Message `%FTD-3-743011: EOBC RPC call failed, return code code.`

Explanation The EOBC RPC client failed to make an RPC to the intended server.

Recommended Action Call the Cisco TAC.

746012

Error Message `%FTD-7-746012: user-identity: Add IP-User mapping ip_address - domain_name\user_name result - reason`

Explanation A new user-IP mapping has been added to the user-to-IP address mapping database. The status of the operation (success or failure) is indicated. The success reason is VPN user. The failure reasons include the following: Maximum user limit reached and Duplicated address.

Recommended Action None required.

746013

Error Message `%FTD-7-746013: user-identity: Delete IP-User mapping ip_address - domain_name\user name - result reason`

Explanation A change has been made to the user-to-IP address mapping database. The status of the operation (success or failure) is indicated. The success reasons include the following: Inactive timeout, NetBIOS probing failed, PIP notification, VPN user logout, Cut-through-proxy user logout, and MAC address mismatch. The failure reason is PIP notification.

Recommended Action None required.

746014

Error Message `%FTD-5-746014: user-identity: [FQDN] fqdn address IP_Address obsolete`

Explanation A fully qualified domain name has become obsolete.

Recommended Action None required.

746015

Error Message `%FTD-5-746015: user-identity: [FQDN] fqdn resolved IP_address`

Explanation A fully qualified domain name lookup has succeeded.

Recommended Action None required.

746016

Error Message `%FTD-3-746016: user-identity: DNS lookup for ip failed, reason:reason`

Explanation A DNS lookup has failed. Failure reasons include timeout, unresolvable, and no memory.

Recommended Action Verify that the FQDN is valid, and that the DNS server is reachable from the FTD. If the problem persists, contact the Cisco TAC.

747001

Error Message `%FTD-3-747001: State machine event queue depleted. Event (event-id,ptr-in-hex,ptr-in-hex) dropped. Current state state-name, stack ptr-in-hex ptr-in-hex ptr-in-hex ptr-in-hex ptr-in-hex ptr-in-hex`

Explanation The cluster FSM event queue is full, and a new event has been dropped.

Recommended Action None.

747002

Error Message `%FTD-5-747002: Recovered from state machine dropped event (event-id,ptr-in-hex,ptr-in-hex). Intended state: state-name. Current state: state-name`

Explanation The cluster FSM received an event that is incompatible with the current state.

Recommended Action None.

747003

Error Message `%FTD-5-747003: Recovered from state machine failure to process event (event-id,ptr-in-hex,ptr-in-hex) at state state-name`

Explanation The cluster FSM failed to process an event for all reasons given.

Recommended Action None.

747004

Error Message `%FTD-6-747004: State machine changed from state state-name to state-name`

Explanation The cluster FSM has progressed to a new state.

Recommended Action None.

747005

Error Message `%FTD-7-747005: State machine notify event event-name (event-id,ptr-in-hex,ptr-in-hex)`

Explanation The cluster FSM has notified clients about an event.

Recommended Action None.

747006

Error Message `%FTD-7-747006: State machine is at state state-name`

Explanation The cluster FSM moved to a stable state; that is, Disabled, Slave, or Master.

Recommended Action None.

747007

Error Message `%FTD-5-747007: Recovered from founding stray config sync thread, stack` *`ptr-in-hex ptr-in-hex ptr-in-hex ptr-in-hex ptr-in-hex ptr-in-hex`*

Explanation Astray configuration sync thread has been detected.

Recommended Action None.

747008

Error Message `%FTD-4-747008: New cluster member "`*`name`*`" with serial number` *`serial-number-A`* `rejected due to name conflict with existing unit with serial number` *`serial-number-B`*

Explanation The same unit name has been configured on multiple units.

Recommended Action None.

747009

Error Message `%FTD-2-747009: Fatal error due to failure to creat RPC server for module` *`module name`*

Explanation The Secure Firewall Threat Defense device failed to create an RPC server.

Recommended Action Disable clustering on this unit and try to re-enable it. Contact the Cisco TAC if the problem persists.

747010

Error Message `%FTD-3-747010: Attempted recovery from failed RPC call, message` *`message-name`*`, return code` *`code-value`*

Explanation An RPC call failure has occurred. The system tries to recover from the failure.

Recommended Action None.

747011

Error Message `%FTD-2-747011: Memory allocation failure. Failed to allocate` *`bytes`*

Explanation A memory allocation failure occurred in clustering.

Recommended Action Disable clustering on this unit and try to re-enable it. If the problem persists, check the memory usage on the Secure Firewall Threat Defense device.

747012

Error Message `%FTD-3-747012: Failed to replicate global object id hex-id-value in domain domain-name to peer unit-name, continue operation`

Explanation A global object ID replication failure has occurred.

Recommended Action None.

747013

Error Message `%FTD-3-747013: Failed to remove global object id hex-id-value in domain domain-name from peer unit-name, continue operation`

Explanation A global object ID removal failure has occurred.

Recommended Action None.

747014

Error Message `%FTD-3-747014: Failed to install global object id hex-id-value in domain domain-name, continue operation`

Explanation A global object ID installation failure has occurred.

Recommended Action None.

747015

Error Message `%FTD-4-747015: Forcing stray member unit-name to leave the cluster`

Explanation A stray cluster member has been found.

Recommended Action None.

747016

Error Message `%FTD-4-747016: Found a split cluster with both unit-name-A and unit-name-B as control nodes. Control node role retained by unit-name-A, unit-name-B will leave then join as a data node`

Explanation A split cluster has been found.

Recommended Action None.

747017

Error Message `%FTD-4-747017: Failed to enroll unit unit-name due to maximum member limit[limit-value] reached`

Explanation The Secure Firewall Threat Defense device failed to enroll a new unit because the maximum member limit has been reached.

Recommended Action None.

747018

Error Message `%FTD-3-747018: State progression failed due to timeout in module module-name`

Explanation The cluster FSM progression has timed out.

Recommended Action None.

747019

Error Message `%FTD-4-747019: New cluster member name rejected due to Cluster Control Link IP subnet mismatch (ip-address/ip-mask on new unit, ip-address/ip-mask on local unit)`

Explanation The control unit found that a new joining unit has an incompatible cluster interface IP address.

Recommended Action None.

747020

Error Message `%FTD-4-747020: New cluster member unit-name rejected due to encryption license mismatch`

Explanation The control unit found that a new joining unit has an incompatible encryption license.

Recommended Action None.

747021

Error Message `%FTD-3-747021: Control node unit-name is quitting due to interface health check failure on interface-name, number_of_times times. Rejoin will be attempted after time min.`

Explanation The control unit has disabled clustering because of an interface health check failure.

Recommended Action None.

747022

Error Message `%FTD-3-747022: Asking data node unit-name to quit because it failed interface health check x times (last failure on y), rejoin will be attempted after interface-name min.`

Explanation This syslog message occurs when the maximum number of rejoin attempts has not been exceeded. A data unit has disabled clustering because of an interface health check failure for the specified amount of time. This unit will re-enable itself automatically after the specified amount of time (ms).

Recommended Action None.

747025

Error Message `%FTD-4-747025: New cluster member unit-name rejected due to firewall mode mismatch.reason`

Explanation A control unit found a joining unit that has an incompatible firewall mode.

Recommended Action None.

747026

Error Message `%FTD-4-747026: New cluster member unit-name rejected due to cluster interface name mismatch (ifc-name on new unit, ifc-name on local unit)`

Explanation A control unit found a joining unit that has an incompatible cluster control link interface name.

Recommended Action None.

747027

Error Message `%FTD-4-747027: Failed to enroll unit unit-name due to insufficient size of cluster pool pool-namecontext-name`

Explanation A control unit could not enroll a joining unit because of the size limit of the minimal cluster pool configured.

Recommended Action None.

747028

Error Message `%FTD-4-747028: Found unit unit-name's interface-mode is mode-name, different from mine mode-name, ask it to quit.`

Explanation A control unit found a joining unit that has an incompatible interface-mode, either spanned or individual.

Recommended Action None.

747029

Error Message `%FTD-4-747029: Unit unit-name is quitting due to Cluster Control Link down.`

Explanation A unit disabled clustering because of a cluster interface failure.

Recommended Action None.

747030

Error Message `%FTD-3-747030: Asking data node unit-name to quit because it failed interface health check x times (last failure on interface-name). Clustering must be manually enabled on the unit to rejoin.`

Explanation An interface health check has failed and the maximum number of rejoin attempts has been exceeded. A data unit has disabled clustering because of an interface health check failure.

Recommended Action None.

747031

Error Message `%FTD-3-747031: Platform mismatch between cluster control node (platform-type) and joining unit unit-name (platform-type). unit-name aborting cluster join.`

Explanation The joining unit's platform type does not match with that of the cluster control unit.

- *unit-name* —Name of the unit in the cluster bootstrap
- *platform-type* —Type of Secure Firewall Threat Defense platform

Recommended Action Make sure that the joining unit has the same platform type as that of the cluster control unit.

747032

Error Message `%FTD-3-747032: Service module mismatch between cluster control node (module-name) and joining unit unit-name (module-name) in slot slot-number. unit-name aborting cluster join.`

Explanation The joining unit's external modules are not consistent (module type and order in which they are installed) with those on the cluster control unit.

- *module-name*— Name of the external module
- *unit-name* —Name of the unit in the cluster bootstrap
- *slot-number* —The number of the slot in which the mismatch occurred

Recommended Action Make sure that the modules installed on the joining unit are of the same type and are in the same order as they are in the cluster control unit.

747033

Error Message `%FTD-3-747033: Interface mismatch between cluster control node and joining unit unit-name. unit-name aborting cluster join.`

Explanation The joining unit's interfaces are not the same as those on the cluster control unit.

- *unit-name* —Name of the unit in the cluster bootstrap

Recommended Action Make sure that the interfaces available on the joining unit are the same as those on the cluster control unit.

747034

Error Message `%FTD-4-747034: Unit unit_name is quitting due to Cluster Control Link down (number_times times after last rejoin). Rejoin will be attempted after minutes minutes.`

Explanation Cluster Control Link down and the unit is kicked out with rejoin.

Recommended Action Wait for the unit to rejoin.

747035

Error Message `%FTD-4-747035: Unit unit_name is quitting due to Cluster Control Link down. Clustering must be manually enabled on the unit to rejoin.`

Explanation Cluster Control Link down and the unit is kicked out without rejoin.

Recommended Action Rejoin the unit manually.

747036

Error Message `%FTD-3-747036: Application software mismatch between cluster control node Master unit name (Master application software name) and joining unit (Joining unit application software name). Joining member name aborting cluster join.`

Explanation The applications on control unit and the joining data unit are not the same. Data unit will be kicked out.

Recommended Action Make sure that the data unit run the same applications/services, and manually rejoin the unit.

747042

Error Message `%FTD-3-747042: Control node received the config hash string request message from an unknown member with id cluster-member-id`

Explanation Control unit received the config hash string request event.

Recommended Action Verify requestor member is still in OnCall state.

747043

Error Message `%FTD-3-747043: Get config hash string from control node error.`

Explanation Failed to get config hash string from control unit.

- ret_code□The error return code; 0 indicates OK, and 1 indicates Failed
- string_len□The hash_str length

Recommended Action Contact technical support to troubleshoot the issue on control unit. Ensure to turn on 'debug cluster ccp' to identify the root cause.

747044

Error Message `%FTD-6-747044: Configuration Hash string verification result.`

Explanation The result of configuration hash string comparison..

- result□This result can be PASSED or FAILED

Recommended Action None required.

748001

Error Message `%FTD-5-748001: Blade slot_number in chassis chassis_number is leaving the cluster due to a chassis configuration change`

Explanation A cluster control link has changed in the MIO, a cluster group has been removed in the MIO, or a blade module has been removed in the MIO configuration.

- *slot_number* —The blade slot ID within the chassis
- *chassis_number* —The chassis ID, which is unique for each chassis

Recommended Action None required.

748002

Error Message `%FTD-4-748002: Clustering configuration on the chassis is missing or incomplete; clustering is disabled`

Explanation Configurations are missing or incomplete in the MIO (for example, a cluster group is not configured, or a cluster control link is not configured).

- *slot_number* —The blade slot ID within the chassis
- *chassis_number* —The chassis ID, which is unique for each chassis

Recommended Action Go to the MIO console and configure the cluster service type, add the module to the service type, and define the cluster control link accordingly.

748003

Error Message `%FTD-4-748003: Module slot_number in chassis chassis_number is leaving the cluster due to a chassis health check failure`

Explanation The blade cannot talk to the MIO, so it relies on the MIO to detect this communication problem and de-bundle the data ports. If data ports are de-bundled, the Secure Firewall Threat Defense device will be kicked out by an interface health check.

- *slot_number* —The blade slot ID within the chassis
- *chassis_number* —The chassis ID, which is unique for each chassis

Recommended Action Check if the MIO card is up or if the communication between the MIO and the blade is still up.

748004

Error Message `%FTD-5-748004: Module slot_number in chassis chassis_number is re-joining the cluster due to a chassis health check recovery`

Explanation The MIO blade health check has recovered, and the Secure Firewall Threat Defense device tries to rejoin the cluster.

- *slot_number* —The blade slot ID within the chassis
- *chassis_number* —The chassis ID, which is unique for each chassis

Recommended Action Check if the MIO card is up or if the communication between the MIO and the blade is still up

748005

Error Message `%FTD-3-748005: Failed to bundle the ports for module slot_number in chassis chassis_number; clustering is disabled`

Explanation The MIO failed to bundle the ports for itself.

- *slot_number* —The blade slot ID within the chassis
- *chassis_number* —The chassis ID, which is unique for each chassis

Recommended Action Check if the MIO is operating correctly.

748006

Error Message `%FTD-3-748006: Asking module slot_number in chassis chassis_number to leave the cluster due to a port bundling failure`

Explanation The MIO failed to bundle ports for a blade, so the blade has been kicked out.

- *slot_number* —The blade slot ID within the chassis
- *chassis_number* —The chassis ID, which is unique for each chassis

Recommended Action Check if the MIO is operating correctly.

748007

Error Message `%FTD-2-748007: Failed to de-bundle the ports for module slot_number in chassis chassis_number; traffic may be black holed`

Explanation The MIO failed to de-bundle the ports.

- *slot_number* —The blade slot ID within the chassis
- *chassis_number* —The chassis ID, which is unique for each chassis

Recommended Action Check if the MIO is operating correctly.

748008

Error Message `%FTD-6-748008: [CPU load percentage%% | memory load percentage%%] of module slot_number in chassis chassis_number (member-name) exceeds overflow protection threshold [CPU percentage%% | Memory percentage%%]. System may be oversubscribed on member failure.`

Explanation The CPU load has exceeded (N-1)/N, where N is the total number of active cluster members, or the memory load has exceeded (100 – x) * (N – 1) / N + x, where N is the number of cluster members, and x is the baseline memory usage of the last joining member.

- *percentage* —The CPU load or memory load percentile data
- *slot_number* —The blade slot ID within the chassis
- *chassis_number* —The chassis ID, which is unique for each chassis

Recommended Action Re-plan the network and clustering deployment. Either reduce the amount of traffic or add more blades/chassis.

748009

Error Message `%FTD-6-748009: [CPU load percentage%% | memory load percentage%%] of chassis chassis_number exceeds overflow protection threshold [CPU percentage %% | Memory percentage%%]. System may be oversubscribed on chassis failure.`

Explanation The chassis traffic load exceeded a certain threshold.

- *percentage* —The CPU load or memory load percentile data
- *chassis_number* —The chassis ID, which is unique for each chassis

Recommended Action Re-plan the network and clustering deployment. Either reduce the amount of traffic or add more blades/chassis.

748011

Error Message `%FTD-4-748011: Mismatched resource profile size with Master. Master: cores number CPU cores / RAM size MB RAM, Mine: cores number CPU cores / RAM size MB RAM`

Explanation When the unit that is joining into cluster has different resource profile size compared to control unit, this syslog appears on the joining unit.

Example

```
%Firewall Threat Defense-4-748011: Mismatched resource profile size with Master. Master: 6
 CPU cores / 14426 MB RAM,  Mine: 8 CPU cores 19261 MB RAM.
```

Recommended Action None required.

748012

Error Message `%FTD-4-748012: Mismatched module type with Master. Master: PID, MINE: PID`

Explanation When the unit that is joining into cluster has different module type compared to the control unit, this syslog appears on the joining unit.

Example

```
%Firewall Threat Defense-4-748012: Mismatched module type with Master. Master: FPR4K-SM-24,
 Mine: FPR4K-SM-24s
```

Recommended Action None required.

748100

Error Message `%FTD-3-748100: application_name application status is changed from status to status`

Explanation Detect the application status change from one state to another. Application status change will trigger application health check mechanism.

- application name—snort or disk_full
- status—init, up, down

Recommended Action Verify the status of the application.

748101

Error Message `%FTD-3-748101: Peer unit unit_id reported its application_name application status is status`

Explanation Peer unit reported application status change that will trigger application health check mechanism.

- unit id—the unit id
- application name—snort or disk_full
- status—init, up, down

Recommended Action Verify the status of the application.

748102

Error Message `%FTD-3-748102: Control node unit_id is quitting due to application_name Application health check failure, and control node's application state is status`

Explanation Application health check detects that the control unit is not healthy. The control unit will leave the cluster group.

- unit id—the unit id
- application name—snort or disk_full
- status—init, up, down

Recommended Action Verify the status of the application. When the application (snort) is up again, the unit will rejoin automatically.

748103

Error Message `%FTD-3-748103: Asking data node unit_id to quit due to application_name Application health check failure, and data node's application state is status`

Explanation Application health check detects that the data unit is not healthy. Control unit will evict the data node.

- unit id—the unit id
- application name—snort or disk_full
- status—init, up, down

Recommended Action Verify the status of the application. When the application (snort) is up again, the unit will rejoin automatically.

748201

Error Message `%FTD-4-748201: Application name application on module module id in chassis chassis id is status`

Explanation Status of the application in the service chain gets changed.

- status—up, down

Recommended Action Verify the status of the application in the service chain.

748202

Error Message `%FTD-3-748202: Module module_id in chassis chassis id is leaving the cluster due to application name application failure`

Explanation Unit will be kicked out of cluster if the application such as vDP, fails.

Recommended Action Verify the status of the application in the service chain.

748203

Error Message `%FTD-5-748203: Module module_id in chassis chassis id is re-joining the cluster due to a service chain application recovery`

Explanation Unit automatically rejoins the cluster if the service chain application such as vDP, recovers.

Recommended Action Verify the status of the application in the service chain.

750001

Error Message `%FTD-5-750001: Local:local IP :local port Remote:remote IP : remote port Username: username Received request to request an IPsec tunnel; local traffic selector = local selectors: range, protocol, port range ; remote traffic selector = remote selectors: range, protocol, port range`

Explanation A request is being made for an operation on the IPsec tunnel such as a rekey, a request to establish a connection, and so on.

- *local IP:local port* — Local IP address for this request. The Secure Firewall Threat Defense IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known, or the tunnel group
- *local selectors* —Locally configured traffic selectors or proxies that are being used for this IPsec tunnel
- *remote selectors* —Remote peers requested traffic selectors or proxies for this IPsec tunnel

Recommended Action None required.

750002

Error Message `%FTD-5-750002: Local:local IP :local port Remote: remote IP : remote port Username: username Received a IKE_INIT_SA request`

Explanation An incoming tunnel or SA initiation request (IKE_INIT_SA request) has been received.

- *local IP:local port* — Local IP address for this request. The Secure Firewall Threat Defense IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from

- *username* —Username of the requester for remote access, if known, or the tunnel group

Recommended Action None required.

750003

Error Message `%FTD-4-750003: Local: local IP:local port Remote: remote IP:remote port Username: username Negotiation aborted due to ERROR: error`

Explanation The negotiation of an SA was aborted because of the provided error reason.

- *local IP:local port* — Local IP address for this request. The Secure Firewall Threat Defense IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet
- *error* —Error reason for aborting the negotiation. Errors include the following:

- Failed to send data on the network

- Asynchronous request queued

- Failed to enqueue packet

- A supplied parameter is incorrect

- Failed to allocate memory

- Failed the cookie negotiation

- Failed to find a matching policy

- Failed to locate an item in the database

- Failed to initialize the policy database

- Failed to insert a policy into the database

- The peer's proposal is invalid

- Failed to compute the DH value

- Failed to construct a NONCE

- An expected payload is missing from the packet

- Failed to compute the SKEYSEED

- Failed to create child SA keys

- The peer's KE payload contained the wrong DH group

- Received invalid KE notify, yet we've tried all configured DH groups

- Failed to compute a hash value

- Failed to authenticate the IKE SA

- Failed to compute or verify a signature

- Failed to validate the certificate

- The certificate has been revoked and is consequently invalid

- Failed to build or process a certificate request
- We requested a certificate, but the peer supplied none
- While sending the certificate chain, peer did not send its certificate as the first in the chain
- Detected an unsupported ID type
- Failed to construct an encrypted payload
- Failed to decrypt an encrypted payload
- Detected an invalid value in the packet
- The initiator bit is asserted in packet from original responder
- The initiator bit isn't asserted in packet from original initiator
- The message response bit is asserted in a packet from the exchange initiator
- The message response bit isn't asserted in a packet from the exchange responder
- Detected an invalid IKE SPI
- Packet is a retransmission
- Detected an invalid protocol ID
- Detected unsupported critical payload
- Detected an invalid traffic selector type
- Failed to create new SA
- Failed to delete SA
- Failed to add new SA into session DB
- Failed to add session to PSH
- Failed to delete session from osal
- Failed to delete a session from the database
- Failed to add request to SA
- Throttling request queue exceeds reasonable limit, increase the window size on peer
- Received an IKE msg id outside supported window
- Detected unsupported version number
- Received no proposal chosen notify
- Detected an error notify payload
- Detected NAT-d hash doesn't match
- Initialize sadb failed
- Initialize session db failed
- Failed to get PSH
- Negotiation context locked currently in use
- Negotiation context was not freed!

- Invalid data state found

- Failed to open PKI session

- Failed to insert public keys

- No certificate found

- Unsupported cert encoding found or Peer requested HTTP URL but never sent HTTP_LOOKUP_SUPPORTED Notification

- Sending BUNDLE URL is not supported at least for now. However, processing a BUNDLE URL is supported

- Local certificate has expired

- Failed to construct State Machine

- Error encountered while navigating State Machine

- SM Validation failed

- Could not find neg context

- Failed to add work request to SM Q

- Nonce payload is missing

- Traffic selector payload is missing

- Unsupported DH group

- Expected keypair is unavailable

- Packet isn't encrypted

- Packet is missing KE payload

- Packet is missing SA payload

- Invalid SA

- Invalid negotiation context

- Remote or local ID isn't defined

- Invalid connection id

- Unsupported auth method

- Ipsec policy not found

- Failed to initialize the event priority queue

- Failed to enqueue an item to a list

- Failed to remove an item from list

- Data in the event priority queue is NULL or corrupt

- No local IKE policy found

- Can't delete IKE SA due to in-progress task

- Expected Cookie Notify not received

- Failed to generate auth data: My auth info missing

- Failed to generate auth data: Failed to sign data

- Failed to generate auth data: Signature operation successful but unable to locate generated auth material
- Failed to receive the AUTH msg before the timer expired
- Maximum number of retransmissions reached
- Initial exchange failed
- Auth exchange failed
- Create child exchange failed
- Platform errors
- Failed to log a message
- Unwanted debug level turned on
- There are additional TS possible
- A single pairs of addresses is required
- Invalid session
- There was no IPSEC policy found for received TS
- Cannot remove request from window
- There was no proposal found in configured policy
- Nat-t test failure
- No pskey found
- Invalid compression algorithm
- Failed to get profile name from platform service handle
- Failed to find profile
- Initiator failed to match profile sent by IPSEC with profile found by peer id or certificate
- Failed to get peer id from platform service handle
- The transform attribute is invalid
- Extensible Authentication Protocol failed
- Authenticator sent NULL EAP message
- The config attribute is invalid
- Failed to calculate packet hash
- The AAA context is deleted
- Cannot alloc AAA ID
- Cannot alloc AAA request
- Cannot init AAA request
- The Authen list is not configured
- Fail to send AAA request
- Fail to alloc IP addr

- Invalid message context
- Key Auth memory failure
- EAP method does not generate MSK
- Failed to register new SA with platform
- Failed to async process session register, error: %d
- Failed to insert SA due to ipsec rekey collision
- Failed while handling a ipsec rekey collision
- Failed to accept rekey on SA that caused a rekey collision
- Failed to start timer to ensure IPsec collision SA SPI %s/%s will be deleted by the peer
- Error/Debug codes and strings are not matched
- Failed to initialize SA lifetime
- Failed to find rekey SA
- Failed to generate DH shared secret
- Failed to retrieve issuer public key hash list
- Failed to build certificate payload
- Unable to initialize the timer
- Failed to generate DH shared secret
- Failed to initialized authorization request
- Incorrect author record received from AAA
-Failed to fetch the keys from AAA
-Failed to add attribute to AAA request
-Failed to send tunnel password request to AAA
- Failed to allocate AAA context
- Insertion to policy AVL tree failed
- Deletion from policy AVL tree failed
- No Matching node found in policy AVL tree
- No Matching policy found
- No Matching proposal found
- Proposal is incomplete to be attached to the policy
- Proposal is in use
- Peer authentication method configured is mismatching with the method proposed by peer
- Failed to find the session in osal
- Failed to allocate event
- Failed to create accounting record

- Accounting not required

- Accounting not started for this session

- NAT-T disabled via cli

-Negotiating limit reached, deny SA request

- SA is already in negotiation, hence not negotiating again

- AAA group authorization failed

- AAA user authorization failed

- %% Dropping received fragment, as fragmentation is not negotiated for this SA!

- Maximum number of received fragments reached for the SA

- Number of fragments exceeds maximum allowed

- Assembled packet length %d is greater than maximum ikev2 packet size %d

- Received fragment numbers were NOT continuous or IKEV2_FRAG_FLAG_LAST_FRAGMENT flag was set on the wrong packet

- Received fragment is not valid, hence being dropped

- AAA group authorization failed

- AAA user authorization failed

- AAA author not configured in IKEv2 profile

- Failed to extract the skeyid

- Failed to send a failover msg to the standby unit

- Detected unsupported failover version

- Request was received but failover is not enabled

- Received an active unit request but the negotiated role is %s

- Received a standby unit request but the negotiated role is %s

- Invalid IP Version

- GDOI is not yet supported in IKEv2

- Failed to allocate PSH from platform

- Redirect the session to another gateway

- Redirect check failed

- Accept the session on this gateway after Redirect check

- Detected unsupported Redirect gateway ID type

- Redirect accepted, initiate new request

- Redirect accepted, clean-up IKEv2 SA, platform will initiate new request

- SA got redirected, it should not do any CREATE_CHILD_SA exchange

- DH public key computation failed

- DH secret computation failed

- IN-NEG IKEv2 Rekey SA got deleted

- Number of cert req exceeds the reasonable limit (%d)

- The negotiation context has been freed

- Assembled packet length %d is greater than maximum ikev2 packet size %d

- Received fragment numbers were NOT continuous or IKEV2_FRAG_FLAG_LAST_FRAGMENT flag was set on the wrong packet

- AAA author not configured in IKEv2 profile

- Assembled packet is not valid, hence being dropped

- Invalid VCID context

Recommended Action Review the syslog and follow the flow of the logs to determine if this syslog is the final in the exchange and if it is the cause of a potential failure or a transient error that was renegotiated through. For example, a peer may suggest a DH group via the KE payload that is not configured that causes an initial request to fail, but the correct DH group is communicated so that the peer can come back with the correct group in a new request.

750004

Error Message `%FTD-5-750004: Local: local IP: local port Remote: remote IP: remote port Username: username Sending COOKIE challenge to throttle possible DoS`

Explanation An incoming connection request was challenged with a cookie based on the cookie challenge thresholds that are configured to prevent a possible DoS attack.

- *local IP:local port* — Local IP address for this request. The Secure Firewall Threat Defense IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet

Recommended Action None required.

750005

Error Message `%FTD-5-750005: Local: local IP: local port Remote: remote IP: remote port Username: username IPsec rekey collision detected. I am lowest nonce initiator, deleting SA with inbound SPI SPI`

Explanation A rekey collision was detected (both peers trying to initiate a rekey at the same time), and it was resolved by keeping the one initiated by this Secure Firewall Threat Defense device because it had the lowest nonce. This action caused the indicated SA referenced by the SPI to be deleted.

- *local IP:local port* — Local IP address for this request. The Secure Firewall Threat Defense IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet
- *SPI* —SPI handle of the SA being deleted by resolving the rekey collision that was detected

Recommended Action None required.

750006

Error Message `%FTD-5-750006: Local: local IP: local port Remote: remote IP: remote port Username: username SA UP. Reason: reason`

Explanation An SA came up for the given reason, such as for a newly established connection or a rekey.

- *local IP:local port* — Local IP address for this request. The Secure Firewall Threat Defense IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet
- *reason* —Reason that the SA came into the UP state

Recommended Action None required.

750007

Error Message `%FTD-5-750007: Local: local IP: local port Remote: remote IP: remote port Username: username SA DOWN. Reason: reason`

Explanation An SA was torn down or deleted for the given reason, such as a request by the peer, operator request (via an administrator action), rekey, and so on.

- *local IP:local port* — Local IP address for this request. The Secure Firewall Threat Defense IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet
- *reason* —Reason that the SA came into the DOWN state

Recommended Action None required.

750008

Error Message `%FTD-5-750008: Local: local IP: local port Remote: remote IP: remote port Username: username SA rejected due to system resource low`

Explanation An SA request was rejected to alleviate a low system resource condition.

- *local IP:local port* — Local IP address for this request. The Secure Firewall Threat Defense IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet

Recommended Action Check CAC settings for IKEv2 to determine if this is expected behavior based on configured thresholds; otherwise, if the condition persists, investigate further to alleviate the issue.

750009

Error Message `%FTD-5-750009: Local: local IP: local port Remote: remote IP: remote port Username: username SA request rejected due to CAC limit reached: Rejection reason: reason`

Explanation A Connection Admission Control (CAC) limiting threshold was reached, which caused the SA request to be rejected.

- *local IP:local port* — Local IP address for this request. The Secure Firewall Threat Defense IP address and port number used for this connection
- *remote IP:remote port* — Remote IP address for this request. Peer IP address and port number that the connection is coming from
- *username* —Username of the requester for remote access, if known yet
- *reason* —Reason that the SA was rejected

Recommended Action Check CAC settings for IKEv2 to determine if this is expected behavior based on configured thresholds; otherwise, if the condition persists, investigate further to alleviate the issue.

750010

Error Message `%FTD-5-750010: Local: local-ip Remote: remote-ip Username:username IKEv2 local throttle-request queue depth threshold of threshold reached; increase the window size on peer peer for better performance`

- *local-ip* —Local peer IP address
- *remote-ip* —Remote peer IP address
- *username* —Username of the requester for remote access or tunnel group name for L2L, if known yet
- *threshold* —Queue depth threshold of the local throttle-request queue reached
- *peer* —Remote peer IP address

Explanation The Secure Firewall Threat Defense device overflowed its throttle request queue to the specified peer, indicating that the peer is slow. The throttle request queue holds requests destined for the peer, which cannot be sent immediately because the maximum number of requests allowed to be in-flight based on the IKEv2 window size were already in-flight. As in-flight requests are completed, requests are pulled off of the throttle request queue and sent to the peer. If the peer is not processing these requests quickly, the throttle queue backs up.

Recommended Action If possible, increase the IKEv2 window size on the remote peer to allow more concurrent requests to be in-flight, which may improve performance.

Note The Secure Firewall Threat Defense device does not currently support an increased IKEv2 window size setting.

750011

Error Message `%FTD-3-750011: Tunnel Rejected: Selected IKEv2 encryption algorithm (IKEV2 encry algo ) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo ).`

Explanation The tunnel was rejected because the selected IKEv2 encryption algorithm is not strong enough to secure the proposed IPSEC encryption algorithm.

Recommended Action Configure a stronger IKEv2 encryption algorithm to match or exceed the strength of the IPsec child SA encryption algorithm.

750012

Error Message `%FTD-4-750012: Selected IKEv2 encryption algorithm (IKEV2 encry algo ) is not strong enough to secure proposed IPSEC encryption algorithm (IPSEC encry algo ).`

Explanation The selected IKEv2 encryption algorithm is not strong enough to secure the proposed IPSEC encryption algorithm.

Recommended Action Configure a stronger IKEv2 encryption algorithm to match or exceed the strength of the IPsec child SA encryption algorithm.

750013

Error Message `%FTD-5-750013: IKEv2 SA (iSPI ISPI rRSP rSPI) Peer Moved: Previous prev_remote_ip:prev_remote_port/prev_local_ip:prev_local_port. Updated new_remote_ip:new_remote_port/new_local_ip:new_local_port`

Explanation The new mobike feature allows peer IP to be changed without tearing down the tunnel. For example, a mobile device (smartphone) acquires new IP after connecting to a different network.The following list describes the message values:

- *ip* —Specifies the previous, the new local, and remote IP addresses
- *port* —Specifies the previous, the new local, and remote port information
- *SPI* —Indicates the Initiator and Responder SPI
- *iSPI* —Specifies the Initiator SPI
- *rSPI* —Specifies the Responder SPI

Recommended Action Contact the Development engineers.

751001

Error Message `%FTD-3-751001: Failed to complete Diffie-Hellman operation. Error: error.`

Explanation A failure to complete a Diffie-Hellman operation occurred, as indicated by the error.

- *error* —The error string that indicates the specific error

Recommended Action A low memory issue or other internal error that should be resolved has occurred. If it persists, use the memory tracking tool to isolate the issue.

751002

Error Message `%FTD-3-751002: No pre-shared key or trustpoint configured for self in tunnel group group`

Explanation The Secure Firewall Threat Defense device was unable to find any type of authentication information in the tunnel group that it could use to authenticate itself to the peer.

- *group* —The name of the tunnel group

Recommended Action Check the tunnel group configuration, and configure a preshared key or certificate for self-authentication in the indicated tunnel group.

751003

Error Message `%FTD-7-751003: Need to send a DPD message to peer`

Explanation Dead peer detection needs to be performed for the specified peer to determine if it is still alive. The Secure Firewall Threat Defense device may have terminated a connection to the peer.

Recommended Action None required.

751004

Error Message `%FTD-3-751004: No remote authentication method configured for peer in tunnel group` *`group`*

Explanation A method to authenticate the remote peer was not found in the configuration to allow the connection.

- *group* —The name of the tunnel group

Recommended Action Check the configuration to make sure that a valid remote peer authentication setting is present.

751005

Error Message `%FTD-3-751005: AnyConnect client reconnect authentication failed. Session ID:` *`session_id`*`, Error:` *`error`*

Explanation A failure occurred during an AnyConnect client reconnection attempt using the session token.

- *session_id* —The session ID used to try to reconnect
- *error* —The error string to indicate the specific error that occurred during the reconnection attempt

Recommended Action Take action according to the error specified, if necessary. The error may indicate that a session was removed instead of remaining in resume state because a client disconnect was detected or sessions were cleared on the Secure Firewall Threat Defense device. If necessary, also compare this message to the event logs on the Anyconnect client.

751006

Error Message `%FTD-3-751006: Certificate authentication failed. Error:` *`error`*

Explanation A failure related to certificate authentication occurred.

- *error* —The error string to indicate the specific certificate authentication failure

Recommended Action Take action according to the error specified, if necessary. Check the certificate trustpoint configuration and make sure that the necessary CA certificate exists to be able to correctly verify client certificate chains. Use the **debug crypto ca** commands to isolate the failure.

751007

Error Message `%FTD-5-751007: Configured attribute not supported for IKEv2. Attribute: attribute`

Explanation A configured attribute could not be applied to the IKE version 2 connection because it is not supported for IKE version 2 connections.

- *attribute* —The attribute that is configured to be applied

Recommended Action None required, To eliminate this message from being generated, you can remove the IKE version 2 configuration setting.

751008

Error Message `%FTD-3-751008: Group=group, Tunnel rejected: IKEv2 not enabled in group policy`

Explanation IKE version 2 is not allowed based on the enabled protocols for the indicated group to which a connection attempt was mapped, and the connection was rejected.

- *group* —The tunnel group used for connection

Recommended Action Check the group policy VPN tunnel protocol setting and enable IKE version 2, if desired.

751009

Error Message `%FTD-3-751009: Unable to find tunnel group for peer.`

Explanation A tunnel group could not be found for the peer.

Recommended Action Check the configuration and tunnel group mapping rules, then configure them to allow the peer to land on a configured group.

751010

Error Message `%FTD-3-751010: Local: localIP:port Remote:remoteIP:port Username: username/group Unable to determine self-authentication method. No crypto map setting or tunnel group found.`

Explanation A method for authenticating the Secure Firewall Threat Defense device to the peer could not be found in either the tunnel group or crypto map.

- *localIP:port* —The local IP address and port number
- *remoteIP:port* —The remote IP address and port number
- *username/group* —The username or group associated with this connection attempt

Recommended Action Check the configuration, and configure a self-authentication method in the crypto map for the initiator L2L or in the applicable tunnel group.

751011

Error Message `%FTD-3-751011: Failed user authentication. Error: error`

Explanation A failure occurred during user authentication within EAP for an IKE version 2 remote access connection.

- *error* —The error string that indicates the specific error

Recommended Action Make sure that the correct authentication credentials were provided and debug further to determine the exact cause of failure, if necessary.

751012

Error Message `%FTD-3-751012: Failure occurred during Configuration Mode processing. Error: error`

Explanation A failure occurred during configuration mode processing while settings were being applied to the connection.

- *error* —The error string that indicates the specific error

Recommended Action Take action based on the indicated error. Use the **debug crypto ikev2** commands to determine the cause of the failure, or debug the indicated subsystem that is specified by the error, if necessary.

751013

Error Message `%FTD-3-751013: Failed to process Configuration Payload request for attribute attribute_id. Error: error`

Explanation The Configuration Payload request failed to process and generate a Configuration Payload response for an attribute that was requested by the peer.

- *attribute_id* — The attribute ID on which the failure occurred
- *error* —The error string that indicates the specific error

Recommended Action A memory error, configuration error, or another type of error has occurred. Use the **debug crypto ikev2** commands to help isolate the cause of the failure.

751014

Error Message `%FTD-4-751014: Warning Configuration Payload request for attribute attribute_id could not be processed. Error: error`

Explanation A warning occurred while processing a CP request to generate a CP response for a requested attribute.

- *attribute_id* — The attribute ID on which the failure occurred
- *error* —The error string that indicates the specific error

Recommended Action Take action based on the attribute indicated in the warning and the indicated warning message. For example, a newer client is being used with an older Secure Firewall Threat Defense image, which does not understand a new attribute that has been added to the client. An upgrade of the Secure Firewall Threat Defense image may be necessary to allow the attribute to be processed.

751015

Error Message `%FTD-4-751015: SA request rejected by CAC. Reason: reason`

Explanation The connection was rejected by the call admission control to protect the Secure Firewall Threat Defense device based on configured thresholds or conditions indicated by the reason listed.

- *reason* —The reason that the SA request was rejected

Recommended Action Check the reason and resolve the condition if a new connection should have been accepted or change the configured thresholds.

751016

Error Message `%FTD-4-751016: Remote L2L Peer initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!`

Explanation The peer may be configured for originate-only connections based on the received outer and inner IP addresses for the tunnel.

Recommended Action Check the L2L peer configuration.

751017

Error Message `%FTD-3-751017: Configuration Error: error_description.`

Explanation An error in the configuration that prevented the connection has been detected.

- *error description* —A brief description of the configuration error

Recommended Action Correct the configuration based on the indicated error.

751018

Error Message `%FTD-3-751018: Terminating the VPN connection attempt from attempted group.`

Explanation The tunnel group over which the connection is attempted is not the same as the tunnel group set in the group lock.

- *attempted group* —The tunnel group over which the connection came in

Recommended Action Check the group-lock value in the group policy or the user attributes.

751019

Error Message `%FTD-4-751019: Failed to obtain an licenseType license. Maximum license limit limit exceeded.`

Explanation A session creation failed because the maximum license limit was exceeded, which caused a failure to either initiate or respond to a tunnel request.

- *licenseType* — License type that was exceeded (other VPN or AnyConnect Premium/Essentials)
- *limit* —Number of licenses allowed and was exceeded

Recommended Action Make sure that enough licenses are available for all allowed users and/or obtain more licenses to allow the rejected connections. For multiple context mode, allow more licenses for the context that reported the failure, if necessary.

751020

Error Message `%FTD-3-751020: Local:%A:%u Remote:%A:%u Username:%s An %s remote access connection failed. Attempting to use an NSA Suite B crypto algorithm (%s) without an AnyConnect Premium license.`

Explanation An IKEv2 remote access tunnel could not be created because the AnyConnect Premium license was applied but explicitly disabled with the **anyconnect-essentials** command in the webvpn configuration mode.

Recommended Action Make sure that an AnyConnect Premium license is installed on the Secure Firewall Threat Defense device is configured in the remote access IKEv2 policies or IPsec proposals.

751021

Error Message `%FTD-4-751021: variable_1 variable_2 with variable_3 encryption is not supported with this version of the AnyConnect Client. Please upgrade to the latest Anyconnect Client.`

Explanation An out-of-date AnyConnect client tried to connect to an Secure Firewall Threat Defense device that has IKEv2 with AES-GCM encryption policy configured.

- *variable_1* —Username of the AnyConnect client (may be unknown because this occurs before the user enters a username)
- *variable_2* —Connection protocol type (IKEv1, IKEv2)
- *variable_3* —Combined mode encryption type (AES-GCM, AES-GCM 256)

Recommended Action Upgrade the AnyConnect client to the latest version to use IKEv2 with AES-GCM encryption.

751022

Error Message `%FTD-3-751022: Tunnel rejected: Crypto Map Policy not found for remote traffic selector rem-ts-start/rem-ts-end/rem-ts.startport/rem-ts.endport/rem-ts.protocol local traffic selector local-ts-start/local-ts-end/local-ts.startport/local-ts.endport/local-ts.protocol!`

Explanation The Secure Firewall Threat Defense device was not able to find security policy information for the private networks or hosts indicated in the message. These networks or hosts were sent by the initiator and do not match any crypto ACLs at the Secure Firewall Threat Defense device. This is most likely a misconfiguration.

- *rem-ts-start* —Remote traffic selector start address
- *rem-ts-end* —Remote traffic selector end address
- *rem-ts.startport* —Remote traffic selector start port
- *rem-ts.endport* —Remote traffic selector end port
- *rem-ts.protocol* —Remote traffic selector protocol
- *local-ts-start* —Local traffic selector start address
- *local-ts-end* —Local traffic selector end address
- *local-ts.startport* —Local traffic selector start port
- *local-ts.endport* —Local traffic selector end port
- *local-ts.protocol* —Local traffic selector protocol

Recommended Action Check the protected network configuration in the crypto ACLs on both sides and make sure that the local network on the initiator is the remote network on the responder and vice-versa. Pay special attention to wildcard masks and host addresses as compared to network addresses. Non-Cisco implementations may have the private addresses labeled as proxy addresses or "red" networks.

751023

Error Message `%FTD-6-751023: Unknown client connection.`

Explanation An unknown non-Cisco IKEv2 client has connected to the Secure Firewall Threat Defense device.

Recommended Action Upgrade to a Cisco-supported IKEv2 client.

751024

Error Message `%FTD-3-751024: IPv6 User Filter tempipv6 configured. This setting has been deprecated, terminating connection`

Explanation The IPv6 VPN filter has been deprecated and if it is configured instead of a unified filter for IPv6 traffic access control, the connection will be terminated.

Recommended Action Configure a unified filter with IPv6 entries to control IPv6 traffic for the user.

751025

Error Message `%FTD-5-751025: Group:group-policy IPv4 Address=assigned_IPv4_addr IPv6 address=assigned_IPv6_addr assigned to session`

Explanation This message displays the assigned IP address information for the AnyConnect IKEv2 connection of the specified user.

- *group-policy* —The group policy that allowed the user to gain access
- *assigned_IPv4_addr* —The IPv4 address that is assigned to the client
- *assigned_IPv6_addr* —The IPv6 address that is assigned to the client

Recommended Action None required.

751026

Error Message `%FTD-6-751026: Client OS: client-os Client: client-name client-version`

Explanation The indicated user is attempting to connect with the shown operating system and client version.

- *client-os* —The operating system reported by the client
- *client-name* —The client name reported by the client (usually AnyConnect)
- *client-version* —The client version reported by the client

Recommended Action None required.

751027

Error Message `%FTD-4-751027: Received INVALID_SELECTORS Notification. Peer received a packet (SPI= spi). The decapsulated inner packet didn't match the negotiated policy in the SA. Packet destination pkt_daddr, port pkt_dest_port, source pkt_saddr, port pkt_src_port, protocol pkt_prot.`

Explanation A peer received a packet on an IPsec security association (SA) that did not match the negotiated traffic descriptors for that SA. The peer sent an INVALID_SELECTORS notification containing the SPI and packet data for the offending packet.

- *spi* —SPI of the IPsec SA for the packet
- *pkt_daddr* —Packet destination IP address
- *pkt_dest_port* —Packet destination port
- *pkt_saddr* —Packet source IP address
- *pkt_src_port* —Packet source port
- *pkt_prot* —Packet protocol

Recommended Action Copy the error message, the configuration, and any details about the events leading up to this error, then submit them to Cisco TAC.

751031

Error Message `%FTD-6-716166: Denied SSL remote access session for reqType faddr client_ip laddr <device_ip> by (geo=country_name, id=country_code)`

Explanation The messages appear when an IKEv2 session is denied. This syslog appears under existing vpn logging class.

Recommended Action None required.

752001

Error Message `%FTD-2-752001: Tunnel Manager received invalid parameter to remove record`

Explanation A failure to remove a record from the tunnel manager that might prevent future tunnels to the same peer from initiating has occurred.

Recommended Action Reloading the device will remove the record, but if the error persists or recurs, perform additional debugging of the specific tunnel attempt.

752002

Error Message `%FTD-7-752002: Tunnel Manager Removed entry. Map Tag = mapTag . Map Sequence Number = mapSeq .`

Explanation An entry to initiate a tunnel was successfully removed.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

Recommended Action None required.

752003

Error Message `%FTD-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2. Map Tag = mapTag . Map Sequence Number = mapSeq`

Explanation An attempt is being made to initiate an IKEv2 tunnel that was based on the crypto map indicated.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

Recommended Action None required.

752004

Error Message `%FTD-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1. Map Tag = mapTag . Map Sequence Number = mapSeq`

Explanation An attempt is being made to initiate an IKEv1 tunnel that was based on the crypto map indicated.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

Recommended Action None required.

752005

Error Message `%FTD-2-752005: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Memory may be low. Map Tag = mapTag . Map Sequence Number = mapSeq.`

Explanation An attempt to dispatch a tunnel initiation attempt failed because of an internal error, such as a memory allocation failure.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

Recommended Action Use the memory tracking tools and additional debugging to isolate the issue.

752006

Error Message `%FTD-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Probable mis-configuration of the crypto map or tunnel-group. Map Tag = Tag . Map Sequence Number = num, SRC Addr: address port: port Dst Addr: address port: port .`

Explanation An attempt to dispatch a tunnel initiation attempt failed because of a configuration error of the indicated crypto map or associated tunnel group.

- *Tag* —Name of the crypto map for which the initiation entry was removed
- *num* —Sequence number of the crypto map for which the initiation entry was removed
- *address* —The source IP address or destination IP address
- *port* —The source port number or destination port number

Recommended Action Check the configuration of the tunnel group and crypto map indicated to make sure that it is complete.

752007

Error Message `%FTD-3-752007: Tunnel Manager failed to dispatch a KEY_ACQUIRE message. Entry already in Tunnel Manager. Map Tag = mapTag . Map Sequence Number = mapSeq`

Explanation An attempt was made to re-add an existing entry into the tunnel manager.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

Recommended Action If the issue persists, make sure that the configuration of the peer will allow the tunnel, and debug further to make sure that the tunnel manager entries are being added and removed correctly during tunnel initiation and successful or failed initiation attempts. Debug IKE version 2 or IKE version 1 connections further, because they may still be in the process of creating the tunnel.

752008

Error Message `%FTD-7-752008: Duplicate entry already in Tunnel Manager`

Explanation A duplicate request to initiate a tunnel was made, and the tunnel manager is already attempting to initiate the tunnel.

Recommended Action None required. If the issue persists, either IKE version 1 or IKE version 2 may have attempted a tunnel initiation and not have timed out yet. Debug further using the applicable commands to make sure that the tunnel manager entry is removed after successful or failed initiation attempts.

752009

Error Message `%FTD-4-752009: IKEv2 Doesn't support Multiple Peers`

Explanation An attempt to initiate a tunnel with IKE version 2 failed because the crypto map is configured with multiple peers, which is not supported for IKE version 2. Only IKE version 1 supports multiple peers.

Recommended Action Check the configuration to make sure that multiple peers are not expected for IKE version 2 site-to-site initiation.

752010

Error Message `%FTD-4-752010: IKEv2 Doesn't have a proposal specified`

Explanation No IPsec proposal was found to be able to initiate an IKE version 2 tunnel .

Recommended Action Check the configuration, then configure an IKE version 2 proposal that can be used to initiate the tunnel, if necessary.

752011

Error Message `%FTD-4-752011: IKEv1 Doesn't have a transform set specified`

Explanation No IKE version 1 transform set was found to be able to initiate an IKE version 2 tunnel.

Recommended Action Check the configuration, then configure an IKE version 2 transform set that can be used to initiate the tunnel, if necessary.

752012

Error Message `%FTD-4-752012: IKEv protocol was unsuccessful at setting up a tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq .`

Explanation The indicated protocol failed to initiate a tunnel using the configured crypto map.

- *protocol*— IKE version number 1 or 2 for IKEv1 or IKEv2
- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

Recommended Action Check the configuration, then debug further within the indicated protocol to determine the cause of the failed tunnel attempt.

752013

Error Message `%FTD-4-752013: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2 after a failed attempt. Map Tag = mapTag . Map Sequence Number = mapSeq .`

Explanation The tunnel manager is attempting to initiate the tunnel again after it failed.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

Recommended Action Check the configuration, and make sure that the crypto maps are correctly configured. Then determine if the tunnel is successfully created on the second attempt.

752014

Error Message `%FTD-4-752014: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1 after a failed attempt. Map Tag = mapTag . Map Sequence Number = mapSeq .`

Explanation The tunnel manager is falling back and attempting to initiate the tunnel using IKE version 1 after the tunnel failed.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

Recommended Action Check the configuration, and make sure that the crypto maps are correctly configured. Then determine if the tunnel is successfully created on the second attempt.

752015

Error Message `%FTD-3-752015: Tunnel Manager has failed to establish an L2L SA. All configured IKE versions failed to establish the tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq .`

Explanation An attempt to bring up an L2L tunnel to a peer failed after trying with all configured protocols.

- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

Recommended Action Check the configuration, and make sure that the crypto maps are correctly configured. Debug the individual protocols to isolate the cause of the failure.

752016

Error Message `%FTD-5-752016: IKEv protocol was successful at setting up a tunnel. Map Tag = mapTag . Map Sequence Number = mapSeq.`

Explanation The indicated protocol (IKE version 1 or IKE version 2) successfully created an L2L tunnel.

- *protocol*— IKE version number 1 or 2 for IKEv1 or IKEv2
- *mapTag* —Name of the crypto map for which the initiation entry was removed
- *mapSeq* —Sequence number of the crypto map for which the initiation entry was removed

Recommended Action None required.

752017

Error Message `%FTD-4-752017: IKEv2 Backup L2L tunnel initiation denied on interface interface matching crypto map name, sequence number number . Unsupported configuration.`

Explanation The Secure Firewall Threat Defense device uses IKEv1 to initiate the connection because IKEv2 does not support the backup L2L feature.

Recommended Action None required if IKEv1 is enabled. You must enable IKEv1 to use the backup L2L feature.

753001

Error Message `%FTD-4-753001: Unexpected IKEv2 packet received from ip_address:port. Error: reason`

Explanation This syslog is generated when an IKEv2 packet is received when the cluster is operating in Distributed VPN clustering mode and fails early consistency and/or error checks performed on it in the datapath.

- *ip_address*—source IP address from where the packet was received
- *port*—source port from where the packet was received
- *reason*—Reason why the packet is considered invalid. This value could be *Corrupted SPI detected* or *Expired SPI received*.

Recommended Action None required if IKEv1 is enabled. You must enable IKEv1 to use the backup L2L feature.

767001

Error Message `%FTD-6-767001: Inspect-name : Dropping an unsupported IPv6/IP46/IP64 packet from interface :IP Addr to interface :IP Addr (fail-close)`

Explanation A fail-close option was set for a service policy, and a particular inspect received an IPv6, IP64, or IP46 packet. Based on the fail-close option setting, this syslog message is generated and the packet is dropped.

Recommended Action None required.

768001

Error Message `%FTD-3-768001: QUOTA: resource utilization is high: requested req, current curr, warning level level`

Explanation A system resource allocation level has reached its warning threshold. In the case of a management session, the resource is simultaneous administrative sessions.

- *resource*— The name of the system resource; in this case, it is a management session.
- *req* —The number requested; for a management session, it is always 1.
- *curr* —The current number allocated; equals *level* for a management session
- *level* —The warning threshold, which is 90 percent of the configured limit

Recommended Action None required.

768002

Error Message `%FTD-3-768002: QUOTA: resource quota exceeded: requested req, current curr, limit limit`

Explanation A request for a system resource would have exceeded its configured limit and was denied. In the case of a management session, the maximum number of simultaneous administrative sessions on the system has been reached.

- *resource*— The name of the system resource; in this case, it is a management session.
- *req* —The number requested; for a management session, it is always 1.
- *curr* —The current number allocated; equals *level* for a management session
- *limit* —The configured resource limit

Recommended Action None required.

768003

Error Message `%FTD-3-768003: QUOTA: management_session quota exceeded for user user_name: current 3,user limit 3`

Explanation The current management session exceeded the configured limits for the user.

- *current* —The current number allocated for management session for the user
- *limit* —The configured management session limit. The default value being 15.

Recommended Action None required.

768004

Error Message `%FTD-3-768004: QUOTA: management_session quota exceeded for ssh/telnet/http protocol: current 2, protocol limit 2`

Explanation The maximum number of management sessions for the protocol - ssh, telnet, or http exceeded the configured limit.

- *current* —The current number allocated for a management session
- *limit* —The configured resource limit per protocol. The default values being 5.

Recommended Action None required.

769001

Error Message `%FTD-5-769001: UPDATE: FTD image 'src' was added to system boot list`

Explanation The system image has been updated. The name of a file previously downloaded onto the system has been added to the system boot list.

- *src*— The name or URL of the source image file

Recommended Action None required.

769002

Error Message `%FTD-5-769002: UPDATE: FTD image 'src' was copied to 'dest'`

Explanation The system image has been updated. An image file has been copied onto the system.

- *src*— The name or URL of the source image file
- *dest* —The name of the destination image file

Recommended Action None required.

769003

Error Message `%FTD-5-769003: UPDATE: FTD image 'src' was renamed to 'dest'`

Explanation The system image has been updated. An existing image file has been renamed to an image file name in the system boot list.

- *src*— The name or URL of the source image file
- *dest* —The name of the destination image file

Recommended Action None required.

769004

Error Message `%FTD-2-769004: UPDATE: FTD image 'src_file' failed verification, reason: failure_reason`

Explanation The image failed verification from either the copy command or verify command.

- *src_file* — The file name or URL of the source image file
- *failure_reason* —The file name of the destination image file

Recommended Action Possible failure reasons are: insufficient system memory, no image found in file, checksum failed, signature not found in file, signature invalid, signature algorithm not supported, signature processing issue

769005

Error Message `%FTD-5-769005: UPDATE: FTD image 'image_name' passed verification`

Explanation This is a notification message indicating that the image passed verification.

- *image_name* — The file name of the Secure Firewall Threat Defense image file

Recommended Action None Required.

769006

Error Message `%FTD-3-769006: UPDATE: FTD boot system image 'image_name' was not found on disk`

Explanation This is an error message indicating that the file configured in the boot system list could not be located on disk.

- *image_name* — The file name of the Secure Firewall Threat Defense image file

Recommended Action If the device fails to boot, change the boot system command to point to a valid file or install the missing file to the disk before rebooting the device.

769007

Error Message `%FTD-6-769007: UPDATE: Image version is version_number`

Explanation This message appears when the device is upgraded.

- *version_number* — The version number of the Secure Firewall Threat Defense image file

Recommended Action None required.

769009

Error Message `%FTD-4-769009: UPDATE: Image booted image_name is different from boot images`

Explanation This is an error message appears after upgrading the device indicating that the file configured is different from the existing list of boot images.

- *image_name* — The file name of the Secure Firewall Threat Defense image file

Recommended Action None required.

770001

Error Message `%FTD-4-770001: Resource resource allocation is more than the permitted limit of limit. If this condition persists, the FTD will be rebooted`

Explanation The CPU or memory resource allocation for the Secure Firewall Threat Defense virtual machine has exceeded the allowed limit for this platform. This condition does not occur unless the setting for the Secure Firewall Threat Defense virtual machine has been changed from that specified in the software downloaded from Cisco.com.

Recommended Action To continue Secure Firewall Threat Defense operation, change the CPU or memory resource allocation of the virtual machine to what was specified with the software downloaded from Cisco.com.

770002

Error Message `%FTD-1-770002: Resource resource allocation is more than the permitted limit of limit, Device will be rebooted`

Explanation The CPU or memory resource allocation for the Secure Firewall Threat Defense virtual machine has exceeded the allowed limit for this platform. This condition does not occur unless the setting for the Secure Firewall Threat Defense virtual machine has been changed from that specified in the software downloaded from Cisco.com. The Secure Firewall Threat Defense device will continue to reboot if the resource allocation is not changed.

Recommended Action Change the CPU or memory reosurce allocation to the virtual machine to what was specified with the software downloaded from Cisco.com.

770003

Error Message `%FTD-4-770003: Resource resource allocation is less than the minimum requirement of value.`

Explanation The CPU or memory resource allocation to the Secure Firewall Threat Defense virtual machine is less than the minimum requirement for this platform. If this condition persists, performance will be lower than normal.

Recommended Action To continue Secure Firewall Threat Defense operation, change the CPU or memory reosurce allocation of the virtual machine to what was specified with the software downloaded from Cisco.

771003

Error Message `%FTD-3-771003: CLOCK: Hardware clock UIP bit is set to 1, for duration secs, start time duration secs, end time duration secs. Read clock time from linux system clock`

Explanation Rate-limited.

Recommended Action None required.

772002

Error Message `%FTD-3-772002: PASSWORD: console login warning, user username, cause: password expired`

Explanation A user logged into the system console with an expired password, which is permitted to avoid system lockout.

- *username*— The name of the user

Recommended Action The user should change the login password.

772003

Error Message `%FTD-2-772003: PASSWORD: session login failed, user username, IP ip, cause: password expired`

Explanation A user logged tried to log into the system with an expired password and was denied access.

- *session*— The session type, which can be SSH or Telnet
- *username*— The name of the user
- *ip* —The IP address of the user

Recommended Action If the user has authorized access, an administrator must change the password for the user. Unauthorized access attempts should trigger an appropriate response, for example. traffic from that IP address can be blocked.

772004

Error Message `%FTD-3-772004: PASSWORD: session login failed, user username, IP ip, cause: password expired`

Explanation A user logged tried to log into the system with an expired password and was denied access.

- *session*— The session type, which is ASDM
- *username*— The name of the user
- *ip* —The IP address of the user

Recommended Action If the user has authorized access, an administrator must change the password for the user. Unauthorized access attempts should trigger an appropriate response, for example. traffic from that IP address can be blocked.

772005

Error Message `%FTD-6-772005: REAUTH: user 'username' passed authentication`

Explanation The user authenticated successfully after changing the password.

- *username*— The name of the user

Recommended Action None required.

772006

Error Message `%FTD-2-772006: REAUTH: user 'username' failed authentication`

Explanation The user entered the wrong password while trying to change it. As a result, the password was not changed.

- *username*— The name of the user

Recommended Action The user should retry changing the password using the **change-password** command.

774001

Error Message `%FTD-2-774001: POST: unspecified error`

Explanation The crypto service provider failed the power on self-test.

Recommended Action Contact the Cisco TAC.

774002

Error Message `%FTD-2-774002: POST: error 'err', func 'func', engine eng, algorithm alg, mode mode, dir dir, key len len`

Explanation The crypto service provider failed the power on self-test.

- *err* —The failure cause
- *func* —The function
- *eng* —The engine, which can be NPX, Nlite, or software
- *alg* —The algorithm, which can be any of the following: RSA, DSA, DES, 3DES, AES, RC4, MD5, SHA1, SHA256, SHA386, SHA512, HMAC-MD5, HMAC-SHA1, HMAC-SHA2, or AES-XCBC
- *mode* —The mode, which can be any of the following: none, CBC, CTR, CFB, ECB, stateful-RC4, or stateless-RC4
- *dir* —Either encryption or decryption
- *len* —The key length in bits

Recommended Action Contact the Cisco TAC.

776251

Error Message `%FTD-6-776251: CTS SGT-MAP: Binding binding IP->SGname from SGT added to binding manager.`

Explanation Binding from the specified source was added to the binding manager.

- *binding IP* —IPv4 or IPv6 binding address.
- *SGname* (*SGT*)—Binding SGT information. Has the following format if SGname is available: *SGname* (*SGT*) and the following format if SGname is unavailable: *SGT*.
- *source name* —Name of the contributing source.

Recommended Action None required.

776252

Error Message `%FTD-5-776252: CTS SGT-MAP: Binding binding IP->SGname from SGT deleted from binding manager.`

Explanation Binding from the specified source was deleted from the binding manager.

Binding from the specified source was added to the binding manager.

- *binding IP* —IPv4 or IPv6 binding address.
- *SGname* (*SGT*)—Binding SGT information. Has the following format if SGname is available: *SGname* (*SGT*) and the following format if SGname is unavailable: *SGT*.
- *source name* —Name of the contributing source.

Recommended Action None required.

776253

Error Message `%FTD-6-776253: CTS SGT-MAP: Binding binding IP->new from SGname changed from old sgt: SGT from old sourcenew source name`

Explanation A particular IP to SGT binding has changed in the binding manager.

- *binding IP* —IPv4 or IPv6 binding address.
- *new SGname* (*SGT*)—New binding SGT information. Has the following format if SGname is available: *SGname* (*SGT*) and the following format if SGname is unavailable: *SGT*.
- *new source name* —Name of the new contributing source.
- *old SGname* (*SGT*)—Old binding SGT information. Has the following format if SGname is available: *SGname* (*SGT*) and the following format if SGname is unavailable: *SGT*.
- *old source name* —Name of the old contributing source.

Recommended Action None required.

776254

Error Message `%FTD-3-776254: CTS SGT-MAP: Binding manager unable to action binding binding IP->SGname from SGT.`

Explanation The binding manager cannot insert, delete, or update the binding

- *action*— Binding manager operation. Either insert, delete or update.
- *binding IP* —IPv4 or IPv6 binding address.
- *SGname* (*SGT*)—Binding SGT information. Has the following format if SGname is available: *SGname* (*SGT*) and the following format if SGname is unavailable: *SGT*.
- *source name* —Name of the contributing source.

Recommended Action Contact the Cisco TAC for assistance.