

Syslog Messages 715001 to 721019

This chapter contains the following sections:

- Messages 715001 to 715080, on page 1
- Messages 716001 to 716603, on page 14
- Messages 717001 to 717064, on page 34
- Messages 718001 to 719026, on page 49
- Messages 720001 to 721019, on page 70

Messages 715001 to 715080

This section includes messages from 715001 to 715080.

715001

Error Message `%FTD-7-715001: Descriptive statement`

Explanation A description of an event or problem encountered by the Secure Firewall Threat Defense device appears.

Recommended Action The action depends on the description.

715004

Error Message `%FTD-7-715004: subroutine name () Q Send failure: RetCode (return_code )`

Explanation An internal error occurred when attempting to put messages in a queue.

Recommended Action This is often a benign condition. If the problem persists, contact the Cisco TAC.

715005

Error Message `%FTD-7-715005: subroutine name() Bad message code: Code (message_code )`

Explanation An internal subroutine received a bad message code.

Recommended Action This is often a benign condition. If the problem persists, contact the Cisco TAC.

715006

Error Message `%FTD-7-715006: Group = groupname, Username = username, IP = IP_address IKE got SPI from key engine: SPI = SPI_value`

Explanation The IKE subsystem received an SPI value from IPsec.

Recommended Action None required.

715007

Error Message `%FTD-7-715007: Group = groupname, Username = username, IP = IP_address IKE got a KEY_ADD msg for SA: SPI = SPI_value`

Explanation IKE has completed tunnel negotiation and has successfully loaded the appropriate encryption and hashing keys for IPsec use.

Recommended Action None required.

715008

Error Message `%FTD-7-715008: Could not delete SA SA_address, refCnt = number, caller = calling_subroutine_address`

Explanation The calling subroutine cannot delete the IPsec SA. This might indicate a reference count problem.

Recommended Action If the number of stale SAs grows as a result of this event, contact the Cisco TAC.

715009

Error Message `%FTD-7-715009: Group = groupname, Username = username, IP = IP_address IKE Deleting SA: Remote Proxy IP_address, Local Proxy IP_address`

Explanation SA is being deleted with the listed proxy addresses.

Recommended Action None required.

715013

Error Message `%FTD-7-715013: Group = groupname, Username = username, IP = IP_address Tunnel negotiation in progress for destination IP_address, discarding data`

Explanation IKE is in the process of establishing a tunnel for this data. All packets to be protected by this tunnel will be dropped until the tunnel is fully established.

Recommended Action None required.

715018

Error Message `%FTD-7-715018: Group = groupname, Username = username, IP = IP_address IP Range type id was loaded: Direction %s,  From: %a, Through: %a`

Explanation This syslog message is generated while updating IPSEC SA details.

Recommended Action None required.

715019

Error Message `%FTD-7-715019: Group = group, Username = username, IP = ip Group group Username username IP ip IKEGetUserAttributes: Attribute name = name`

Explanation The **modecfg** attribute name and value pair being processed by the Secure Firewall Threat Defense device appear.

Recommended Action None required.

715020

Error Message `%FTD-7-715020: Group = group, Username = username, IP = ip construct_cfg_set: Attribute name = name`

Explanation The **modecfg** attribute name and value pair being transmitted by the Secure Firewall Threat Defense device appear.

Recommended Action None required.

715021

Error Message `%FTD-7-715021: Group = group, Username = username, IP = ip Delay Quick Mode processing, Cert/Trans Exch/RM DSID in progress`

Explanation Quick mode processing is being delayed until all Phase 1 processing has been completed (for transaction mode).

Recommended Action None required.

715022

Error Message `%FTD-7-715022: Group = group, Username = username, IP = ip Resume Quick Mode processing, Cert/Trans Exch/RM DSID completed`

Explanation Phase 1 processing has completed, and quick mode is being resumed.

Recommended Action None required.

715027

Error Message `%FTD-7-715027: Group = group, Username = username, IP = ip IPsec SA Proposal # chosen_proposal, Transform # chosen_transform acceptable Matches global IPsec SA entry # crypto_map_index`

Explanation The indicated IPsec SA proposal and transform were selected from the payloads that the responder received. This data can be useful when attempting to debug IKE negotiation issues.

Recommended Action None required.

715028

Error Message `%FTD-7-715028: Group = group, Username = username, IP = ip IKE SA Proposal # 1, Transform # chosen_transform acceptable Matches global IKE entry # crypto_map_index`

Explanation The indicated IKE SA transform was selected from the payloads that the responder received. This data can be useful when attempting to debug IKE negotiation issues.

Recommended Action None required.

715031

Error Message `%FTD-7-715031: Obtained IP addr (%s) prior to initiating Mode Cfg (XAuth %s)`

Explanation This syslog is generated when the IP address is assigned by the IP util subsystem.

Recommended Action None required.

715032

Error Message `%FTD-7-715032: Sending subnet mask (%s) to remote client`

Explanation This syslog is generated when the IP address is assigned by the IP util subsystem.

Recommended Action None required.

715033

Error Message `%FTD-7-715033: Group = group, Username = username, IP = ip Processing CONNECTED notify (MsgId message_number )`

Explanation The Secure Firewall Threat Defense device is processing a message containing a notify payload with the notify type CONNECTED (16384). The CONNECTED notify type is used to complete the commit bit processing and should be included in the fourth overall quick mode packet, which is sent from the responder to the initiator.

Recommended Action None required.

715034

Error Message `%FTD-7-715034: IP = ip action IOS keep alive payload: proposal=time 1 /time 2 sec.`

Explanation Processing for sending or receiving a keepalive payload message is being performed.

Recommended Action None required.

715035

Error Message `%FTD-7-715035: IP = ip Starting IOS keepalive monitor: seconds sec.`

Explanation The keepalive timer will monitor for a variable number of seconds for keepalive messages.

Recommended Action None required.

715036

Error Message `%FTD-7-715036: Group = group, Username = username, IP = ip Sending keep-alive of type notify_type (seq number number )`

Explanation Processing for sending a keepalive notify message is being performed.

Recommended Action None required.

715037

Error Message `%FTD-7-715037: Group = group, Username = username, IP = ip Unknown IOS Vendor ID version: major.minor.variance`

Explanation The capabilities of this version of the Cisco IOS are not known.

Recommended Action There may be interoperability issues with features such as IKE keepalives. If the problem persists, contact the Cisco TAC.

715038

Error Message `%FTD-7-715038: Group = group, Username = username, IP = ip action Spoofing_information Vendor ID payload (version: major.minor.variance, capabilities: value )`

Explanation Processing for the Cisco IOS vendor ID payload has been performed. The action being performed might be Altiga spoofing the Cisco IOS.

Recommended Action None required.

715039

Error Message `%FTD-7-715039: Group = group, Username = username, IP = ip Unexpected cleanup of tunnel table entry during SA delete.`

Explanation An entry in the IKE tunnel table was never removed when the SA was freed. This indicates a defect in the state machine.

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

715040

Error Message `%FTD-7-715040: Deleting active auth handle during SA deletion: handle = internal_authentication_handle`

Error Message The authentication handle was still active during SA deletion. This is part of cleanup recovery during the error condition.

Recommended Action None required.

715041

Error Message `%FTD-7-715041: Group = group, Username = username, IP = ip Received keep-alive of type keepalive_type, not the negotiated type`

Explanation A keepalive of the type indicated in the message was received unexpectedly.

Recommended Action Check the keepalive configuration on both peers.

715042

Error Message `%FTD-7-715042: Group = group, Username = username, IP = ip IKE received response of type failure_type to a request from the IP_address utility`

Explanation A request for an IP address for a remote access client from the internal utility that provides these addresses cannot be satisfied. Variable text in the message string indicates more specifically what went wrong.

Recommended Action Check the IP address assignment configuration and adjust accordingly.

715044

Error Message `%FTD-7-715044: IP = ip Ignoring Keepalive payload from vendor not support KeepAlive capability`

Explanation A Cisco IOS keepalive payload from a vendor was received without keepalive capabilities being set. The payload is ignored.

Recommended Action None required.

715045

Error Message `%FTD-7-715045: ERROR: malformed Keepalive payload`

Explanation A malformed keepalive payload has been received. The payload is ignored.

Recommended Action None required.

715046

Error Message `%FTD-7-715046: Group = groupname, Username = username, IP = IP_address Group = groupname, Username = username, IP = IP_address, constructing payload_description payload`

Explanation An IP address from a remote client for a specific group and user shows details about the IKE payload being constructed.

Recommended Action None required.

715047

Error Message `%FTD-7-715047: Group = groupname, Username = username, IP = IP_address processing payload_description payload`

Explanation Details of the IKE payload received and being processed appear.

Recommended Action None required.

715048

Error Message `%FTD-7-715048: Group = groupname, Username = username, IP = IP_address Send VID_type VID`

Explanation The type of vendor ID payload being sent appears.

Recommended Action None required.

715049

Error Message `%FTD-7-715049: Group = groupname, Username = username, IP = IP_address Received VID_type VID`

Explanation The type of vendor ID payload received appears.

Recommended Action None required.

715050

Error Message `%FTD-7-715050: Group = groupname, Username = username, IP = IP_address Claims to be IOS but failed authentication`

Explanation The vendor ID received looks like a Cisco IOS VID, but does not match **hmac_sha**.

Recommended Action Check the vendor ID configuration on both peers. If this issue affects interoperability and the problem persists, contact the Cisco TAC.

715051

Error Message `%FTD-7-715051: IP = IP_address Received unexpected TLV type TLV_type while processing FWTYPE ModeCfg Reply`

Explanation An unknown TLV was received in an Secure Firewall Threat Defense record while an FWTYPE ModeCfg Reply was being processed. The TLV will be discarded. This might occur either because of packet corruption or because the connecting client supports a later version of the Secure Firewall Threat Defense protocol.

Recommended Action Check the personal FW installed on the Cisco VPN client and the personal firewall configuration on the Secure Firewall Threat Defense device. This may also indicate a version mismatch between the VPN client and the Secure Firewall Threat Defense device.

715052

Error Message `%FTD-7-715052: Group = groupname, Username = username, IP = IP_address Old P1 SA is being deleted but new SA is DEAD, cannot transition centries`

Explanation The old P1 SA is being deleted, but has no new SA to transition to because it was marked for deletion as well. This generally indicates that the two IKE peers are out-of-sync with each other and may be using different rekey times. The problem should correct itself, but there may be some small amount of data loss until a fresh P1 SA is reestablished.

Recommended Action None required.

715053

Error Message `%FTD-7-715053: Group = groupname, Username = username, IP = IP_address MODE_CFG: Received request for attribute_info !`

Explanation The Secure Firewall Threat Defense device received a mode configuration message requesting the specified attribute.

Recommended Action None required.

715054

Error Message `%FTD-7-715054: MODE_CFG: Received attribute_name reply: value`

Explanation The Secure Firewall Threat Defense received a mode configuration reply message from the remote peer.

Recommended Action None required.

715055

Error Message `%FTD-7-715055: Group = groupname, Username = username, IP = IP_address Send attribute_name`

Explanation The Secure Firewall Threat Defense device sent a mode configuration message to the remote peer.

Recommended Action None required.

715056

Error Message `%FTD-7-715056: Group = groupname, Username = username, IP = IP_address Client is configured for TCP_transparency`

Explanation Because the remote end (client) is configured for IPsec over TCP, the headend Secure Firewall Threat Defense device must not negotiate IPsec over UDP or IPsec over NAT-T with the client.

Recommended Action The NAT transparency configuration may require adjustment of one of the peers if the tunnel does not come up.

715057

Error Message `%FTD-7-715057: Group = groupname, Username = username, IP = IP_address Auto-detected a NAT device with NAT-Traversal. Ignoring IPsec-over-UDP configuration.`

Explanation IPsec-over-UDP mode configuration information will not be exchanged because NAT-Traversal was detected.

Recommended Action None required.

715058

Error Message `%FTD-7-715058: Group = groupname, Username = username, IP = IP_address NAT-Discovery payloads missing. Aborting NAT-Traversal.`

Explanation The remote end did not provide NAT-Discovery payloads required for NAT-Traversal after exchanging NAT-Traversal VIDs. At least two NAT-Discovery payloads must be received.

Recommended Action This may indicate a nonconforming NAT-T implementation. If the offending peer is a Cisco product and the problem persists, contact the Cisco TAC. If the offending peer is not a Cisco product, then contact the manufacturer support team.

715059

Error Message `%FTD-7-715059: Group = groupname, Username = username, IP = IP_address Proposing/Selecting only UDP-Encapsulated-Tunnel and UDP-Encapsulated-Transport modes defined by NAT-Traversal`

Explanation You need to use these modes instead of the usual transport and tunnel modes defined in the SA to successfully negotiate NAT-Traversal.

Recommended Action None required.

715060

Error Message `%FTD-7-715060: Group = groupname, Username = username, IP = IP_address Dropped received IKE fragment. Reason: reason`

Explanation The reason for dropping the fragment appears.

Recommended Action The recommended action depends on the drop reason, but might indicate a problem with an intervening NAT device or a nonconforming peer.

715061

Error Message `%FTD-7-715061: Group = groupname, Username = username, IP = IP_address Rcv'd fragment from a new fragmentation set. Deleting any old fragments.`

Explanation A resend of the same packet occurred, but fragmented to a different MTU, or another packet altogether.

Recommended Action None required.

715062

Error Message `%FTD-7-715062: Group = groupname, Username = username, IP = IP_address Error assembling fragments! Fragment numbers are non-continuous.`

Explanation There is a gap in fragment numbers.

Recommended Action This might indicate a network problem. If the condition persists and results in dropped tunnels or prevents certain peers from negotiating with the Secure Firewall Threat Defense device, contact the Cisco TAC.

715063

Error Message `%FTD-7-715063: Group = groupname, Username = username, IP = IP_address Successfully assembled an encrypted pkt from rcv'd fragments!`

Explanation Assembly for a fragmented packet that was received was successful.

Recommended Action None required.

715064

Error Message `%FTD-7-715064: IKE Peer included IKE fragmentation capability flags: Main Mode: true /false Aggressive Mode: true /false`

Explanation The peer supports IKE fragmentation based on the information provided in the message.

Recommended Action None required.

715065

Error Message `%FTD-7-715065: Group = groupname, Username = username, IP = IP_address IKE state_machine subtype FSM error history (struct data_structure_address ) state, event : state /event pairs`

Explanation A Phase 1 error occurred and the **state**, **event** history pairs will be displayed in reverse chronological order.

Recommended Action Most of these errors are benign. If the problem persists, contact the Cisco TAC.

715066

Error Message `%FTD-7-715066: Group = groupname, Username = username, IP = IP_address Can't load an IPsec SA! The corresponding IKE SA contains an invalid logical ID.`

Explanation The logical ID in the IKE SA is NULL. The Phase II negotiation will be torn down.

Recommended Action An internal error has occurred. If the problem persists, contact the Cisco TAC.

715067

Error Message `%FTD-7-715067: QM IsRekeyed: existing sa from different peer, rejecting new sa`

Explanation The LAN-TO-LAN SA that is being established already exists, that is, an SA with the same remote network, but is sourced from a different peer. This new SA will be deleted, because this is not a legal configuration.

Recommended Action Check the LAN-TO-LAN configuration on all associated peers. Specifically, multiple peers should not be sharing private networks.

715068

Error Message `%FTD-7-715068: Group = groupname, Username = username, IP = IP_address QM IsRekeyed: duplicate sa found by address, deleting old sa`

Explanation The remote access SA that is being established already exists, that is, an SA with the same remote network, but is sourced from a different peer. The old SA will be deleted, because the peer may have changed its IP address.

Recommended Action This may be a benign condition, especially if a client tunnel was terminated abruptly. If the problem persists, contact the Cisco TAC.

715069

Error Message `%FTD-7-715069: Group = groupname, Username = username, IP = IP_address Invalid ESP SPI size of SPI_size`

Explanation The Secure Firewall Threat Defense device received an IPsec SA proposal with an invalid ESP SPI size. This proposal will be skipped.

Recommended Action Generally, this is a benign condition but might indicate that a peer may be nonconforming. If the problem persists, contact the Cisco TAC.

715070

Error Message `%FTD-7-715070: Group = groupname, Username = username, IP = IP_address Invalid IPComp SPI size of SPI_size`

Explanation The Secure Firewall Threat Defense device received an IPsec SA proposal with an invalid IPComp SPI size. This proposal will be skipped.

Recommended Action Generally, this is a benign condition but might indicate that a peer is nonconforming. If the problem persists, contact the Cisco TAC.

715071

Error Message `%FTD-7-715071: Group = groupname, Username = username, IP = IP_address AH proposal not supported`

Explanation The IPsec AH proposal is not supported. This proposal will be skipped.

Recommended Action None required.

715072

Error Message `%FTD-7-715072: Group = groupname, Username = username, IP = IP_address Received proposal with unknown protocol ID protocol_ID`

Explanation The Secure Firewall Threat Defense device received an IPsec SA proposal with an unknown protocol ID. This proposal will be skipped.

Recommended Action Generally, this is a benign condition, but might indicate that a peer is nonconforming. If the problem persists, contact the Cisco TAC.

715074

Error Message `%FTD-7-715074: Group = groupname, Username = username, IP = IP_address Could not retrieve authentication attributes for peer IP_address`

Explanation The Secure Firewall Threat Defense device cannot get authorization information for the remote user.

Recommended Action Make sure that authentication and authorization settings have been configured correctly. If the problem persists, contact the Cisco TAC.

715075

Error Message `%FTD-7-715075: Group = group_name, Username = username, IP = IP_address Group = group_name, IP = IP_address Received keep-alive of type message_type (seq number number )`

Explanation This message is paired with DPD R-U-THERE message 715036, which logs the DPD sending messages.

- **group_name**—The VPN group name of the peer
- **IP_address**—IP address of the VPN peer
- **message_type**—The message type (DPD R-U-THERE or DPD R-U-THERE-ACK)
- **number**—The DPD sequence number

Two possible cases:

- Received peer sending DPD R-U-THERE message
- Received peer reply DPD R-U-THERE-ACK message

Be aware of the following:

- The DPD R-U-THERE message is received and its sequence number matches the outgoing DPD reply messages.

If the Secure Firewall Threat Defense device sends a DPD R-U-THERE-ACK message without first receiving a DPD R-U-THERE message from the peer, it is likely experiencing a security breech.

- The received DPD R-U-THERE-ACK message's sequence number is matched with previously sent DPD messages.

If the Secure Firewall Threat Defense device did not receive a DPD R-U-THERE-ACK message within a reasonable amount of time after sending a DPD R-U-THERE message to the peer, the tunnel is most likely down.

Recommended Action None required.

715076

Error Message `%FTD-7-715076: Group = group_name, Username = username, IP = IP_address Computing hash for ISAKMP`

Explanation IKE computed various hash values.

This object will be prepended as follows:

Group = >*groupname* , Username = >*username* , IP = >*ip_address* ...

Recommended Action None required.

715077

Error Message `%FTD-7-715077: Pitcher: msg string, spi spi`

Explanation Various messages have been sent to IKE.

msg_string can be one of the following:

- Received a key acquire message
- Received SPI for nonexistent SA
- Received key delete msg
- Received KEY_UPDATE
- Received KEY_REKEY_IB
- Received KEY_REKEY_OB
- Received KEY_SA_ACTIVE
- Could not find IKE SA to activate IPSEC (OB)
- Could not find IKE SA to rekey IPSEC (OB)
- KEY_SA_ACTIVE no centry found
- KEY_ADD centry not found
- KEY_UPDATE centry not found

This object will be prepended as follows:

Group = >*groupname* , Username = >*username* , IP = >*ip_address* ,...

Recommended Action None required.

715078

Error Message `%FTD-7-715078: Group = group_name, Username = username, IP = IP_address Received %s LAM attribute`

Explanation This syslog is generated during parsing of challenge/response payload.

Recommended Action None required.

715079

Error Message `%FTD-7-715079: Group = group_name, Username = username, IP = IP_address INTERNAL_ADDRESS: Received request for %s`

Explanation This syslog is generated during processing of internal address payload.

Recommended Action None required.

715080

Error Message `%FTD-7-715080: Group = group_name, Username = username, IP = IP_address VPN: Starting P2 rekey timer: 28800 seconds.`

Error Message An IKE rekey timer has started.

Recommended Action None required.

Messages 716001 to 716603

This section includes messages from 716001 to 716603.

716001

Error Message `%FTD-6-716001: Group group User user IP ip WebVPN session started.`

Explanation The WebVPN session has started for the user in this group at the specified IP address. When the user logs in via the WebVPN login page, the WebVPN session starts.

Recommended Action None required.

716002

Error Message `%FTD-6-716002: Group GroupPolicy User username IP ip WebVPN session terminated: User_Requested.`

Explanation The WebVPN session has been terminated by a user request. Possible reasons include:

- Lost carrier
- Lost service
- Idle timeout
- Max time exceeded
- Administrator reset
- Administrator reboot
- Administrator shutdown
- Port error
- NAS error
- NAS request
- NAS reboot
- Port unneeded
- Port preempted. This reason indicates that the allowed number of simultaneous (same user) logins has been exceeded. To resolve this problem, increase the number of simultaneous logins or have users only log in once with a given username and password.
- Port suspended
- Service unavailable
- Callback
- User error
- Host requested
- Bandwidth management error
- ACL parse error
- VPN simultaneous logins limit specified in the group policy
- Unknown

Recommended Action Unless the reason indicates a problem, then no action is required.

716003

Error Message `%FTD-6-716003: Group group User user IP ip WebVPN access GRANTED: url://string/string`

Explanation The WebVPN user in this group at the specified IP address has been granted access to this URL. The user access to various locations can be controlled using WebVPN-specific ACLs.

Recommended Action None required.

716004

Error Message `%FTD-6-716004: Group group User user IP ip WebVPN access DENIED to specified location: url://string/string`

Explanation The WebVPN user in this group has been denied access to this URL. The WebVPN user access to various locations can be controlled using WebVPN-specific ACLs. In this case, a particular entry is denying access to this URL.

Recommended Action None required.

716005

Error Message `%FTD-6-716005: Group group User user IP ip WebVPN ACL Parse Error: reason string`

Explanation The ACL for the WebVPN user in the specified group failed to parse correctly.

Recommended Action Correct the WebVPN ACL.

716006

Error Message `%FTD-6-716006: Group name User user IP iP WebVPN session not allowed. WebVPN protocol is disabled for this user.`

Explanation The WebVPN session was not created for the user in the specified group because the VPN tunnel protocol is not set to WebVPN.

Recommended Action None required.

716007

Error Message `%FTD-4-716007: Group group User user IP IP WebVPN Unable to create session.`

Explanation The WebVPN session was not created for the user in the specified group because of resource issues. For example, the user may have reached the maximum login limit.

Recommended Action None required.

716008

Error Message `%FTD-7-716008: WebVPN ACL: action string`

Explanation The WebVPN ACL has begun performing an action (for example, begin parsing).

Recommended Action None required.

716009

Error Message `%FTD-6-716009: Group group User user IP IP WebVPN session not allowed. ACL parse error.`

Explanation The WebVPN session for the specified user in this group is not allowed because the associated ACL did not parse. The user will not be allowed to log in via WebVPN until this error has been corrected.

Recommended Action Correct the WebVPN ACL.

716010

Error Message `%FTD-7-716010: Group group User user IP ip Browse network.`

Explanation The WebVPN user in the specified group browsed the network.

Recommended Action None required.

716011

Error Message `%FTD-7-716011: Group group User user IP ip Browse domain domain.`

Explanation The WebVPN specified user in this group browsed the specified domain.

Recommended Action None required.

716012

Error Message `%FTD-7-716012: Group group User user IP ip Browse directory directory.`

Explanation The specified WebVPN user browsed the specified directory.

Recommended Action None required.

716013

Error Message `%FTD-7-716013: Group group User user IP ip Close file filename.`

Explanation The specified WebVPN user closed the specified file.

Recommended Action None required.

716014

Error Message `%FTD-7-716014: Group group User user IP ip View file filename.`

Explanation The specified WebVPN user viewed the specified file.

Recommended Action None required.

716015

Error Message `%FTD-7-716015: Group group User user IP ip Remove file filename.`

Explanation The WebVPN user in the specified group removed the specified file.

Recommended Action None required.

716016

Error Message `%FTD-7-716016: Group group User user IP ip Rename file old_filename to new_filename.`

Explanation The specified WebVPN user renamed the specified file.

Recommended Action None required.

716017

Error Message `%FTD-7-716017: Group group User user IP ip Modify file filename.`

Explanation The specified WebVPN user modified the specified file.

Recommended Action None required.

716018

Error Message `%FTD-7-716018: Group group User user IP ip Create file filename.`

Explanation The specified WebVPN user created the specified file.

Recommended Action None required.

716019

Error Message `%FTD-7-716019: Group group User user IP ip Create directory directory.`

Explanation The specified WebVPN user created the specified directory.

Recommended Action None required.

716020

Error Message `%FTD-7-716020: Group group User user IP ip Remove directory directory.`

Explanation The specified WebVPN user removed the specified directory.

Recommended Action None required.

716021

Error Message `%FTD-7-716021: File access DENIED, filename.`

Explanation The specified WebVPN user was denied access to the specified file.

Recommended Action None required.

716022

Error Message `%FTD-4-716022: Unable to connect to proxy server reason.`

Explanation The WebVPN HTTP/HTTPS redirect failed for the specified reason.

Recommended Action Check the HTTP/HTTPS proxy configuration.

716023

Error Message `%FTD-4-716023: Group name User user IP ip Session could not be established: session limit of maximum_sessions reached.`

Explanation The user session cannot be established because the current number of sessions exceeds the maximum session load.

Recommended Action Increase the configured limit, if possible, to create a load-balanced cluster.

716024

Error Message `%FTD-7-716024: Group name User user IP ip Unable to browse the network.Error: description`

Explanation The user was unable to browse the Windows network using the CIFS protocol, as indicated by the description. For example, "Unable to contact necessary server" indicates that the remote server is unavailable or unreachable. This might be a transient condition or may require further troubleshooting.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall Threat Defense device.

716025

Error Message `%FTD-7-716025: Group name User user IP ip Unable to browse domain domain.Error: description`

Explanation The user was unable to browse the remote domain using the CIFS protocol.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Check the NetBIOS name server configuration on the Secure Firewall Threat Defense device.

716026

Error Message `%FTD-7-716026: Group name User user IP ip Unable to browse directory directory.Error: description`

Explanation The user was unable to browse the remote directory using the CIFS protocol.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall Threat Defense device.

716027

Error Message `%FTD-7-716027: Group name User user IP ip Unable to view file filename.Error: description.`

Explanation The user was unable to view the remote file using the CIFS protocol.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall Threat Defense device.

716028

Error Message `%FTD-7-716028: Group name User user IP ip Unable to remove file filename.Error: description`

Explanation The user was unable to remove the remote file using the CIFS protocol, probably caused by a lack of file permissions.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall Threat Defense device and the file permissions.

716029

Error Message `%FTD-7-716029: Group name User user IP ip Unable to rename file filename.Error: description`

Explanation The user was unable to rename the remote file using the CIFS protocol, probably caused by lack of file permissions.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall Threat Defense device and the file permissions.

716030

Error Message `%FTD-7-716030: Group name User user IP ip Unable to modify file filename.Error: description`

Explanation A problem occurred when a user attempted to modify an existing file using the CIFS protocol, probably caused by a lack of file permissions.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall Threat Defense device and the file permissions.

716031

Error Message `%FTD-7-716031: Group name User user IP ip Unable to create file filename.Error: description`

Explanation A problem occurred when a user attempted to create a file using the CIFS protocol, probably caused by a file permissions problem.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall Threat Defense device and the file permissions.

716032

Error Message `%FTD-7-716032: Group name User user IP ip Unable to create folder folder.Error: description`

Explanation A problem occurred when a user attempted to create a folder using the CIFS protocol, probably caused by a file permissions problem.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall Threat Defense device and the file permissions.

716033

Error Message `%FTD-7-716033: Group name User user IP ip Unable to remove folder folder.Error: description`

Explanation A problem occurred when a user of the CIFS protocol attempted to remove a folder, which probably occurred because of a permissions problem or a problem communicating with the server on which the file resides.

Recommended Action Check the connectivity between the WebVPN device and the server being accessed by the CIFS protocol. Also check the NetBIOS name server configuration on the Secure Firewall Threat Defense device.

716034

Error Message `%FTD-7-716034: Group name User user IP ip Unable to write to file filename.`

Explanation A problem occurred when a user attempted to write to a file using the CIFS protocol, probably caused by a permissions problem or a problem communicating with the server on which the file resides.

Recommended Action None required.

716035

Error Message `%FTD-7-716035: Group name User user IP ip Unable to read file filename.`

Explanation A problem occurred when a user of the CIFS protocol tried to read a file, probably caused by a file permissions problem.

Recommended Action Check the file permissions.

716036

Error Message `%FTD-7-716036: Group name User user IP ip File Access: User user logged into the server server.`

Explanation A user successfully logged into the server using the CIFS protocol

Recommended Action None required.

716037

Error Message `%FTD-7-716037: Group name User user IP ip File Access: User user failed to login into the server server.`

Explanation A user attempted to log in to a server using the CIFS protocol, but was unsuccessful.

Recommended Action Verify that the user entered the correct username and password.

716038

Error Message `%FTD-6-716038: Group group User user IP ip Authentication: successful, Session Type: WebVPN.`

Explanation Before a WebVPN session can start, the user must be authenticated successfully by a local or remote server (for example, RADIUS or TACACS+).

Recommended Action None required.

716039

Error Message `%FTD-6-716039: Group name User user IP ip Authentication: rejected, Session Type: session-type.`

Explanation Before a WebVPN session starts, the user must be authenticated successfully by a local or remote server (for example, RADIUS or TACACS+). In this case, the user credentials (username and password) either did not match, or the user does not have permission to start a WebVPN session. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- **%s**—The session type, which can be either WebVPN or admin

Recommended Action Verify the user credentials on the local or remote server and that WebVPN is configured for the user.

716040

Error Message `%FTD-6-716040: Reboot pending, new sessions disabled. Denied user login.`

Explanation A user was unable to log in to WebVPN because the Secure Firewall Threat Defense device is in the process of rebooting.

- **user**—The session user

Recommended Action None required.

716041

Error Message `%FTD-6-716041: access-list acl_ID action url url hit-cnt count`

Explanation The WebVPN URL named **acl_ID** has been hit **count** times for location **url,** whose **action** is permitted or denied.

- **acl_ID**—The WebVPN URL ACL
- *count* —The number of times the URL was accessed
- *url* —The URL that was accessed
- *action* —The user action

Recommended Action None required.

716042

Error Message `%FTD-6-716042: access-list acl_ID action tcp source_interface/source_address(source_port) -> dest_interface/dest_address(dest_port) hit-cnt count`

Explanation The WebVPN TCP named **acl_ID** has been hit **count** times for packet received on the source interface **source_interface**/**source_address** and source port **source_port** forwarded to **dest_interface**/**dest_address** destination **dest_port,** whose **action** is permitted or denied.

- *count* —The number of times the ACL was accessed
- *source_interface* —The source interface
- *source_address* —The source IP address
- *source_port* —The source port
- *dest_interface* —The destination interface
- *dest_address* —The destination IP address
- *action* —The user action

Recommended Action None required.

716043

Error Message `%FTD-6-716043: Group <group-name> User <user-name> IP <IP_address> WebVPN Port Forwarding Java applet started. Created new hosts file mappings.`

Explanation The user has launched a TCP port-forwarding applet from a WebVPN session.

- **group-name**—Group name associated with the session
- **user-name**—Username associated with the session
- **IP_address**—Source IP address associated with the session

Recommended Action None required.

716044

Error Message `%FTD-4-716044: Group group-name User user-name IP IP_address AAA parameter param-name value param-value out of range.`

Explanation The given parameter has a bad value.

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

Recommended Action Modify the configuration to correct the indicated parameter. If the parameter is vlan or nac-settings, verify that it is correctly configured on the AAA server and the Secure Firewall Threat Defense device.

716045

Error Message `%FTD-4-716045: Group group-name User user-name IP IP_address AAA parameter param-name value invalid.`

Explanation The given parameter has a bad value. The value is not shown because it might be very long.

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

Recommended Action Modify the configuration to correct the indicated parameter.

716046

Error Message `%FTD-4-716046: Group group-name User user-name IP IP_address User ACL access-list-name from AAA doesn't exist on the device, terminating connection.`

Explanation The specified ACL was not found 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
- **access-list-name—**The name of the ACL

Recommended Action Modify the configuration to add the specified ACL or to correct the ACL name.

716047

Error Message `%FTD-4-716047: Group group-name User user-name IP IP_address User ACL access-list-name from AAA ignored, AV-PAIR ACL used instead.`

Explanation The specified ACL was not used because a Cisco AV-PAIR ACL was used.

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

Recommended Action Determine the correct ACL to use and correct the configuration.

716048

Error Message `%FTD-4-716048: Group group-name User user-name IP IP_address No memory to parse ACL.`

Explanation There was not enough memory to parse the ACL.

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

Recommended Action Purchase more memory, upgrade the Secure Firewall Threat Defense device, or reduce the load on it.

716049

Error Message `%FTD-6-716049: Group group-name User user-name IP IP_address Empty SVC ACL.`

Explanation The ACL to be used by the client was empty.

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

Recommended Action Determine the correct ACL to use and modify the configuration.

716050

Error Message `%FTD-6-716050: Error adding to ACL: ace_command_line`

Explanation The ACL entry had a syntax error.

- **ace_command_line**—The ACL entry that is causing the error

Recommended Action Correct the downloadable ACL configuration.

716051

Error Message `%FTD-6-716051: Group group-name User user-name IP IP_address Error adding dynamic ACL for user.`

Explanation There is not enough memory to perform the action.

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

Recommended Action Purchase more memory, upgrade the Secure Firewall Threat Defense device, or reduce the load on it.

716052

Error Message `%FTD-4-716052: Group group-name User user-name IP IP_address Pending session terminated.`

Explanation A user did not complete login and the pending session was terminated. This may be due to an SVC that was unable to connect.

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

Recommended Action Check the user PC for SVC compatibility.

716053

Error Message `%FTD-5-716053: SAML Server added: Name: name Type: SP`

Explanation A SAML IDP server entry has been added to the webvpn configuration.

- **name**—The entityID of the SAML IDP

Recommended Action None required.

716054

Error Message `%FTD-5-716054: SAML Server deleted: Name: name Type: SP`

Explanation A SAML IDP server entry has been removed from the webvpn configuration. .

- **name**—The entityID of the SAML IDP

Recommended Action None required.

716057

Error Message `%FTD-3-716057: Group group User user IP ip Session terminated, no type license available`

Explanation A user has attempted to connect to the Secure Firewall Threat Defense device using a client that is not licensed. This message may also occur if a temporary license has expired.

- *group* —The group policy that the user logged in with
- *user* —The name of the user
- *IP* —The IP address of the user
- *type* —The type of license requested, which can be one of the following:

- AnyConnect Mobile

- LinkSys Phone

- The type of license requested by the client (if other than the AnyConnect Mobile or LinkSys Phone)

- Unknown

Recommended Action A permanent license with the appropriate feature should be purchased and installed.

716058

Error Message `%FTD-6-716058: Group group User user IP ip AnyConnect session lost connection. Waiting to resume.`

Explanation The SSL tunnel was dropped and the AnyConnect session enters the inactive state, which can be caused by a hibernating host, a standby host, or a loss of network connectivity.

- *group* —The tunnel group name associated with the AnyConnect session
- *user* —The name of the user associated with the session
- *ip* —The source IP address of the session

Recommended Action None required.

716059

Error Message `%FTD-6-716059: Group group User user IP ip AnyConnect session resumed connection from IP ip2.`

Explanation An AnyConnect session resumed from the inactive state.

- *group* —The tunnel group name associated with the AnyConnect session
- *user* —The name of the user associated with the session
- *ip* —The source IP address of the session
- *ip2* —The source IP address of the host on which the session is resumed

Recommended Action None required.

716060

Error Message `%FTD-6-716060: Group group User user IP ip Terminated AnyConnect session in inactive state to accept a new connection: License limit reached.`

Explanation An AnyConnect session in the inactive state was logged out to allow a new incoming SSL VPN (AnyConnect or clientless) connection.

- *group* —The tunnel group name associated with the AnyConnect session
- *user* —The name of the user associated with the session
- *ip* —The source IP address of the session

Recommended Action None required.

716061

Error Message `%FTD-3-716061: Group DfltGrpPolicy User user IP ip_addr IPv6 User Filter tempipv6 configured for AnyConnect. 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.

716158

Error Message `%FTD-3-716158: Failed to create SAML logout request, initiated by user. reason: reason.`

Explanation The device was unable to inform the SAML IDP of a user logout because it encountered an error while creating the SAML Logout request. The reasons could be *profile is empty*, *could not create logout object*, and so on.

Recommended Action None

716159

Error Message `%FTD-3-716159: Failed to process SAML logout request. reason: reason.`

Explanation The device encountered an error while processing a SAML logout request initiated by the IDP. The reasons could be *NameID is invalid*, *could not create logout object*, and so on.

Recommended Action None

716160

Error Message `%FTD-3-716160: Failed to create SAML authentication request. reason: reason.`

Explanation The device was unable to authenticate a user with the SAML IDP because it encountered an error while creating the SAML authn request. The reasons could be *NameIDPolicy is invalid*, *could not create new login instance*, and so on.

Recommended Action None

716162

Error Message `%FTD-3-716162: Failed to consume SAML assertion. reason: reason.`

Explanation The device encountered an error while processing an authentication response from a SAML IDP. The reasons could be *response or assertion is empty*, *could not create new login instance*, *assertion is expired or not valid*, *assertion is empty*, *issuer is empty*, *subject is empty*, *issuer content is empty*, *name_id or content is empty*, and so on.

Recommended Action None

716163

Error Message `%FTD-3-716163: SAML response relay state failed data integrity check. Client IP: IP address. Local-base-url: Local-base URL.`

Explanation This syslog is generated when the relay state failed the data integrity validation. The local-base-url from SAML response RelayState helps to differentiate between the device that originally generated the SAML request from the device that received the response. If the local-base-url is not specified in the response, the message displays 'not received'.

Recommended Action None

716164

Error Message `%FTD-3-716164: SAML response relay state missing data integrity hash. Client IP: IP address. Local-base-url: Local-base URL.`

Explanation This syslog is generated when the relay state is missing the data integrity hash. The local-base-url from SAML response RelayState helps to differentiate between the device that originally generated the SAML request from the device that received the response. If the local-base-url is not specified in the response, the message displays 'not received'.

Recommended Action None

716166

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 SSL session is denied. This syslog is added under existing webvpn logging class.

Recommended Action None required.

717067

Error Message `%FTD-5-717067: Starting ACME certificate enrollment for trustpoint tpname with CA ca_name. Mode mode.`

Explanation The enrollment is triggered for ACME trustpoint.

- *tpname* —Name of the trustpoint being enrolled
- *ca_name* —CA hostname or IP address as provided in the ACME configuration
- *mode*—Enrollment trigger: Manual or Automatic

Recommended Action None required.

717068

Error Message `%FTD-5-717068: ACME Certificate enrollment succeeded for trustpoint tpname with CA ca. Received a new certificate with Subject Name subject, Issuer Name issuer, Serial Number serial .`

Explanation The ACME certificate enrollment is sucessful for the trustpoint.

- *tpname* —Name of the trustpoint being enrolled
- *ca* —CA hostname or IP address as provided in the ACME configuration
- *subject*—Subject Name from the received certificate
- *issuer*—Issuer Name from the received certificate
- *serial*—Serial Number from the received certificate

Recommended Action None required.

717069

Error Message `%FTD-3-717069: ACME Certificate enrollment failed for trustpoint tpname with CA ca.`

Explanation The ACME certificate enrollment failed for the trustpoint.

- *tpname* —Name of the trustpoint being enrolled
- *ca* —CA hostname or IP address as provided in the ACME configuration

Recommended Action Use the `debug crypto ca acme <1-255>`command to identify the failure reasons from the debug traces.

717070

Error Message `%FTD-5-717070: Keypair keyname in trustpoint tpname is regenerated for mode ACME certificate renewal.`

Explanation Sucessful regeneration of the ACME keypair for the trustpoint.

- *keyname* —Name of the keypair in the trustpoint
- *tpname* —Name of the trustpoint being enrolled
- *mode*—Enrollment trigger: Manual or Automatic

Recommended Action None required.

717071

Error Message `%FTD-3-717071: CRL signature validation failed. Issuer: issuer name. Last Update: date and time. Next Update: date and time.`

Explanation This syslog is generated during the X509 certificate verification process when an error is detected, where the message displays a certificate revocation list (CRL) information for the failed signature validation.

Recommended Action None required.

716500

Error Message `%FTD-2-716500: Fiber library cannot locate AK47 instance`

Explanation The fiber library cannot locate the application kernel layer 4 to 7 instance.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716501

Error Message `%FTD-2-716501: Fiber library cannot attach AK47 instance`

Explanation The fiber library cannot attach the application kernel layer 4 to 7 instance.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716502

Error Message `%FTD-2-716502: Fiber library cannot allocate default arena`

Explanation The fiber library cannot allocate the default arena.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716503

Error Message `%FTD-2-716503: Fiber library cannot allocate fiber descriptors pool`

Explanation The fiber library cannot allocate the fiber descriptors pool.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716504

Error Message `%FTD-2-716504: Fiber library cannot allocate fiber stacks pool`

Explanation The fiber library cannot allocate the fiber stack pool.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716505

Error Message `%FTD-2-716505: Fiber has joined fiber in unfinished state`

Explanation The fiber has joined fiber in an unfinished state.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716506

Error Message `%FTD-2-716506: Fiber has joined fiber waited upon by someone else`

Explanation An internal fiber library was generated.

Recommended Action Contact the Cisco TAC.

716507

Error Message `%FTD-1-716507: Fiber scheduler has reached unreachable code. Cannot continue, terminating`

Explanation The Secure Firewall Threat Defense device has experienced an unexpected error and has recovered.

Recommended Action Check for high CPU usage or CPU hogs, and potential memory leaks. If the problem persists, contact the Cisco TAC.

716508

Error Message `%FTD-1-716508: Fiber scheduler is scheduling rotten fiber. Cannot continue, terminating`

Explanation The fiber scheduler is scheduling rotten fiber, so it cannot continue terminating.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716509

Error Message `%FTD-1-716509: Fiber scheduler is scheduling alien fiber. Cannot continue, terminating`

Explanation The fiber scheduler is scheduling alien fiber, so it cannot continue terminating.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716510

Error Message `%FTD-1-716510: Fiber scheduler is scheduling finished fiber. Cannot continue, terminating`

Explanation The fiber scheduler is scheduling finished fiber, so it cannot continue terminating.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716512

Error Message `%FTD-2-716512: Non-joinable fiber being destroyed has waiters`

Explanation The fiber has joined fiber that is waited upon by someone else.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716513

Error Message `%FTD-2-716513: Fiber in callback blocked on other channel`

Explanation The fiber in the callback was blocked on the other channel.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716515

Error Message `%FTD-2-716515: OCCAM failed to allocate memory for AK47 instance`

Explanation The OCCAM failed to allocate memory for the AK47 instance.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716516

Error Message `%FTD-1-716516: OCCAM has corrupted ROL array. Cannot continue, terminating`

Explanation The OCCAM has a corrupted ROL array, so it cannot continue terminating.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716517

Error Message `%FTD-2-716517: OCCAM cached block has no associated arena`

Explanation The OCCAM cached block has no associated arena.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716518

Error Message `%FTD-2-716518: OCCAM pool has no associated arena`

Explanation The OCCAM pool has no associated arena.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716519

Error Message `%FTD-1-716519: OCCAM has corrupted pool list. Cannot continue, terminating`

Explanation The OCCAM has a corrupted pool list, so it cannot continue terminating.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716520

Error Message `%FTD-2-716520: OCCAM pool has no block list`

Explanation The OCCAM pool has no block list.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716521

Error Message `%FTD-2-716521: OCCAM no realloc allowed in named pool`

Explanation The OCCAM did not allow reallocation in the named pool.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716522

Error Message `%FTD-2-716522: OCCAM corrupted standalone block`

Explanation The OCCAM has a corrupted standalone block.

Recommended Action To determine the cause of the problem, contact the Cisco TAC.

716525

Error Message `%FTD-2-716525: SAL private data changed after callback in close`

Explanation An internal SAL error has occurred.

Recommended Action Contact the Cisco TAC.

716526

Error Message `%FTD-2-716526: WebVPN session load failed: Failure to attach to a configured permanent storage server`

Explanation A failure in the mounting of the permanent storage server directory occurred.

Recommended Action Contact the Cisco TAC.

716527

Error Message `%FTD-2-716527: WebVPN session store failed: Failure to attach to a configured permanent storage server`

Explanation A failure in the mounting of the permanent storage file occurred.

Recommended Action Contact the Cisco TAC.

716528

Error Message `%FTD-1-716528: Unexpected fiber scheduler error; possible out-of-memory condition`

Explanation The Secure Firewall Threat Defense device has experienced an unexpected error and has recovered.

Recommended Action Check for high CPU usage or CPU hogs, and potential memory leaks. If the problem persists, contact the Cisco TAC.

716600

Error Message `%FTD-3-716600: Rejected` *`size-recv`* `Hostscan data from IP` *`src-ip`*`. Hostscan results exceed` *`default`* `limit of` *`configured`*`.`

Explanation When the size of the received Hostscan data exceeds the limit configured on the Secure Firewall Threat Defense device, the data is discarded.

- *size-recv* —Size of received Hostscan data in kilobytes
- *src-ip* —Source IP address
- *default* | *configured* —Keyword specifying whether the value of the Hostscan data limit is the default or configured by the administrator
- *size-conf* —Configured upper limit on the size of the Hostscan data that the Secure Firewall Threat Defense device accepts from clients

Recommended Action Contact Cisco TAC to increase the upper limit on the size of Hostscan data that the Secure Firewall Threat Defense device accepts from clients.

716601

Error Message `%FTD-3-716601: Rejected size-recv Hostscan data from IP src-ip. System-wide limit on the amount of Hostscan data stored on default reached the limit of configured`

Explanation When the amount of Hostscan data stored on the Secure Firewall Threat Defense device exceeds the limit, new Hostscan results are rejected.

- *size-recv* —Size of received Hostscan data in kilobytes
- *src-ip* —Source IP address
- *data-max* —Limit on the amount of Hostscan results to be stored by the Secure Firewall Threat Defense device in kilobytes

Recommended Action Contact Cisco TAC to change the limit on stored Hostscan data.

716602

Error Message `%FTD-3-716602: Memory allocation error. Rejected size-recv Hostscan data from IP src-ip.`

Explanation An error occurred while memory was being allocated for Hostscan data.

- *size-recv* —Size of received Hostscan data in kilobytes
- *src-ip* —Source IP address

Recommended Action Set the Hostscan limit to the default value if it is configured. If the problem persists, contact Cisco TAC.

716603

Error Message `%FTD-7-716603: Received size-recv KB Hostscan data from IP src-ip.`

Explanation The Hostscan data of a specified size was successfully received.

- *size-recv* —Size of received Hostscan data in kilobytes
- *src-ip* —Source IP address

Recommended Action None required.

Messages 717001 to 717064

This section includes messages from 717001 to 717064.

717001

Error Message `%FTD-3-717001: Querying keypair failed.`

Explanation A required keypair was not found during an enrollment request.

Recommended Action Verify that a valid keypair exists in the trustpoint configuration, then resubmit the enrollment request.

717002

Error Message `%FTD-3-717002: Certificate enrollment failed for trustpoint trustpoint_name. Reason: reason_string.`

Explanation An enrollment request for this trustpoint has failed.

- *trustpoint name* —Trustpoint name that the enrollment request was for
- *reason_string* —The reason the enrollment request failed

Recommended Action Check the CA server for the failure reason.

717003

Error Message `%FTD-6-717003: Certificate received from Certificate Authority for trustpoint trustpoint_name.`

Explanation A certificate was successfully received from the CA for this trustpoint.

- *trustpoint_name* —Trustpoint name

Recommended Action None required

717004

Error Message `%FTD-6-717004: PKCS #12 export failed for trustpoint trustpoint_name.`

Explanation The trustpoint failed to export, because of one of the following: only a CA certificate exists, and an identity certificate does not exist for the trustpoint, or a required keypair is missing.

- *trustpoint_name* —Trustpoint name

Recommended Action Make sure that required certificates and keypairs are present for the given trustpoint.

717005

Error Message `%FTD-6-717005: PKCS #12 export succeeded for trustpoint trustpoint_name.`

Explanation The trustpoint was successfully exported.

- *trustpoint_name* —Trustpoint name

Recommended Action None required

717006

Error Message `%FTD-6-717006: PKCS #12 import failed for trustpoint trustpoint_name.`

Explanation Import of the requested trustpoint failed to be processed.

- *trustpoint_name* —Trustpoint name

Recommended Action Verify the integrity of the imported data. Then make sure that the entire pkcs12 record is correctly pasted, and reimport the data.

717007

Error Message `%FTD-6-717007: PKCS #12 import succeeded for trustpoint trustpoint_name.`

Explanation Import of the requested trustpoint was successfully completed.

- *trustpoint_name* —Trustpoint name

Recommended Action None required.

717008

Error Message `%FTD-2-717008: Insufficient memory to process_requiring_memory.`

Explanation An internal error occurred while attempting to allocate memory for the process that reqires memory. Other processes may experience problems allocating memory and prevent further processing.

- **process_requiring_memory**—The specified process that requires memoryr

Recommended Action Collect memory statistics and logs for further debugging and reload the Secure Firewall Threat Defense device.

717009

Error Message `%FTD-3-717009: Certificate validation failed. reason_string.`

Explanation A certificate validation failed, which might be caused by a validation attempt of a revoked certificate, invalid certificate attributes, or configuration issues.

- *reason_string* —The reason that the certificate validation failed

Recommended Action Make sure the configuration has a valid trustpoint configured for validation if the reason indicates that no suitable trustpoints were found. Check the Secure Firewall Threat Defense device time to ensure that it is accurate relative to the certificate authority time. Check the reason for the failure and correct any issues that are indicated. If certificate validation fails due to the CA key size being too small or a weak crypto being used, you can use the enable weak crypto option for the device in the Firewall Management Center to override these restrictions.

717010

Error Message `%FTD-3-717010: CRL polling failed for trustpoint trustpoint_name.`

Explanation .CRL polling has failed and may cause connections to be denied if CRL checking is required.

- **trustpoint_name**—The name of the trustpoint that requested the CRL

Recommended Action Verify that connectivity exists with the configured CRL distribution point and make sure that manual CRL retrieval also functions correctly.

717011

Error Message `%FTD-2-717011: Unexpected event: event event_ID`

Explanation An event that is not expected under normal conditions has occurred.

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

717012

Error Message `%FTD-3-717012: Failed to refresh CRL cache entry from the server for trustpoint trustpoint_name at time_of_failure`

Explanation An attempt to refresh a cached CRL entry has failed for the specified trustpoint at the indicated time of failure. This may result in obsolete CRLs on the Secure Firewall Threat Defense device, which may cause connections that require a valid CRL to be denied.

- **trustpoint_name**—The name of the trustpoint
- *time_of_failure* —The time of failure

Recommended Action Check connectivity issues to the server, such as a downed network or server. Try to retrieve the CRL manually using the **crypto ca crl retrieve** command.

717013

Error Message `%FTD-5-717013: Removing a cached CRL to accommodate an incoming CRL Issuer: issuer`

Explanation When the device is configured to authenticate IPsec tunnels using digital certificates, CRLs may be cached in memory to avoid requiring a CRL download during each connection. If the cache fills to the point where an incoming CRL cannot be accommodated, older CRLs will be removed until the required space is made available. This message is generated for each purged CRL.

- **issuer**—The name of the device that removes cached CRLs

Recommended Action None required.

717014

Error Message `%FTD-5-717014: Unable to cache a CRL received from CDP due to size limitations(CRL size = size, available cache space = space)`

Explanation When the device is configured to authenticate IPsec tunnels using digital certificates, CRLs may be cached in memory to avoid requiring a CRL download during each connection. This message is generated if a received CRL is too large to fit in the cache. Large CRLs are still supported even though they are not cached. This means that the CRL will be downloaded with each IPsec connection, which may affect performance during IPsec connection bursts.

Recommended Action None required.

717015

Error Message `%FTD-3-717015: CRL received from issuer is too large to process (CRL size = crl_size , maximum CRL size = max_crl_size )`

Explanation An IPsec connection caused a CRL that is larger than the maximum permitted CRL size to be downloaded. This error condition causes the connection to fail. This message is rate limited to one message every 10 seconds.

Recommended Action Scalability is perhaps the most significant drawback to the CRL method of revocation checking. To solve this problem, the only options are to investigate a CA-based solution to reduce the CRL size or configure the Secure Firewall Threat Defense device not to require CRL validation.

717016

Error Message `%FTD-6-717016: Removing expired CRL from the CRL cache. Issuer: issuer`

Explanation When the Secure Firewall Threat Defense device is configured to authenticate IPsec tunnels using digital certificates, CRLs may be cached in memory to avoid requiring a CRL download during each connection. This message is generated when either the CA specified expiration time or the configured cache time has lapsed and the CRL is removed from the cache.

Recommended Action None required.

717017

Error Message `%FTD-3-717017: Failed to query CA certificate for trustpoint trustpoint_name from enrollment_url.`

Explanation An error occurred when an attempt was made to authenticate a trustpoint by requesting a CA certificate from a certificate authority.

Recommended Action Make sure that an enrollment URL is configured with this trustpoint, ensure connectivity with the CA server, then retry the request.

717018

Error Message `%FTD-3-717018: CRL received from issuer has too many entries to process (number of entries = number_of_entries , maximum number allowed = max_allowed )`

Explanation An IPsec connection caused a CRL that includes more revocation entries than can be supported to be downloaded. This is an error condition that will cause the connection to fail. This message is rate limited to one message every 10 seconds.

- **issuer**—The X.500 name of the CRLs issuer
- **number_of_entries**—The number of revocation entries in the received CRL
- **max_allowed**—The maximum number of CRL entries that the Secure Firewall Threat Defense device supports

Recommended Action Scalability is perhaps the most significant drawback to the CRL method of revocation checking. The only options to solve this problem are to investigate a CA-based solution to reduce the CRL size or configure the Secure Firewall Threat Defense device not to require CRL validation.

717019

Error Message `%FTD-3-717019: Failed to insert CRL for trustpoint trustpoint_name. Reason: failure_reason.`

Explanation A CRL is retrieved, but found to be invalid and cannot be inserted into the cache because of the **failure_reason**.

- **trustpoint_name**—The name of the trustpoint that requested the CRL
- **failure_reason**—The reason that the CRL failed to be inserted into cache

Recommended Action Make sure that the current Secure Firewall Threat Defense device time is correct relative to the CA time. If the NextUpdate field is missing, configure the trustpoint to ignore the NextUpdate field.

717020

Error Message `%FTD-3-717020: Failed to install device certificate for trustpoint label. Reason: reason_string.`

Explanation A failure occurred while trying to enroll or import an enrolled certificate into a trustpoint.

- *label* —Label of the trustpoint that failed to install the enrolled Secure Firewall Threat Defense certificate
- *reason_string* —The reason that the certificate cannot be verified

Recommended Action Use the failure reason to remedy the cause of failure and retry the enrollment. Common failures are due to invalid certificates being imported into the Secure Firewall Threat Defense device or a mismatch of the public key included in the enrolled certificate with the keypair referenced in the trustpoint.

717021

Error Message `%FTD-3-717021: Certificate data could not be verified. Reason: reason_string, key length in certificate: serial_number bits.`

Explanation An attempt to verify the certificate that is identified by the serial number and subject name was unsuccessful for the specified reason. When verifying certificate data using the signature, several errors can occur that should be logged, including invalid key types and unsupported key size.

- *reason_string* —The reason that the certificate cannot be verified
- *serial number* —Serial number of the certificate that is being verified
- *subject name* —Subject name included in the certificate that is being verified
- *key length* —The number of bits in the key used to sign this certificate

Recommended Action Check the specified certificate to ensure that it is valid, that it includes a valid key type, and that it does not exceed the maximum supported key size.

717022

Error Message `%FTD-6-717022: Certificate was successfully validated. certificate_identifiers.`

Explanation The identified certificate was successfully validated.

- *certificate_identifiers* —Information to identify the certificate that was validated successfully, which might include a reason, serial number, subject name, and additional information

Recommended Action None required.

717023

Error Message `%FTD-3-717023: SSL failed to set device certificate for trustpoint trustpoint_name. Reason: reason_string.`

Explanation A failure occurred while trying to set an Secure Firewall Threat Defense certificate for the given trustpoint for authenticating the SSL connection.

- *trustpoint name* —Name of the trustpoint for which SSL failed to set an Secure Firewall Threat Defense certificate
- *reason_string* —Reason indicating why the Secure Firewall Threat Defense certificate cannot be set

Recommended Action Resolve the issue indicated by the reason reported for the failure by doing the following:

- Make sure that the specified trustpoint is enrolled and has an Secure Firewall Threat Defense certificate.
- Make sure the Secure Firewall Threat Defense certificate is valid.
- Reenroll the trustpoint, if required.

717024

Error Message `%FTD-7-717024: Checking CRL from trustpoint: trustpoint name for purpose`

Explanation A CRL is being retrieved.

- *trustpoint name* —Name of the trustpoint for which the CRL is being retrieved
- *purpose* —Reason that the CRL is being retrieved

Recommended Action None required.

717025

Error Message `%FTD-7-717025: Validating certificate chain containing number_of_certs certificate(s).`

Explanation A certificate chain is being validated.

- >*number of certs*— Number of certificates in the chain

Recommended Action None required.

717026

Error Message `%FTD-4-717026: Name lookup failed for hostname hostname during PKI operation.`

Explanation The given hostname cannot be resolved while attempting a PKI operation.

- >*hostname* —The hostname that failed to resolve

Recommended Action Check the configuration and the DNS server entries for the given hostname to make sure that it can be resolved. Then retry the operation.

717027

Error Message `%FTD-3-717027: Certificate chain failed validation. reason_string.`

Explanation A certificate chain cannot be validated.

- *reason_string*—Reason for the failure to validate the certificate chain. The reasons could be non reacheability of a CA server, trustpoint not being available, the validity period for the certificate identity has elapsed, or when the certificate is revoked.

Recommended Action Resolve the issue noted by the reason and retry the validation attempt by performing any of the following actions:

- Make sure that connectivity to a CA is available if CRL checking is required.
- Make sure that a trustpoint is authenticated and available for validation.
- Make sure that the identity certificate within the chain is valid based on the validity dates.
- Make sure that the certificate is not revoked.

717028

Error Message `%FTD-6-717028: Certificate chain was successfully validated additional_info.`

Explanation A certificate chain was successfully validated.

- >*additional info* —More information for how the certificate chain was validated (for example, “with warning” indicates that a CRL check was not performed)

Recommended Action None required.

717029

Error Message `%FTD-7-717029: Identified client certificate within certificate chain. serial_number.`

Explanation The certificate specified as the client certificate is identified.

- **serial_number**—Serial number of the certificate that is identified as the client certificate
- **subject_name**—Subject name included in the certificate that is identified as the client certificate

Recommended Action None required.

717030

Error Message `%FTD-7-717030: Found a suitable trustpoint trustpoint_name to validate certificate.`

Explanation A suitable or usable trustpoint is found that can be used to validate the certificate.

- *trustpoint name* —Trustpoint that will be used to validate the certificate

Recommended Action None required.

717031

Error Message `%FTD-4-717031: Failed to find a suitable trustpoint for the issuer: issuer Reason: reason_string`

Explanation A usable trustpoint cannot be found. During certificate validation, a suitable trustpoint must be available in order to validate a certificate.

- >*issuer* —Issuer of the certificate that was being validated
- *reason_string* —The reason that a suitable trustpoint cannot be found

Recommended Action Resolve the issue indicated in the reason by checking the configuration to make sure that a trustpoint is configured, authenticated, and enrolled. Also make sure that the configuration allows for specific types of certificates, such as identity certificates.

717032

Error Message `%FTD-3-717032: OCSP status check failed. Reason: reason_string.`

Explanation When the OCSP status check fails, this message is generated with the reason for the failure. The following list mentions the failure reasons:

- HTTP transaction failed for OCSP request.
- Invalid OCSP Response Status - unauthorized.
- Failed OCSP response processing.
- Failed to query an OCSP response from the server
- Failed to parse HTTP OCSP response from the server
- Invalid revocation status, server returned status: unknown
- Invalid OCSP response type
- Nonce missing in OCSP response
- NONCE mismatch
- Failed to verify OCSP response
- Validity period of OCSP response invalid
- Certificate is revoked
- CRL check for OCSP responder cert failed

Recommended Action None.

717033

Error Message `%FTD-6-717033: OCSP response received.`

Explanation An OCSP status check response was received successfully.

Recommended Action None required.

717034

Error Message `%FTD-7-717034: No-check extension found in certificate. CRL check bypassed.`

Explanation An OCSP responder certificate was received that includes an "id-pkix-ocsp-nocheck" extension, which allows this certificate to be validated without an OCSP status check.

Recommended Action None required.

717035

Error Message `%FTD-4-717035: OCSP status is being checked for certificate. certificate_identifier..`

Explanation The certificate for which an OCSP status check occurs is identified.

- *certificate_identifier* —Information that identifies the certificate being processed by the certificate map rules

Recommended Action None required.

717036

Error Message `%FTD-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with certificate_identifier.`

Explanation The peer certificate identified by the certificate identifier is being processed through the configured certificate maps to attempt a possible tunnel group match.

- *certificate_identifier* —Information that identifies the certificate being processed by the certificate map rules

Recommended Action None required.

717037

Error Message `%FTD-4-717037: Tunnel group search using certificate maps failed for peer certificate: certificate_identifier.`

Explanation The peer certificate identified by the certificate identifier was processed through the configured certificate maps to attempt a possible tunnel group match, but no match can be found.

- *certificate_identifier* —Information that identifies the certificate being processed by the certificate map rules

Recommended Action Make sure that the warning is expected based on the received peer certificate and the configured crypto CA certificate map rules.

717038

Error Message `%FTD-7-717038: Tunnel group match found. Tunnel Group: tunnel_group_name, Peer certificate: certificate_identifier.`

Explanation The peer certificate identified by the certificate identifier was processed by the configured certificate maps, and a match was found to the tunnel group.

- *certificate_identifier* —Information that identifies the certificate being processed by the certificate map rules
- *tunnel_group_name* —The name of the tunnel group matched by the certificate map rules

Recommended Action None required.

717050

Error Message `%FTD-5-717050: SCEP Proxy: Processed request type type from IP client_ip_address, User username, TunnelGroup tunnel_group_name, GroupPolicy group-policy_name to CA ca_ip_address`

Explanation The SCEP proxy received a message and relayed it to the CA. The response from the CA is relayed back to the client.

- *type* —The request type string that is received by the SCEP proxy, which can be one of the following SCEP message types: PKIOperation, GetCACaps, GetCACert, GetNextCACert, and GetCACertChain.
- *client ip address* —The source IP address of the request received
- *username* —The username that is associated with the VPN session in which the SCEP request is received
- *tunnel-group name* —The tunnel group that is associated with the VPN session in which the SCEP request is received
- *group-policy name* —The group policy that is associated with the VPN session in which the SCEP request is received
- *ca ip address* —The IP address of the CA that is configured in the group policy

Recommended Action None required.

717051

Error Message `%FTD-3-717051: SCEP Proxy: Denied processing the request type type from IP client_ip_address, User username, TunnelGroup tunnel_group_name, GroupPolicy group_policy_name to CA ca_ip_address. Reason: msg`

Explanation The SCEP proxy denied processing of the request, which may be caused by a misconfiguration, an error condition in the proxy, or an invalid request.

- *type* —The request type string that is received by the SCEP proxy, which can be one of the following SCEP message types: PKIOperation, GetCACaps, GetCACert, GetNextCACert, and GetCACertChain.
- *client ip address* —The source IP address of the request received
- *username* —The username that is associated with the VPN session in which the SCEP request is received
- *tunnel-group name* —The tunnel group that is associated with the VPN session in which the SCEP request is received
- *group-policy name* —The group policy that is associated with the VPN session in which the SCEP request is received
- *ca ip address* —The IP address of the CA that is configured in the group policy
- **msg**—The reason string that explains the reason or error for why the request processing is denied

Recommended Action Identify the cause from the reason printed. If the reason indicates that the request is invalid, check the CA URL configuration. Otherwise, confirm that the tunnel group is enabled for SCEP enrollment and debug further by using the **debug crypto ca scep-proxy** command.

717052

Error Message `%FTD-4-717052: Group group_name User user_name IP IP_Address Session disconnected due to periodic certificate authentication failure. Subject Name id_subject_name Issuer Name id_issuer_name Serial Number id_serial_number`

Explanation Periodic certificate authentication failed, and the session was disconnected.

- *group name* —The name of the group policy to which the session belongs
- *user name* —The username of the session
- *IP* —The public IP address of the session
- *id subject name* —The subject name in the ID certificate of the session
- *id issuer name* —The issuer name in the ID certificate of the session
- *id serial number* —The serial number in the ID certificate of the session

Recommended Action None required.

717053

SSP-whole topic

Error Message `%FTD-5-717053: Group group_name User user_name IP IP_Address Periodic certificate authentication succeeded. Subject Name id_subject_name Issuer Name id_issuer_name Serial Number id_serial_number`

Explanation Periodic certificate authentication succeeded.

- *group name* —The name of the group policy to which the session belongs
- *user name* —The username of the session
- *id subject name* —The subject name in the ID certificate of the session
- *id issuer name* —The issuer name in the ID certificate of the session
- *id serial number* —The serial number in the ID certificate of the session

Recommended Action None required.

717054

SSP-whole topic

Error Message `%FTD-1-717054: The type certificate in the trustpoint tp_name is due to expire in number days. Expiration date_and_time Subject Name subject_name Issuer Name issuer_name Serial Number serial_number`

Explanation The specified certificate in the trustpoint is about to expire.

- *type* —The type of certificate: CA or ID
- *tp name* —The name of the trustpoint to which the certificate belongs
- *number* —The number of days until expiration
- *date and time* : The expiration date and time
- *subject name* —The subject name in the certificate
- *issuer name* —The issuer name in the certificate
- *serial number* —The serial number in the certificate

Recommended Action Renew the certificate.

717055

Error Message `%FTD-1-717055: The type certificate in the trustpoint tp_name has expired. Expiration date_and_time Subject Name subject_name Issuer Name issuer_name Serial Number serial_number`

Explanation The specified certificate in the trustpoint has expired.

- *type* —The type of certificate: CA or ID
- *tp name* —The name of the trustpoint to which the certificate belongs
- *date and time* : The expiration date and time
- *subject name* —The subject name in the certificate
- *issuer name* —The issuer name in the certificate
- *serial number* —The serial number in the certificate

Recommended Action Renew the certificate.

717056

Only heading title SSP

Error Message `%FTD-6-717056: Attempting type revocation check from Src:Interface/Src to IP/Src_Port using Dst_IP.`

Explanation The CA was attempting to download a CRL or send an OCSP revocation check request.

- *type* —Type of revocation check, which can be OCSP or CRL
- *Src Interface* —Name of the interface from which the revocation checking is being done
- *Src IP* —IP address from which the revocation checking is being done
- *Src Port* —Port number from which the revocation checking is being done
- *Dst IP* —IP address of the server to which the revocation checking request is being sent
- *Dst Port* —Port number of the server to which the revocation checking request is being sent
- *Protocol* —Protocol being used for revocation checking, which can be HTTP, LDAP, or SCEP

Recommended Action None required.

717057

Error Message `%FTD-3-717057: Automatic import of trustpool certificate bundle has failed. Maximum_retry_attempts_reached|Failed_to_reach_CA_server|Cisco_root_bundle_signature_validation_failed|Failed_to_update_trustpool_bundle_in_flash|Failed_to_install_trustpool_bundle_in_memory`

Explanation This syslog is generated with one of these error messages. This syslog is meant to update the user with results of the auto import operation and steer them towards the right debug messages especially in cases of failure. Details of each error are present in the debug output.

Recommended Action Verify CA accessibility and make space on flash CA root certificate.

717058

Error Message `%FTD-6-717058: Automatic import of trustpool certificate bundle is successful: No_change_in_trustpool_bundle|Trustpool_updated_in_flash`

Explanation This syslog is generated with one of these success messages. This syslog is meant to update the user with results of the auto import operation and steer them towards the right debug messages, especially in cases of failure. Details of each error are present in the debug output.

Recommended Action None.

717059

Error Message `%FTD-6-717059: Peer certificate with serial_number:serial,subject:subject_name,issuer:issuer_name matched the configured certificate map map_name`

Explanation This log is generated when an ASDM connection is authenticated via certificates and allowed based on the configured certificate map rules.

Recommended Action None required.

717060

Error Message `%FTD-3-717060: Peer certificate with serial_number:serial,subject:subject_name,issuer:issuer_name failed to match the configured certificate map map_name`

Explanation This log is generated when an ASDM connection is authenticated via certificates and not allowed based on the configured certificate map rules.

Recommended Action If the peer certificate referenced in the log is supposed to be allowed, check certificate map configuration for the referenced map_name and correct the map to allow the connection as needed.

717061

SSP-only heading title

Error Message `%FTD-5-717061: Starting protocol certificate enrollment for the trustpoint tpname with the CA ca_name. Request Type type Mode mode`

Explanation A CMP enrollment request has been triggered.

- *tpname* —Name of the trustpoint being enrolled
- *ca* —CA hostname or IP address as provided in the CMP configuration
- *type* —CMP request type: Initialization Request, Certification Request, and Key Update Request
- *mode* —Enrollment trigger: Manual or Automatic
- *protocol* —Enrollment protocol: CMP

Recommended Action None required.

717062

Error Message `%FTD-5-717062: protocol Certificate enrollment succeeded for the trustpoint tpname with the CA ca using CMP. Received a new certificate with Subject Name subject Issuer Name issuer Serial Number serial`

Explanation CMP enrollment request succeeded. New certificate received.

- *tpname* —Name of the trustpoint being enrolled
- *ca* —CA hostname or IP address as provided in the CMP configuration
- *subject* —Subject Name from the received certificate
- *issuer* —Issuer Name from the received certificate
- serial—Serial Number from the received certificate
- *protocol* —Enrollment protocol: CMP

Recommended Action None required.

717063

SSP Only heading title

Error Message `%FTD-3-717063: protocol Certificate enrollment failed for the trustpoint tpname with the CA ca`

Explanation CMP enrollment request failed.

- *tpname* —Name of the trustpoint being enrolled
- *ca* —CA hostname or IP address as provided in the CMP configuration
- *protocol* —Enrollment protocol: CMP

Recommended Action Use the CMP debug traces to fix the enrollment failure.

717064

SSP - only heading

Error Message `%FTD-5-717064: Keypair keyname in the trustpoint tpname is regenerated for mode protocol certificate enrollment`

Explanation The keypair in the trustpoint is regenerated for certificate enrollment using CMP.

- *tpname* —Name of the trustpoint being enrolled
- *keyname* —Name of the keypair in the trustpoint
- mode—Enrollment trigger: Manual or Automatic
- *protocol* —Enrollment protocol: CMP

Recommended Action None required.

717072

Error Message `%FTD-5-717072: A CRL with an older version than the currently cached one was downloaded.`

`Issuer: Issuer name`

`New CRL Last Update: Date and time`

`Removed CRL Last Update: Date and time`

`Associated Trustpoint: Trustpoint`

Explanation This syslog is generated when the current CRL in the cache is replaced by the one that has an older version. This message appears during the certificate revocation list verification and CRL insertion process.

Recommended Action None required.

Messages 718001 to 719026

This section includes messages from 718001 to 719026.

718001

Error Message `%FTD-7-718001: Internal interprocess communication queue send failure: code [error_code].`

Explanation An internal software error has occurred while attempting to enqueue a message on the VPN load balancing queue.

Recommended Action This is generally a benign condition. If the problem persists, contact the Cisco TAC.

718002

Error Message `%FTD-5-718002: Create peer IP_address failure, already at maximum of [number_of_peers]`

Explanation The maximum number of load-balancing peers has been exceeded. The new peer is ignored.

Recommended Action Check your load balancing and network configuration to ensure that the number of load-balancing peers does not exceed the maximum allowed.

718003

Error Message `%FTD-6-718003: Got unknown peer message [message_number] from [IP_address], local version [version_number], remote version [version_number]`

Explanation An unrecognized load-balancing message was received from one of the load-balancing peers. This may indicate a version mismatch between peers, but is most likely caused by an internal software error.

Recommended Action Verify that all load-balancing peers are compatible. If they are and this condition persists or is linked to undesirable behavior, contact the Cisco TAC.

718004

Error Message `%FTD-6-718004: Got unknown internal message [message_number]`

Explanation An internal software error occurred.

Recommended Action This is generally a benign condition. If the problem persists, contact the Cisco TAC.

718005

Error Message `%FTD-5-718005: Fail to send to IP_address, port port`

Explanation An internal software error occurred during packet transmission on the load-balancing socket. This mght indicate a network problem.

Recommended Action Check the network-based configuration on the Secure Firewall Threat Defense device and verify that interfaces are active and protocol data is flowing through the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

718006

Error Message `%FTD-5-718006: Invalid load balancing state transition [cur=state_number][event=event_number]`

Explanation A state machine error has occurred. This might indicate an internal software error.

Recommended Action This is generally a benign condition. If the problem persists, contact the Cisco TAC.

718007

Error Message `%FTD-5-718007: Socket open failure [failure_code]: failure_text`

Explanation An error occurred when the load-balancing socket tried to open. This might indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the Secure Firewall Threat Defense device and verify that interfaces are active and protocol data is flowing through the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

718008

Error Message `%FTD-5-718008: Socket bind failure [failure_code]: failure_text`

Explanation An error occurred when the Secure Firewall Threat Defense device tried to bind to the load-balancing socket. This might indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the Secure Firewall Threat Defense device and verify that interfaces are active and protocol data is flowing through the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

718009

Error Message `%FTD-5-718009: Send HELLO response failure to [IP_address]`

Explanation An error occurred when the Secure Firewall Threat Defense device tried to send a hello response message to one of the load-balancing peers. This might indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the Secure Firewall Threat Defense device and verify that interfaces are active and protocol data is flowing through the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

718010

Error Message `%FTD-5-718010: Sent HELLO response to [IP_address]`

Explanation The Secure Firewall Threat Defense device transmitted a hello response message to a load-balancing peer.

Recommended Action None required.

718011

Error Message `%FTD-5-718011: Send HELLO request failure to [IP_address]`

Explanation An error occurred when the Secure Firewall Threat Defense device tried to send a hello request message to one of the load-balancing peers. This may indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the Secure Firewall Threat Defense device and verify that interfaces are active and protocol data is flowing through the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

718012

Error Message `%FTD-5-718012: Sent HELLO request to [IP_address]`

Explanation The Secure Firewall Threat Defense device transmitted a hello request message to a load-balancing peer.

Recommended Action None required.

718013

Error Message `%FTD-6-718013: Peer[IP_address] is not answering HELLO`

Explanation The load-balancing peer is not answering a hello request message.

Recommended Action Check the status of the load-balancing SSF peer and the network connections.

718014

Error Message `%FTD-5-718014: Master peer[IP_address] is not answering HELLO`

Explanation The load balancing director peer is not answering the hello request message.

Recommended Action Check the status of the load balancing SSF director peer and the network connections.

718015

Error Message `%FTD-5-718015: Received HELLO request from [IP_address]`

Explanation The Secure Firewall Threat Defense device received a hello request message from the load balancing peer.

Recommended Action None required.

718016

Error Message `%FTD-5-718016: Received HELLO response from [IP_address]`

Explanation The Secure Firewall Threat Defense device received a Hello Response packet from a load balancing peer.

Recommended Action None required.

718017

Error Message `%FTD-7-718017: Got timeout for unknown peer[IP_address] msg type[message_type]`

Explanation The Secure Firewall Threat Defense device processed a timeout for an unknown peer. The message was ignored because the peer may have already been removed from the active list.

Recommended Action If the message persists or is linked to undesirable behavior, check the load balancing peers and verify that all are configured correctly.

718018

Error Message `%FTD-7-718018: Send KEEPALIVE request failure to [IP_address]`

Explanation An error has occurred while attempting to send a Keepalive Request message to one of the load balancing peers. This t indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the Secure Firewall Threat Defense device and verify that interfaces are active and protocol data is flowing through the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

718019

Error Message `%FTD-7-718019: Sent KEEPALIVE request to [IP_address]`

Explanation The Secure Firewall Threat Defense device transmitted a Keepalive Request message to a load balancing peer.

Recommended Action None required.

718020

Error Message `%FTD-7-718020: Send KEEPALIVE response failure to [IP_address]`

Explanation An error has occurred while attempting to send a Keepalive Response message to one of the load balancing peers. This may indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the Secure Firewall Threat Defense device and verify that interfaces are active and protocol data is flowing through the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

718021

Error Message `%FTD-7-718021: Sent KEEPALIVE response to [IP_address]`

Explanation The Secure Firewall Threat Defense device transmitted a Keepalive Response message to a load balancing peer.

Recommended Action None required.

718022

Error Message `%FTD-7-718022: Received KEEPALIVE request from [IP_address]`

Explanation The Secure Firewall Threat Defense device received a Keepalive Request message from a load balancing peer.

Recommended Action None required.

718023

Error Message `%FTD-7-718023: Received KEEPALIVE response from [IP_address]`

Explanation The Secure Firewall Threat Defense device received a Keepalive Response message from a load balancing peer.

Recommended Action None required.

718024

Error Message `%FTD-5-718024: Send CFG UPDATE failure to [IP_address]`

Explanation An error has occurred while attempting to send a Configuration Update message to one of the load balancing peers. This might indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the Secure Firewall Threat Defense device and verify that interfaces are active and protocol data is flowing through the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

718025

Error Message `%FTD-7-718025: Sent CFG UPDATE to [IP_address]`

Explanation The Secure Firewall Threat Defense device transmitted a Configuration Update message to a load balancing peer.

Recommended Action None required.

718026

Error Message `%FTD-7-718026: Received CFG UPDATE from [IP_address]`

Explanation The Secure Firewall Threat Defense device received a Configuration Update message from a load balancing peer.

Recommended Action None required.

718027

Error Message `%FTD-6-718027: Received unexpected KEEPALIVE request from [IP_address]`

Explanation The Secure Firewall Threat Defense device received an unexpected Keepalive request message from a load balancing peer.

Recommended Action If the problem persists or is linked with undesirable behavior, verify that all load balancing peers are configured and discovered correctly.

718028

Error Message `%FTD-5-718028: Send OOS indicator failure to [IP_address]`

Explanation An error has occurred while attempting to send an OOS indicator message to one of the load balancing peers. This might indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the Secure Firewall Threat Defense device and verify that interfaces are active and protocol data is flowing through the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

718029

Error Message `%FTD-7-718029: Sent OOS indicator to [IP_address]`

Explanation The Secure Firewall Threat Defense device transmitted an OOS indicator message to a load balancing peer.

Recommended Action None required.

718030

Error Message `%FTD-6-718030: Received planned OOS from [IP_address]`

Explanation The Secure Firewall Threat Defense device received a planned OOS message from a load balancing peer.

Recommended Action None required.

718031

Error Message `%FTD-5-718031: Received OOS obituary for [IP_address]`

Explanation The Secure Firewall Threat Defense device received an OOS obituary message from a load balancing peer.

Recommended Action None required.

718032

Error Message `%FTD-5-718032: Received OOS indicator from [IP_address]`

Explanation The Secure Firewall Threat Defense device received an OOS indicator message from a load balancing peer.

Recommended Action None required.

718033

Error Message `%FTD-5-718033: Send TOPOLOGY indicator failure to [IP_address]`

Explanation An error has occurred while attempting to send a Topology indicator message to one of the load balancing peers. This might indicate a network problem or an internal software error.

Recommended Action Check the network-based configuration on the Secure Firewall Threat Defense device. Verify that interfaces are active, and protocol data is flowing through the Secure Firewall Threat Defense device. If the problem persists, contact the Cisco TAC.

718034

Error Message `%FTD-7-718034: Sent TOPOLOGY indicator to [IP_address]`

Explanation The Secure Firewall Threat Defense device sent a Topology indicator message to a load balancing peer.

Recommended Action None required.

718035

Error Message `%FTD-7-718035: Received TOPOLOGY indicator from [IP_address]`

Explanation The Secure Firewall Threat Defense device received a Topology indicator message from a load balancing peer.

Recommended Action None required.

718036

Error Message `%FTD-7-718036: Process timeout for req-type[type_value], exid[exchange_ID], peer[IP_address]`

Explanation The Secure Firewall Threat Defense device processed a peer timeout.

Recommended Action Verify that the peer should have been timed out. If not, check the load balancing peer configuration and the network connection between the peer and the Secure Firewall Threat Defense device.

718037

Error Message `%FTD-6-718037: Master processed number_of_timeouts timeouts`

Explanation The Secure Firewall Threat Defense device in the director role processed the specified number of peer timeouts.

Recommended Action Verify that the timeouts are legitimate. If not, check the peer load balancing configuration and the network connection between the peer and the Secure Firewall Threat Defense device.

718038

Error Message `%FTD-6-718038: Slave processed number_of_timeouts timeouts`

Explanation The Secure Firewall Threat Defense device in the member role processed the specified number of peer timeouts.

Recommended Action Verify that the timeouts are legitimate. If not, check the peer load balancing configuration and the network connection between the peer and the Secure Firewall Threat Defense device.

718039

Error Message `%FTD-6-718039: Process dead peer[IP_address]`

Explanation The Secure Firewall Threat Defense device has detected a dead peer.

Recommended Action Verify that the dead peer detection is legitimate. If not, check the peer load balancing configuration and the network connection between the peer and the Secure Firewall Threat Defense device.

718040

Error Message `%FTD-6-718040: Timed-out exchange ID[exchange_ID] not found`

Explanation The Secure Firewall Threat Defense device has detected a dead peer, but the exchange ID is not recognized.

Recommended Action None required.

718041

Error Message `%FTD-7-718041: Timeout [msgType=type] processed with no callback`

Explanation The Secure Firewall Threat Defense device has detected a dead peer, but a call back was not used in the processing.

Recommended Action None required.

718042

Error Message `%FTD-5-718042: Unable to ARP for [IP_address].`

Explanation The Secure Firewall Threat Defense device experienced an ARP failure when attempting to contact a peer.

Recommended Action Verify that the network is operational and that all peers can communicate with each other.

718043

Error Message `%FTD-5-718043: Updating/removing duplicate peer entry [IP_address]`

Explanation The Secure Firewall Threat Defense device found and is removing a duplicate peer entry.

Recommended Action None required.

718044

Error Message `%FTD-5-718044: Deleted peer[IP_address]`

Explanation The Secure Firewall Threat Defense device is deleting a load balancing peer.

Recommended Action None required.

718045

Error Message `%FTD-5-718045: Created peer[IP_address]`

Explanation The Secure Firewall Threat Defense device has detected a load balancing peer.

Recommended Action None required.

718046

Error Message `%FTD-7-718046: Create group policy [policy_name]`

Explanation The Secure Firewall Threat Defense device has created a group policy to securely communicate with the load balancing peers.

Recommended Action None required.

718047

Error Message `%FTD-7-718047: Fail to create group policy [policy_name]`

Explanation The Secure Firewall Threat Defense device experienced a failure when attempting to create a group policy for securing the communication between load balancing peers.

Recommended Action Verify that the load balancing configuration is correct.

718048

Error Message `%FTD-5-718048: Create of secure tunnel failure for peer [IP_address]`

Explanation The Secure Firewall Threat Defense device experienced a failure when attempting to establish an IPsec tunnel to a load balancing peer.

Recommended Action Verify that the load balancing configuration is correct and that the network is operational.

718049

Error Message `%FTD-7-718049: Created secure tunnel to peer[IP_address]`

Explanation The Secure Firewall Threat Defense device successfully established an IPsec tunnel to a load balancing peer.

Recommended Action None required.

718050

Error Message `%FTD-5-718050: Delete of secure tunnel failure for peer [IP_address]`

Explanation The Secure Firewall Threat Defense device experienced a failure when attempting to terminate an IPsec tunnel to a load balancing peer.

Recommended Action Verify that the load balancing configuration is correct and that the network is operational.

718051

Error Message `%FTD-6-718051: Deleted secure tunnel to peer[IP_address]`

Explanation The Secure Firewall Threat Defense device successfully terminated an IPsec tunnel to a load balancing peer.

Recommended Action None required.

718052

Error Message `%FTD-5-718052: Received GRAT-ARP from duplicate control node[MAC_address]`

Explanation The Secure Firewall Threat Defense device received a gratuitous ARP from a duplicate director.

Recommended Action Check the load balancing configuration and verify that the network is operational.

718053

Error Message `%FTD-5-718053: Detected duplicate control node, mastership stolen[MAC_address]`

Explanation The Secure Firewall Threat Defense device detected a duplicate director and a stolen director.

Recommended Action Check the load balancing configuration and verify that the network is operational.

718054

Error Message `%FTD-5-718054: Detected duplicate control node[MAC_address] and going to SLAVE`

Explanation The Secure Firewall Threat Defense device detected a duplicate director and is switching to member mode.

Recommended Action Check the load balancing configuration and verify that the network is operational.

718055

Error Message `%FTD-5-718055: Detected duplicate control node[MAC_address] and staying MASTER`

Explanation The Secure Firewall Threat Defense device detected a duplicate director and is staying in member mode.

Recommended Action Check the load balancing configuration and verify that the network is operational.

718056

Error Message `%FTD-7-718056: Deleted Master peer, IP IP_address`

Explanation The Secure Firewall Threat Defense device deleted the load balancing director from its internal tables.

Recommended Action None required.

718057

Error Message `%FTD-5-718057: Queue send failure from ISR, msg type failure_code`

Explanation An internal software error has occurred while attempting to enqueue a message on the VPN load balancing queue from an Interrupt Service Routing.

Recommended Action This is generally a benign condition. If the problem persists, contact the Cisco TAC.

718058

Error Message `%FTD-7-718058: State machine return code: action_routine, return_code`

Explanation The return codes of action routines belonging to the load balancing finite state machine are being traced.

Recommended Action None required.

718059

Error Message `%FTD-7-718059: State machine function trace: state=state_name, event=event_name, func=action_routine.`

Explanation The events and states of the load balancing finite state machine are being traced.

Recommended Action None required.

718060

Error Message `%FTD-5-718060: Inbound socket select fail: context=context_ID.`

Explanation The socket select call returned an error and the socket cannot be read. This might indicate an internal software error.

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

718061

Error Message `%FTD-5-718061: Inbound socket read fail: context=context_ID.`

Explanation The socket read failed after data was detected through the select call. This might indicate an internal software error.

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

718062

Error Message `%FTD-5-718062: Inbound thread is awake (context=context_ID).`

Explanation The load balancing process is awakened and begins processing.

Recommended Action None required.

718063

Error Message `%FTD-5-718063: Interface interface_name is down.`

Explanation The load balancing process found the interface down.

Recommended Action Check the interface configuration to make sure that the interface is operational.

718064

Error Message `%FTD-5-718064: Admin. interface interface_name is down.`

Explanation The load balancing process found the administrative interface down.

Recommended Action Check the administrative interface configuration to make sure that the interface is operational.

718065

Error Message `%FTD-5-718065: Cannot continue to run (public=up, private=down, enable=up, control node=down, session=LB_state).`

Explanation The load balancing process can not run because all prerequisite conditions have not been met. The prerequisite conditions are two active interfaces and load balancing enabled.

Recommended Action Check the interface configuration to make sure at least two interfaces are operational and load balancing is enabled.

718066

Error Message `%FTD-5-718066: Cannot add secondary address to interface interface_name, ip IP_address.`

Explanation Load balancing requires a secondary address to be added to the outside interface. A failure occurred in adding that secondary address.

Recommended Action Check the address being used as the secondary address and make sure that it is valid and unique. Check the configuration of the outside interface.

718067

Error Message `%FTD-5-718067: Cannot delete secondary address to interface interface_name, ip IP_address.`

Explanation The deletion of the secondary address failed, which might indicate an addressing problem or an internal software error.

Recommended Action Check the addressing information of the outside interface and make sure that the secondary address is valid and unique. If the problem persists, contact the Cisco TAC.

718068

Error Message `%FTD-5-718068: Start VPN Load Balancing in context context_ID.`

Explanation The load balancing process has been started and initialized.

Recommended Action None required.

718069

Error Message `%FTD-5-718069: Stop VPN Load Balancing in context context_ID.`

Explanation The load balancing process has been stopped.

Recommended Action None required.

718070

Error Message `%FTD-5-718070: Reset VPN Load Balancing in context context_ID.`

Explanation The LB process has been reset.

Recommended Action None required.

718071

Error Message `%FTD-5-718071: Terminate VPN Load Balancing in context context_ID.`

Explanation The LB process has been terminated.

Recommended Action None required.

718072

Error Message `%FTD-5-718072: Becoming control node of Load Balancing in context context_ID.`

Explanation The Secure Firewall Threat Defense device has become the LB director.

Recommended Action None required.

718073

Error Message `%FTD-5-718073: Becoming data node of Load Balancing in context context_ID.`

Explanation The Secure Firewall Threat Defense device has become the LB member.

Recommended Action None required.

718074

Error Message `%FTD-5-718074: Fail to create access list for peer context_ID.`

Explanation ACLs are used to create secure tunnels over which the LB peers can communicate. The Secure Firewall Threat Defense device was unable to create one of these ACLs. This might indicate an addressing problem or an internal software problem.

Recommended Action Check the addressing information of the inside interface on all peers and ensure that all peers are discovered correctly. If the problem persists, contact the Cisco TAC.

718075

Error Message `%FTD-5-718075: Peer IP_address access list not set.`

Explanation While removing a secure tunnel, the Secure Firewall Threat Defense device detected a peer entry that did not have an associated ACL.

Recommended Action None required.

718076

Error Message `%FTD-5-718076: Fail to create tunnel group for peer IP_address.`

Explanation The Secure Firewall Threat Defense device experienced a failure when trying to create a tunnel group for securing the communication between load balancing peers.

Recommended Action Verify that the load balancing configuration is correct.

718077

Error Message `%FTD-5-718077: Fail to delete tunnel group for peer IP_address.`

Explanation The Secure Firewall Threat Defense device experienced a failure when attempting to delete a tunnel group for securing the communication between load balancing peers.

Recommended Action None required.

718078

Error Message `%FTD-5-718078: Fail to create crypto map for peer IP_address.`

Explanation The Secure Firewall Threat Defense device experienced a failure when attempting to create a crypto map for securing the communication between load balancing peers.

Recommended Action Verify that the load balancing configuration is correct.

718079

Error Message `%FTD-5-718079: Fail to delete crypto map for peer IP_address.`

Explanation The Secure Firewall Threat Defense device experienced a failure when attempting to delete a crypto map for securing the communication between load balancing peers.

Recommended Action None required.

718080

Error Message `%FTD-5-718080: Fail to create crypto policy for peer IP_address.`

Explanation The Secure Firewall Threat Defense device experienced a failure when attempting to create a transform set to be used in securing the communication between load balancing peers. This might indicate an internal software problem.

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

718081

Error Message `%FTD-5-718081: Fail to delete crypto policy for peer IP_address.`

Explanation The Secure Firewall Threat Defense device experienced a failure when attempting to delete a transform set used in securing the communication between load balancing peers.

Recommended Action None required.

718082

Error Message `%FTD-5-718082: Fail to create crypto ipsec for peer IP_address.`

Explanation When cluster encryption for VPN load balancing is enabled, the VPN load balancing device creates a set of site-to-site tunnels for every other device in the load balancing cluster. For each tunnel, a set of crypto parameters (access list, crypto maps, and transform set) is created dynamically. One or more crypto parameters failed to be created or configured.

- **IP_address**—The IP address of the remote peer

Recommended Action Examine the message for other entries specific to the type of crypto parameters that failed to be created.

718083

Error Message `%FTD-5-718083: Fail to delete crypto ipsec for peer IP_address.`

Explanation When the local VPN load balancing device is removed from the cluster, crypto parameters are removed. One or more crypto parameters failed to be deleted.

- **IP_address**—The IP address of the remote peer

Recommended Action Examine the message for other entries specific to the type of crypto parameters that failed to be deleted.

718084

Error Message `%FTD-5-718084: Public/cluster IP not on the same subnet: public IP_address, mask netmask, cluster IP_address`

Explanation The cluster IP address is not on the same network as the outside interface of the Secure Firewall Threat Defense device.

Recommended Action Make sure that both the cluster (or virtual) IP address and the outside interface address are on the same network.

718085

Error Message `%FTD-5-718085: Interface interface_name has no IP address defined.`

Explanation The interface does not have an IP address configured.

Recommended Action Configure an IP address for the interface.

718086

Error Message `%FTD-5-718086: Fail to install LB NP rules: type rule_type, dst interface_name, port port.`

Explanation The Secure Firewall Threat Defense device experienced a failure when attempting to create a SoftNP ACL rule to be used in securing the communication between load balancing peers. This may indicate an internal software problem.

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

718087

Error Message `%FTD-5-718087: Fail to delete LB NP rules: type rule_type, rule rule_ID.`

Explanation The Secure Firewall Threat Defense device experienced a failure when attempting to delete the SoftNP ACL rule used in securing the communication between load balancing peers.

Recommended Action None required.

718088

Error Message `%FTD-7-718088: Possible VPN LB misconfiguration. Offending device MAC [MAC_address].`

Explanation The presence of a duplicate director indicates that one of the load balancing peers may be misconfigured.

Recommended Action Check the load balancing configuration on all peers, but pay special attention to the peer identified.

719001

Error Message `%FTD-6-719001: Email Proxy session could not be established: session limit of maximum_sessions has been reached.`

Explanation The incoming e-mail proxy session cannot be established because the maximum session limit has been reached.

- **maximum_sessions**—The maximum session number

Recommended Action None required.

719002

Error Message `%FTD-3-719002: Email Proxy session pointer from source_address has been terminated due to reason error.`

Explanation The session has been terminated because of an error. The possible errors are failure to add a session to the session database, failure to allocate memory, and failure to write data to a channel.

- **pointer**—The session pointer
- **source_address—**The e-mail proxy client IP address
- **reason—**The error type

Recommended Action None required.

719003

Error Message `%FTD-6-719003: Email Proxy session pointer resources have been freed for source_address .`

Explanation The dynamic allocated session structure has been freed and set to NULL after the session terminated.

- **pointer**—The session pointer
- **source_address**—The e-mail proxy client IP address

Recommended Action None required.

719004

Error Message `%FTD-6-719004: Email Proxy session pointer has been successfully established for source_address .`

Explanation A new incoming e-mail client session has been established.

Recommended Action None required.

719005

Error Message `%FTD-7-719005: FSM NAME has been created using protocol for session pointer from source_address .`

Explanation The FSM has been created for an incoming new session.

- NAME—The FSM instance name for the session
- **protocol**—The e-mail protocol type (for example, POP3, IMAP, and SMTP)
- **pointer**—The session pointer
- **source_address**—The e-mail proxy client IP address

Recommended Action None required.

719006

Error Message `%FTD-7-719006: Email Proxy session pointer has timed out for source_address because of network congestion.`

Explanation Network congestion is occurring, and data cannot be sent to either an e-mail client or an e-mail server. This condition starts the block timer. After the block timer is timed out, the session expires.

- **pointer**—The session pointer
- **source_address**—The e-mail proxy client IP address

Recommended Action Retry the operation after a few minutes.

719007

Error Message `%FTD-7-719007: Email Proxy session pointer cannot be found for source_address .`

Explanation A matching session cannot be found in the session database. The session pointer is bad.

- **pointer**—The session pointer
- **source_address**—The e-mail proxy client IP address

Recommended Action None required.

719008

Error Message `%FTD-3-719008: Email Proxy service is shutting down.`

Explanation The e-mail proxy is disabled. All resources are cleaned up, and all threads are terminated.

Recommended Action None required.

719009

Error Message `%FTD-7-719009: Email Proxy service is starting.`

Explanation The e-mail proxy is enabled.

Recommended Action None required.

719010

Error Message `%FTD-6-719010: protocol Email Proxy feature is disabled on interface interface_name .`

Explanation The e-mail proxy feature is disabled on a specific entry point, invoked from the CLI. This is the main off switch for the user. When all protocols are turned off for all interfaces, the main shut-down routine is invoked to clean up global resources and threads.

- **protocol**—The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)
- **interface_name** —The Secure Firewall Threat Defense interface name

Recommended Action None required.

719011

Error Message `%FTD-6-719011: Protocol Email Proxy feature is enabled on interface interface_name .`

Explanation The e-mail proxy feature is enabled on a specific entry point, invoked from the CLI. This is the main on switch for the user. When it is first used, the main startup routine is invoked to allocate global resources and threads. Subsequent calls only need to start listening threads for the particular protocol.

- **protocol**—The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)
- **interface_name** —The Secure Firewall Threat Defense interface name

Recommended Action None required.

719012

Error Message `%FTD-6-719012: Email Proxy server listening on port port for mail protocol protocol .`

Explanation A listening channel is opened for a specific protocol on a configured port and has added it to a TCP select group.

- **port—**The configured port number
- **protocol**—The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)

Recommended Action None required.

719013

Error Message `%FTD-6-719013: Email Proxy server closing port port for mail protocol protocol .`

Explanation A listening channel is closed for a specific protocol on a configured port and has removed it from the TCP select group.

- **port—**The configured port number
- **protocol**—The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)

Recommended Action None required.

719014

Error Message `%FTD-5-719014: Email Proxy is changing listen port from old_port to new_port for mail protocol protocol .`

Explanation A change is signaled in the listening port for the specified protocol. All enabled interfaces for that port have their listening channels closed and have restarted listening on the new port. This action is invoked from the CLI.

- **old_port—**The previously configured port number
- **new_port** —The newly configured port number
- **protocol**—The e-mail proxy protocol type (for example, POP3, IMAP, and SMTP)

Recommended Action None required.

719015

Error Message `%FTD-7-719015: Parsed emailproxy session pointer from source_address username: mailuser = mail_user , vpnuser = VPN_user , mailserver = server`

Explanation The username string is received from the client in the format vpnuser (name delimiter) mailuser (server delimiter) mailserver (for example: xxx:yyy@cisco.com). The name delimiter is optional. When the delimiter is not there, the VPN username and mail username are the same. The server delimiter is optional. When it is not present, the default configured mail server will be used.

- **pointer**—The session pointer
- **source_address**—The e-mail proxy client IP address
- mail_user—The e-mail account username
- **VPN_user**—The WebVPN username
- **server**—The e-mail server

Recommended Action None required.

719016

Error Message `%FTD-7-719016: Parsed emailproxy session pointer from source_address password: mailpass = ******, vpnpass= ******`

Explanation The password string is received from the client in the format, vpnpass (name delimiter) mailpass (for example: xxx:yyy). The name delimiter is optional. When it is not present, the VPN password and mail password are the same.

- **pointer**—The session pointer
- **source_address**—The e-mail proxy client IP address

Recommended Action None required.

719017

Error Message `%FTD-6-719017: WebVPN user: vpnuser invalid dynamic ACL.`

Explanation The WebVPN session is aborted because the ACL has failed to parse for this user. The ACL determines what the user restrictions are on e-mail account access. The ACL is downloaded from the AAA server. Because of this error, it is unsafe to proceed with login.

- **vpnuser**—The WebVPN username

Recommended Action Check the AAA server and fix the dynamic ACL for this user.

719018

Error Message `%FTD-6-719018: WebVPN user: vpnuser ACL ID acl_ID not found`

Explanation The ACL cannot be found at the local maintained ACL list. The ACL determines what the user restrictions are on e-mail account access. The ACL is configured locally. Because of this error, you cannot be authorized to proceed.

- **vpnuser**—The WebVPN username
- **acl_ID**—The local configured ACL identification string

Recommended Action Check the local ACL configuration.

719019

Error Message `%FTD-6-719019: WebVPN user: vpnuser authorization failed.`

Explanation The ACL determines what the user restrictions are on e-mail account access. The user cannot access the e-mail account because the authorization check fails.

- **vpnuser**—The WebVPN username

Recommended Action None required.

719020

Error Message `%FTD-6-719020: WebVPN user vpnuser authorization completed successfully.`

Explanation The ACL determines what the user restrictions are on e-mail account access. The user is authorized to access the e-mail account.

- **vpnuser**—The WebVPN username

Recommended Action None required.

719021

Error Message `%FTD-6-719021: WebVPN user: vpnuser is not checked against ACL.`

Explanation The ACL determines what the user restrictions are on e-mail account access. The authorization checking using the ACL is not enabled.

- **vpnuser**—The WebVPN username

Recommended Action Enable the ACL checking feature, if necessary.

719022

Error Message `%FTD-6-719022: WebVPN user vpnuser has been authenticated.`

Explanation The username is authenticated by the AAA server.

- **vpnuser**—The WebVPN username

Recommended Action None required.

719023

Error Message `%FTD-6-719023: WebVPN user vpnuser has not been successfully authenticated. Access denied.`

Explanation The username is denied by the AAA server. The session will be aborted. The user is not allowed to access the e-mail account.

- **vpnuser**—The WebVPN username

Recommended Action None required.

719024

Error Message `%FTD-6-719024: Email Proxy piggyback auth fail: session = pointer user=vpnuser addr=source_address`

Explanation The Piggyback authentication is using an established WebVPN session to verify the username and IP address matching in the WebVPN session database. This is based on the assumption that the WebVPN session and e-mail proxy session are initiated by the same user, and a WebVPN session is already established. Because the authentication has failed, the session will be aborted. The user is not allowed to access the e-mail account.

- **pointer**—The session pointer
- **vpnuser**—The WebVPN username
- **source_address**—The client IP address

Recommended Action None required.

719025

Error Message `%FTD-6-719025: Email Proxy DNS name resolution failed for hostname .`

Explanation The hostname cannot be resolved with the IP address because it is not valid, or no DNS server is available.

- **hostname**—The hostname that needs to be resolved

Recommended Action Check DNS server availability and whether or not the configured mail server name is valid.

719026

Error Message `%FTD-6-719026: Email Proxy DNS name hostname resolved to IP_address .`

Explanation The hostname has successfully been resolved with the IP address.

- **hostname**—The hostname that needs to be resolved
- **IP_address**—The IP address resolved from the configured mail server name

Recommended Action None required.

Messages 720001 to 721019

This section includes messages from 720001 to 721019.

720001

Error Message `%FTD-4-720001: (VPN-unit ) Failed to initialize with Chunk Manager.`

Explanation The VPN failover subsystem fails to initialize with the memory buffer management subsystem. A system-wide problem has occurred, and the VPN failover subsystem cannot be started.

- **unit**—Either Primary or Secondary

Recommended Action Examine the messages for any sign of system-level initialization problems.

720002

Error Message `%FTD-6-720002: (VPN-unit ) Starting VPN Stateful Failover Subsystem...`

Explanation The VPN failover subsystem is starting and booting up.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720003

Error Message `%FTD-6-720003: (VPN-unit ) Initialization of VPN Stateful Failover Component completed successfully`

Explanation The VPN failover subsystem initialization is completed at boot time.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720004

Error Message `%FTD-6-720004: (VPN-unit ) VPN failover main thread started.`

Explanation The VPN failover main processing thread is started at boot time.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720005

Error Message `%FTD-6-720005: (VPN-unit ) VPN failover timer thread started.`

Explanation The VPN failover timer processing thread is started at boot time.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720006

Error Message `%FTD-6-720006: (VPN-unit ) VPN failover sync thread started.`

Explanation The VPN failover bulk synchronization processing thread is started at boot time.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720007

Error Message `%FTD-4-720007: (VPN-unit ) Failed to allocate chunk from Chunk Manager.`

Explanation The set of preallocated memory buffers is running out. The Secure Firewall Threat Defense device has a resource issue. The Secure Firewall Threat Defense device may be under heavy load when too many messages are being processed.

- **unit**—Either Primary or Secondary

Recommended Action This condition may be improved later when the VPN failover subsystem processes outstanding messages and frees up previously allocated memory.

720008

Error Message `%FTD-4-720008: (VPN-unit ) Failed to register to High Availability Framework.`

Explanation The VPN failover subsystem failed to register to the core failover subsystem. The VPN failover subsystem cannot be started, which may be caused by initialization problems of other subsystems.

- **unit**—Either Primary or Secondary

Recommended Action Search the message for any sign of system-wide initialization problems.

720009

Error Message `%FTD-4-720009: (VPN-unit ) Failed to create version control block.`

Explanation The VPN failover subsystem failed to create a version control block. This step is required for the VPN failover subsystem to find out the backward compatible firmware versions for the current release. The VPN failover subsystem cannot be started, which may be caused by initialization problems of other subsystems.

- **unit**—Either Primary or Secondary

Recommended Action Search the message for any sign of system-wide initialization problems.

720010

Error Message `%FTD-6-720010: (VPN-unit ) VPN failover client is being disabled`

Explanation An operator enabled failover without defining a failover key. In order to use a VPN failover, a failover key must be defined.

- **unit**—Either Primary or Secondary

Recommended Action Use the **failover key** command to define a shared secret key between the active and standby units.

720011

Error Message `%FTD-4-720011: (VPN-unit ) Failed to allocate memory`

Explanation The VPN failover subsystem cannot allocate a memory buffer, which indicates a system-wide resource problem. The Secure Firewall Threat Defense device may be under heavy load.

- **unit**—Either Primary or Secondary

Recommended Action This condition may be improved later when you reduce the load on the Secure Firewall Threat Defense device by reducing incoming traffic. By reducing incoming traffic, memory allocated for processing the existing work load will be available, and the Secure Firewall Threat Defense device may return to normal operation.

720012

Error Message `%FTD-6-720012: (VPN-unit ) Failed to update IPsec failover runtime data on the standby unit.`

Explanation The VPN failover subsystem cannot update IPsec-related runtime data because the corresponding IPsec tunnel has been deleted on the standby unit.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720013

Error Message `%FTD-4-720013: (VPN-unit ) Failed to insert certificate in trustpoint trustpoint_name`

Explanation The VPN failover subsystem tried to insert a certificate in the trustpoint.

- **unit**—Either Primary or Secondary
- **trustpoint_name**—The name of the trustpoint

Recommended Action Check the certificate content to determine if it is invalid.

720014

Error Message `%FTD-6-720014: (VPN-unit ) Phase 2 connection entry (msg_id=message_number , my cookie=mine , his cookie=his ) contains no SA list.`

Explanation No security association is linked to the Phase 2 connection entry.

- **unit**—Either Primary or Secondary
- **message_number—**The message ID of the Phase 2 connection entry
- **mine**—The My Phase 1 cookie
- **his**—The peer Phase 1 cookie

Recommended Action None required.

720015

Error Message `%FTD-6-720015: (VPN-unit ) Cannot found Phase 1 SA for Phase 2 connection entry (msg_id=message_number ,my cookie=mine , his cookie=his ).`

Explanation The corresponding Phase 1 security association for the given Phase 2 connection entry cannot be found.

- **unit**—Either Primary or Secondary

- **message_number—**The message ID of the Phase 2 connection entry
- **mine**—The My Phase 1 cookie
- **his**—The peer Phase 1 cookie

Recommended Action None required.

720016

Error Message `%FTD-5-720016: (VPN-unit) Failed to initialize default timer #index .`

Explanation The VPN failover subsystem failed to initialize the given timer event. The VPN failover subsystem cannot be started at boot time.

- **unit**—Either Primary or Secondary
- **index**—The internal index of the timer event

Recommended Action Search the message for any sign of system-wide initialization problems.

720017

Error Message `%FTD-5-720017: (VPN-unit ) Failed to update LB runtime data`

Explanation The VPN failover subsystem failed to update the VPN load balancing runtime data.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720018

Error Message `%FTD-5-720018: (VPN-unit ) Failed to get a buffer from the underlying core high availability subsystem. Error code code.`

Explanation The Secure Firewall Threat Defense device may be under heavy load. The VPN failover subsystem failed to obtain a failover buffer.

- **unit**—Either Primary or Secondary
- **code**—The error code returned by the high-availability subsystem

Recommended Action Decrease the amount of incoming traffic to improve the current load condition. With decreased incoming traffic, the Secure Firewall Threat Defense device will free up memory allocated for processing the incoming load.

720019

Error Message `%FTD-5-720019: (VPN-unit ) Failed to update cTCP statistics.`

Explanation The VPN failover subsystem failed to update the IPsec/cTCP-related statistics.

- **unit**—Either Primary or Secondary

Recommended Action None required. Updates are sent periodically, so the standby unit IPsec/cTCP statistics should be updated with the next update message.

720020

Error Message `%FTD-5-720020: (VPN-unit ) Failed to send type timer message.`

Explanation The VPN failover subsystem failed to send a periodic timer message to the standby unit.

- **unit**—Either Primary or Secondary
- **type**—The type of timer message

Recommended Action None required. The periodic timer message will be resent during the next timeout.

720021

Error Message `%FTD-5-720021: (VPN-unit ) HA non-block send failed for peer msg message_number . HA error code .`

Explanation The VPN failover subsystem failed to send a nonblock message. This is a temporary condition caused by the Secure Firewall Threat Defense device being under load or out of resources.

- **unit**—Either Primary or Secondary
- **message_number**—The ID number of the peer message
- **code**—The error return code

Recommended Action The condition will improve as more resources become available to the Secure Firewall Threat Defense device.

720022

Error Message `%FTD-4-720022: (VPN-unit ) Cannot find trustpoint trustpoint`

Explanation An error occurred when the VPN failover subsystem tried to look up a trustpoint by name.

- **unit**—Either Primary or Secondary
- **trustpoint**—The name of the trustpoint.

Recommended Action The trustpoint may be deleted by an operator.

720023

Error Message `%FTD-6-720023: (VPN-unit ) HA status callback: Peer is not present.`

Explanation The VPN failover subsystem is notified by the core failover subsystem when the local Secure Firewall Threat Defense device detected that a peer is available or becomes unavailable.

- **unit**—Either Primary or Secondary
- **not**—Either “not” or left blank

Recommended Action None required.

720024

Error Message `%FTD-6-720024: (VPN-unit ) HA status callback: Control channel is status .`

Explanation The failover control channel is either up or down. The failover control channel is defined by the **failover link** and **show failover** commands, which indicate whether the failover link channel is up or down.

- **unit**—Either Primary or Secondary
- **status**— Up or Down

Recommended Action None required.

720025

Error Message `%FTD-6-720025: (VPN-unit ) HA status callback: Data channel is status .`

Explanation The failover data channel is up or down.

- **unit**—Either Primary or Secondary
- **status**—Up or Down

Recommended Action None required.

720026

Error Message `%FTD-6-720026: (VPN-unit ) HA status callback: Current progression is being aborted.`

Explanation An operator or other external condition has occurred and has caused the current failover progression to abort before the failover peer agrees on the role (either active or standby). For example, when the **failover active** command is entered on the standby unit during the negotiation, or when the active unit is being rebooted.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720027

Error Message `%FTD-6-720027: (VPN-unit ) HA status callback: My state state .`

Explanation The state of the local failover device is changed.

- **unit**—Either Primary or Secondary
- **state**—Current state of the local failover device

Recommended Action None required.

720028

Error Message `%FTD-6-720028: (VPN-unit ) HA status callback: Peer state state .`

Explanation The current state of the failover peer is reported.

- **unit**—Either Primary or Secondary
- **state**—Current state of the failover peer

Recommended Action None required.

720029

Error Message `%FTD-6-720029: (VPN-unit ) HA status callback: Start VPN bulk sync state.`

Explanation The active unit is ready to send all the state information to the standby unit.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720030

Error Message `%FTD-6-720030: (VPN-unit ) HA status callback: Stop bulk sync state.`

Explanation The active unit finished sending all the state information to the standby unit.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720031

Error Message `%FTD-7-720031: (VPN-unit ) HA status callback: Invalid event received. event=event_ID .`

Explanation The VPN failover subsystem received an invalid callback event from the underlying failover subsystem.

- **unit**—Either Primary or Secondary
- **event_ID**—The invalid event ID received

Recommended Action None required.

720032

Error Message `%FTD-6-720032: (VPN-unit) HA status callback: id=ID , seq=sequence_# , grp=group , event=event , op=operand , my=my_state , peer=peer_state .`

Explanation The VPN failover subsystem indicated that a status update was notified by the underlying failover subsystem.

- **unit**—Either Primary or Secondary
- **ID**—Client ID number
- **sequence_#**—Sequence number
- **group**—Group ID
- **event**—Current event
- **operand**—Current operand
- **my_state**—The system current state
- **peer_state**—The current state of the peer

Recommended Action None required.

720033

Error Message `%FTD-4-720033: (VPN-unit ) Failed to queue add to message queue.`

Explanation System resources may be running low. An error occurred when the VPN failover subsystem tried to queue an internal message. This may be a temporary condition indicating that the Secure Firewall Threat Defense device is under heavy load, and the VPN failover subsystem cannot allocate resource to handle incoming traffic.

- **unit**—Either Primary or Secondary

Recommended Action This error condition may disappear if the current load of the Secure Firewall Threat Defense device is reduced, and additional system resources become available for processing new messages again.

720034

Error Message `%FTD-7-720034: (VPN-unit ) Invalid type (type ) for message handler.`

Explanation An error occurred when the VPN failover subsystem tried to process an invalid message type.

- **unit**—Either Primary or Secondary
- **type**—Message type

Recommended Action None required.

720035

Error Message `%FTD-5-720035: (VPN-unit ) Fail to look up CTCP flow handle`

Explanation The cTCP flow may be deleted on the standby unit before the VPN failover subsystem tries to do a lookup.

- **unit**—Either Primary or Secondary

Recommended Action Look for any sign of cTCP flow deletion in the message to determine the reason (for example, idle timeout) why the flow was deleted.

720036

Error Message `%FTD-5-720036: (VPN-unit ) Failed to process state update message from the active peer.`

Explanation An error occurred when the VPN failover subsystem tried to process a state update message received by the standby unit.

- **unit** - Either Primary or Secondary

Recommended Action None required. This may be a temporary condition because of the current load or low system resources.

720037

Error Message `%FTD-6-720037: (VPN-unit ) HA progression callback: id=id ,seq=sequence_number ,grp=group ,event=event ,op=operand , my=my_state ,peer=peer_state .`

Explanation The status of the current failover progression is reported.

- **unit**—Either Primary or Secondary
- **id**—Client ID
- **sequence_number**—Sequence number
- **group**—Group ID
- **event**—Current event
- **operand**—Current operand
- **my_state**—Current state of the Secure Firewall Threat Defense device
- **peer_state**—Current state of the peer

Recommended Action None required.

720038

Error Message `%FTD-4-720038: (VPN-unit ) Corrupted message from active unit.`

Explanation The standby unit received a corrupted message from the active unit. Messages from the active unit are corrupted, which may be caused by incompatible firmware running between the active and standby units. The local unit has become the active unit of the failover pair.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720039

Error Message `%FTD-6-720039: (VPN-unit ) VPN failover client is transitioning to active state`

Explanation The local unit has become the active unit of the failover pair.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720040

Error Message `%FTD-6-720040: (VPN-unit ) VPN failover client is transitioning to standby state.`

Explanation The local unit has become the standby unit of the failover pair.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720041

Error Message `%FTD-7-720041: (VPN-unit ) Sending type message id to standby unit`

Explanation A message has been sent from the active unit to the standby unit.

- **unit**—Either Primary or Secondary
- **type**—Message type
- **id**—Identifier for the message

Recommended Action None required.

720042

Error Message `%FTD-7-720042: (VPN-unit ) Receiving type message id from active unit`

Explanation A message has been received from the active unit by the standby unit.

- **unit**—Either Primary or Secondary
- **type**—Message type
- **id**—Identifier for the message

Recommended Action None required.

720043

Error Message `%FTD-4-720043: (VPN-unit ) Failed to send type message id to standby unit`

Explanation An error occurred when the VPN failover subsystem tried to send a message from the active unit to the standby unit. The error may be caused by message 720018, in which the core failover subsystem runs out of failover buffer or the failover LAN link is down.

- **unit**—Either Primary or Secondary
- **type**—Message type
- **id**—Identifier for the message

Recommended Action Use the **show failover** command to see if the failover pair is running correctly and the failover LAN link is up.

720044

Error Message `%FTD-4-720044: (VPN-unit ) Failed to receive message from active unit`

Explanation An error occurred when the VPN failover subsystem tried to receive a message on the standby unit. The error may be caused by a corrupted message or an inadequate amount of memory allocated for storing the incoming message.

- **unit**—Either Primary or Secondary

Recommended Action Use the **show failover** command and look for receive errors to determine if this is a VPN failover-specific problem or a general failover issue. Corrupted messages may be caused by incompatible firmware versions running on the active and standby units. Use the **show memory** command to determine if a low memory condition exists.

720045

Error Message `%FTD-6-720045: (VPN-unit ) Start bulk syncing of state information on standby unit.`

Explanation The standby unit has been notified to start receiving bulk synchronization information from the active unit.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720046

Error Message `%FTD-6-720046: (VPN-unit ) End bulk syncing of state information on standby unit`

Explanation The standby unit has been notified that bulk synchronization from the active unit is completed.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720047

Error Message `%FTD-4-720047: (VPN-unit ) Failed to sync SDI node secret file for server IP_address on the standby unit.`

Explanation An error occurred when the VPN failover subsystem tried to synchronize a node secret file for the SDI server on the standby unit. The SDI node secret file is stored in flash. The error may indicate that the flash file system is full or corrupted.

- **unit**—Either Primary or Secondary
- **IP_address**—IP address of the server

Recommended Action Use the **dir** command to display the flash contents. The node secret file has the filename, *ip* .sdi.

720048

Error Message `%FTD-7-720048: (VPN-unit ) FSM action trace begin: state=state , last event=event , func=function .`

Explanation A VPN failover subsystem finite state machine function has started.

- **unit**—Either Primary or Secondary
- **state**—Current state
- **event**—Last event
- **function**—Current executing function

Recommended Action None required.

720049

Error Message `%FTD-7-720049: (VPN-unit ) FSM action trace end: state=state , last event=event , return=return , func=function .`

Explanation A VPN failover subsystem finite state machine function has finished.

- **unit**—Either Primary or Secondary
- **state**—Current state
- **event**—Last event
- **return**—Return code
- **function**—Current executing function

Recommended Action None required.

720050

Error Message `%FTD-7-720050: (VPN-unit ) Failed to remove timer. ID = id .`

Explanation A timer cannot be removed from the timer processing thread.

- **unit**—Either Primary or Secondary
- **id**—Timer ID

Recommended Action None required.

720051

Error Message `%FTD-4-720051: (VPN-unit ) Failed to add new SDI node secret file for server id on the standby unit.`

Explanation An error occurred when the VPN failover subsystem tried to add a node secret file for the SDI server on the standby unit. The SDI node secret file is stored in flash. The error may indicate that the flash file system is full or corrupted.

- **unit**—Either Primary or Secondary
- **id**—IP address of the SDI server

Recommended Action Use the **dir** command to display the flash contents. The node secret file has the filename, **ip**.sdi.

720052

Error Message `%FTD-4-720052: (VPN-unit ) Failed to delete SDI node secret file for server id on the standby unit.`

Explanation An error occurred when the VPN failover subsystem tried to delete a node secret file on the active unit. The node secret file being deleted may not exist in the flash file system, or there was problem reading the flash file system.

- **unit**—Either Primary or Secondary
- **IP_address**—IP address of the SDI server

Recommended Action Use the **dir** command to display the flash contents. The node secret file has the filename, **ip**.sdi.

720053

Error Message `%FTD-4-720053: (VPN-unit ) Failed to add cTCP IKE rule during bulk sync, peer=IP_address , port=port`

Explanation An error occurred when the VPN failover subsystem tried to load a cTCP IKE rule on the standby unit during bulk synchronization. The standby unit may be under heavy load, and the new IKE rule request may time out before completion.

- **unit**—Either Primary or Secondary
- **IP_address**—Peer IP address
- **port**—Peer port number

Recommended Action None required.

720054

Error Message `%FTD-4-720054: (VPN-unit ) Failed to add new cTCP record, peer=IP_address , port=port .`

Explanation A cTCP record is replicated to the standby unit and cannot be updated. The corresponding IPsec over cTCP tunnel may not be functioning after failover. The cTCP database may be full, or a record with the same peer IP address and port number exists already.

- **unit**—Either Primary or Secondary
- **IP_address**—Peer IP address
- **port**—Peer port number

Recommended Action This may be a temporary condition and may improve when the existing cTCP tunnel is restored.

720055

Error Message `%FTD-4-720055: (VPN-unit ) VPN Stateful failover can only be run in single/non-transparent mode.`

Explanation The VPN subsystem does not start unless it is running in single (nontransparent) mode.

- **unit**—Either Primary or Secondary

Recommended Action Configure the Secure Firewall Threat Defense device for the appropriate mode to support VPN failover and restart the Secure Firewall Threat Defense device.

720056

Error Message `%FTD-6-720056: (VPN-unit ) VPN Stateful failover Message Thread is being disabled.`

Explanation The VPN failover subsystem main message processing thread is disabled when you have tried to enable failover, but a failover key is not defined. A failover key is required for VPN failover.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720057

Error Message `%FTD-6-720057: (VPN-unit ) VPN Stateful failover Message Thread is enabled.`

Explanation The VPN failover subsystem main message processing thread is enabled when failover is enabled and a failover key is defined.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720058

Error Message `%FTD-6-720058: (VPN-unit ) VPN Stateful failover Timer Thread is disabled.`

Explanation The VPN failover subsystem main timer processing thread is disabled when the failover key is not defined and failover is enabled.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720059

Error Message `%FTD-6-720059: (VPN-unit ) VPN Stateful failover Timer Thread is enabled.`

Explanation The VPN failover subsystem main timer processing thread is enabled when the failover key is defined and failover is enabled.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720060

Error Message `%FTD-6-720060: (VPN-unit ) VPN Stateful failover Sync Thread is disabled.`

Explanation The VPN failover subsystem main bulk synchronization processing thread is disabled when failover is enabled, but the failover key is not defined.

- **unit**—Either Primary or Secondary.

Recommended Action None required.

720061

Error Message `%FTD-6-720061: (VPN-unit ) VPN Stateful failover Sync Thread is enabled.`

Explanation The VPN failover subsystem main bulk synchronization processing thread is enabled when failover is enabled and the failover key is defined.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720062

Error Message `%FTD-6-720062: (VPN-unit ) Active unit started bulk sync of state information to standby unit.`

Explanation The VPN failover subsystem active unit has started bulk synchronization of state information to the standby unit.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720063

Error Message `%FTD-6-720063: (VPN-unit ) Active unit completed bulk sync of state information to standby.`

Explanation The VPN failover subsystem active unit has completed bulk synchronization of state information to the standby unit.

- **unit**—Either Primary or Secondary

Recommended Action None required.

720064

Error Message `%FTD-4-720064: (VPN-unit ) Failed to update cTCP database record for peer=IP_address , port=port during bulk sync.`

Explanation An error occurred while the VPN failover subsystem attempted to update an existing cTCP record during bulk synchronization. The cTCP record may have been deleted from the cTCP database on the standby unit and cannot be found.

- **unit**—Either Primary or Secondary
- **IP_address**—Peer IP address
- **port**—Peer port number

Recommended Action Search in the message.

720065

Error Message `%FTD-4-720065: (VPN-unit ) Failed to add new cTCP IKE rule, peer=peer , port=port .`

Explanation An error occurred when the VPN failover subsystem tried to add a new IKE rule for the cTCP database entry on the standby unit. The Secure Firewall Threat Defense device may be under heavy load, and the request for adding a cTCP IKE rule timed out and was never completed.

- **unit**—Either Primary or Secondary
- **IP_address**—Peer IP address
- **port**—Peer port number

Recommended Action This may be a temporary condition.

720066

Error Message `%FTD-4-720066: (VPN-unit ) Failed to activate IKE database.`

Explanation An error occurred when the VPN failover subsystem tried to activate the IKE security association database while the standby unit was transitioning to the active state. There may be resource-related issues on the standby unit that prevent the IKE security association database from activating.

- **unit**—Either Primary or Secondary

Recommended Action Use the **show failover** command to see if the failover pair is still working correctly and/or look for other IKE-related errors in the message.

720067

Error Message `%FTD-4-720067: (VPN-unit ) Failed to deactivate IKE database.`

Explanation An error occurred when the VPN failover subsystem tried to deactivate the IKE security association database while the active unit was transitioning to the standby state. There may be resource-related issues on the active unit that prevent the IKE security association database from deactivating.

- **unit**—Either Primary or Secondary

Recommended Action Use the **show failover** command to see if the failover pair is still working correctly and/or look for IKE-related errors in the message.

720068

Error Message `%FTD-4-720068: (VPN-unit ) Failed to parse peer message.`

Explanation An error occurred when the VPN failover subsystem tried to parse a peer message received on the standby unit. The peer message received on the standby unit cannot be parsed.

- **unit**—Either Primary or Secondary

Recommended Action Make sure that both active and standby units are running the same version of firmware. Also, use the **show failover** command to ensure that the failover pair is still working correctly.

720069

Error Message `%FTD-4-720069: (VPN-unit ) Failed to activate cTCP database.`

Explanation An error occurred when the VPN failover subsystem tried to activate the cTCP database while the standby unit was transitioning to the active state. There may be resource-related issues on the standby unit that prevent the cTCP database from activating.

- **unit**—Either Primary or Secondary

Recommended Action Use the **show failover** command to see if the failover pair is still working correctly and/or look for other cTCP related errors in the message.

720070

Error Message `%FTD-4-720070: (VPN-unit ) Failed to deactivate cTCP database.`

Explanation An error occurred when the VPN failover subsystem tried to deactivate the cTCP database while the active unit was transitioning to the standby state. There may be resource-related issues on the active unit that prevent the cTCP database from deactivating.

- **unit**—Either Primary or Secondary.

Recommended Action Use the **show failover** command to see if the failover pair is still working correctly and/or look for cTCP related errors in the message.

720071

Error Message `%FTD-5-720071: (VPN-unit ) Failed to update cTCP dynamic data.`

Explanation An error occurred while the VPN failover subsystem tried to update cTCP dynamic data.

- **unit**—Either Primary or Secondary.

Recommended Action This may be a temporary condition. Because this is a periodic update, wait to see if the same error recurs. Also, look for other failover-related messages in the message.

720072

Error Message `%FTD-5-720072: Timeout waiting for Integrity Firewall Server [interface ,ip ] to become available.`

Explanation The Zonelab Integrity Server cannot reestablish a connection before timeout. In an active/standby failover setup, the SSL connection between a Zonelab Integrity Server and the Secure Firewall Threat Defense device needs to be reestablished after a failover.

- *interface* —The interface to which the Zonelab Integrity Server is connected
- *ip* —The IP address of the Zonelab Integrity Server

Recommended Action Check that the configuration on the Secure Firewall Threat Defense device and the Zonelab Integrity Server match, and verify communication between the Secure Firewall Threat Defense device and the Zonelab Integrity Server.

720073

Error Message `%FTD-4-720073: VPN Session failed to replicate - ACL acl_name not found`

Explanation When replicating VPN sessions to the standby unit, the standby unit failed to find the associated filter ACL.

- **acl_name**—The name of the ACL that was not found

Recommended Action Verify that the configuration on the standby unit has not been modified while in standby state. Resynchronize the standby unit by issuing the **write standby** command on the active unit.

721001

Error Message `%FTD-6-721001: device WebVPN Failover SubSystem started successfully.`

Explanation The WebVPN failover subsystem in the current failover unit, either primary or secondary, has been started successfully.

- **(device)**—Either the WebVPN primary or the WebVPN secondary device

Recommended Action None required.

721002

Error Message `%FTD-6-721002: device HA status change: event event, my state my_state, peer state peer.`

Explanation The WebVPN failover subsystem receives status notification from the core HA component periodically. The incoming event, the new state of the local Secure Firewall Threat Defense device, and the new state of the failover peer are reported.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **event**—New HA event
- **my_state**—The new state of the local Secure Firewall Threat Defense device
- **peer**—The new state of the peer

Recommended Action None required.

721003

Error Message `%FTD-6-721003: device HA progression change: event event, my state my_state, peer state peer.`

Explanation The WebVPN failover subsystem transitions from one state to another state based on the event notified by the core HA component. The incoming event, the new state of the local Secure Firewall Threat Defense device, and the new state of the failover peer are being reported.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **event**—New HA event
- **my_state**—The new state of the local Secure Firewall Threat Defense device
- **peer**—The new state of the peer

Recommended Action None required.

721004

Error Message `%FTD-6-721004: device Create access list list_name on standby unit.`

Explanation A WebVPN-specific access list is replicated from the active unit to the standby unit. A successful installation of the WebVPN access list on the standby unit has occurred.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device

- **list_name**—The access list name

Recommended Action None required.

721005

Error Message `%FTD-6-721005: device Fail to create access list list_name on standby unit.`

Explanation When a WebVPN-specific access list is installed on the active unit, a copy is installed on the standby unit. The access list failed to be installed on the standby unit. The access list may have existed on the standby unit already.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **list_name**—Name of the access list that failed to install on the standby unit

Recommended Action Use the **show access-list** command on both the active and standby units. Compare the content of the output and determine whether there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

721006

Error Message `%FTD-6-721006: device Update access list list_name on standby unit.`

Explanation The content of the access list has been updated on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **list_name**—Name of the access list that was updated

Recommended Action None required.

721007

Error Message `%FTD-4-721007: device Fail to update access list list_name on standby unit.`

Explanation An error occurred while the standby unit tried to update a WebVPN-specific access list. The access list cannot be located on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN-= secondary Secure Firewall Threat Defense device
- **list_name**—Name of the access list that was not updated

Recommended Action Use a **show access-list** command on both the active and standby units. Compare the content of the output and determine whether or not there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

721008

Error Message `%FTD-6-721008: device Delete access list list_name on standby unit.`

Explanation When a WebVPN-specific access list is removed from the active unit, a message is sent to the standby unit requesting that the same access list be removed. As a result, a WebVPN-specific access list has been removed from the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **list_name**—Name of the access list that was removed

Recommended Action None required.

721009

Error Message `%FTD-6-721009: device Fail to delete access list list_name on standby unit.`

Explanation When a WebVPN-specific access list is removed on the active unit, a message is sent to the standby unit requesting the same access list be removed. An error condition occurred when an attempt was made to remove the corresponding access list on the standby unit. The access list did not exist on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **list_name**—Name of the access list that was deleted

Recommended Action Use a **show access-list** command on both the active and standby units. Compare the content of the output and determine whether there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

721010

Error Message `%FTD-6-721010: device Add access list list_name on standby unit.`

Explanation When an access list rule is added to the active unit, the same rule is added on the standby unit. A new access list rule was added successfully on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **list_name**—Name of the access list that was deleted
- **line_no**—Line number of the rule added to the access list

Recommended Action None required.

721011

Error Message `%FTD-4-721011: device Fail to add access list list_name on standby unit.`

Explanation When an access list rule is added to the active unit, an attempt is made to add the same access list rule to the standby unit. An error occurred when an attempt is made to add a new access list rule to the standby unit. The same access list rule may exist on the standby unit.

- *(device)* —Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **list_name**—Name of the access list that was deleted
- **line_no**—Line number of the rule added to the access list

Recommended Action Use a **show access-list** command on both the active and standby units. Compare the content of the output and determine if there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

721012

Error Message `%FTD-6-721012: device Enable APCF XML file file_name on the standby unit.`

Explanation When an APCF XML file is installed on the active unit, an attempt is made to install the same file on the standby unit. An APCF XML file was installed successfully on the standby unit. Use the **dir** command on the standby unit to show that the XML file exists in the flash file system.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **file_name**—Name of the XML file on the flash file system

Recommended Action None required.

721013

Error Message `%FTD-4-721013: device Fail to enable APCF XML file file_name on the standby unit.`

Explanation When an APCF XML file is installed on the active unit, an attempt is made to install the same file on the standby unit. An APCF XML file failed to install on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **file_name**—Name of the XML file on the flash file system

Recommended Action Use a **dir** command on both the active and standby unit. Compare the directory listing and determine if there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

721014

Error Message `%FTD-6-721014: device Disable APCF XML file file_name on the standby unit.`

Explanation When an APCF XML file is removed on the active unit, an attempt is made to remove the same file on the standby unit. An APCF XML file was removed from the standby unit successfully.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **file_name**—Name of the XML file on the flash file system

Recommended Action None required.

721015

Error Message `%FTD-4-721015: device Fail to disable APCF XML file file_name on the standby unit.`

Explanation When an APCF XML file is removed on the active unit, an attempt is made to remove the same file on the standby unit. An error occurred when an attempt was made to remove an APCF XML file from the standby unit. The file may not be installed on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device

- **file_name**—Name of the XML file on the flash file system

Recommended Action Use a **show running-config webvpn** command to make sure the APCF XML file of interest is not enabled. As long as it is not enabled, you may ignore this message. Otherwise, try to disable the file by using the **no apcf file_name** command in the webvpn configuration submode.

721016

Error Message `%FTD-6-721016: device WebVPN session for client user_name has been created.`

Explanation A remote WebVPN user has logged in successfully and the login information has been installed on the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **user_name**—Name of the user
- **IP version**—Version of the IP address-IPv4 or IPv6
- **ip_address**—IP address of the remote user

Recommended Action None required.

721017

Error Message `%FTD-4-721017: device .Fail to create WebVPN session for client user_name.`

Explanation When a WebVPN user logs in to the active unit, the login information is replicated to the standby unit. An error occurred while replicating the login information to the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **user_name**—Name of the user
- **ip_address**—IP address of the remote user

Recommended Action Use the **show vpn-sessiondb detail webvpn** command for a regular WebVPN user, or the **show vpn-sessiondb detail svc** command for a WebVPN SVC user on both the active and standby units. Compare the entries and determine whether the same user session record appears on both Secure Firewall Threat Defense devices. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.

721018

Error Message `%FTD-6-721018: device WebVPN session for client user_name has been deleted.`

Explanation When a WebVPN user logs out on the active unit, a logout message is sent to the standby unit to remove the user session from the standby unit. A WebVPN user record was removed from the standby unit successfully.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **user_name**—Name of the user
- **ip_address**—IP address of the remote user

Recommended Action None required.

721019

Error Message `%FTD-4-721019: device .Fail to delete WebVPN session for client user_name.`

Explanation When a WebVPN user logs out on the active unit, a logout message is sent to the standby unit to remove the user session from the standby unit. An error occurred when an attempt was made to remove a WebVPN user record from the standby unit.

- **(device)**—Either the WebVPN primary or the WebVPN secondary Secure Firewall Threat Defense device
- **user_name**—Name of the user
- **ip_address**—IP address of the remote user

Recommended Action Use the **show vpn-sessiondb detail webvpn** command for a regular WebVPN user, or the **show vpn-sessiondb detail svc** command for a WebVPN SVC user on both the active and standby units. Check whether there is any discrepancy. Resynchronize the standby unit, if needed, by using the **write standby** command on the active unit.