

Syslog Messages 201002 to 219002

This chapter contains the following sections:

- Messages 201002 to 210022, on page 1
- Messages 211001 to 219002, on page 9

Messages 201002 to 210022

This chapter includes messages from 201002 to 210022.

201002

Error Message `%FTD-3-201002: Too many TCP connections on {static|xlate} global_address ! econns_nconns`

Explanation The maximum number of TCP connections to the specified global address was exceeded.

- econns—The maximum number of embryonic connections
- nconns—The maximum number of connections permitted for the static or xlate global address

Recommended Action Use the **show static** or show nat command to check the limit imposed on connections to a static address. The limit is configurable.

201003

Error Message `%FTD-2-201003: Embryonic limit exceeded nconns/elimit for outside_address/outside_port to inside_address(global_address)/inside_port on interface interface_name`

Explanation The number of embryonic connections from the specified foreign address with the specified static global address to the specified local address exceeds the embryonic limit. When the limit on embryonic connections to the Secure Firewall Threat Defense device is reached, the Secure Firewall Threat Defense device attempts to accept them anyway, but puts a time limit on the connections. This situation allows some connections to succeed even if the Secure Firewall Threat Defense device is very busy. This message indicates a more serious overload than message 201002, which can be caused by a SYN attack, or by a very heavy load of legitimate traffic.

- nconns—The maximum number of embryonic connections received
- *elimit* —The maximum number of embryonic connections specified in the static or nat command

Recommended Action Use the show static command to check the limit imposed on embryonic connections to a static address.

201004

Error Message `%FTD-3-201004: Too many udp connections on {static|xlate} global_address! udp_connections_limit`

Explanation The maximum number of UDP connections to the specified global address was exceeded.

- udp conn limit—The maximum number of UDP connections permitted for the static address or translation

Recommended Action Use the **show static** or show nat command to check the limit imposed on connections to a static address. You can configure the limit.

201005

Error Message `%FTD-3-201005: FTP data connection failed for IP_address`

Explanation The Secure Firewall Threat Defense device cannot allocate a structure to track the data connection for FTP because of insufficient memory.

Recommended Action Reduce the amount of memory usage or purchase additional memory.

201006

Error Message `%FTD-3-201006: RCMD backconnection failed for IP_address/port`

Explanation The Secure Firewall Threat Defense device cannot preallocate connections for inbound standard output for **rsh** commands because of insufficient memory.

Recommended Action Check the **rsh** client version; the Secure Firewall Threat Defense device only supports the Berkeley **rsh** client version. You can also reduce the amount of memory usage, or purchase additional memory.

201008

Error Message `%FTD-3-201008: Disallowing new connections.`

Explanation You have enabled TCP system log messaging and the syslog server cannot be reached.

Recommended Action Disable TCP syslog messaging. Also, make sure that the syslog server is up and you can ping the host from the Secure Firewall Threat Defense console. Then restart TCP system message logging to allow traffic.

201009

Error Message `%FTD-3-201009: TCP connection limit of number for host IP_address on interface_name exceeded`

Explanation The maximum number of connections to the specified static address was exceeded.

- number—The maximum of connections permitted for the host

- **IP_address**—The host IP address
- *interface_name*— The name of the interface to which the host is connected

Recommended Action Use the show static and show nat commands to check the limit imposed on connections to an address. The limit is configurable.

201010

Error Message `%FTD-6-201010: Embryonic connection limit exceeded econns/limit for dir packet from source_address/source_port to dest_address/dest_port on interface interface_name`

Explanation An attempt to establish a TCP connection failed because of an exceeded embryonic connection limit, which was configured with the **set connection embryonic-conn-max** MPC command for a traffic class.

To reduce the impact of anomalous incoming traffic on device's different management or data interfaces and protocols, the interfaces are configured with a default embryonic limit of 100. This syslog message appears when the embryonic connections to an interface exceeds 100. This default value cannot be modified or disabled.

- **econns**—The current count of embryonic connections associated to the configured traffic class
- **limit**—The configured embryonic connection limit for the traffic class
- **dir**—input: The first packet that initiates the connection is an input packet on the interface **interface_name** output: The first packet that initiates the connection is an output packet on the interface **interface_name**
- *source_address/source_port* —The source real IP address and the source port of the packet initiating the connection
- *dest_address/dest_port* —The destination real IP address and the destination port of the packet initiating the connection
- **interface_name**—The name of the interface on which the policy limit is enforced

Recommended Action None required.

201011

Error Message `%FTD-3-201011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name`

Explanation A new connection through the Secure Firewall Threat Defense device resulted in exceeding at least one of the configured maximum connection limits. This message applies both to connection limits configured using a **static** command, or to those configured using Cisco Modular Policy Framework. The new connection will not be allowed through the Secure Firewall Threat Defense device until one of the existing connections is torn down, which brings the current connection count below the configured maximum.

- *cnt* —Current connection count
- *limit* —Configured connection limit
- *dir* —Direction of traffic, inbound or outbound
- *sip* —Source real IP address
- *sport* —Source port
- *dip* —Destination real IP address
- *dpor* t—Destination port
- *if_name* —Name of the interface on which the traffic was received

Recommended Action None required.

201012

Error Message `%FTD-6-201012: Per-client embryonic connection limit exceeded curr_num/limit for [input|output] packet from ip_address/port to ip_address/port on interface interface_name`

Explanation An attempt to establish a TCP connection failed because the per-client embryonic connection limit was exceeded. By default, this message is rate limited to 1 message every 10 seconds.

- *curr_num*—The current number
- *limit*—The configured limit
- *[input|output]*—Input or output packet on interface **interface_name**
- *ip_address*—Real IP address
- *port*—TCP or UDP port
- *interface_name*—The name of the interface on which the policy is applied

Recommended Action When the limit is reached, any new connection request will be proxied by the Secure Firewall Threat Defense device to prevent a SYN flood attack. The Secure Firewall Threat Defense device will only connect to the server if the client is able to finish the three-way handshake. This usually does not affect the end user or the application. However, if this creates a problem for any application that has a legitimate need for a higher number of embryonic connections, you can adjust the setting by entering the **set connection per-client-embryonic-max** command.

201013

Error Message `%FTD-3-201013: Per-client connection limit exceeded curr_num/limit for [input|output] packet from ip_address/port to ip_address/port on interface interface_name`

Explanation A connection was rejected because the per-client connection limit was exceeded.

- *curr num*—The current number
- *limit*—The configured limit
- *[input|output]*—The input or output packet on interface **interface_name**
- *ip*—The real IP address
- *port*—The TCP or UDP port
- interface_name—The name of the interface on which the policy is applied

Recommended Action When the limit is reached, any new connection request will be silently dropped. Normally an application will retry the connection, which will cause a delay or even a timeout if all retries also fail. If an application has a legitimate need for a higher number of concurrent connections, you can adjust the setting by entering the **set connection per-client-max** command.

202010

Error Message-1 `%FTD-3-202010: {NAT | PAT} pool exhausted in pool'pool_name' IP ip_addressport_range [1-511 | 512-1023 | 1024-65535] Unable to create protocol connection from inside_interface:src_ip/src_port to outside_interface:dest_ip/dest_port.`

Error Message-2 `%FTD-3-202010: NAT/PAT pool exhausted in pool 'pool_name' IP ip_address. Unable to create connection.`

Explanation

- *pool_name* —The name of the NAT or PAT pool. If the interface PAT or mapped IP is a raw address, pool name is logged as empty string ("").
- *protocol* —The protocol used to create the connection
- *inside_interface* —The ingress interface
- *src_ip* —The source IP address
- *src_port* —The source port
- *outside_interface* —The egress interface
- *dest_ip* —The destination IP address
- *dest_port* —The destination port

The Secure Firewall Threat Defense device has no more address translation pools available.

Recommended Action Use the **show nat pool** and **show nat detail** commands to determine why all addresses and ports in the pool are used up. If this occurs under normal conditions, then add additional IP addresses to the NAT/PAT pool.

202016

Error Message `%FTD-3-202016: Unable to pre-allocate SIP ip_protocol secondary channel for message from src_ifname:src_ip_addr/src_port to dst_ifname:dest_ip_addr/dest_port with PAT and missing port information.`

Explanation

When SIP application generates an SDP payload with Media port set to 0, you cannot allocate a PAT xlate for such invalid port request and drop the packet with this syslog.

Recommended Action None. This is an application specific issue.

208005

Error Message `%FTD-3-208005: Clear (command) return code`

Explanation The Secure Firewall Threat Defense device received a nonzero value (an internal error) when attempting to clear the configuration in flash memory. The message includes the reporting subroutine filename and line number.

Recommended Action For performance reasons, the end host should be configured not to inject IP fragments. This configuration change is probably because of NFS. Set the read and write size equal to the interface MTU for NFS.

209003

Error Message `%FTD-4-209003: Fragment database limit of number exceeded: src = source_address , dest = dest_address , proto = protocol , id = number`

Explanation Too many IP fragments are currently awaiting reassembly. By default, the maximum number of fragments is 200 (to raise the maximum, see the **fragment size** command in the command reference guide). The Secure Firewall Threat Defense device limits the number of IP fragments that can be concurrently reassembled. This restriction prevents memory depletion at the Secure Firewall Threat Defense device under abnormal network conditions. In general, fragmented traffic should be a small percentage of the total traffic mix. An exception is in a network environment with NFS over UDP where a large percentage is fragmented traffic; if this type of traffic is relayed through the Secure Firewall Threat Defense device, consider using NFS

over TCP instead. To prevent fragmentation, see the **sysopt connection tcpmss bytes** command in the command reference guide.

Recommended Action If this message persists, a denial of service (DoS) attack might be in progress. Contact the remote peer administrator or upstream provider.

209004

Error Message `%FTD-4-209004: Invalid IP fragment, size = bytes exceeds maximum size = bytes : src = source_address , dest = dest_address , proto = protocol , id = number`

Explanation An IP fragment is malformed. The total size of the reassembled IP packet exceeds the maximum possible size of 65,535 bytes.

Recommended Action A possible intrusion event may be in progress. If this message persists, contact the remote peer administrator or upstream provider.

209005

Error Message `%FTD-4-209005: Discard IP fragment set with more than number elements: src = Too many elements are in a fragment set.`

Explanation The Secure Firewall Threat Defense device disallows any IP packet that is fragmented into more than 24 fragments. For more information, see the **fragment** command in the command reference guide.

Recommended Action A possible intrusion event may be in progress. If the message persists, contact the remote peer administrator or upstream provider. You can change the number of fragments per packet by using the **fragment chain xxx interface_name** command.

209006

Error Message `%FTD-4-209006: Fragment queue threshold exceeded, dropped protocol fragment from IP address/port to IP address/port on outside interface.`

Explanation The Secure Firewall Threat Defense device drops the fragmented packets when the fragment database threshold, that is 2/3 of the queue size per interface, has exceeded.

Recommended Action None required.

210001

Error Message `%FTD-3-210001: LU sw_module_name error = number`

Explanation A Stateful Failover error occurred.

Recommended Action If this error persists after traffic lessens through the Secure Firewall Threat Defense device, report this error to the Cisco TAC.

210002

Error Message `%FTD-3-210002: LU allocate block (bytes) failed`

Explanation Stateful Failover cannot allocate a block of memory to transmit stateful information to the standby Secure Firewall Threat Defense device.

Recommended Action Check the failover interface using the **show interface** command to make sure its transmit is normal. Also check the current block memory using the **show block** command. If current available count is 0 within any of the blocks of memory, then reload the Secure Firewall Threat Defense software to recover the lost blocks of memory.

210003

Error Message `%FTD-3-210003: Unknown LU Object` *`number`*

Explanation Stateful Failover received an unsupported Logical Update object and was unable to process it. This can be caused by corrupted memory, LAN transmissions, and other events.

Recommended Action If you see this error infrequently, then no action is required. If this error occurs frequently, check the Stateful Failover link LAN connection. If the error was not caused by a faulty failover link LAN connection, determine if an external user is trying to compromise the protected network. Also check for misconfigured clients.

210005

Error Message `%FTD-3-210005: LU allocate` *`secondary`* `(`*`optional`*` ) connection failed for` *`protocol`* `[`*`TCP |UDP`*` ] connection from` *`ingress interface name`* `:`*`Real IP Address /Real Port`* `to` *`egress interface name`* `:`*`Real IP Address /Real Port`*

Explanation Stateful Failover cannot allocate a new connection on the standby unit. This may be caused by little or no RAM memory available within the Secure Firewall Threat Defense device. This could additionally be caused by flow creation failure due to resource limitation or reaching configured resource usage limits.

Note The *secondary* field in the syslog message is optional and appears only if the connection is a secondary connection.

Recommended Action Check the available memory using the **show memory** command to make sure that the Secure Firewall Threat Defense device has free memory. If there is no available memory, add more physical memory to the Secure Firewall Threat Defense device. Check resource limitation using the **show resource usage** command and **show asp drop** to ensure that the device is not reaching the resource limitation.

210006

Error Message `%FTD-3-210006: LU look NAT for` *`IP_address`* `failed`

Explanation Stateful Failover was unable to locate a NAT group for the IP address on the standby unit. The active and standby Secure Firewall Threat Defense devices may be out-of-sync with each other.

Recommended Action Use the **write standby** command on the active unit to synchronize system memory with the standby unit.

210007

Error Message `%FTD-3-210007: LU allocate xlate failed for type-staticdynamic NAT translation from PAT:secondary(optional)/protocol (ingress_interface_name/Real_IP_Address) to real_port:Mapped_IP_Address/Mapped_Port (egress_interface_name/Real_IP_Address)`

Explanation Stateful Failover failed to allocate a translation slot record.

Recommended Action Check the available memory by using the **show memory** command to make sure that the Secure Firewall Threat Defense device has free memory available. If no memory is available, add more memory.

210008

Error Message `%FTD-3-210008: LU no xlate for inside_address/inside_port outside_address/outside_port`

Explanation The Secure Firewall Threat Defense device cannot find a translation slot record for a Stateful Failover connection; as a result, the Secure Firewall Threat Defense device cannot process the connection information.

Recommended Action Use the **write standby** command on the active unit to synchronize system memory between the active and standby units.

210010

Error Message `%FTD-3-210010: LU make UDP connection for outside_address:outside_port inside_address:inside_port failed`

Explanation Stateful Failover was unable to allocate a new record for a UDP connection.

Recommended Action Check the available memory by using the **show memory** command to make sure that the Secure Firewall Threat Defense device has free memory available. If no memory is available, add more memory.

210020

Error Message `%FTD-3-210020: LU PAT port port reserve failed`

Explanation Stateful Failover is unable to allocate a specific PAT address that is in use.

Recommended Action Use the **write standby** command on the active unit to synchronize system memory between the active and standby units.

210021

Error Message `%FTD-3-210021: LU create static xlate global_address ifc interface_name failed`

Explanation Stateful Failover is unable to create a translation slot.

Recommended Action Enter the **write standby** command on the active unit to synchronize system memory between the active and standby units.

210022

Error Message `%FTD-6-210022: LU missed number updates`

Explanation Stateful Failover assigns a sequence number for each record sent to the standby unit. When a received record sequence number is out of sequence with the last updated record, the information in between is assumed to be lost, and this error message is sent as a result.

Recommended Action Unless LAN interruptions occur, check the available memory on both Secure Firewall Threat Defense units to ensure that enough memory is available to process the stateful information. Use the **show failover** command to monitor the quality of stateful information updates.

Messages 211001 to 219002

This chapter includes messages from 211001 to 219002.

211001

Error Message `%FTD-3-211001: Memory allocation Error`

Explanation The Secure Firewall Threat Defense device failed to allocate RAM system memory.

Recommended Action If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC.

211003

Error Message `%FTD-3-211003: Error in computed percentage CPU usage value`

Explanation The percentage of CPU usage is greater than 100 percent.

Recommended Action If this message occurs periodically, it can be ignored. If it repeats frequently, contact the Cisco TAC.

211004

Error Message `%FTD-1-211004: WARNING: Minimum Memory Requirement for device version ver not met. min MB required, actual MB found.`

Explanation The Secure Firewall Threat Defense device does not meet the minimum memory requirements for this version.

- **ver**—Running image version number
- **min**—Minimum required amount of RAM to run the installed image.
- **actual**—Amount of RAM currently installed in the system

Recommended Action Install the required amount of RAM.

212001

Error Message `%FTD-3-212001: Unable to open SNMP channel (UDP port port) on interface "interface_number", error code = code`

Explanation The Secure Firewall Threat Defense device is unable to receive SNMP requests destined for the Secure Firewall Threat Defense device from SNMP management stations located on this interface. The SNMP traffic passing through the Secure Firewall Threat Defense device on any interface is not affected. The error codes are as follows:

- An error code of -1 indicates that the Secure Firewall Threat Defense device cannot open the SNMP transport for the interface. This can occur when the user attempts to change the port on which SNMP accepts queries to one that is already in use by another feature. In this case, the port used by SNMP will be reset to the default port for incoming SNMP queries (UDP 161).
- An error code of -2 indicates that the Secure Firewall Threat Defense device cannot bind the SNMP transport for the interface.

Recommended Action After the Secure Firewall Threat Defense device reclaims some of its resources when traffic is lighter, reenter the snmp-server host command for that interface.

212002

Error Message `%FTD-3-212002: Unable to open SNMP trap channel (UDP port port) on interface "interface_number", error code = code`

Explanation The Secure Firewall Threat Defense device is unable to send its SNMP traps from the Secure Firewall Threat Defense device to SNMP management stations located on this interface. The SNMP traffic passing through the Secure Firewall Threat Defense device on any interface is not affected. The error codes are as follows:

- An error code of -1 indicates that the Secure Firewall Threat Defense device cannot open the SNMP trap transport for the interface.
- An error code of -2 indicates that the Secure Firewall Threat Defense device cannot bind the SNMP trap transport for the interface.
- An error code of -3 indicates that the Secure Firewall Threat Defense device cannot set the trap channel as write-only.

Recommended Action After the Secure Firewall Threat Defense device reclaims some of its resources when traffic is lighter, reenter the snmp-server host command for that interface.

212003

Error Message `%FTD-3-212003: Unable to receive an SNMP request on interface "interface_number", error code = code, will try again.`

Explanation An internal error occurred in receiving an SNMP request destined for the Secure Firewall Threat Defense device on the specified interface. The error codes are as follows:

- An error code of -1 indicates that the Secure Firewall Threat Defense device cannot find a supported transport type for the interface.
- An error code of -5 indicates that the Secure Firewall Threat Defense device received no data from the UDP channel for the interface.

- An error code of -7 indicates that the Secure Firewall Threat Defense device received an incoming request that exceeded the supported buffer size.
- An error code of -14 indicates that the Secure Firewall Threat Defense device cannot determine the source IP address from the UDP channel.
- An error code of -22 indicates that the Secure Firewall Threat Defense device received an invalid parameter.

Recommended Action None required. The Secure Firewall Threat Defense SNMP agent goes back to wait for the next SNMP request.

212004

Error Message `%FTD-3-212004: Unable to send an SNMP response to IP_address, error code = port`

Explanation An internal error occurred in sending an SNMP response from the Secure Firewall Threat Defense device to the specified host on the specified interface. The error codes are as follows:

- An error code of -1 indicates that the Secure Firewall Threat Defense device cannot find a supported transport type for the interface.
- An error code of -2 indicates that the Secure Firewall Threat Defense device sent an invalid parameter.
- An error code of -3 indicates that the Secure Firewall Threat Defense device was unable to set the destination IP address in the UDP channel.
- An error code of -4 indicates that the Secure Firewall Threat Defense device sent a PDU length that exceeded the supported UDP segment size.
- An error code of -5 indicates that the Secure Firewall Threat Defense device was unable to allocate a system block to construct the PDU.

Recommended Action None required.

212005

Error Message `%FTD-3-212005: incoming SNMP request (number bytes) from interface_name exceeds data buffer size, discarding this SNMP request.`

Explanation The length of the incoming SNMP request that is destined for the Secure Firewall Threat Defense device exceeds the size of the internal data buffer (512 bytes) used for storing the request during internal processing. The Secure Firewall Threat Defense device is unable to process this request. The SNMP traffic passing through the Secure Firewall Threat Defense device on any interface is not affected.

Recommended Action Have the SNMP management station resend the request with a shorter length. For example, instead of querying multiple MIB variables in one request, try querying only one MIB variable in a request. You may need to modify the configuration of the SNMP manager software.

212006

Error Message `%FTD-3-212006: Dropping SNMP request from src_addr/src_port to ifc:dst_addr/dst_port because: reasonusername`

Explanation The Secure Firewall Threat Defense device cannot process the SNMP request being sent to it for the following reasons:

- user not found—The username cannot be located in the local SNMP user database.

- username exceeds maximum length—The username embedded in the PDU exceeds the maximum length allowed by the SNMP RFCs.
- authentication algorithm failure—An authentication failure caused by an invalid password or a packet authenticated using the incorrect algorithm.
- privacy algorithm failure—A privacy failure caused by an invalid password or a packet encrypted using the incorrect algorithm.
- error decrypting request—An error occurred in the platform crypto module decrypting the user request.
- error encrypting response—An error occurred in the platform crypto module encrypting the user response or trap notification.
- engineBoots has reached maximum value—The engineBoots variable has reached the maximum allowed value. For more information, see message 212011.

Note The username appears after each reason listed.

Recommended Action Check the Secure Firewall Threat Defense SNMP server settings and confirm that the NMS configuration is using the expected user, authentication, and encryption settings. Enter the **show crypto accelerator statistics** command to isolate errors in the platform crypto module.

212009

Error Message `%FTD-5-212009: Configuration request for SNMP group groupname failed. User username reason`

Explanation A user has tried to change the SNMP server group configuration. One or more users that refer to the group have insufficient settings to comply with the requested group changes.

- **groupname**—A string that represents the group name
- *username* —A string that represents the username
- **reason**—A string that represents one of the following reasons:

- *missing auth-password* —A user has tried to add authentication to the group, and the user has not specified an authentication password

- *missing priv-password* —A user has tried to add privacy to the group, and the user has not specified an encryption password

- *reference group intended for removal* —A user has tried to remove a group that has users belonging to it

Recommended Action The user must update the indicated user configurations before changing the group or removing indicated users, and then add them again after making changes to the group.

212010

Error Message `%FTD-3-212010: Configuration request for SNMP user s failed. Host s reason`

Explanation A user has tried to change the SNMP server user configuration by removing one or more hosts that reference the user. One message is generated per host.

- **%s**—A string that represents the username or hostname
- *reason* —A string the represents the following reason:

- *references user intended for removal*— The name of the user to be removed from the host.

Recommended Action The user must either update the indicated host configuration before changing a user or remove the indicated hosts, then add them again after making changes to the user.

212011

Error Message `%FTD-3-212011: engineBoots is set to maximum value. Reason: Reason. User intervention necessary.`

For example:

```
%FTD-3-212011: SNMP engineBoots is set to maximum value. Reason: error accessing persistent
 data. User intervention necessary.
```

Explanation The device has rebooted 214783647 times, which is the maximum allowed value of the engineBoots variable, or an error reading the persistent value from flash memory has occurred. The engineBoots value is stored in flash memory in the flash:/snmp/*ctx-name* file, where *ctx-name* is the name of the context. In single mode, the name of this file is flash:/snmp/single_vf. In multi-mode, the name of the file for the admin context is flash:/snmp/admin. During a reboot, if the device is unable to read from the file or write to the file, the engineBoots value is set to the maximum.

- **%s**—A string that represents the reason that the engineBoots value is set to the maximum allowed value. The two valid strings are "device reboots" and "error accessing persistent data."

Recommended Action For the first string, the administrator must delete all SNMP Version 3 users and add them again to reset the engineBoots variable to 1. All subsequent Version 3 queries will fail until all users have been removed. For the second string, the administrator must delete the context-specific file, then delete all SNMP Version users, and add them again to reset the engineBoots variable to 1. All subsequent Version 3 queries will fail until all users have been removed.

212012

Error Message `%FTD-3-212012: Unable to write engine data to persistent storage.`

Explanation The SNMP engine data is written to the file, flash:/snmp/*context-name* . For example: in single mode, the data is written to the file, flash:/snmp/single_vf. In the admin context in multi-mode, the file is written to the directory, flash:/snmp/admin. The error may be caused by a failure to create the flash:/snmp directory or the flash:/snmp/*context-name* file. The error may also be caused by a failure to write to the file.

Recommended Action The system administrator should remove the flash:/snmp/*context-name* file, then remove all SNMP Version 3 users, and add them again. This procedure should recreate the flash:/snmp/*context-name* file. If the problem persists, the system administrator should try reformatting the flash.

214001

Error Message `%FTD-2-214001: Terminating manager session from IP_address on interface interface_name. Reason: incoming encrypted data (number bytes) longer than number bytes`

Explanation An incoming encrypted data packet destined for the Secure Firewall Threat Defense management port indicates a packet length exceeding the specified upper limit. This may be a hostile event. The Secure Firewall Threat Defense device immediately terminates this management connection.

Recommended Action Ensure that the management connection was initiated by Cisco Secure Policy Manager.

215001

Error Message `%FTD-2-215001:Bad route_compress() call, sdb = number`

Explanation An internal software error occurred.

Recommended Action Contact the Cisco TAC.

216001

Error Message `%FTD-n-216001: internal error in function: message`

Explanation Various internal errors have occurred that should not appear during normal operation. The severity level varies depending on the cause of the message.

- **n—**The message severity
- **function—**The affected component
- **message—**A message describing the cause of the problem

Recommended Action Search the Bug Toolkit for the specific text message and try to use the Output Interpreter to resolve the problem. If the problem persists, contact the Cisco TAC.

216002

Error Message `%FTD-3-216002: Unexpected event (major: major_id, minor: minor_id) received by task_string in function at line: line_num`

Explanation A task registers for event notification, but the task cannot handle the specific event. Events that can be watched include those associated with queues, booleans, and timer services. If any of the registered events occur, the scheduler wakes up the task to process the event. This message is generated if an unexpected event woke up the task, but it does not know how to handle the event.

If an event is left unprocessed, it can wake up the task very often to make sure that it is processed, but this should not occur under normal conditions. If this message appears, it does not necessarily mean the device is unusable, but something unusual has occurred and needs to be investigated.

- *major_id* —Event identifier
- *minor_id* — Event identifier
- *task_string* —Custom string passed by the task to identify itself
- *function* —The function that received the unexpected event
- *line_num* —Line number in the code

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

216003

Error Message `%FTD-3-216003: Unrecognized timer timer_ptr, timer_id received by task_string in function at line: line_num`

Explanation An unexpected timer event woke up the task, but the task does not know how to handle the event. A task can register a set of timer services with the scheduler. If any of the timers expire, the scheduler

wakes up the task to take action. This message is generated if the task is awakened by an unrecognized timer event.

An expired timer, if left unprocessed, wakes up the task continuously to make sure that it is processed, and this is undesirable. This should not occur under normal conditions. If this message appears, it does not necessarily mean the device is unusable, but something unusual has occurred and needs to be investigated.

- *timer_ptr* —Pointer to the timer
- *timer_id* —Timer identifier
- *task_string* —Custom string passed by the task to identify itself
- *function* —The function that received the unexpected event
- *line_num* —Line number in the code

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

216004

Error Message `%FTD-4-216004: prevented: error in function at file(line) - stack trace`

Explanation An internal logic error has occurred, which should not occur during normal operation.

- *error* —Internal logic error. Possible errors include the following:

- Exception

- Dereferencing null pointer

- Array index out of bounds

- Invalid buffer size

- Writing from input

- Source and destination overlap

- Invalid date

- Access offset from array indices

- *function* —The calling function that generated the error
- *file(line)* —The file and line number that generated the error
- *stack trace* —Full call stack traceback, starting with the calling function. For example: (“0x001010a4 0x00304e58 0x00670060 0x00130b04”)

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

217001

Error Message `%FTD-2-217001: No memory for string in string`

Explanation An operation failed because of low memory.

Recommended Action If sufficient memory exists, then send the error message, the configuration, and any details about the events leading up to the error to the Cisco TAC.

218001

Error Message `%FTD-2-218001: Failed Identification Test in slot# [fail #/res ].`

Explanation The module in **slot#** of the Secure Firewall Threat Defense device cannot be identified as a genuine Cisco product. Cisco warranties and support programs apply only to genuine Cisco products. If Cisco determines that the cause of a support issue is related to non-Cisco memory, SSM modules, SSC modules, or other modules, Cisco may deny support under your warranty or under a Cisco support program such as SmartNet.

Recommended Action If this message recurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.

218002

Error Message `%FTD-2-218002: Module slot# is a registered proto-type for Cisco Lab use only, and not certified for live network operation.`

Explanation The hardware in the specified location is a prototype module that came from a Cisco lab.

Recommended Action If this message reoccurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.

218003

Error Message `%FTD-2-218003: Module Version in slot# is obsolete. The module in slot = slot# is obsolete and must be returned via RMA to Cisco Manufacturing. If it is a lab unit, it must be returned to Proto Services for upgrade.`

Explanation Obsolete hardware has been detected or the **show module** command has been run for the module. This message is generated once per minute after it first appears.

Recommended Action If this message recurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.

218004

Error Message `%FTD-2-218004: Failed Identification Test in slot# [fail#/res]`

Explanation A problem occurred while identifying hardware in the specified location.

Recommended Action If this message recurs, copy it exactly as it appears on the console or in the system log. Research and try to resolve the error using the Output Interpreter. Also perform a search with the Bug Toolkit. If the problem persists, contact the Cisco TAC.

218005

Error Message `%FTD-2-218005: Inconsistency detected in the system information programmed in non-volatile memory.`

Explanation System information programmed in non-volatile memory is not consistent. This syslog will be generated during bootup if Secure Firewall Threat Defense device detects that the contents of the IDPROM are not identical to the contents of ACT2 EEPROM. Since the IDPROM and ACT2 EEPROM are programmed with exactly the same contents in manufacturing, this would happen either due to an error in manufacturing or if the IDPROM contents are tampered with.

Recommended Action If the message recurs, collect the output of the show tech-support command and contact Cisco TAC.

219002

Error Message `%FTD-3-219002: I2C_API_name() error, slot = slot_number, device = device_number, address = address, byte count = count. Reason: reason_string`

Explanation The I2C serial bus API has failed because of a hardware or software problem.

- *I2C_API_name* —The I2C API that failed, which can be one of the following:
  - I2C_read_byte_w_wait()
  - I2C_read_word_w_wait()
  - I2C_read_block_w_wait()
  - I2C_write_byte_w_wait()
  - I2C_write_word_w_wait()
  - I2C_write_block_w_wait()
  - I2C_read_byte_w_suspend()
  - I2C_read_word_w_suspend()
  - I2C_read_block_w_suspend()
  - I2C_write_byte_w_suspend()
  - I2C_write_word_w_suspend()
  - I2C_write_block_w_suspend()
- *slot_number* —The hexadecimal number of the slot where the I/O operation that generated the message occurred. The slot number cannot be unique to a slot in the chassis. Depending on the chassis, two different slots might have the same I2C slot number. Also, the value is not necessarily less than or equal to the number of slots. The value depends on the way the I2C hardware is wired.
- *device_number* —The hexadecimal number of the device on the slot for which the I/O operation was performed
- *address* —The hexadecimal address of the device on which the I/O operation occurred
- *byte_count* —The byte count in decimal format of the I/O operation
- *error_string* —The reason for the error, which can be one of the following:
  - I2C_BUS_TRANSACTION_ERROR
  - I2C_CHKSUM_ERROR
  - I2C_TIMEOUT_ERROR
  - I2C_BUS_COLLISION_ERROR
  - I2C_HOST_BUSY_ERROR
  - I2C_UNPOPULATED_ERROR
  - I2C_SMBUS_UNSUPPORT
  - I2C_BYTE_COUNT_ERROR
  - I2C_DATA_PTR_ERROR

Recommended Action Perform the following steps:

1. Log and review the messages and the errors associated with the event. If the message does not occur continuously and disappears after a few minutes, it might be because the I2C serial bus is busy.
2. Reboot the software running on the Secure Firewall Threat Defense device.
3. Power cycle the device. When you turn off the power, make sure that you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.