Syslog Messages 701001 to 714011

This chapter contains the following sections:

Messages 701001 to 713109

This section includes messages from 701001 to 713109.

701001

Error Message `%FTD-7-701001:` alloc_user() out of Tcp_user objects

Explanation A AAA message that appears if the user authentication rate is too high for the module to handle new AAA requests.

Recommended Action Enable Flood Defender with the floodguard enable command.

701002

Error Message `%FTD-7-701002: alloc_user() out of Tcp_proxy objects`

Explanation A AAA message that appears if the user authentication rate is too high for the module to handle new AAA requests.

Recommended Action Enable Flood Defender with the floodguard enable command.

703001

Error Message `%FTD-7-703001: H.225 message received from` *`interface_name`* `:`*`IP_address`* `/`*`port`* `to` *`interface_name`* `:`*`IP_address`* `/`*`port`* `is using an unsupported version` *`number`*

Explanation The Secure Firewall Threat Defense device received an H.323 packet with an unsupported version number. The Secure Firewall Threat Defense device might reencode the protocol version field of the packet to the highest supported version.

Recommended Action Use the version of H.323 that the Secure Firewall Threat Defense device supports in the VoIP network.

703002

Error Message `%FTD-7-703002: Received H.225 Release Complete with newConnectionNeeded for interface_name :IP_address to interface_name :IP_address /port`

Explanation The Secure Firewall Threat Defense device received the specified H.225 message, and the Secure Firewall Threat Defense device opened a new signaling connection object for the two specified H.323 endpoints.

Recommended Action None required.

703008

Error Message `%FTD-7-703008: Allowing early-message: %s before SETUP from %s:%Q/%d to %s:%Q/%d`

Explanation This message indicates that an outside endpoint requested an incoming call to an inside host and wants the inside host to send FACILITY message before SETUP message towards Gatekeeper and wants to follow H.460.18.

Recommended Action Ensure that the setup indeed intends to allow early FACILITY message before SETUP message for incoming H323 calls as described in H.640.18.

709001, 709002

Error Message `%FTD-7-709001: FO replication failed: cmd=command returned=code`

Error Message `%FTD-7-709002: FO unreplicable: cmd=command`

Explanation Failover messages that only appear during the development debugging and testing phases.

Recommended Action None required.

709003

Error Message `%FTD-1-709003: (Primary) Beginning configuration replication: Sending to mate.`

Explanation A failover message that appears when the active unit starts replicating its configuration to the standby unit. Primary can also be listed as Secondary for the secondary unit.

Recommended Action None required.

709004

Error Message `%FTD-1-709004: (Primary) End Configuration Replication (ACT)`

Explanation A failover message that appears when the active unit completes replication of its configuration on the standby unit. Primary can also be listed as Secondary for the secondary unit.

Recommended Action None required.

709005

Error Message `%FTD-1-709005: (Primary) Beginning configuration replication: Receiving from mate.`

Explanation The standby Secure Firewall Threat Defense device received the first part of the configuration replication from the active Secure Firewall Threat Defense device. Primary can also be listed as Secondary for the secondary unit.

Recommended Action None required.

709006

Error Message `%FTD-1-709006: (Primary) End Configuration Replication (STB)`

Explanation A failover message that appears when the standby unit completes replication of a configuration sent by the active unit. Primary can also be listed as Secondary for the secondary unit.

Recommended Action None required.

709007

Error Message `%FTD-2-709007: Configuration replication failed for command`

Explanation A failover message that appears when the standby unit is unable to complete replication of a configuration sent by the active unit. The command that caused the failure appears at the end of the message.

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

709008

Error Message `%FTD-4-709008: (Primary | Secondary) Configuration sync in progress. Command: 'command ' executed from (terminal/http) will not be replicated to or executed by the standby unit.`

Explanation A command was issued during the configuration sync, which triggered an interactive prompt to indicate that this command would not be issued on the standby unit. To continue, note that the command will be issued on the active unit only and will not be replicated on the standby unit.

- Primary | Secondary—The device is either primary or secondary
- *command* —The command issued while the configuration sync is in progress
- terminal/http—Issued from the terminal or via HTTP.

Recommended Action None.

709009

Error Message `%FTD-6-709009: (unit-role) Configuration on Active and Standby is matching. No config sync. Time elapsed time-elapsed ms`

Explanation This message is generated when the hash computed on both the active and joining unit matches. It also displays the time elapsed, from the time of sending the hash request to the time of getting and comparing the hash response..

Recommended Action None.

709010

Error Message `%FTD-6-709010: Configuration between units doesn't match. Going for config sync. Time elapsed` *`time-elapsed`* `ms.`

Explanation This syslog message is generated when the hash that is computed on both the active and joining unit does not match. It also displays the time elapsed, from the time of sending the hash request to the time of getting and comparing the hash response.

Recommended Action None.

709011

Error Message `%FTD-6-709011: Total time to sync the config` *`time`* `ms.`

Explanation This message displays the time taken to synchronize the config, in the case of hash not matching, and therefore going for a full configuration sync process.

Recommended Action None.

709012

Error Message `%FTD-6-709012: Skip configuration replication from mate as configuration on Active and Standby is matching.`

Explanation This message is generated when the configuration replication is skipped because, the configuration between active and joining unit matches.

Recommended Action None.

709013

Error Message `%FTD-4-709013: Failover configuration replication hash comparison timeout expired.`

Explanation This syslog message is generated when the hash computation, transfer, and comparison has timed out. Due to the timeout, the full configuration sync operation is trigerred. The timeout value is 60 secs and you cannot modify this value.

Recommended Action None.

709015

Error Message `%FTD-3-709015: Command sync Error: Sync failed for command` **`no nameif`** `with error code =` *`code`*

Explanation The messages appear on HA joining unit during failure of configuration sync, delta sync, or dynamic ACL sync commands.

Recommended Action None required.

710003

Error Message `%FTD-3-710003: {TCP|UDP} access denied by ACL from source_IP/source_port to interface_name :dest_IP/service`

Explanation The Secure Firewall Threat Defense device denied an attempt to connect to the interface service. For example, the Secure Firewall Threat Defense device received an SNMP request from an unauthorized SNMP management station. If this message appears frequently, it can indicate an attack.

For example:

```
%threat defense-3-710003: UDP access denied by ACL from 95.1.1.14/5000 to
outside:95.1.1.13/1005
```

Recommended Action Use the **show run http**, **show run ssh**, or **show run telnet** commands to verify that the Secure Firewall Threat Defense device is configured to permit the service access from the host or network.

710004

Error Message `%FTD-7-710004: TCP connection limit exceeded from Src_ip /Src_port to In_name :Dest_ip /Dest_port (current connections/connection limit = Curr_conn/Conn_lmt)`

Explanation The maximum number of Secure Firewall Threat Defense management connections for the service was exceeded. The Secure Firewall Threat Defense device permits at most five concurrent management connections per management service. Alternatively, an error may have occurred in the to-the-box connection counter.

- *Src_ip* —The source IP address of the packet
- *Src_por* t—The source port of the packet
- *In_ifc* —The input interface
- *Dest_ip* —The destination IP address of the packet
- *Dest_port* —The destination port of the packet
- *Curr_conn* —The number of current to-the-box admin connections
- *Conn_lmt* —The connection limit

Recommended Action From the console, use the **kill** command to release the unwanted session. If the message was generated because of an error in the to-the-box counter, run the **show conn all** command to display connection details.

710005

Error Message `%FTD-7-710005: {TCP|UDP|SCTP} request discarded from source_address /source_port to interface_name :dest_address /service`

Explanation The Secure Firewall Threat Defense device does not have a UDP server that services the UDP request. Also, a TCP packet that does not belong to any session on the Secure Firewall Threat Defense device may have been discarded. In addition, this message appears (with the SNMP service) when the Secure Firewall Threat Defense device receives an SNMP request with an empty payload, even if it is from an authorized

host. When the service is SNMP, this message occurs a maximum of once every 10 seconds so that the log receiver is not overwhelmed. This message is also applicable for SCTP packets.

Recommended Action In networks that use broadcasting services such as DHCP, RIP, or NetBIOS extensively, the frequency of this message can be high. If this message appears in excessive numbers, it may indicate an attack.

710006

Error Message `%FTD-7-710006: protocol request discarded from source_address to interface_name :dest_address`

Explanation The Secure Firewall Threat Defense device does not have an IP server that services the IP protocol request; for example, the Secure Firewall Threat Defense device receives IP packets that are not TCP or UDP, and the Secure Firewall Threat Defense device cannot service the request.

Recommended Action In networks that use broadcasting services such as DHCP, RIP, or NetBIOS extensively, the frequency of this message can be high. If this message appears in excessive numbers, it may indicate an attack.

710007

Error Message `%FTD-7-710007: NAT-T keepalive received from 86.1.161.1/1028 to outside:86:1.129.1/4500`

Explanation The Secure Firewall Threat Defense device received NAT-T keepalive messages.

Recommended Action None required.

711001

Error Message `%FTD-7-711001: debug_trace_msg`

Explanation You have entered the **logging debug-trace** command for the logging feature. When the **logging debug-trace** command is enabled, all debugging messages will be redirected to the message for processing. For security reasons, the message output must be encrypted or sent over a secure out-of-band network.

Recommended Action None required.

711002

Error Message `%FTD-4-711002: Task ran for elapsed_time msecs, process = process_name , PC = PC Tracebeback = traceback`

Explanation A process used the CPU for more than 100 milliseconds. This message is used for debugging CPU purposes, and can appear once every five seconds for each offending process.

- **PC**—Instruction pointer of the CPU hogging process
- **traceback**—Stack trace of the CPU hogging process, which can include up to 12 addresses

Recommended Action None required.

711003

Error Message `%FTD-7-711003: Unknown/Invalid interface identifier(vpifnum ) detected.`

Explanation An internal inconsistency that should not occur during normal operation has occurred. However, this message is not harmful if it rarely occurs. If it occurs frequently, it might be worthwhile debugging.

- *vpifnum* —The 32-bit value corresponding to the interface

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

711004

Error Message `%FTD-4-711004: Task ran for msec msec, Process = process_name , PC = pc , Call stack = call stack`

Explanation A process used the CPU for more than 100 milliseconds. This message is used for debugging CPU purposes, and can appear once every five seconds for each offending process.

- **msec—**Length of the detected CPU hog in milliseconds
- *process_name* —Name of the hogging process
- **pc**—Instruction pointer of the CPU hogging process
- **call stack**—Stack trace of the CPU hogging process, which can include up to 12 addresses

Recommended Action None required.

711005

Error Message `%FTD-5-711005: Traceback: call_stack`

Explanation An internal software error that should not occur has occurred. The device can usually recover from this error, and no harmful effect to the device results.

- *call_stack* —The EIPs of the call stack

Recommended Action Contact the Cisco TAC.

711006

Error Message `%FTD-7-711006: CPU profiling has started for n-samples samples. Reason: reason-string .`

Explanation CPU profiling has started.

- *n-samples* —The specified number of CPU profiling samples
- *reason-string* —The possible values are:

"CPU utilization passed *cpu-utilization* %"

"Process process-name CPU utilization passed *cpu-utilization* %"

Recommended Action "None specified"

Recommended Action Collect CPU profiling results and provide them to Cisco TAC.

713004

Error Message `%FTD-3-713004: device scheduled for reboot or shutdown, IKE key acquire message on interface interface num , for Peer IP_address ignored`

Explanation The Secure Firewall Threat Defense device has received an IKE packet from a remote entity trying to initiate a tunnel. Because the Secure Firewall Threat Defense device is scheduled for a reboot or shutdown, it does not allow any more tunnels to be established. The IKE packet is ignored and dropped.

Recommended Action None required.

713201

Error Message `%FTD-5-713201: Duplicate Phase Phase packet detected. Action`

Explanation The Secure Firewall Threat Defense device has received a duplicate of a previous Phase 1 or Phase 2 packet, and will transmit the last message. A network performance or connectivity issue may have occurred, in which the peer is not receiving sent packets in a timely manner.

- **Phase**—Phase 1 or 2
- **Action**—Retransmitting last packet, or No last packet to transmit.

Recommended Action Verify network performance or connectivity.

713202

Error Message `%FTD-6-713202: Duplicate IP_addr packet detected.`

Explanation The Secure Firewall Threat Defense device has received a duplicate first packet for a tunnel that the Secure Firewall Threat Defense device is already aware of and negotiating, which indicates that the Secure Firewall Threat Defense device probably received a retransmission of a packet from the peer.

- **IP_addr**—The IP address of the peer from which the duplicate first packet was received

Recommended Action None required, unless the connection attempt is failing. If this is the case, debug further and diagnose the problem.

713006

Error Message `%FTD-5-713006: Failed to obtain state for message Id message_number , Peer Address: IP_address`

Explanation The Secure Firewall Threat Defense device does not know about the received message ID. The message ID is used to identify a specific IKE Phase 2 negotiation. An error condition on the Secure Firewall Threat Defense device may have occurred, and may indicate that the two IKE peers are out-of-sync.

Recommended Action None required.

713008

Error Message `%FTD-3-713008: Key ID in ID payload too big for pre-shared IKE tunnel`

Explanation A key ID value was received in the ID payload, which was longer than the maximum allowed size of a group name for this IKE session using preshared keys authentication. This is an invalid value, and

the session is rejected. Note that the key ID specified would never work because a group name of that size cannot be created in the Secure Firewall Threat Defense device.

Recommended Action Make sure that the client peer (most likely an Altiga remote access client) specifies a valid group name. Notify the user to change the incorrect group name on the client. The current maximum length for a group name is 32 characters.

713009

Error Message `%FTD-3-713009: OU in DN in ID payload too big for Certs IKE tunnel`

Explanation An OU value in the DN was received in the ID payload, which was longer than the maximum allowed size of a group name for this IKE session using Certs authentication. This OU is skipped, and another OU or other criteria may find a matching group.

Recommended Action For the client to be able to use an OU to find a group in the Secure Firewall Threat Defense device, the group name must be a valid length. The current maximum length of a group name is 32 characters.

713010

Error Message `%FTD-5-713010: IKE area: failed to find centry for message Id` *message_number*

An attempt was made to locate a conn_entry (IKE phase 2 structure that corresponds to an IPsec SA) using the unique message ID, which failed. The internal structure was not found, which may occur if a session was terminated in a nonstandard way, but it is more likely that an internal error occurred.

If this problem persists, investigate the peer.

713012

Error Message `%FTD-3-713012: Unknown protocol (`*protocol*`). Not adding SA w/spi=SPI` *value*

Explanation An illegal or unsupported IPsec protocol has been received from the peer.

Recommended Action Check the ISAKMP Phase 2 configuration on the peer(s) to make sure it is compatible with the Secure Firewall Threat Defense device.

713014

Error Message `%FTD-3-713014: Unknown Domain of Interpretation (DOI):` *DOI value*

Explanation The ISAKMP DOI received from the peer is unsupported.

Recommended Action Check the ISAKMP DOI configuration on the peer.

713016

Error Message `%FTD-3-713016: Unknown identification type, Phase 1 or 2, Type` *ID_Type*

Explanation The ID received from the peer is unknown. The ID can be an unfamiliar valid ID or an invalid or corrupted ID.

Recommended Action Check the configuration on the headend and peer.

713017

Error Message `%FTD-3-713017: Identification type not supported, Phase 1 or 2, Type ID_Type`

Explanation The Phase 1 or Phase 2 ID received from the peer is legal, but not supported.

Recommended Action Check the configuration on the headend and peer.

713018

Error Message `%FTD-3-713018: Unknown ID type during find of group name for certs, Type ID_Type`

Explanation Tn internal software error has occurred.

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

713020

Error Message `%FTD-3-713020: No Group found by matching OU(s) from ID payload: OU_value`

Explanation Tn internal software error has occurred.

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

713022

Error Message `%FTD-3-713022: No Group found matching peer_ID or IP_address for Pre-shared key peer IP_address`

Explanation group exists in the group database with the same name as the value (key ID or IP address) specified by the peer.

Recommended Action Verify the configuration on the peer.

713024

Error Message `%FTD-7-713024: Group group IP ip Received local Proxy Host data in ID Payload: Address IP_address , Protocol protocol , Port port`

Explanation The Secure Firewall Threat Defense device has received the Phase 2 local proxy ID payload from the remote peer.

Recommended Action None required.

713025

Error Message `%FTD-7-713025: Received remote Proxy Host data in ID Payload: Address IP_address , Protocol protocol , Port port`

Explanation The Secure Firewall Threat Defense device has received the Phase 2 local proxy ID payload from the remote peer.

Recommended Action None required.

713028

Error Message `%FTD-7-713028: Received local Proxy Range data in ID Payload: Addresses IP_address - IP_address , Protocol protocol , Port port`

Explanation The Secure Firewall Threat Defense device has received the Phase 2 local proxy ID payload of the remote peer, which includes an IP address range.

Recommended Action None required.

713029

Error Message `%FTD-7-713029: Received remote Proxy Range data in ID Payload: Addresses IP_address - IP_address , Protocol protocol , Port port`

Explanation The Secure Firewall Threat Defense device has received the Phase 2 local proxy ID payload of the remote peer, which includes an IP address range.

Recommended Action None required.

713032

Error Message `%FTD-3-713032: Received invalid local Proxy Range IP_address - IP_address`

Explanation The local ID payload included the range ID type, and the specified low address was not less than the high address. A configuration problem may exist.

Recommended Action Check the configuration of ISAKMP Phase 2 parameters.

713033

Error Message `%FTD-3-713033:` Received invalid remote Proxy Range *IP_address - IP_address*

Explanation The remote ID payload included the range ID type, and the specified low address was not less than the high address. A configuration problem may exist.

Recommended Action Check the configuration of ISAKMP Phase 2 parameters.

713034

Error Message `%FTD-7-713034: Received local IP Proxy Subnet data in ID Payload: Address IP_address , Mask netmask , Protocol protocol , Port port`

Explanation The local IP proxy subnet data has been received in the Phase 2 ID payload.

Recommended Action None required.

713035

Error Message `%FTD-7-713035: Group group IP ip Received remote IP Proxy Subnet data in ID Payload: Address IP_address , Mask netmask , Protocol protocol , Port port`

Explanation The remote IP proxy subnet data has been received in the Phase 2 ID payload.

Recommended Action None required.

713039

Error Message `%FTD-7-713039: Send failure: Bytes (number ), Peer: IP_address`

Explanation An internal software error has occurred, and the ISAKMP packet cannot be transmitted.

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

713040

Error Message `%FTD-7-713040: Could not find connection entry and can not encrypt: msgid message_number`

Explanation An internal software error has occurred, and a Phase 2 data structure cannot be found.

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

713041

Error Message `%FTD-5-713041: IKE Initiator: new or rekey Phase 1 or 2, Intf interface_number , IKE Peer IP_address local Proxy Address IP_address , remote Proxy Address IP_address , Crypto map (crypto map tag )`

Explanation Secure Firewall Threat Defense device is negotiating a tunnel as the initiator.

Recommended Action None required.

713042

Error Message `%FTD-3-713042: IKE Initiator unable to find policy: Intf interface_number , Src: source_address , Dst: dest_address`

Explanation The IPsec fast path processed a packet that triggered IKE, but the IKE policy lookup failed. This error may be timing related. The ACLs that triggered IKE might have been deleted before IKE processed the initiation request. This problem will most likely correct itself.

Recommended Action If the condition persists, check the L2L configuration, paying special attention to the type of ACL associated with crypto maps.

713043

Error Message `%FTD-3-713043: Cookie/peer address IP_address session already in progress`

Explanation IKE has been triggered again while the original tunnel is in progress.

Recommended Action None required.

713048

Error Message `%FTD-3-713048: Error processing payload: Payload ID: id`

Explanation A packet has been received with a payload that cannot be processed.

Recommended Action If this problem persists, a misconfiguration may exist on the peer.

713049

Error Message `%FTD-5-713049: Security negotiation complete for tunnel_type type (group_name ) Initiator /Responder , Inbound SPI = SPI , Outbound SPI = SPI`

Explanation An IPsec tunnel has been started.

Recommended Action None required.

713050

Error Message `%FTD-5-713050: Connection terminated for peer IP_address . Reason: termination reason Remote Proxy IP_address , Local Proxy IP_address`

Explanation An IPsec tunnel has been terminated. Possible termination reasons include:

- IPsec SA Idle Timeout
- IPsec SA Max Time Exceeded
- Administrator Reset
- Administrator Reboot
- Administrator Shutdown
- Session Disconnected
- Session Error Terminated
- Peer Terminate

Recommended Action None required.

713052

Error Message `%FTD-7-713052: User (user ) authenticated.`

Explanation remote access user was authenticated.

Recommended Action None required.

713056

Error Message `%FTD-3-713056: Tunnel rejected: SA (SA_name ) not found for group (group_name )!`

Explanation The IPsec SA was not found.

Recommended Action If this is a remote access tunnel, check the group and user configuration, and verify that a tunnel group and group policy have been configured for the specific user group. For externally authenticated users and groups, check the returned authentication attributes.

713060

Error Message `%FTD-3-713060: Tunnel Rejected: User (user ) not member of group (group_name ), group-lock check failed.`

Explanation The user is configured for a different group than what was sent in the IPsec negotiation.

Recommended Action If you are using the Cisco VPN client and preshared keys, make sure that the group configured on the client is the same as the group associated with the user on the Secure Firewall Threat Defense device. If you are using digital certificates, the group is dictated either by the OU field of the certificate, or the user automatically defaults to the remote access default group.

713061

Error Message `%FTD-3-713061: Tunnel rejected: Crypto Map Policy not found for Src:source_address , Dst: dest_address !`

Explanation The Secure Firewall Threat Defense device was not able to find security policy information for the private networks or hosts indicated in the message. These networks or hosts were sent by the initiator and do not match any crypto ACLs at the Secure Firewall Threat Defense device. This is most likely a misconfiguration.

Recommended Action Check the protected network configuration in the crypto ACLs on both sides and make sure that the local net on the initiator is the remote net on the responder and vice-versa. Pay special attention to wildcard masks, and host addresses versus network addresses. Non-Cisco implementations may have the private addresses labeled as proxy addresses or red networks.

713062

Error Message `%FTD-3-713062: IKE Peer address same as our interface address IP_address`

Explanation The IP address configured as the IKE peer is the same as the IP address configured on one of the Secure Firewall Threat Defense IP interfaces.

Recommended Action Check the L2L and IP interface configurations.

713063

Error Message `%FTD-3-713063: IKE Peer address not configured for destination IP_address`

Explanation The IKE peer address is not configured for an L2L tunnel.

Recommended Action Check the L2L configuration.

713065

Error Message `%FTD-3-713065: IKE Remote Peer did not negotiate the following: proposal attribute`

Explanation An internal software error has occurred.

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

713066

Error Message `%FTD-7-713066: IKE Remote Peer configured for SA: SA_name`

Explanation The crypto policy settings of the peer have been configured.

Recommended Action None required.

713068

Error Message `%FTD-5-713068: Received non-routine Notify message: notify_type (notify_value)`

Explanation Notification messages that caused this event are not explicitly handled in the notify processing code.

Recommended Action Examine the specific reason to determine the action to take. Many notification messages indicate a configuration mismatch between the IKE peers.

713072

Error Message `%FTD-3-713072: Password for user (user ) too long, truncating to number characters`

Explanation The password of the user is too long.

Recommended Action Correct password lengths on the authentication server.

713073

Error Message `%FTD-5-713073: Responder forcing change of Phase 1 /Phase 2 rekeying duration from larger_value to smaller_value seconds`

Explanation Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the initiator is the lower one.

Recommended Action None required.

713074

Error Message `%FTD-5-713074: Responder forcing change of IPsec rekeying duration from larger_value to smaller_value Kbs`

Explanation Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the initiator is the lower one.

Recommended Action None required.

713075

Error Message `%FTD-5-713075: Overriding Initiator's IPsec rekeying duration from larger_value to smaller_value seconds`

Explanation Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the responder is the lower one.

Recommended Action None required.

713076

Error Message `%FTD-5-713076: Overriding Initiator's IPsec rekeying duration from larger_value to smaller_value Kbs`

Explanation Rekeying durations are always set to the lower of the values proposed by IKE peers. The value of the responder is the lower one.

Recommended Action None required.

713078

Error Message `%FTD-2-713078: Temp buffer for building mode config attributes exceeded: bufsize available_size , used value`

Explanation An internal software error has occurred while processing modecfg attributes.

Recommended Action Disable any unnecessary tunnel group attributes, or shorten any text messages that are excessively long. If the problem persists, contact the Cisco TAC.

713081

Error Message `%FTD-3-713081: Unsupported certificate encoding type encoding_type`

Explanation One of the loaded certificates is unreadable, and may be an unsupported encoding scheme.

Recommended Action Check the configuration of digital certificates and trustpoints.

713082

Error Message `%FTD-3-713082: Failed to retrieve identity certificate`

Explanation The identity certificate for this tunnel cannot be found.

Recommended Action Check the configuration of digital certificates and trustpoints.

713083

Error Message `%FTD-3-713083: Invalid certificate handle`

Explanation The identity certificate for this tunnel cannot be found.

Recommended Action Check the configuration of digital certificates and trustpoints.

713084

Error Message `%FTD-3-713084: Received invalid phase 1 port value (port ) in ID payload`

Explanation The port value received in the IKE phase 1 ID payload was incorrect. Acceptable values are 0 or 500 (ISAKMP is also known as IKE).

Recommended Action Make sure that a peer conforms to the IKE standards to avoid a network problem resulting in corrupted packets.

713085

Error Message `%FTD-3-713085: Received invalid phase 1 protocol (protocol ) in ID payload`

Explanation The protocol value received in the IKE phase 1 ID payload was incorrect. Acceptable values are 0 or 17 (UDP).

Recommended Action Make sure that a peer conforms to the IKE standards to avoid a network problem resulting in corrupted packets.

713086

Error Message `%FTD-3-713086: Received unexpected Certificate payload Possible invalid Auth Method (Auth method (auth numerical value))`

Explanation A certificate payload was received, but our internal certificate handle indicates that we do not have an identity certificate. The certificate handle was not obtained through a normal enrollment method. One likely reason this can happen is that the authentication method is not made through RSA or DSS signatures, although the IKE SA negotiation should fail if each side is misconfigured.

Recommended Action Check the trustpoint and ISAKMP configuration settings on the Secure Firewall Threat Defense device and its peer.

713088

Error Message `%FTD-3-713088: Set Cert filehandle failure: no IPsec SA in group group_name`

Explanation The tunnel group cannot be found, based on the digital certificate information.

Recommended Action Verify that the tunnel group is set up correctly to handle the certificate information of the peer.

713092

Error Message `%FTD-5-713092: Failure during phase 1 rekeying attempt due to collision`

Explanation An internal software error has occurred. This is often a benign event.

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

713094

Error Message `%FTD-7-713094: Cert validation failure: handle invalid for Main /Aggressive Mode Initiator /Responder !`

Explanation An internal software error has occurred.

Recommended Action You may have to reenroll the trustpoint. If the problem persists, contact the Cisco TAC.

713098

Error Message `%FTD-3-713098: Aborting: No identity cert specified in IPsec SA (SA_name )!`

Explanation An attempt was made to establish a certificate-based IKE session, but no identity certificate has been specified in the crypto policy.

Recommended Action Specify the identity certificate or trustpoint that you want to transmit to peers.

713099

Error Message `%FTD-7-713099: Tunnel Rejected: Received NONCE length number is out of range!`

Explanation An internal software error has occurred.

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

713102

Error Message `%FTD-3-713102: Phase 1 ID Data length number too long - reject tunnel!`

Explanation IKE has received an ID payload that includes an identification data field of 2 K or larger.

Recommended Action None required.

713103

Error Message `%FTD-7-713103: Invalid (NULL) secret key detected while computing hash`

Explanation An internal software error has occurred.

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

713104

Error Message `%FTD-7-713104: Attempt to get Phase 1 ID data failed while hash computation`

Explanation An internal software error has occurred.

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

713105

Error Message `%FTD-3-713105: Zero length data in ID payload received during phase 1 or 2 processing`

Explanation A peer sent an ID payload without including any ID data, which is invalid.

Recommended Action Check the configuration of the peer.

713107

Error Message `%FTD-3-713107: IP_Address request attempt failed!`

Explanation An internal software error has occurred.

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

713109

Error Message `%FTD-3-713109: Unable to process the received peer certificate`

Explanation The Secure Firewall Threat Defense device was unable to process the certificate received from the remote peer, which can occur if the certificate data was malformed (for example, if the public key size is larger than 4096 bits) or if the data in the certificate cannot be stored by the Secure Firewall Threat Defense device.

Recommended Action Try to reestablish the connection using a different certificate on the remote peer.

Messages 713112 to 714011

This section includes messages from 713112 to 714011.

713112

Error Message `%FTD-3-713112: Failed to process CONNECTED notify (SPI` *`SPI_value`* `)!`

Explanation The Secure Firewall Threat Defense device was unable to successfully process the notification payload that included the CONNECTED notify type. This may occur if the IKE phase 2 structure cannot be found using the SPI to locate it, or the commit bit had not been set in the received ISAKMP header. The latter case may indicate a nonconforming IKE peer.

Recommended Action If the problem persists, check the configuration of the peer and/or disable commit bit processing.

713113

Error Message `%FTD-7-713113: Deleting IKE SA with associated IPsec connection entries. IKE peer:` *`IP_address`* `, SA address:` *`internal_SA_address`* `, tunnel count:` *`count`*

Explanation An IKE SA is being deleted with a nonzero tunnel count, which means that either the IKE SA tunnel count has lost synchronization with the associated connection entries or the associated connection cookie fields for the entries have lost synchronization with the cookie fields of the IKE SA to which the connection entry points. If this occurs, the IKE SA and its associated data structures will not be freed, so that the entries that may point to it will not have a stale pointer.

Recommended Action None required. Error recovery is built-in.

713114

Error Message `%FTD-7-713114: Connection entry (conn entry internal address) points to IKE SA (SA_internal_address ) for peer IP_address , but cookies don't match`

Explanation An internal software error has occurred.

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

713115

Error Message `%FTD-5-713115: Client rejected NAT enabled IPsec request, falling back to standard IPsec`

Explanation The client rejected an attempt by the Secure Firewall Threat Defense device to use IPsec over UDP. IPsec over UDP is used to allow multiple clients to establish simultaneous tunnels to the Secure Firewall Threat Defense device through a NAT device. The client may have rejected the request, either because it does not support this feature or because it is configured not to use it.

Recommended Action Verify the configuration on the headend and peer.

713117

Error Message `%FTD-7-713117: Received Invalid SPI notify (SPI SPI_Value )!`

Explanation The IPsec SA identified by the SPI value is no longer active on the remote peer, which might indicate that the remote peer has rebooted or been reset.

Recommended Action This problem should correct itself once DPDs recognize that the peer no longer has the appropriate SAs established. If DPD is not enabled, this may require you to manually reestablish the affected tunnel.

713118

Error Message `%FTD-3-713118: Detected invalid Diffie-Helmann group_descriptor group_number , in IKE area`

Explanation The **group_descriptor** field included an unsupported value. Currently we support only groups 1, 2, 5, and 7. In the case of a centry, the **group_descriptor** field may also be set to 0 to indicate that perfect forward secrecy is disabled.

Recommended Action Check the peer Diffie-Hellman configuration.

713119

Error Message `%FTD-5-713119: Group group IP ip PHASE 1 COMPLETED`

Explanation IKE Phase 1 has completed successfully.

Recommended Action None required.

713120

Error Message `%FTD-5-713120: PHASE 2 COMPLETED (msgid=msg_id )`

Explanation IKE Phase 2 has completed successfully.

Recommended Action None required.

713121

Error Message `%FTD-7-713121: Keep-alive type for this connection: keepalive_type`

Explanation The type of keepalive mechanism that is being used for this tunnel is specified.

Recommended Action None required.

713122

Error Message `%FTD-3-713122: Keep-alives configured keepalive_type but peer IP_address support keep-alives (type = keepalive_type )`

Explanation Keepalives were configured on or off for this device, but the IKE peer does or does not support keepalives.

Recommended Action No action is required if this configuration is intentional. If it is not intentional, change the keepalive configuration on both devices.

713123

Error Message `%FTD-3-713123: IKE lost contact with remote peer, deleting connection (keepalive type: keepalive_type )`

Explanation The remote IKE peer did not respond to keepalives within the expected window of time, so the connection to the IKE peer was terminated. The message includes the keepalive mechanism used.

Recommended Action None required.

713124

Error Message `%FTD-3-713124: Received DPD sequence number rcv_sequence_# in DPD Action, description expected seq #`

Explanation The remote IKE peer sent a DPD with a sequence number that did not match the expected sequence number. The packet is discarded. This might indicate a packet loss problem with the network.

Recommended Action None required.

713127

Error Message `%FTD-3-713127: Xauth required but selected Proposal does not support xauth, Check priorities of ike xauth proposals in ike proposal list`

Explanation The peer wanted to perform a XAUTH, but the Secure Firewall Threat Defense device did not choose the XAUTH IKE proposal.

Recommended Action Check the priorities of the IKE xauth proposals in the IKE proposal list.

713128

Error Message `%FTD-6-713128: Connection attempt to VCPIP redirected to VCA peer IP_address via load balancing`

Explanation A connection attempt has been made to the VCPIP and has been redirected to a less loaded peer using load balancing.

Recommended Action None required.

713129

Error Message `%FTD-3-713129: Received unexpected Transaction Exchange payload type: payload_id`

Explanation An unexpected payload has been received during XAUTH or Mode Cfg, which may indicate that the two peers are out-of-sync, that the XAUTH or Mode Cfg versions do not match, or that the remote peer is not complying with the appropriate RFCs.

Recommended Action Verify the configuration between peers.

713130

Error Message `%FTD-5-713130: Received unsupported transaction mode attribute: attribute id`

Explanation The device received a request for a valid transaction mode attribute (XAUTH or Mode Cfg) that is currently not supported. This is generally a benign condition.

Recommended Action None required.

713131

Error Message `%FTD-5-713131: Received unknown transaction mode attribute: attribute_id`

Explanation The Secure Firewall Threat Defense device has received a request for a transaction mode attribute (XAUTH or Mode Cfg) that is outside the range of known attributes. The attribute may be valid but only supported in later versions of configuration mode, or the peer may be sending an illegal or proprietary value. This should not cause connectivity problems, but may affect the functionality of the peer.

Recommended Action None required.

713132

Error Message `%FTD-3-713132: Cannot obtain an IP_address for remote peer`

Explanation A request for an IP address for a remote access client from the internal utility that provides these addresses cannot be satisfied.

Recommended Action Check the configuration of IP address assignment methods.

713133

Error Message `%FTD-3-713133: Mismatch: Overriding phase 2 DH Group(DH group DH group_id ) with phase 1 group(DH group DH group_number`

Explanation The configured Phase 2 PFS Group differed from the DH group that was negotiated for Phase 1.

Recommended Action None required.

713134

Error Message `%FTD-3-713134: Mismatch: P1 Authentication algorithm in the crypto map entry different from negotiated algorithm for the L2L connection`

Explanation The configured LAN-to-LAN proposal is different from the one accepted for the LAN-to-LAN connection. Depending on which side is the initiator, different proposals will be used.

Recommended Action None required.

713135

Error Message `%FTD-5-713135: message received, redirecting tunnel to IP_address .`

Explanation The tunnel is being redirected because of load balancing on the remote Secure Firewall Threat Defense device. A REDIRECT_CONNECTION notify packet was received.

Recommended Action None required.

713136

Error Message `%FTD-5-713136: IKE session establishment timed out [IKE_state_name ], aborting!`

Explanation The Reaper has detected an Secure Firewall Threat Defense device stuck in an inactive state. The Reaper will try to remove the inactive Secure Firewall Threat Defense device.

Recommended Action None required.

713137

Error Message `%FTD-5-713137: Reaper overriding refCnt [ref_count] and tunnelCnt [tunnel_count] -- deleting SA!`

Explanation An internal software error has occurred.

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

713138

Error Message `%FTD-3-713138: Group group_name not found and BASE GROUP default preshared key not configured`

Explanation No group exists in the group database with the same name as the IP address of the peer. In Main Mode, the Secure Firewall Threat Defense device will fall back and try to use the default preshared key configured in one of the default groups. The default preshared key is not configured.

Recommended Action Verify the configuration of the preshared keys.

713139

Error Message `%FTD-5-713139: group_name not found, using BASE GROUP default preshared key`

Explanation No tunnel group exists in the group database with the same name as the IP address of the peer. In Main Mode, the Secure Firewall Threat Defense device will fall back and use the default preshared key configured in the default group.

Recommended Action None required.

713140

Error Message `%FTD-3-713140: Split Tunneling Policy requires network list but none configured`

Explanation The split tunneling policy is set to either split tunneling or to allow local LAN access. A split tunneling ACL must be defined to represent the information required by the VPN client.

Recommended Action Check the configuration of the ACLs.

713141

Error Message `%FTD-3-713141: Client-reported firewall does not match configured firewall: action tunnel. Received -- Vendor: vendor(id) , Product product(id) , Caps: capability_value . Expected -- Vendor: vendor(id) , Product: product(id) , Caps: capability_value`

Explanation The Secure Firewall Threat Defense device installed on the client does not match the configured required Secure Firewall Threat Defense device. This message lists the actual and expected values, and whether the tunnel is terminated or allowed.

Recommended Action You may need to install a different personal Secure Firewall Threat Defense device on the client or change the configuration on the Secure Firewall Threat Defense device.

713142

Error Message `%FTD-3-713142: Client did not report firewall in use, but there is a configured firewall: action tunnel. Expected -- Vendor: vendor(id) , Product product(id) , Caps: capability_value`

Explanation The client did not report an Secure Firewall Threat Defense device in use using ModeCfg, but one is required. The event lists the expected values and whether the tunnel is terminated or allowed. Note that the number following the product string is a bitmask of all of the allowed products.

Recommended Action You may need to install a different personal Secure Firewall Threat Defense device on the client or change the configuration on the Secure Firewall Threat Defense device.

713143

Error Message `%FTD-7-713143: Processing firewall record. Vendor: vendor(id) , Product: product(id) , Caps: capability_value , Version Number: version_number , Version String: version_text`

Explanation Debugging information about the Secure Firewall Threat Defense device installed on the client appears.

Recommended Action None required.

713144

Error Message `%FTD-5-713144: Ignoring received malformed firewall record; reason - error_reason TLV type attribute_value correction`

Explanation Bad Secure Firewall Threat Defense device information was received from the client.

Recommended Action Check the personal configuration on the client and the Secure Firewall Threat Defense device.

713145

Error Message `%FTD-6-713145: Detected Hardware Client in network extension mode, adding static route for address: IP_address , mask: netmask`

Explanation A tunnel with a hardware client in network extension mode has been negotiated, and a static route is being added for the private network behind the hardware client. This configuration enables the Secure Firewall Threat Defense device to make the remote network known to all the routers on the private side of the headend.

Recommended Action None required.

713146

Error Message `%FTD-3-713146: Could not add route for Hardware Client in network extension mode, address: IP_address , mask: netmask`

Explanation An internal software error has occurred. A tunnel with a hardware client in network extension mode has been negotiated, and an attempt to add the static route for the private network behind the hardware client failed. The routing table may be full, or a possible addressing error has occurred.

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

713147

Error Message `%FTD-6-713147: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address , mask: netmask`

Explanation A tunnel to a hardware client in network extension mode is being removed, and the static route for the private network is being deleted behind the hardware client.

Recommended Action None required.

713148

Error Message `%FTD-5-713148: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address , mask: netmask`

Explanation While a tunnel to a hardware client in network extension mode was being removed, a route to the private network behind the hardware client cannot be deleted. This might indicate an addressing or software problem.

Recommended Action Check the routing table to ensure that the route is not there. If it is, it may have to be removed manually, but only if the tunnel to the hardware client has been completely removed.

713149

Error Message `%FTD-3-713149: Hardware client security attribute attribute_name was enabled but not requested.`

Explanation The headend Secure Firewall Threat Defense device has the specified hardware client security attribute enabled, but the attribute was not requested by the VPN 3002 hardware client.

Recommended Action Check the configuration on the hardware client.

713152

Error Message `%FTD-3-713152: Unable to obtain any rules from filter ACL_tag to send to client for CPP, terminating connection.`

Explanation The client is required to use CPP to provision its Secure Firewall Threat Defense device, but the headend device was unable to obtain any ACLs to send to the client. This is probably due to a misconfiguration.

Recommended Action Check the ACLs specified for CPP in the group policy for the client.

713154

Error Message `%FTD-4-713154: DNS lookup for peer_description Server [server_name ] failed!`

Explanation This message appears when a DNS lookup for the specified server has not been resolved.

Recommended Action Check the DNS server configuration on the Secure Firewall Threat Defense device. Also check the DNS server to ensure that it is operational and has hostname to IP address mapping.

713155

Error Message `%FTD-5-713155: DNS lookup for Primary VPN Server [server_name ] successfully resolved after a previous failure. Resetting any Backup Server init.`

Explanation A previous DNS lookup failure for the primary server might have caused the Secure Firewall Threat Defense device to initialize a backup peer. This message indicates that a later DNS lookup on the primary server finally succeeded and is resetting any backup server initializations. A tunnel initiated after this point will be aimed at the primary server.

Recommended Action None required.

713156

Error Message `%FTD-5-713156: Initializing Backup Server [server_name or IP_address ]`

Explanation The client is failing over to a backup server, or a failed DNS lookup for the primary server caused the Secure Firewall Threat Defense device to initialize a backup server. A tunnel initiated after this point will be aimed at the specified backup server.

Recommended Action None required.

713157

Error Message `%FTD-4-713157: Timed out on initial contact to server [server_name or IP_address ] Tunnel could not be established.`

Explanation The client tried to initiate a tunnel by sending out IKE MSG1, but did not receive a response from the Secure Firewall Threat Defense device on the other end. If backup servers are available, the client will attempt to connect to one of them.

Recommended Action Verify connectivity to the headend Secure Firewall Threat Defense device.

713158

Error Message `%FTD-5-713158: Client rejected NAT enabled IPsec Over UDP request, falling back to IPsec Over TCP`

Explanation The client is configured to use IPsec over TCP. The client rejected the attempt by the Secure Firewall Threat Defense device to use IPsec over UDP.

Recommended Action If TCP is desired, no action is required. Otherwise, check the client configuration.

713159

Error Message `%FTD-3-713159: TCP Connection to Firewall Server has been lost, restricted tunnels are now allowed full network access`

Explanation The TCP connection to the Secure Firewall Threat Defense server was lost for a certain reason, such as the server has rebooted, a network problem has occurred, or an SSL mismatch has occurred.

Recommended Action If the server connection was lost after the initial connection was made, then the server and network connections must be checked. If the initial connection is lost immediately, this might indicate an SSL authentication problem.

713160

Error Message `%FTD-7-713160: Remote user (session Id - id ) has been granted access by the Firewall Server`

Explanation Normal authentication of the remote user to the Secure Firewall Threat Defense server has occurred.

Recommended Action None required.

713161

Error Message `%FTD-3-713161: Remote user (session Id - id ) network access has been restricted by the Firewall Server`

Explanation The Secure Firewall Threat Defense server has sent the Secure Firewall Threat Defense device a message indicating that this user must be restricted. There are several reasons for this, including Secure Firewall Threat Defense software upgrades or changes in permissions. The Secure Firewall Threat Defense server will transition the user back into full access mode as soon as the operation has been completed.

Recommended Action No action is required unless the user is never transitioned back into full access state. If this does not happen, refer to the Secure Firewall Threat Defense server for more information on the operation that is being performed and the state of the Secure Firewall Threat Defense software running on the remote machine.

713162

Error Message `%FTD-3-713162: Remote user (session Id - id ) has been rejected by the Firewall Server`

Explanation The Secure Firewall Threat Defense server has rejected this user.

Recommended Action Check the policy information on the Secure Firewall Threat Defense server to make sure that the user is configured correctly.

713163

Error Message `%FTD-3-713163: Remote user (session Id - id ) has been terminated by the Firewall Server`

Explanation The Secure Firewall Threat Defense server has terminated this user session, which can occur if the integrity agent stops running on the client machine or if the security policy is modified by the remote user in any way.

Recommended Action Verify that the Secure Firewall Threat Defense software on the client machine is still running and that the policy is correct.

713164

Error Message `%FTD-7-713164: The Firewall Server has requested a list of active user sessions`

Explanation The Secure Firewall Threat Defense server will request the session information if it detects that it has stale data or if it loses the session data (because of a reboot).

Recommended Action None required.

713165

Error Message `%FTD-3-713165: Client IKE Auth mode differs from the group's configured Auth mode`

Explanation The client negotiated with preshared keys while its tunnel group points to a policy that is configured to use digital certificates.

Recommended Action Check the client configuration.

713166

Error Message `%FTD-3-713166: Headend security gateway has failed our user authentication attempt - check configured username and password`

Explanation The hardware client has failed extended authentication. This is most likely a username and password problem or an authentication server issue.

Recommended Action Verify that the configured username and password values on each side match. Also verify that the authentication server at the headend is operational.

713167

Error Message `%FTD-3-713167: Remote peer has failed user authentication - check configured username and password`

Explanation The remote user has failed to extend authentication. This is most likely a username or password problem, or an authentication server issue.

Recommended Action Verify that the configured username and password values on each side match. Also verify that the authentication server being used to authenticate the remote user is operational.

713168

Error Message `%FTD-3-713168: Re-auth enabled, but tunnel must be authenticated interactively!`

Explanation Reauthentication on rekeying has been enabled, but the tunnel authentication requires manual intervention.

Recommended Action If manual intervention is desired, no action is required. Otherwise, check the interactive authentication configuration.

713169

Error Message `%FTD-7-713169: IKE Received delete for rekeyed SA IKE peer: IP_address , SA address: internal_SA_address , tunnelCnt: tunnel_count`

Explanation IKE has received a delete message from the remote peer to delete its old IKE SA after a rekey has completed.

Recommended Action None required.

713170

Error Message `%FTD-7-713170: Group group IP ip IKE Received delete for rekeyed centry IKE peer: IP_address , centry address: internal_address , msgid: id`

Explanation IKE has received a delete message from the remote peer to delete its old centry after Phase 2 rekeying is completed.

Recommended Action None required.

713171

Error Message `%FTD-7-713171: NAT-Traversal sending NAT-Original-Address payload`

Explanation UDP-Encapsulated-Transport was either proposed or selected during Phase 2. Send this payload for NAT-Traversal in this case.

Recommended Action None required.

713172

Error Message `%FTD-6-713172: Automatic NAT Detection Status: Remote end` *`is |is not`* `behind a NAT device This end` *`is |is not`* `behind a NAT device`

Explanation NAT-Traversal auto-detected NAT.

Recommended Action None required.

713174

Error Message `%FTD-3-713174: Hardware Client connection rejected! Network Extension Mode is not allowed for this group!`

Explanation A hardware client is attempting to tunnel in using network extension mode, but network extension mode is not allowed.

Recommended Action Verify the configuration of the network extension mode versus PAT mode.

713176

Error Message `%FTD-2-713176:` *`Device_type`* `memory resources are critical, IKE key acquire message on interface` *`interface_number`* `, for Peer` *`IP_address`* `ignored`

Explanation The Secure Firewall Threat Defense device is processing data intended to trigger an IPsec tunnel to the indicated peer. Because memory resources are at a critical state, it is not initiating any more tunnels. The data packet has been ignored and dropped.

Recommended Action If condition persists, verify that the Secure Firewall Threat Defense device is efficiently configured. An Secure Firewall Threat Defense device with increased memory may be required for this application.

713177

Error Message `%FTD-6-713177: Received remote Proxy Host FQDN in ID Payload: Host Name:` *`host_name`* `Address` *`IP_address`* `, Protocol` *`protocol`* `, Port` *`port`*

Explanation A Phase 2 ID payload containing an FQDN has been received from the peer.

Recommended Action None required.

713178

Error Message `%FTD-5-713178: IKE Initiator received a packet from its peer without a Responder cookie`

Explanation An internal software error has occurred.

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

713179

Error Message `%FTD-5-713179: IKE AM Initiator received a packet from its peer without a` *`payload_type`* `payload`

Explanation An internal software error has occurred.

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

713182

Error Message `%FTD-3-713182: IKE could not recognize the version of the client! IPsec Fragmentation Policy will be ignored for this connection!`

Explanation An internal software error has occurred.

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

713184

Error Message `%FTD-6-713184: Client Type:` *`Client_type`* `Client Application Version:` *`Application_version_string`*

Explanation The client operating system and application version appear. If the information is not available, then N/A will be indicated.

Recommended Action None required.

713185

Error Message `%FTD-3-713185: Error: Username too long - connection aborted`

Explanation The client returned an invalid length username, and the tunnel was torn down.

Recommended Action Check the username and make changes, if necessary.

713186

Error Message `%FTD-3-713186: Invalid secondary domain name list received from the authentication server. List Received:` *`list_text`* `Character` *`index`* `(`*`value`*` ) is illegal`

Explanation An invalid secondary domain name list was received from an external RADIUS authentication server. When split tunnelling is used, this list identifies the domains that the client should resolve through the tunnel.

Recommended Action Correct the specification of the Secondary-Domain-Name-List attribute (vendor-specific attribute 29) on the RADIUS server. The list must be specified as a comma-delimited list of domain names. Domain names may include only alphanumeric characters, a hyphen, an underscore, and a period.

713187

Error Message `%FTD-7-713187: Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy IKE peer address: IP_address , Remote peer address: IP_address`

Explanation The IKE peer that is attempting to bring up this tunnel is not the one that is configured in the ISAKMP configuration that is bound to the received remote subnet.

Recommended Action Verify that L2L settings are correct on the headend and peer.

713189

Error Message `%FTD-3-713189: Attempted to assign network or broadcast IP_address , removing ( IP_address ) from pool.`

Explanation The IP address from the pool is either the network or broadcast address for this subnet. This address will be marked as unavailable.

Recommended Action This error is generally benign, but the IP address pool configuration should be checked.

713190

Error Message `%FTD-7-713190: Got bad refCnt ( ref_count_value ) assigning IP_address ( IP_address )`

Explanation The reference counter for this SA is invalid.

Recommended Action None required.

713191

Error Message `%FTD-3-713191: Maximum concurrent IKE negotiations exceeded!`

Explanation To minimize CPU-intensive cryptographic calculations, the Secure Firewall Threat Defense device limits the number of connection negotiations in progress. When a new negotiation is requested and the Secure Firewall Threat Defense device is already at its limit, the new negotiation is rejected. When an existing connection negotiation completes, new connection negotiation will again be permitted.

Recommended Action See the **crypto ikev1 limit max-in-negotiation-sa** command. Increasing the limit can degrade performance..

713193

Error Message `%FTD-3-713193: Received packet with missing payload, Expected payload: payload_id`

Explanation The Secure Firewall Threat Defense device received an encrypted or unencrypted packet of the specified exchange type that had one or more missing payloads. This usually indicates a problem on the peer.

Recommended Action Verify that the peer is sending valid IKE messages.

713194

Error Message `%FTD-3-713194: Sending IKE |IPsec Delete With Reason message: termination_reason`

Explanation A delete message with a termination reason code was received.

Recommended Action None required.

713195

Error Message `%FTD-3-713195: Tunnel rejected: Originate-Only: Cannot accept incoming tunnel yet!`

Explanation The originate-only peer can accept incoming connections only after it brings up the first P2 tunnel. At that point, data from either direction can initiate additional Phase 2 tunnels.

Recommended Action If a different behavior is desired, the originate-only configuration needs to be revised.

713196

Error Message `%FTD-5-713196: Remote L2L Peer IP_address initiated a tunnel with same outer and inner addresses. Peer could be Originate Only - Possible misconfiguration!`

Explanation The remote L2L peer has initiated a public-public tunnel. The remote L2L peer expects a response from the peer at the other end, but does not receive one, because of a possible misconfiguration.

Recommended Action Check the L2L configuration on both sides.

713197

Error Message `%FTD-5-713197: The configured Confidence Interval of number seconds is invalid for this tunnel_type connection. Enforcing the second default.`

Explanation The configured confidence interval in the group is outside of the valid range.

Recommended Action Check the confidence setting in the group to make sure it is within the valid range.

713198

Error Message `%FTD-3-713198: User Authorization failed: user User authorization failed. Username could not be found in the certificate`

Explanation A reason string that states that a username cannot be found in the certificate appears.

Recommended Action Check the group configuration and client authorization.

713199

Error Message `%FTD-5-713199: Reaper corrected an SA that has not decremented the concurrent IKE negotiations counter ( counter_value )!`

Explanation The Reaper corrected an internal software error.

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

713203

Error Message `%FTD-3-713203: IKE Receiver: Error reading from socket.`

Explanation An error occurred while reading a received IKE packet. This is generally an internal error and might indicate a software problem.

Recommended Action This problem is usually benign, and the system will correct itself. If the problem persists, contact the Cisco TAC.

713204

Error Message `%FTD-7-713204: Adding static route for client address: IP_address`

Explanation This message indicates that a route to the peer-assigned address or to the networks protected by a hardware client was added to the routing table.

Recommended Action None required.

713205

Error Message `%FTD-3-713205: Could not add static route for client address: IP_address`

Explanation An attempt to add a route to the client-assigned address or to the networks protected by a hardware client failed. This might indicate duplicate routes in the routing table or a corrupted network address. The duplicate routes might be caused by routes that were not cleaned up correctly or by having multiple clients sharing networks or addresses.

Recommended Action Check the IP local pool configuration as well as any other IP address-assigning mechanism being used (for example, DHCP or RADIUS). Make sure that routes are being cleared from the routing table. Also check the configuration of networks and/or addresses on the peer.

713206

Error Message `%FTD-3-713206: Tunnel Rejected: Conflicting protocols specified by tunnel-group and group-policy`

Explanation A tunnel was dropped because the allowed tunnel specified in the group policy was different from the allowed tunnel in the tunnel group configuration.

Recommended Action Check the tunnel group and group policy configuration.

713207

Error Message `%FTD-4-713207: Terminating connection: IKE Initiator and tunnel group specifies L2TP Over IPSec`

Explanation This syslog is displayed for ikev1 while terminating the connection if GW is an initiator and tunnel group type is L2TP over IPSEC.

Recommended Action None required.

713208

Error Message `%FTD-3-713208: Cannot create dynamic rule for Backup L2L entry rule` *`rule_id`*

Explanation A failure occurred in creating the ACLs that trigger IKE and allow IPsec data to be processed properly. The failure was specific to the backup L2L configuration, which may indicate a configuration error, a capacity error, or an internal software error.

Recommended Action If the Secure Firewall Threat Defense device is running the maximum number of connections and VPN tunnels, there may be a memory issue. If not, check the backup L2L and crypto map configurations, specifically the ACLs associated with the crypto maps.

713209

Error Message `%FTD-3-713209: Cannot delete dynamic rule for Backup L2L entry rule id`

Explanation A failure occurred in deleting the ACLs that trigger IKE and allow IPsec data to be processed correctly. The failure was specific to the backup L2L configuration. This may indicate an internal software error.

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

713210

Error Message `%FTD-3-713210: Cannot create dynamic map for Backup L2L entry rule_id`

Explanation A failure occurred in creating a run-time instance of the dynamic crypto map associated with backup L2L configuration. This may indicate a configuration error, a capacity error, or an internal software error.

Recommended Action If the Secure Firewall Threat Defense device is running the maximum number of connections and VPN tunnels, there may be a memory issue. If not, check the backup L2L and crypto map configurations, and specifically the ACLs associated with the crypto maps.

713212

Error Message `%FTD-3-713212:` Could not add route for L2L peer coming in on a dynamic map. address: *IP_address* , mask: *netmask*

Explanation The Secure Firewall Threat Defense device failed while attempting to add a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. This might indicate duplicate routes, a full routing table, or a failure of the Secure Firewall Threat Defense device to remove previously used routes.

Check the routing table to make sure there is room for additional routes and that obsolete routes are not present. If the table is full or includes obsolete routes, remove the routes and try again. If the problem persists, contact the Cisco TAC.

713213

Error Message `%FTD-6-713213: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address , mask: netmask`

Explanation The Secure Firewall Threat Defense device is deleting a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

Recommended Action None required.

713214

Error Message `%FTD-3-713214: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address , mask: netmask`

Explanation The Secure Firewall Threat Defense device experienced a failure while deleting a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. The route may have already been deleted,or an internal software error has occurred.

Recommended Action If the route has already been deleted, the condition is benign and the device will function normally. If the problem persists or can be linked to routing issues over VPN tunnels, then check the routing and addressing portions of the VPN L2L configuration. Check the reverse route injection and the ACLs associated with the appropriate crypto map. If the problem persists, contact the Cisco TAC.

713215

Error Message `%FTD-6-713215: No match against Client Type and Version rules. Client: type version is /is not allowed by default`

Explanation The client type and the version of a client did not match any of the rules configured on the Secure Firewall Threat Defense device. The default action appears.

Recommended Action Determine what the default action and deployment requirements are, and make the applicable changes.

713216

Error Message `%FTD-5-713216: Rule: action [Client type]: version Client: type version allowed/not allowed`

Explanation The client type and the version of a client have matched one of the rules. The results of the match and the rule are displayed.

Recommended Action Determine what the deployment requirements are, and make the appropriate changes.

713217

Error Message `%FTD-3-713217: Skipping unrecognized rule: action: action client type: client_type client version: client_version`

Explanation A malformed client type and version rule exist. The required format is action client type | client version action. Either permit or deny client type and client version are displayed under Session Management. Only one wildcard per parameter (*) is supported.

Recommended Action Correct the rule.

713218

Error Message `%FTD-3-713218: Tunnel Rejected: Client Type or Version not allowed.`

The client was denied access according to the configured rules.

None required.

713219

Error Message `%FTD-6-713219: Queuing KEY-ACQUIRE messages to be processed when P1 SA is complete.`

Explanation Phase 2 messages are being enqueued after Phase 1 completes.

Recommended Action None required.

713220

Error Message `%FTD-6-713220: De-queuing KEY-ACQUIRE messages that were left pending.`

Explanation Queued Phase 2 messages are being processed.

Recommended Action None required.

713221

Error Message `%FTD-7-713221: Static Crypto Map check, checking map = crypto_map_tag , seq = seq_number...`

Explanation The Secure Firewall Threat Defense device is iterating through the crypto maps looking for configuration information.

Recommended Action None required.

713222

Error Message `%FTD-7-713222: Group group Username username IP ip  Static Crypto Map check, map = crypto_map_tag , seq = seq_number , ACL does not match proxy IDs src:source_address dst:dest_address`

Explanation While iterating through the configured crypto maps, the Secure Firewall Threat Defense device cannot match any of the associated ACLs. This generally means that an ACL was misconfigured.

Recommended Action Check the ACLs associated with this tunnel peer, and make sure that they specify the appropriate private networks from both sides of the VPN tunnel.

713223

Error Message `%FTD-7-713223: Static Crypto Map check, map = crypto_map_tag , seq = seq_number , no ACL configured`

Explanation The crypto map associated with this peer is not linked to an ACL.

Recommended Action Make sure an ACL associated with this crypto map exists, and that the ACL includes the appropriate private addresses or network from both sides of the VPN tunnel.

713224

Error Message `%FTD-7-713224: Static Crypto Map Check by-passed: Crypto map entry incomplete!`

Explanation The crypto map associated with this VPN tunnel is missing critical information.

Recommended Action Verify that the crypto map is configured correctly with both the VPN peer, a transform set, and an associated ACL.

713225

Error Message `%FTD-7-713225: [IKEv1], Static Crypto Map check, map map_name , seq = sequence_number is a successful match`

Explanation The Secure Firewall Threat Defense device found a valid matching crypto map for this VPN tunnel.

Recommended Action None required.

713226

Error Message `%FTD-3-713226: Connection failed with peer IP_address , no trust-point defined in tunnel-group tunnel_group`

Explanation When the device is configured to use digital certificates, a trustpoint must be specified in the configuration. When the trustpoint is missing from the configuration, this message is generated to flag an error.

- **IP_address**—IP address of the peer
- **tunnel_group**—Tunnel group for which the trustpoint was missing in the configuration

Recommended Action The administrator of the device has to specify a trustpoint in the configuration.

713227

Error Message `%FTD-3-713227: Rejecting new IPsec SA negotiation for peer Peer_address . A negotiation was already in progress for local Proxy Local_address /Local_netmask , remote Proxy Remote_address /Remote_netmask`

Explanation When establishing a Phase SA, the Secure Firewall Threat Defense device will reject a new Phase 2 matching this proxy.

Recommended Action None required.

713228

Error Message `%FTD-6-713228: Group = group , Username = uname , IP = remote_IP_address Assigned private IP address assigned_private_IP to remote user`

Explanation IKE obtained a private IP address for the client from DHCP or from the address pool.

- *group*— The name of the group
- *uname* —The name of the user
- *remote_IP_address* —The IP address of the remote client
- *assigned_private_IP* —The client IP address assigned by DHCP or from the local address pool

Recommended Action None required.

713229

Error Message `%FTD-5-713229: Auto Update - Notification to client client_ip of update string: message_string .`

Explanation A VPN remote access client is notified that updated software is available for download. The remote client user is responsible for choosing to update the client access software.

- **client_ip**—The IP address of the remote client
- **message_string**—The message text sent to the remote client

Recommended Action None required.

713230

Error Message `%FTD-3-713230 Internal Error, ike_lock trying to lock bit that is already locked for type type`

Explanation An internal error occurred, which is reporting that the IKE subsystem is attempting to lock memory that has already been locked. This indicates errors on semaphores that are used to protect memory violations for IKE SAs. This message does not indicate that anything is seriously wrong. However, an unexpected event has occurred, and steps are automatically being taken for recovery.

- >*type* —String that describes the type of semaphore that had a locking issue

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

713231

Error Message `%FTD-3-713231 Internal Error, ike_lock trying to unlock bit that is not locked for type type`

Explanation An internal error has occurred, which is reporting that the IKE subsystem is attempting to unlock memory that is not currently locked. This indicates errors on semaphores that are used to protect memory violations for IKE SAs. This message does not indicate that anything is seriously wrong. However, an unexpected event has occurred, and steps are automatically being taken for recovery.

- *type* —String that describes the type of semaphore that had a locking issue

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

713232

Error Message `%FTD-3-713232 SA lock refCnt = value , bitmask = hexvalue , p1_decrypt_cb = value , qm_decrypt_cb = value , qm_hash_cb = value , qm_spi_ok_cb = value , qm_dh_cb = value , qm_secret_key_cb = value , qm_encrypt_cb = value`

Explanation All the IKE SA are locked, and a possible error has been detected. This message reports errors on semaphores that are used to protect memory violations for IKE SAs.

- >*value* —Decimal value
- >*hexvalue* —Hexadecimal value

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

713233

Error Message `%FTD-7-713233: (VPN-unit ) Remote network (remote network ) validated for network extension mode.`

Explanation The remote network received during the Phase 2 negotiation was validated. The message indicates the results of the remote network check during Phase 2 negotiations for Network Extension Mode clients. This is part of an existing feature that prevents users from misconfiguring their hardware client network (for example, configuring overlapping networks or the same network on multiple clients).

- *remote network* —Subnet address and subnet mask from Phase 2 proxy

Recommended Action None required.

713234

Error Message `%FTD-7-713234: (VPN-unit) Remote network (remote network ) from network extension mode client mismatches AAA configuration (aaa network ).`

Explanation The remote network received during the Phase 2 negotiation does not match the framed-ip-address and framed-subnet-mask that were returned from the AAA server for this session.

- *remote network* —Subnet address and subnet mask from Phase 2 proxy
- *aaa network* —Subnet address and subnet mask configured through AAA

Recommended Action Do one of the following:

- Check the address assignment for this user and group, then check the network configuration on the HW client, and correct any inconsistencies.
- Disable address assignment for this user and group.

713235

Error Message `%FTD-6-713235: Attempt to send an IKE packet from standby unit. Dropping the packet!`

Explanation Normally, IKE packets should never be sent from the standby unit to the remote peer. If such an attempt is made, an internal logic error may have occurred. The packet never leaves the standby unit because of protective code. This message facilitates debugging.

Recommended Action None required.

713236

Error Message `%FTD-7-713236: IKE_DECODE tx/rx Message (msgid=msgid) with payloads:payload1 (payload1_len) + payload2 (payload2_len)...total length: tlen`

Explanation IKE sent or received various messages.

The following example shows the output when IKE receives a message with an 8-byte hash payload, an 11-byte notify payload, and two 13-byte vendor-specific payloads:

```
%threat defense-7-713236: IKE_DECODE RECEIVED Message msgid=0) with payloads: HDR + HASH
(8) + NOTIFY (11) + VENDOR (13) + VENDOR (13) + NONE (0)
```

Recommended Action None required.

713237

Error Message `%FTD-5-713237: ACL update (`*`access_list`*` ) received during re-key re-authentication will not be applied to the tunnel.`

Explanation The Phase 1 rekey of a remote access IPsec tunnel appears under the following conditions:

- The tunnel is configured to reauthenticate the user when the tunnel is rekeyed.
- The RADIUS server returns an access list or a reference to a locally configured access list that is different from the one that was returned when the tunnel was first established.

Recommended Action Under these conditions, the Secure Firewall Threat Defense device ignores the new access list and this message is generated.

- >*access_list* —Name associated with the static or dynamic access list, as displayed in the output of the **show access-list** command

IPsec users must reconnect for new user-specific access lists to take effect.

713238

Error Message `%FTD-3-713238: Invalid source proxy address: 0.0.0.0! Check private address on remote client`

Explanation The private side address of a network extension mode client came across as 0.0.0.0. This usually indicates that no IP address was set on the private interface of the hardware client.

Recommended Action Verify the configuration of the remote client.

713239

Error Message `%FTD-4-713239: `*`IP_Address`*` : Tunnel Rejected: The maximum tunnel count allowed has been reached`

Explanation An attempt to create a tunnel has occurred after the maximum number of tunnels allowed has been reached.

- **IP_Address**—The IP address of the peer

Recommended Action None required.

713240

Error Message `%FTD-4-713240: Received DH key with bad length: received length=rlength expected length=elength`

Explanation A Diffie-Hellman key with the incorrect length was received from the peer.

- rlength—The length of the DH key that was received
- elength—The expected length (based on the DH key size)

Recommended Action None required.

713241

Error Message `%FTD-4-713241: IE Browser Proxy Method setting_number is Invalid`

Explanation An invalid proxy setting was found during ModeCfg processing. P1 negotiation will fail.

Recommended Action Check the **msie-proxy method** command settings (a subcommand of the **group-policy** command), which should conform to one of the following: [**auto-detect** | **no-modify** | **no-proxy** | **use-server**] . Any other value or no value is incorrect. Try resetting the **msie-proxy method** command settings. If the problem persists, contact the Cisco TAC.

713242

Error Message `%FTD-4-713242: Remote user is authenticated using Hybrid Authentication. Not starting IKE rekey.`

Explanation The Secure Firewall Threat Defense device has detected a request to start an IKE rekey for a tunnel configured to use Hybrid Xauth, but the rekey was not started. The Secure Firewall Threat Defense device will wait for the client to detect and initiate an IKE rekey.

Recommended Action None required.

713243

Error Message `%FTD-4-713243: META-DATA Unable to find the requested certificate`

Explanation The IKE peer requested a certificate from the cert-req payload. However, no valid identity certificate issued by the requested DN was found.

Recommended Action Perform the following steps:

1. Check the identity certificates.
2. Enroll or import the desired certificate.
3. Enable certificate debugging for more details.

713244

Error Message `%FTD-4-713244: META-DATA Received Legacy Authentication Method(LAM) type type is different from the last type received type .`

Explanation The LAM attribute type received differs from the last type received. The type must be consistent throughout the user authentication process. The user authentication process cannot proceed, and the VPN connection will not be established.

- **type**—The LAM type

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

713245

Error Message `%FTD-4-713245: META-DATA Unknown Legacy Authentication Method(LAM) type type received.`

Explanation An unsupported LAM type was received during the CRACK challenge or response user authentication process. The user authentication process cannot proceed, and the VPN connection will not be established.

- **type**—The LAM type

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

713246

Error Message `%FTD-4-713246: META-DATA Unknown Legacy Authentication Method(LAM) attribute type type received.`

Explanation The Secure Firewall Threat Defense device received an unknown LAM attribute type, which should not cause connectivity problems, but might affect the functionality of the peer.

- **type**—The LAM attribute type

Recommended Action None required.

713247

Error Message `%FTD-4-713247: META-DATA Unexpected error: in Next Card Code mode while not doing SDI.`

Explanation An unexpected error occurred during state processing.

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

713248

Error Message `%FTD-5-713248: META-DATA Rekey initiation is being disabled during CRACK authentication.`

Explanation When an IKE SA is negotiated using the CRACK authentication method, the Phase 1 SA rekey timer at the headend expired before a successful rekey. Because the remote client is always the initiator of the exchange when using the CRACK authentication method, the headend will not initiate the rekey. Unless the remote peer initiates a successful rekey before the IKE SA expires, the connection will come down upon IKE SA expiration.

Recommended Action None required.

713249

Error Message `%FTD-4-713249: META-DATA Received unsupported authentication results: result`

Explanation While negotiating an IKE SA using the CRACK authentication method, the IKE subsystem received a result that is not supported during CRACK authentication from the authentication subsystem. The user authentication fails, and the VPN connection is torn down.

- *result* —The result returned from the authentication subsystem

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

713250

Error Message `%FTD-5-713250: META-DATA Received unknown Internal Address attribute: attribute`

Explanation The Secure Firewall Threat Defense device received a request for an internal address attribute that is not recognizable. The attribute might be valid, but not currently supported, or the peer might be sending an illegal value. This should not cause connectivity problems, but might affect the functionality of the peer.

Recommended Action None required.

713251

Error Message `%FTD-4-713251: META-DATA Received authentication failure message`

Explanation The Secure Firewall Threat Defense device received a notification message that indicated an authentication failure while an IKE SA is negotiated using the CRACK authentication method. The connection is torn down.

Recommended Action None required.

713252

Error Message `%FTD-5-713252: Group = group , Username = user , IP = ip , Integrity Firewall Server is not available. VPN Tunnel creation rejected for client.`

Explanation When the group policy is configured to require the client to authenticate with a Zonelab Integrity Server, the server might need to be connected to the concentrator depending on the failure policy configured. If the fail policy is to reject the client connection, this message is generated when a Zonelab Integrity Server is not connected to the Secure Firewall Threat Defense device at the time the client is connecting.

- *group* —The tunnel group to which the remote access user is connecting
- *user* —The remote access user
- *ip* —The IP address of the remote access user

Recommended Action Check that the configurations on the concentrator and the Zonelab Integrity Server match. Then verify that communication exists between the concentrator and the Zonelab Integrity Server.

713253

Error Message `%FTD-5-713253: Group = group , Username = user , IP = ip , Integrity Firewall Server is not available. Entering ALLOW mode. VPN Tunnel created for client.`

Explanation When the group policy is configured to require a client to authenticate with a Zonelab Integrity Server, the server might need to be connected to the concentrator, depending on the failure policy configured. If the failure policy is to accept the client connection, and provide unrestricted network access, this message is generated when a Zonelab Integrity Server is not connected to the Secure Firewall Threat Defense device at the time the client is connecting.

- *group* —The tunnel group to which the remote access user is connecting
- *user* —The remote access user
- *ip* —The IP address of the remote access user

Recommended Action Check that the configurations on the Secure Firewall Threat Defense device and the Zonelab Integrity Server match, and verify that communication exists between the Secure Firewall Threat Defense device and the Zonelab Integrity Server.

713254

Error Message `%FTD-3-713254: Group = groupname , Username = username , IP = peerip , Invalid IPsec/UDP port = portnum , valid range is minport - maxport , except port 4500, which is reserved for IPsec/NAT-T`

Explanation You cannot use UDP port 4500 for IPsec/UDP connections, because it is reserved for IPsec or NAT-T connections. The CLI does not allow this configuration for local groups. This message should only occur for externally defined groups.

- *groupname* —The name of the user group
- *username* —The name of the user
- *peerip* —The IP address of the client
- *portnum* —The IPsec/UDP port number on the external server
- *minport* —The minimum valid port number for a user-configurable port, which is 4001
- *maxport* —The maximum valid port number for a user-configurable port, which is 49151

Recommended Action Change the IPsec or UDP port number on the external server to another port number. Valid port numbers are 4001 to 49151.

713255

Error Message `%FTD-4-713255: IP = peer-IP , Received ISAKMP Aggressive Mode message 1 with unknown tunnel group name group-name`

Explanation An unknown tunnel group was specified in ISAKMP Aggressive Mode message 1.

- *peer-ip* —The address of the peer
- *group-name* —The group name specified by the peer

Recommended Action Check the tunnel group and client configurations to make sure that they are valid.

713256

Error Message `%FTD-6-713256: IP = peer-IP , Sending spoofed ISAKMP Aggressive Mode message 2 due to receipt of unknown tunnel group. Aborting connection.`

Explanation When the peer specifies an invalid tunnel group, the Secure Firewall Threat Defense device will still send message 2 to prevent the peer from gleaning tunnel group information.

- *peer-ip* —The address of the peer

Recommended Action None required.

713257

Error Message `%FTD-5-713257: Phase var1 failure: Mismatched attribute types for class var2 : Rcv'd: var3 Cfg'd: var4`

Explanation An Secure Firewall Threat Defense device has acted as the responder in a LAN-to-LAN connection. It indicates that the Secure Firewall Threat Defense crypto configuration does not match the configuration of the initiator. The message specifies during which phase the mismatch occurred, and which attributes both the responder and the initiator had that were different.

- *var1* —The phase during which the mismatch occurred
- *var2* —The class to which the attributes that do not match belong
- *var3* —The attribute received from the initiator
- *var4* —The attribute configured

Recommended Action Check the crypto configuration on both of the LAN-to-LAN devices for inconsistencies. In particular, if a mismatch between UDP-Tunnel (NAT-T) and something else is reported, check the crypto maps. If one configuration has NAT-T disabled on the matched crypto map and the other does not, this will cause a failure.

713258

Error Message `%FTD-3-713258: IP = var1 , Attempting to establish a phase2 tunnel on var2 interface but phase1 tunnel is on var3 interface. Tearing down old phase1 tunnel due to a potential routing change.`

Explanation The Secure Firewall Threat Defense device tries to establish a Phase 2 tunnel on an interface, and a Phase 1 tunnel already exists on a different interface. The existing Phase 1 tunnel is torn down to allow the establishment of a new tunnel on the new interface.

- *var1* —The IP address of the peer
- *var2* —The interface on which the Secure Firewall Threat Defense device is trying to establish a Phase 2 tunnel
- *var3* —The interface on which the Phase 1 tunnel exists

Recommended Action Check whether or not the route of the peer has changed. If the route has not changed, a possible misconfiguration may exist.

713259

Error Message `%FTD-5-713259: Group = groupname , Username = username , IP = peerIP , Session is being torn down. Reason: reason`

Explanation The termination reason for the ISAKMP session appears, which occurs when the session is torn down through session management.

- *groupname* —The tunnel group of the session being terminated
- *username* —The username of the session being terminated
- *peerIP* —The peer address of the session being terminated

• *reason* —The RADIUS termination reason of the session being terminated. Reasons include the following:

- Port Preempted (simultaneous logins)

- Idle Timeout

- Max Time Exceeded

- Administrator Reset

Recommended Action None required.

713260

Error Message `%FTD-3-713260: Output interface %d to peer was not found`

Explanation When trying to create a Phase 1 SA, the interface database could not be found for the interface ID.

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

713261

Error Message `%FTD-3-713261: IPV6 address on output interface %d was not found`

Explanation When trying to create a Phase 1 SA, no IPv6 address is specified on the local interface.

Recommended Action For information about how to set up an IPv6 address on a desired interface, see the "Configuring IPv6 Addressing" section in the CLI configuration guide.

713262

Error Message `%FTD-3-713262: Rejecting new IPSec SA negotiation for peer Peer_address . A negotiation was already in progress for local Proxy Local_address /Local_prefix_len , remote Proxy Remote_address /Remote_prefix_len`

Explanation When establishing a Phase SA, the Secure Firewall Threat Defense device will reject a new Phase 2 SA matching this proxy.

- *Peer_address* —The new address attempting to intiate Phase 2 with a proxy matching an existing negotiation
- *Local_address* —The address of the previous local peer currently negotiating Phase 2
- *Local_prefix_len* —The length of the subnet prefix according to CIDR notation
- *Remote_address* —The address of the proxy
- *Remote_prefix_len* —The length of the subnet prefix according to CIDR notation

Recommended Action None required.

713263

Error Message `%FTD-7-713263: Received local IP Proxy Subnet data in ID Payload: Address IP_address , Mask /prefix_len , Protocol protocol , Port port`

Explanation The Secure Firewall Threat Defense device is adding a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- *IP_address* —The base IP address of the destination network of the peer
- *prefix_len* —The length of the subnet prefix according to CIDR notation
- *protocol* — The proxy protocol
- *port* —The proxy port

Recommended Action None required.

713264

Error Message `%FTD-7-713264: Received local IP Proxy Subnet data in ID Payload: Address IP_address , Mask/prefix_len , Protocol protocol , Port port {"Received remote IP Proxy Subnet data in ID Payload: Address %a , Mask/%d , Protocol %u , Port %u "}`

Explanation The Secure Firewall Threat Defense device is adding a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- *IP_address* —The base IP address of the destination network of the peer
- *prefix_len* —The length of the subnet prefix according to CIDR notation
- *protocol* — The proxy protocol
- *port* —The proxy port

Recommended Action None required.

713265

Error Message `%FTD-6-713265: Adding static route for L2L peer coming in on a dynamic map. address: IP_address , mask: /prefix_len`

Explanation The Secure Firewall Threat Defense device is adding a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- *IP_address* —The base IP address of the destination network of the peer
- *prefix_len* —The length of the subnet prefix according to CIDR notation

Recommended Action None required.

713266

Error Message `%FTD-3-713266: Could not add route for L2L peer coming in on a dynamic map. address: IP_address , mask: /prefix_len`

Explanation The Secure Firewall Threat Defense device failed while attempting to add a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. This might indicate duplicate routes, a full IPv6 routing table, or a failure of the Secure Firewall Threat Defense device to remove previously used routes.

- *IP_address* —The base IP address of the destination network of the peer

- *prefix_len* —The length of the subnet prefix according to CIDR notation

Recommended Action Check the IPv6 routing table to make sure there is room for additional routes, and that obsolete routes are not present. If the table is full or includes obsolete routes, remove the routes and try again. If the problem persists, contact the Cisco TAC.

713267

Error Message `%FTD-6-713267: Deleting static route for L2L peer that came in on a dynamic map. address: IP_address , mask: /prefix_len`

Explanation The Secure Firewall Threat Defense device failed while attempting to add a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel.

- *IP_address* —The base IP address of the destination network of the peer
- *prefix_len* —The length of the subnet prefix according to CIDR notation

Recommended Action None required.

713268

Error Message `%FTD-3-713268: Could not delete route for L2L peer that came in on a dynamic map. address: IP_address , mask: /prefix_len`

Explanation The Secure Firewall Threat Defense device experienced a failure while deleting a route for the private address or networks of the peer. In this case, the peer is either a client or a L2L peer with an unknown address. Both of these cases use dynamic crypto maps to allow the tunnel. The route may have already been deleted, or an internal software error has occurred.

- *IP_address* —The base IP address of the destination network of the peer
- *prefix_len* —The length of the subnet prefix according to CIDR notation

Recommended Action If the route has already been deleted, the condition is benign and the device will function normally. If the problem persists or can be linked to routing issues over VPN tunnels, then check the routing and addressing portions of the VPN L2L configuration. Also check the reverse route injection and the ACLs associated with the appropriate crypto map. If the problem persists, contact the Cisco TAC.

713269

Error Message `%FTD-6-713269: Detected Hardware Client in network extension mode, adding static route for address: IP_address , mask: /prefix_len`

Explanation A tunnel with a hardware client in network extension mode has been negotiated, and a static route is being added for the private network behind the hardware client. This configuration enables the Secure Firewall Threat Defense device to make the remote network known to all the routers on the private side of the headend.

- *IP_address* —The base IP address of the destination network of the peer
- *prefix_len* —The length of the subnet prefix according to CIDR notation

Recommended Action None required.

713270

Error Message `%FTD-3-713270: Could not add route for Hardware Client in network extension mode, address: IP_address , mask: /prefix_len`

Explanation An internal software error has occurred. A tunnel with a hardware client in network extension mode has been negotiated, and an attempt to add the static route for the private network behind the hardware client failed. The IPv6 routing table may be full, or a possible addressing error has occurred.

- *IP_address* —The base IP address of the destination network of the peer
- *prefix_len* —The length of the subnet prefix according to CIDR notation

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

713271

Error Message `%FTD-6-713271: Terminating tunnel to Hardware Client in network extension mode, deleting static route for address: IP_address , mask:/prefix_len`

Explanation A tunnel to a hardware client in network extension mode is being removed, and the static route for the private network is being deleted behind the hardware client.

- *IP_address* —The base IP address of the destination network of the peer
- *prefix_len* —The length of the subnet prefix according to CIDR notation

Recommended Action None required.

713272

Error Message `%FTD-3-713272: Terminating tunnel to Hardware Client in network extension mode, unable to delete static route for address: IP_address , mask: /prefix_len`

Explanation While a tunnel to a hardware client in network extension mode was being removed, a route to the private network behind the hardware client cannot be deleted. This might indicate an addressing or software problem.

- *IP_address* —The base IP address of the destination network of the peer
- *prefix_len* —The length of the subnet prefix according to CIDR notation

Recommended Action Check the IPv6 routing table to ensure that the route is not there. If it is, it may have to be removed manually, but only if the tunnel to the hardware client has been completely removed.

713273

Error Message `%FTD-7-713273: Deleting static route for client address: IP_Address IP_Address address of client whose route is being removed`

Explanation A route to the peer-assigned address or the networks protected by a hardware client were removed from the routing table.

Recommended Action None required.

713274

Error Message `%FTD-3-713274: Could not delete static route for client address: IP_Address IP_Address address of client whose route is being removed`

Explanation While a tunnel to an IPsec client was being removed, its entry in the routing table could not be removed. This condition may indicate a networking or software problem.

Recommended Action Check the routing table to make sure that the route does not exist. If it does, it may need to be removed manually, but only if the tunnel has been closed successfully.

713275

Error Message `%FTD-3-713275: IKEv1 Unsupported certificate keytype %s found at trustpoint %s`

Explanation This syslog is displayed for ikev1 when certificate key type is not of type ECDSA. Ensure that certificates of valid KEY type is installed on the GW.

Recommended Action None required.

713276

Error Message `%FTD-3-713276: Dropping new negotiation - IKEv1 in-negotiation context limit of %u reached`

Explanation This syslog message is displayed for ikev1 in multi context when maximum in negotiation limit is reached.

Recommended Action None required.

713900

Error Message `%FTD-1-713900: Descriptive_event_string.`

Explanation A serious event or failure has occurred. For example, the Secure Firewall Threat Defense device is trying to generate a Phase 2 deletion, but the SPI did not match any of the existing Phase 2 SAs.

Recommended Action In the example described, both peers are deleting Phase 2 SAs at the same time. In this case, it is a benign error and can be ignored. If the error is persistent and results in negative side effects such as dropped tunnels or device reboots, it may reflect a software failure. In this case, copy the error message exactly as it appears on the console or in the system log, and then contact the Cisco TAC for further assistance.

713901

Error Message `%FTD-2-713901: Descriptive_event_string .`

Explanation An error has occurred, which may be the result of a configuration error on the headend or remote access client. The event string provides details about the error that occurred.

Recommended Action You may need to troubleshoot the message to determine what caused the error. Check the ISAKMP and crypto map configuration on both peers.

713902

Error Message `%FTD-3-713902: Descriptive_event_string.`

Explanation An error has occurred, which may be the result of a configuration error either on the headend or remote access client.

Recommended Action It might be necessary to troubleshoot the configuration to determine the cause of the error. Check the ISAKMP and crypto map configuration on both peers.

713903

Error Message `%FTD-4-713903: IKE error message reason reason.`

Explanation This syslog ID is used for IKE warning messages which can display multiple other syslogs.

Recommended Action None required.

Examples:

`%FTD-4-713903: Group = group policy , Username = user name , IP = remote IP , ERROR: Failed to install Redirect URL: redirect URL Redirect ACL: non_exist for assigned IP`

`%FTD-4-713903: IKE Receiver: Runt ISAKMP packet discarded on Port Port_Number from Source_URL`

`%FTD-4-713903: IP = IP address, Header invalid, missing SA payload! (next payload = x)`

`%FTD-4-713903: Group = DefaultRAGroup, IP = IP address, Error: Unable to remove PeerTblEntry`

713904

Error Message `%FTD-5-713904: Descriptive_event_string .`

Explanation Notification status information appears, which is used to track events that have occurred.

Recommended Action None required.

713905

Error Message `%FTD-6-713905: Descriptive_event_string.`

Explanation Information status details appear, which are used to track events that have occurred.

Example

`%threat defense-6-713905: IKE successfully unreserved UDP port 27910 on interface outside`

Recommended Action None required.

713906

Error Message `%FTD-7-713906: Descriptive_event_string .`

Explanation Debugging status information appears, which is used to track events that have occurred.

Recommended Action None required.

714001

Error Message `%FTD-7-714001: description_of_event_or_packet`

Explanation A description of an IKE protocol event or packet was provided.

Recommended Action None required.

714002

Error Message `%FTD-7-714002: IKE Initiator starting QM: msg id = message_number`

Explanation The Secure Firewall Threat Defense device has sent the first packet of the Quick mode exchange as the Phase 2 initiator.

Recommended Action None required.

714003

Error Message `%FTD-7-714003: IKE Responder starting QM: msg id = message_number`

Explanation The Secure Firewall Threat Defense device has received the first packet of the Quick mode exchange as the Phase 2 responder.

Recommended Action None required.

714004

Error Message `%FTD-7-714004: IKE Initiator sending 1st QM pkt: msg id = message_number`

Explanation The protocol of the first Quick Mode packet was decoded.

Recommended Action None required.

714005

Error Message `%FTD-7-714005: IKE Responder sending 2nd QM pkt: msg id = message_number`

Explanation The protocol of the second Quick Mode packet was decoded.

Recommended Action None required.

714006

Error Message `%FTD-7-714006: IKE Initiator sending 3rd QM pkt: msg id = message_number`

Explanation The protocol of the third Quick Mode packet was decoded.

Recommended Action None required.

714007

Error Message `%FTD-7-714007: IKE Initiator sending Initial Contact`

Explanation The Secure Firewall Threat Defense device is building and sending the initial contact payload.

Recommended Action None required.

714011

Error Message `%FTD-7-714011: Description of received ID values`

Explanation The Secure Firewall Threat Defense device received the displayed ID information during the negotiation.

Recommended Action None required.