

# Syslog Messages 101001 to 199021

This chapter contains the following sections:


- Messages 101001 to 109213, on page 1
- Messages 110002 to 113045, on page 28
- Messages 114001 to 199021, on page 44


# Messages 101001 to 109213

This section includes messages from 101001 to 109213.

## 101001

**Error Message** `%FTD-1-101001: (Primary) Failover cable OK.`

**Explanation** The failover cable is present and functioning correctly. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

## 101002

**Error Message** `%FTD-1-101002: (Primary) Bad failover cable.`

**Explanation** The failover cable is present, but not functioning correctly. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Replace the failover cable.

## 101003, 101004

**Error Message** `%FTD-1-101003: (Primary) Failover cable not connected (this unit)`

**Error Message** `%FTD-1-101004: (Secondary) Failover cable not connected (other unit)`

**Explanation** Failover mode is enabled, but the failover cable is not connected to one unit of the failover pair. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Connect the failover cable to both units of the failover pair.

# 101005

**Error Message** `%FTD-1-101005: (Primary) Error reading failover cable status.`

**Explanation** The failover cable is connected, but the primary unit is unable to determine its status.

**Recommended Action** Replace the cable.

# 103001

**Error Message** `%FTD-1-103001: (Primary) No response from other firewall (reason code = code).`

**Explanation** The primary unit is unable to communicate with the secondary unit over the failover cable. Primary can also be listed as Secondary for the secondary unit. The following table lists the reason codes and the descriptions to determine why the failover occurred.

| Reason Code | Description |
|---|---|
| 1 | The local unit is not receiving the hello packet on the failover LAN interface when LAN failover occurs or on the serial failover cable when serial failover occurs, and declares that the peer is down. |
| 2 | An interface did not pass one of the four failover tests, which are as follows: 1) Link Up, 2) Monitor for Network Traffic, 3) ARP, and 4) Broadcast Ping. |
| 3 | No proper ACK for 15+ seconds after a command was sent on the serial cable. |
| 4 | The failover LAN interface is down, and other data interfaces are not responding to additional interface testing. In addition, the local unit is declaring that the peer is down. |

| Reason Code | Description |
|---|---|
| 5 | The standby peer went down during the configuration synchronization process. |
| 6 | Replication is not complete; the failover unit is not synchronized. |

**Recommended Action** Verify that the failover cable is connected correctly and both units have the same hardware, software, and configuration. If the problem persists, contact the Cisco TAC.

# 103002

**Error Message** `%FTD-1-103002: (Primary) Other firewall network interface` *`interface_number`* `OK.`

**Explanation** The primary unit has detected that the network interface on the secondary unit is okay. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

# 103003

**Error Message** `%FTD-1-103003: (Primary) Other firewall network interface` *`interface_number`* `failed.`

**Explanation** The primary unit has detected a bad network interface on the secondary unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Check the network connections on the secondary unit and the network hub connection. If necessary, replace the failed network interface.

# 103004

**Error Message** `%FTD-1-103004: (Primary) Other firewall reports this firewall failed.` *`reason-string`*

**Explanation** The primary unit received a message from the secondary unit indicating that the primary unit has failed. Primary can also be listed as Secondary for the secondary unit. The reason can be one of the following:

- Missed poll packets on failover command interface exceeded threshold.
- LAN failover interface failed.
- Peer failed to enter Standby Ready state.
- Failed to complete configuration replication. This firewall's configuration may be out of sync.
- Failover message transmit failure and no ACK for busy condition received.

**Recommended Action** Verify the status of the primary unit.

# 103005

**Error Message** `%FTD-1-103005: (Primary) Other firewall reporting failure. Reason: SSM_card_failure`

**Explanation** The secondary unit has reported an SSM card failure to the primary unit. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Verify the status of the secondary unit.

# 103006

**Error Message** `%FTD-1-103006: (Primary|Secondary) Mate version ver_num is not compatible with ours ver_num.`

**Explanation** The Secure Firewall Threat Defense device has detected a peer unit that is running a version that is different than the local unit and is not compatible with the HA Hitless Upgrade feature.

- *ver_num* —Version number.

**Recommended Action** Install the same or a compatible version image on both units.

# 103007

**Error Message** `%FTD-1-103007: (Primary|Secondary) Mate version ver_num is not identical with ours ver_num.`

**Explanation** The Secure Firewall Threat Defense device has detected that the peer unit is running a version that is not identical, but supports Hitless Upgrade and is compatible with the local unit. The system performance may be degraded because the image version is not identical, and the Secure Firewall Threat Defense device may develop a stability issue if the nonidentical image runs for an extended period.

- **ver_num**—Version number

**Recommended Action** Install the same image version on both units as soon as possible.

# 103008

**Error Message** `%FTD-1-103008: host Mate hwdib index Idx is not identical with ours.`

**Explanation** The number of interfaces on the active and standby units is not the same.

**Recommended Action** Verify that the units have the same number of interfaces. You might need to install additional interface modules, or use different devices. After the physical interfaces match, force a configuration sync by suspending and then resuming HA.

# 104001, 104002

**Error Message** `%FTD-1-104001: (Primary) Switching to ACTIVE - string.`

**Error Message** `%FTD-1-104002: (Secondary) Switching to STANDBY - string.`

**Explanation** You have forced the failover pair to switch roles, either by entering the **failover active** command on the standby unit, or the **no failover active** command on the active unit. Primary can also be listed as Secondary for the secondary unit. Possible values for the string variable are as follows:

- state check
- bad/incomplete config
- ifc [interface] check, mate is healthier
- the other side wants me to standby
- in failed state, cannot be active
- switch to failed state
- other unit set to active by CLI config command fail active

**Recommended Action** If the message occurs because of manual intervention, no action is required. Otherwise, use the cause reported by the secondary unit to verify the status of both units of the pair.

# 104003

**Error Message** `%FTD-1-104003: (Primary) Switching to FAILED.`

**Explanation** The primary unit has failed.

**Recommended Action** Check the messages for the primary unit for an indication of the nature of the problem (see message 104001). Primary can also be listed as Secondary for the secondary unit.

# 104004

**Error Message** `%FTD-1-104004: (Primary) Switching to OK.`

**Explanation** A previously failed unit reports that it is operating again. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

# 105001

**Error Message** `%FTD-1-105001: (Primary) Disabling failover.`

**Explanation** In version 7.x and later, this message may indicate the following: failover has been automatically disabled because of a mode mismatch (single or multiple), a license mismatch (encryption or context), or a hardware difference (one unit has an IPS SSM installed, and its peer has a CSC SSM installed). Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

# 105002

**Error Message** `%FTD-1-105002: (Primary) Enabling failover.`

**Explanation** You have used the **failover** command with no arguments on the console, after having previously disabled failover. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

# 105003

**Error Message** `%FTD-1-105003: (Primary) Monitoring on interface interface_name waiting`

**Explanation** The Secure Firewall Threat Defense device is testing the specified network interface with the other unit of the failover pair. Primary can also be listed as Secondary for the secondary unit.

**Note** There could be delay in the logging of syslog when compared to the actual status change. This delay is due to the poll time and hold time that is configured for the interface monitoring.

**Recommended Action** None required. The Secure Firewall Threat Defense device monitors its network interfaces frequently during normal operation.

# 105004

**Error Message** `%FTD-1-105004: (Primary) Monitoring on interface interface_name normal`

**Explanation** The test of the specified network interface was successful. Primary can also be listed as Secondary for the secondary unit.

**Note** There could be delay in the logging of syslog when compared to the actual status change. This delay is due to the poll time and hold time that is configured for the interface monitoring.

**Recommended Action** None required.

# 105005

**Error Message** `%FTD-1-105005: (Primary) Lost Failover communications with mate on interface interface_name`

**Explanation** One unit of the failover pair can no longer communicate with the other unit of the pair. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Verify that the network connected to the specified interface is functioning correctly.

# 105006, 105007

**Error Message** `%FTD-1-105006: (Primary) Link status 'Up' on interface interface_name`

**Error Message** `%FTD-1-105007: (Primary) Link status 'Down' on interface interface_name.`

**Explanation** The results of monitoring the link status of the specified interface have been reported. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** If the link status is down, verify that the network connected to the specified interface is operating correctly.

# 105008

**Error Message** `%FTD-1-105008: (Primary) Testing Interface interface_name`

**Explanation** Testing of a specified network interface has occurred. This testing is performed only if the Secure Firewall Threat Defense device fails to receive a message from the standby unit on that interface after the expected interval. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required.

# 105009

**Error Message** `%FTD-1-105009: (Primary) Testing on interface interface_name {Passed|Failed}`

**Explanation** The result (either Passed or Failed) of a previous interface test has been reported. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** None required if the result is Passed. If the result is Failed, you should check the network cable connection to both failover units, that the network itself is functioning correctly, and verify the status of the standby unit.

# 105010

**Error Message** `%FTD-3-105010: (Primary) Failover message block alloc failed`

**Explanation** Block memory was depleted. This is a transient message and the Secure Firewall Threat Defense device should recover. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Use the show blocks command to monitor the current block memory.

# 105011

**Error Message** `%FTD-1-105011: (Primary) Failover cable communication failure`

**Explanation** The failover cable is not permitting communication between the primary and secondary units. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Ensure that the cable is connected correctly.

# 105020

**Error Message** `%FTD-1-105020: (Primary) Incomplete/slow config replication`

**Explanation** When a failover occurs, the active Secure Firewall Threat Defense device detects a partial configuration in memory. Normally, this is caused by an interruption in the replication service. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** After the Secure Firewall Threat Defense device detects the failover, the Secure Firewall Threat Defense device automatically reboots and loads the configuration from flash memory and/or resynchronizes with another Secure Firewall Threat Defense device. If failovers occurs continuously, check the failover configuration and make sure that both Secure Firewall Threat Defense devices can communicate with each other.

# 105021

**Error Message** `%FTD-1-105021: (Failover_unit) Standby unit failed to sync due to a locked context_name config. Lock held by lock_owner_name`

**Explanation** During configuration synchronization, a standby unit will reload itself if some other process locks the configuration for more than five minutes, which prevents the failover process from applying the new configuration. This can occur when an administrator pages through a running configuration on the standby unit while configuration synchronization is in process. See also the **show running-config** command in privileged EXEC mode and the **pager lines num** command in global configuration mode in the *Command Reference Guides*.

**Recommended Action** Avoid viewing or modifying the configuration on the standby unit when it first boots up and is in the process of establishing a failover connection with the active unit.

# 105022

**Error Message** `%FTD-1-105022: (host) Config replication failed with reason = reason`

**Explanation** When high availability replication fails, the message is generated. Where,

- *host*—Indicates the current failover unit, namely, primary or secondary.
- *reason*—The time out expiry reason for termination of the failover configuration replication:
  - CFG_SYNC_TIMEOUT—Where, the 60-second timer for the configuration to be replicated from active to standby lapses, and the device starts to reboot.
  - CFG_PROGRESSION_TIMEOUT—Where, the interval timer of 6 hours which governs the high availability configuration replication lapses.

**Recommended Action** None.

# 105031

**Error Message** `%FTD-1-105031: Failover LAN interface is up`

**Explanation** The LAN failover interface link is up.

**Recommended Action** None required.

# 105032

**Error Message** `%FTD-1-105032: LAN Failover interface is down`

**Explanation** The LAN failover interface link is down.

**Recommended Action** Check the connectivity of the LAN failover interface. Make sure that the speed or duplex setting is correct.

# 105033

**Error Message** `%FTD-1-105033: LAN FO cmd Iface down and up again`

**Explanation** LAN interface of failover gone down.

**Recommended Action** Verify the failover link, might be a communication problem.

## 105034

**Error Message** `%FTD-1-105034: Receive a LAN_FAILOVER_UP message from peer.`

**Explanation** The peer has just booted and sent the initial contact message.

**Recommended Action** None required.

## 105035

**Error Message** `%FTD-1-105035: Receive a LAN failover interface down msg from peer.`

**Explanation** The peer LAN failover interface link is down. The unit switches to active mode if it is in standby mode.

**Recommended Action** Check the connectivity of the peer LAN failover interface.

## 105036

**Error Message** `%FTD-1-105036: dropped a LAN Failover command message.`

**Explanation** The Secure Firewall Threat Defense device dropped an unacknowledged LAN failover command message, indicating a connectivity problem exists on the LAN failover interface.

**Recommended Action** Check that the LAN interface cable is connected.

## 105037

**Error Message** `%FTD-1-105037: (`*`Primary and Standby`*` ) Both units are switching back and forth as the active unit`

**Explanation** The primary and standby units are switching back and forth as the active unit, indicating a LAN failover connectivity problem or software bug exists.

**Recommended Action** Make sure that the LAN interface cable is connected.

## 105038

**Error Message** `%FTD-1-105038: (Primary) Interface count mismatch`

**Explanation** When a failover occurs, the active Secure Firewall Threat Defense device detects a partial configuration in memory. Normally, this is caused by an interruption in the replication service. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Once the failover is detected by the Secure Firewall Threat Defense device, the Secure Firewall Threat Defense device automatically reboots and loads the configuration from flash memory and/or resynchronizes with another Secure Firewall Threat Defense device. If failovers occur continuously, check the failover configuration and make sure that both Secure Firewall Threat Defense devices can communicate with each other.

# 105039

**Error Message** `%FTD-1-105039: (Primary) Unable to verify the Interface count with mate. Failover may be disabled in mate.`

**Explanation** Failover initially verifies that the number of interfaces configured on the primary and secondary Secure Firewall Threat Defense devices are the same. This message indicates that the primary Secure Firewall Threat Defense device is not able to verify the number of interfaces configured on the secondary Secure Firewall Threat Defense device. This message indicates that the primary Secure Firewall Threat Defense device is not able to communicate with the secondary Secure Firewall Threat Defense device over the failover interface. Primary can also be listed as Secondary for the secondary unit.

**Recommended Action** Verify the failover LAN, interface configuration, and status on the primary and secondary Secure Firewall Threat Defense devices. Make sure that the secondary Secure Firewall Threat Defense device is running the Secure Firewall Threat Defense device application and that failover is enabled.

# 105040

**Error Message** `%FTD-1-105040: (Primary) Mate failover version is not compatible.`

**Explanation** The primary and secondary Secure Firewall Threat Defense devices should run the same failover software version to act as a failover pair. This message indicates that the secondary Secure Firewall Threat Defense device failover software version is not compatible with the primary Secure Firewall Threat Defense device. Failover is disabled on the primary Secure Firewall Threat Defense device. Primary can also be listed as Secondary for the secondary Secure Firewall Threat Defense device.

**Recommended Action** Maintain consistent software versions between the primary and secondary Secure Firewall Threat Defense devices to enable failover.

# 105041

**Error Message** `%FTD-1-105041: cmd failed during sync`

**Explanation** Replication of the nameif command failed, because the number of interfaces on the active and standby units is not the same.

**Recommended Action** Verify that the units have the same number of interfaces. You might need to install additional interface modules, or use different devices. After the physical interfaces match, force a configuration sync by suspending and then resuming HA.

# 105042

**Error Message** `%FTD-1-105042: (Primary) Failover interface OK`

**Explanation** The interface that sends failover messages could go down when physical status of the failover link is down or when L2 connectivity between the failover peers is lost resulting in dropping of ARP packets. This message is generated after restoring the L2 ARP connectivity.

**Recommended Action** None required.

# 105043

**Error Message** `%FTD-1-105043: (Primary) Failover interface failed`

**Explanation** This syslog is generated when physical status of the failover link is down or when L2 connectivity between the failover peers is lost. The disconnection results in loss of ARP packets flowing between the units.

**Recommended Action**

- Check the physical status of the failover link, ensure its physical and operational status is functional.
- Ensure ARP packets flow through the transit path of the failover links between the failover pairs.

# 105044

**Error Message** `%FTD-1-105044: (Primary) Mate operational mode (mode) is not compatible with my mode (mode).`

**Explanation** When the operational mode (single or multiple) does not match between failover peers, failover will be disabled.

**Recommended Action** Configure the failover peers to have the same operational mode, and then reenable failover.

# 105045

**Error Message** `%FTD-1-105045: (Primary) Mate license (number_contexts) is not compatible with my license (number_contexts).`

**Explanation** When the feature licenses do not match between failover peers, failover will be disabled.

**Recommended Action** Configure the failover peers to have the same feature license, and then reenable failover.

# 105046

**Error Message** `%FTD-1-105046: (Primary|Secondary) Mate has a different chassis`

**Explanation** Two failover units have a different type of chassis. For example, one has a three-slot chassis; the other has a six-slot chassis.

**Recommended Action** Make sure that the two failover units are the same.

# 105047

**Error Message** `%FTD-1-105047: Mate has a io_card_name1 card in slot slot_number which is different from my io_card_name2`

**Explanation** The two failover units have different types of cards in their respective slots.

**Recommended Action** Make sure that the card configurations for the failover units are the same.

# 105048

**Error Message** `%FTD-1-105048: (unit) Mate's service module (application) is different from mine (application).`

**Explanation** The failover process detected that different applications are running on the service modules in the active and standby units. The two failover units are incompatible if different service modules are used.

- **unit**—Primary or secondary
- **application**—The name of the application, such as InterScan Security Card

**Recommended Action** Make sure that both units have identical service modules before trying to reenable failover.

# 105050

**Error Message** `%FTD-3-105050: (host) Number of Ethernet interfaces on Standby unit (int_number) is less than number on Active unit (int_number).`

**Explanation** Number of Ethernet interfaces on standby unit is less than that on active unit.

**Recommended Action** Secure Firewall Threat Defense device with same number of interfaces should be paired up with each other. Verify that the units have the same number of interfaces. You might need to install additional interface modules, or use different devices. After the physical interfaces match, force a configuration sync by suspending and then resuming HA.

# 105052

**Error Message** `%FTD-3-105052: HA:cipher in use algorithm name strong encryption is status, please reboot to use strong cipher and preferably change the key in use`

**Explanation** When the failover key is configured prior to a license update, the weaker cipher is not switched to a stronger cipher automatically. This syslog is generated, every 30 seconds to alert that a weaker cipher is still being used when a stronger cipher is available.

**Example** %FTD-3-105052 HA cipher in use DES strong encryption is AVAILABLE, please reboot to use strong cipher and preferably change the key in use.

**Recommended Action** Remove the failover key configuration and reconfigure the key. Reload the standby, and then reload the active device.

# 106001

**Error Message** `%FTD-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`

**Explanation** An attempt was made to connect to an inside address is denied by the security policy that is defined for the specified traffic type. The IP address displayed is the real IP address instead of the IP address that appears through NAT. Possible tcp_flags values correspond to the flags in the TCP header that were present when the connection was denied. For example, a TCP packet arrived for which no connection state exists in the Secure Firewall Threat Defense device, and it was dropped. The tcp_flags in this packet are FIN and ACK.

The tcp_flags are as follows:

- ACK—The acknowledgment number was received
- FIN—Data was sent
- PSH—The receiver passed data to the application
- RST—The connection was reset

- SYN—Sequence numbers were synchronized to start a connection
- URG—The urgent pointer was declared valid

**Recommended Action** None required.

# 106002

**Error Message** `%FTD-2-106002: protocol Connection denied by outbound list acl_ID src inside_address dest outside_address`

**Explanation** The specified connection failed because of an **outbound deny** command. The **protocol** variable can be ICMP, TCP, or UDP.

**Recommended Action** Use the **show outbound** command to check outbound lists.

# 106006

**Error Message** `%FTD-2-106006: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name`

**Explanation** An inbound UDP packet was denied by the security policy that is defined for the specified traffic type.

**Recommended Action** None required.

# 106007

**Error Message** `%FTD-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}`

**Explanation** A UDP packet containing a DNS query or response was denied.

**Recommended Action** If the inside port number is 53, the inside host probably is set up as a caching name server. Add an **access-list** command statement to permit traffic on UDP port 53 and a translation entry for the inside host. If the outside port number is 53, a DNS server was probably too slow to respond, and the query was answered by another server.

# 106010

**Error Message** `%FTD-3-106010: Deny inbound protocolsrc [interface_name : source_address/source_port ] [([idfw_user | FQDN_string ], sg_info )] dst [interface_name : dest_address /dest_port ][([idfw_user | FQDN_string ], sg_info )]`

**Explanation** An inbound connection was denied by your security policy.

**Recommended Action** Modify the security policy if traffic should be permitted. If the message occurs at regular intervals, contact the remote peer administrator.

# 106011

**Error Message** `%FTD-3-106011: Deny inbound (No xlate) protocol_src_Interface:IP/port_dst_Interface-nameif:IP/port`

**Explanation** The message appears under normal traffic conditions if there are internal users that are accessing the Internet through a web browser. Any time a connection is reset, when the host at the end of the connection sends a packet after the Secure Firewall Threat Defense device receives the connection reset, this message appears. It can typically be ignored.

**Recommended Action** Prevent this message from getting logged to the syslog server by entering the **no logging message 106011** command.

# 106012

**Error Message** `%FTD-6-106012: Deny IP from IP_address to IP_address, IP options: "hex"`

**Explanation** An IP packet was seen with IP options. Because IP options are considered a security risk, the packet was discarded.

**Recommended Action** Contact the remote host system administrator to determine the problem. Check the local site for loose source routing or strict source routing.

# 106013

**Error Message** `%FTD-2-106013: Dropping echo request from IP_address to PAT address IP_address`

**Explanation** The Secure Firewall Threat Defense device discarded an inbound ICMP Echo Request packet with a destination address that corresponds to a PAT global address. The inbound packet is discarded because it cannot specify which PAT host should receive the packet.

**Recommended Action** None required.

# 106014

**Error Message** `%FTD-3-106014: Deny inbound src`

**Explanation** The Secure Firewall Threat Defense device denied any inbound ICMP packet access. By default, all ICMP packets are denied access unless specifically allowed.

**Recommended Action** None required.

# 106015

**Error Message** `%FTD-6-106015: Deny TCP (no connection) from IP_address /port to IP_address /port flags tcp_flags on interface interface_name.`

**Explanation** The Secure Firewall Threat Defense device discarded a TCP packet that has no associated connection in the Secure Firewall Threat Defense connection table. The Secure Firewall Threat Defense device looks for a SYN flag in the packet, which indicates a request to establish a new connection. If the SYN flag is not set, and there is no existing connection, the Secure Firewall Threat Defense device discards the packet.

**Recommended Action** None required unless the Secure Firewall Threat Defense device receives a large volume of these invalid TCP packets. If this is the case, trace the packets to the source and determine the reason these packets were sent.

# 106016

**Error Message** `%FTD-2-106016: Deny IP spoof from (ip_address) to ip_address on interface interface_name`

**Explanation** A packet arrived at the Secure Firewall Threat Defense interface that has a destination IP address of 0.0.0.0 and a destination MAC address of the Secure Firewall Threat Defense interface. In addition, this message is generated when the Secure Firewall Threat Defense device discarded a packet with an invalid source address, which may include one of the following or some other invalid address:

- Loopback network (127.0.0.0)
- Broadcast (limited, net-directed, subnet-directed, and all-subnets-directed)
- The destination host (land.c)

To further enhance spoof packet detection, use the **icmp** command to configure the Secure Firewall Threat Defense device to discard packets with source addresses belonging to the internal network, because the **access-list** command has been deprecated and is no longer guaranteed to work correctly.

**Recommended Action** Determine if an external user is trying to compromise the protected network. Check for misconfigured clients.

# 106017

**Error Message** `%FTD-2-106017: Deny IP due to Land Attack from IP_address to IP_address`

**Explanation** The Secure Firewall Threat Defense device received a packet with the IP source address equal to the IP destination, and the destination port equal to the source port. This message indicates a spoofed packet that is designed to attack systems. This attack is referred to as a Land Attack.

**Recommended Action** If this message persists, an attack may be in progress. The packet does not provide enough information to determine where the attack originates.

# 106018

**Error Message** `%FTD-2-106018: ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address`

**Explanation** The outgoing ICMP packet with the specified ICMP from local host (inside_address) to the foreign host (outside_address) was denied by the outbound ACL list.

**Recommended Action** None required.

# 106020

**Error Message** `%FTD-2-106020: Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address`

**Explanation** The Secure Firewall Threat Defense device discarded an IP packet with a teardrop signature containing either a small offset or fragment overlapping. This is a hostile event that circumvents the Secure Firewall Threat Defense device or an Intrusion Detection System.

**Recommended Action** Contact the remote peer administrator or escalate this issue according to your security policy.

# 106021

**Error Message** `%FTD-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name`

**Explanation** An attack is in progress. Someone is attempting to spoof an IP address on an inbound connection. Unicast RPF, also known as reverse route lookup, detected a packet that does not have a source address represented by a route and assumes that it is part of an attack on your Secure Firewall Threat Defense device.

This message appears when you have enabled Unicast RPF with the ip verify reverse-path command. This feature works on packets input to an interface; if it is configured on the outside, then the Secure Firewall Threat Defense device checks packets arriving from the outside.

The Secure Firewall Threat Defense device looks up a route based on the source_address. If an entry is not found and a route is not defined, then this message appears and the connection is dropped.

If there is a route, the Secure Firewall Threat Defense device checks which interface it corresponds to. If the packet arrived on another interface, it is either a spoof or there is an asymmetric routing environment that has more than one path to a destination. The Secure Firewall Threat Defense device does not support asymmetric routing.

If the Secure Firewall Threat Defense device is configured on an internal interface, it checks static route command statements or RIP, and if the source_address is not found, then an internal user is spoofing their address.

**Recommended Action** Even though an attack is in progress, if this feature is enabled, no user action is required. The Secure Firewall Threat Defense device repels the attack.

# 106022

**Error Message** `%FTD-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name`

**Explanation** A packet matching a connection arrived on a different interface from the interface on which the connection began. In addition, the ip verify reverse-path command is not configured.

For example, if a user starts a connection on the inside interface, but the Secure Firewall Threat Defense device detects the same connection arriving on a perimeter interface, the Secure Firewall Threat Defense device has more than one path to a destination. This is known as asymmetric routing and is not supported on the Secure Firewall Threat Defense device.

An attacker also might be attempting to append packets from one connection to another as a way to break into the Secure Firewall Threat Defense device. In either case, the Secure Firewall Threat Defense device shows this message and drops the connection.

**Recommended Action** Check that the routing is not asymmetric.

# 106023

**Error Message** `%FTD-4-106023: Deny interface_name by access-group "source_address" [source_port, idfw_user]`

**Explanation** A real IP packet was denied by the ACL. This message appears even if you do not have the **log** option enabled for an ACL. The IP address is the real IP address instead of the values that display through NAT. Both user identity information and FQDN information is provided for the IP addresses if a matched

one is found. The Secure Firewall Threat Defense device logs either identity information (domain\user) or FQDN (if the username is not available). If the identity information or FQDN is available, the Secure Firewall Threat Defense device logs this information for both the source and destination.

**Recommended Action** If messages persist from the same source address, a footprinting or port scanning attempt might be occurring. Contact the remote host administrator.

# 106024

**Error Message** `%FTD-2-106024: Access rules memory exhausted. Aborting current compilation and continuing to use the existing access rules`

**Explanation** The access list compilation process has run out of memory. All configuration information that has been added since the last successful access list was removed from the Secure Firewall Threat Defense device, and the most recently compiled set of access lists will continue to be used.

**Recommended Action** Access lists, AAA, ICMP, SSH, Telnet, and other rule types are stored and compiled as access list rule types. Remove some of these rule types so that others can be added.

# 106025, 106026

**Error Message** `%FTD-6-106025: Failed to determine security context for packet: vlan`*`source Vlan`* `src` *`source_address/source_port`* `dest` *`dest_address/dest_port_protocol`*

**Error Message** `%FTD-6-106026: Failed to determine security context for packet:` *`source_vlan`* `src` *`source_address/source_port`* `dest` *`dest_address/dest_port_protocol`*

**Explanation** The security context of the packet in multiple context mode cannot be determined. Both messages can be generated for IP packets being dropped in either router and transparent mode.

**Recommended Action** None required.

# 106027

**Error Message** `%FTD-4-106027: Deny` *`int_type`* `src` *`src_address:src_mac`* `dst` *`dst_address:dest_mac`* `by access-group` *`"access-list name"`*.

**Explanation** An non IP packet was denied by the ACL. This message is displayed even if you do not have the log option enabled for an extended ACL.

**Recommended Action** If messages persist from the same source address, it might indicate a foot-printing or port-scanning attempt. Contact the remote host administrator.

# 106100

**Error Message** `%FTD-6-106100: access-list` *`acl_ID protocol interface_name source_address/source_port(idfw_user)sg_info -> interface_name/dest_address(dest_port)idfw_user`* `hit-cnt` *`sg_info number [string, number]`*

**Explanation** The initial occurrence or the total number of occurrences during an interval are listed. This message provides more information than message 106023, which only logs denied packets, and does not include the hit count or a configurable level.

When an access-list line has the *log* argument, it is expected that this message ID might be triggered because of a nonsynchronized packet reaching the Secure Firewall Threat Defense device and being evaluated by the access list. For example, if an ACK packet is received on the Secure Firewall Threat Defense device (for which no TCP connection exists in the connection table), the Secure Firewall Threat Defense device might generate message 106100, indicating that the packet was permitted; however, the packet is later correctly dropped because of no matching connection.

The following list describes the message values:

- permitted | denied | est-allowed—These values specify if the packet was permitted or denied by the ACL. If the value is est-allowed, the packet was denied by the ACL but was allowed for an already established session (for example, an internal user is allowed to accesss the Internet, and responding packets that would normally be denied by the ACL are accepted).
- *protocol* —TCP, UDP, ICMP, or an IP protocol number.
- *interface_name* —The interface name for the source or destination of the logged flow. The VLAN interfaces are supported.
- *source_address* —The source IP address of the logged flow. The IP address is the real IP address instead of the values that display through NAT.
- *dest_address* —The destination IP address of the logged flow. The IP address is the real IP address instead of the values that display through NAT.
- *source_port* —The source port of the logged flow (TCP or UDP). For ICMP, the number after the source port is the message type.
- *idfw_user*— The user identity username, including the domain name that is added to the existing syslog when the Secure Firewall Threat Defense device can find the username for the IP address.
- *sg_info*— The security group tag that is added to the syslog when the Secure Firewall Threat Defense device can find a security group tag for the IP address. The security group name is displayed with the security group tag, if available.
- *dest_port* —The destination port of the logged flow (TCP or UDP). For ICMP, the number after the destination port is the ICMP message code, which is available for some message types. For type 8, it is always 0. For a list of ICMP message types, see the following URL: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- hit-cnt *number* —The number of times this flow was permitted or denied by this ACL entry in the configured time interval. The value is 1 when the Secure Firewall Threat Defense device generates the first message for this flow.
- first hit—The first message generated for this flow.
- *number* -second interval—The interval in which the hit count is accumulated. Set this interval using the **access-list** command with the **interval** option.
- hash codes—Two are always printed for the object group ACE and the constituent regular ACE. Values are determined on which ACE that the packet hit. To display these hash codes, enter the **show-access list** command.

**Recommended Action** None required.

# 106101

**Error Message** `%FTD-1-106101: Number of cached deny-flows for ACL log has reached limit (number)`

**Explanation**If you have enabled the **log** option for an extended ACL and through FlexConfig replaced the Global Access Group on the Secure Firewall Threat Defense device, and when a traffic flow matches the ACL statement, the device caches the flow information and this syslog is generated. This message indicates that

the number of matching flows that are cached on the Secure Firewall Threat Defense device exceeds the user-configured limit (using the **access-list deny-flow-max** command). This message might be generated as a result of a DoS attack.

- *number*— The limit configured using the **access-list deny-flow-max** command

**Recommended Action** None required.

# 106102

**Error Message** `%FTD-[1-7]-106102: access-list acl_ID permitted source_address for user 'user_name'source_address/source_port(interface_name) -> dest_address/dest_port(interface_name) hit-cnt sg_info number [string, number]`

**Explanation** A packet was either permitted or denied by an access-list that was applied through a VPN filter. This message is the VPN/AAA filter equivalent of message 106100.

**Recommended Action** None required.

# 106103

**Error Message** `%FTD-4-106103: access-list acl_ID denied protocol for user 'username' source_address/source_port_interface_name(interface_name) -> dest_address/dest_port(interface_name) hit-cnt sg_info number [string, number]`

**Explanation** A packet was denied by an access-list that was applied through a VPN filter. This message is the VPN/AAA filter equivalent of message106023.

**Recommended Action** None required.

# 107001

**Error Message** `%FTD-1-107001: RIP auth failed from IP_address: version=number, type=string, mode=string, sequence=number on interface interface_name`

**Explanation** The Secure Firewall Threat Defense device received a RIP reply message with bad authentication. This message might be caused by a misconfiguration on the router or the Secure Firewall Threat Defense device or by an unsuccessful attempt to attack the routing table of the Secure Firewall Threat Defense device.

**Recommended Action** This message indicates a possible attack and should be monitored. If you are not familiar with the source IP address listed in this message, change your RIP authentication keys between trusted entities. An attacker might be trying to determine the existing keys.

# 109011

**Error Message** `%FTD-2-109011: Authen Session Start: user 'user', sid number`

**Explanation** An authentication session started between the host and the Secure Firewall Threat Defense device and has not yet completed.

**Recommended Action** None required.

# 109012

**Error Message** `%FTD-5-109012: Authen Session End: user 'user', sid number, elapsed number seconds`

**Explanation** The authentication cache has timed out. Users must reauthenticate on their next connection. You can change the duration of this timer with the timeout uauth command.

**Recommended Action** None required.

# 109013

**Error Message** `%FTD-3-109013: User must authenticate before using this service`

**Explanation** The user must be authenticated before using the service.

**Recommended Action** Authenticate using FTP, Telnet, or HTTP before using the service.

# 109016

**Error Message** `%FTD-3-109016: Cannot find authorization ACL 'acl_id' on 'server_name' for user 'user'`

**Explanation** The specified on the AAA server for this user does not exist on the Secure Firewall Threat Defense device. This error can occur if you configure the AAA server before you configure the Secure Firewall Threat Defense device. The Vendor-Specific Attribute (VSA) on your AAA server might be one of the following values:

- acl=acl_ID
- shell:acl=acl_ID
- ACS:CiscoSecured-Defined-ACL=acl_ID

**Recommended Action** Add the ACL to the Secure Firewall Threat Defense device, making sure to use the same name specified on the AAA server.

# 109018

**Error Message** `%FTD-3-109018: Downloaded ACL 'acl_ID' is empty`

**Explanation** The downloaded authorization has no ACEs. This situation might be caused by misspelling the attribute string *ip:inacl#* or omitting the access-list command.

```
junk:junk# 1=permit tcp any any eq junk ip:inacl#1=”
```

**Recommended Action** Correct the ACL components that have the indicated error on the AAA server.

# 109019

**Error Message** `%FTD-3-109019: Downloaded ACL 'acl_ID' has parsing error; ACE: 'string'; string`

**Explanation** An error occurred during parsing the sequence number NNN in the attribute string ip:inacl#NNN= of a downloaded authorization. The reasons include: - missing = - contains nonnumeric, nonpace characters between # and = - NNN is greater than 999999999.

```
ip:inacl# 1 permit tcp any any
ip:inacl# 1junk2=permit tcp any any
ip:inacl# 1000000000=permit tcp any any
```

**Recommended Action** Correct the ACL element that has the indicated error on the AAA server.

# 109020

**Error Message** `%FTD-3-109020: Downloaded ACL has config error; ACE`

**Explanation** One of the components of the downloaded authorization has a configuration error. The entire text of the element is included in the message. This message is usually caused by an invalid access-list command statement.

**Recommended Action** Correct the ACL component that has the indicated error on the AAA server.

# 109026

**Error Message** `%FTD-3-109026: [ aaa_protocol ] Invalid reply digest received; shared server key may be mismatched.`

**Explanation** The response from the AAA server cannot be validated. The configured server key is probably incorrect. This message may be generated during transactions with RADIUS or TACACS+ servers.

Verify that the server key, configured using the **aaa-server** command, is correct.

# 109027

**Error Message** `%FTD-4-109027: [ aaa_protocol ] Unable to decipher response message Server = server_IP_address, User = user`

**Explanation** The response from the AAA server cannot be validated. The configured server key is probably incorrect. This message may be displayed during transactions with RADIUS or TACACS+ servers. The server_IP_address is the IP address of the relevant AAA server. The user is the user name associated with the connection.

**Recommended Action** Verify that the server key, configured using the **aaa-server** command, is correct.

# 109029

**Error Message** `%FTD-5-109029: Parsing downloaded ACL: string`

**Explanation** A syntax error occurred while parsing an access list that was downloaded from a RADIUS server during user authentication.

- *string* —An error message detailing the syntax error that prevented the access list from parsing correctly

**Recommended Action** Use the information presented in this message to identify and correct the syntax error in the access list definition within the RADIUS server configuration.

# 109030

**Error Message** `%FTD-4-109030: Autodetect ACL convert wildcard did not convert ACL access_list_source dest netmask netmask`

**Explanation**A dynamic ACL that is configured on a RADIUS server is not converted by the mechanism for automatically detecting wildcard netmasks. The problem occurs because this mechanism cannot determine if the netmask is a wildcard or a normal netmask.

- **access_list—**The access list that cannot be converted
- **source—**The source IP address
- **dest—**The destination IP address
- **netmask—**The subnet mask for the destination or source address in dotted-decimal notation

**Recommended Action** Check the access list netmask on the RADIUS server for the wildcard configuration. If the netmask is supposed to be a wildcard, and if all access list netmasks on that server are wildcards, then use the wildcard setting for **acl-netmask-convert** for the AAA server. Otherwise, change the netmask to a normal netmask or to a wildcard netmask that does not contain holes (that is, where the netmask presents consecutive binary 1s. For example, 00000000.00000000.00011111.11111111 or hex 0.0.31.255). If the mask is supposed to be normal and all access list netmasks on that server are normal, then use the normal setting for **acl-netmask-convert** for the AAA server.

# 109032

**Error Message** `%FTD-3-109032: Unable to install ACL 'access_list', downloaded for user username; Error in ACE: 'ace'`

**Explanation** The Secure Firewall Threat Defense device received an access control list from a RADIUS server to apply to a user connection, but an entry in the list contains a syntax error. Th euse of a list containing an error could result in the violation of a security policy, so the Secure Firewall Threat Defense device failed to authenticate the user.

- *access_list* —The name assigned to the dynamic access list as it would appear in the output of the **show access-list** command
- *username* —The name of the user whose connection will be subject to this access list
- *ace* —The access list entry that was being processed when the error was detected

**Recommended Action** Correct the access list definition in the RADIUS server configuration.

# 109033

**Error Message** `%FTD-4-109033: Authentication failed for admin user user from src_IP. Interactive challenge processing is not supported for protocol`

**Explanation** AAA challenge processing was triggered during authentication of an administrative connection, but the Secure Firewall Threat Defense device cannot initiate interactive challenge processing with the client application. When this occurs, the authentication attempt will be rejected and the connection denied.

- *user* —The name of the user being authenticated
- *src_IP* —The IP address of the client host
- *protocol* —The client connection protocol (SSH v1 or administrative HTTP)

**Recommended Action** Reconfigure AAA so that challenge processing does not occur for these connection types. This generally means to avoid authenticating these connection types to RSA SecurID servers or to any token-based AAA server via RADIUS.

# 109034

**Error Message** `%FTD-4-109034: Authentication failed for network user user from src_IP/port to dst_IP/port. Interactive challenge processing is not supported for protocol connections`

**Explanation** AAA challenge processing was triggered during authentication of a network connection, but the Secure Firewall Threat Defense device cannot initiate interactive challenge processing with the client application. When this occurs, the authentication attempt will be rejected and the connection denied.

- *user* —The name of the user being authenticated
- *src_IP/port* —The IP address and port of the client host
- *dst_IP/port* —The IP address and port of the server to which the client is attempting to connect
- *protocol* —The client connection protocol (for example, FTP)

**Recommended Action** Reconfigure AAA so that challenge processing does not occur for these connection types. This generally means to avoid authenticating these connection types to RSA SecurID servers or to any token-based AAA server via RADIUS.

# 109035

**Error Message** `%FTD-3-109035: Exceeded maximum number (999) of DAP attribute instances for user = user`

**Explanation** This log is generated when the number of DAP attributes received from the RADIUS server exceeds the maximum number allowed when authenticating a connection for the specified user.

**Recommended Action** Modify the DAP attribute configuration to reduce the number of DAP attributes below the maximum number allowed as specified in the log so that the specified user can connect.

# 109036

**Error Message** `%FTD-6-109036: Exceeded 1000 attribute values for the attribute_name attribute for user username`

**Explanation** The LDAP response message contains an attribute that has more than 1000 values.

- *attribute_name* —The LDAP attribute name
- *username* —The username at login

**Recommended Action** None required.

# 109037

**Error Message** `%FTD-3-109037: Exceeded 5000 attribute values for the attribute_name attribute for user username`

**Explanation** The Secure Firewall Threat Defense device supports multiple values of the same attribute received from a AAA server. If the AAA server sends a response containing more than 5000 values for the same attribute, then the Secure Firewall Threat Defense device treats this response message as being malformed

and rejects the authentication. This condition has only been seen in lab environments using specialized test tools. It is unlikely that the condition would occur in a real-world production network.

- *attribute_name* —The LDAP attribute name
- *username* —The username at login

**Recommended Action** Capture the authentication traffic between the Secure Firewall Threat Defense device and AAA server using a protocol sniffer (such as WireShark), then forward the trace file to the Cisco TAC for analysis.

# 109038

**Error Message** `%FTD-3-109038: Attribute internal-attribute-name value "string-from-server" from AAA server could not be parsed as a type`

**Explanation** The AAA subsystem tried to parse an attribute from the AAA server into an internal representation and failed.

- *string-from-server*— String received from the AAA server, truncated to 40 characters.
- *type* —The type of the specified attribute

**Recommended Action** Verify that the attribute is being generated correctly on the AAA server. For additional information, use the **debug ldap** and **debug radius** commands.

# 109039

**Error Message** `%FTD-5-109039: AAA Authentication: Dropping an unsupported IPv6/IP46/IP64 packet from lifc:laddr to fifc:faddr`

**Explanation** A packet containing IPv6 addresses or IPv4 addresses translated to IPv6 addresses by NAT requires AAA authentication or authorization. AAA authentication and authorization do not support IPv6 addresses. The packet is dropped.

- *lifc* —The ingress interface
- *laddr* —The source IP address
- *fifc* —The egress interface
- *faddr* —The destination IP address after NAT translation, if any

**Recommended Action** None required.

# 109100

**Error Message** `%FTD-6-109100: Received CoA update from coa-source-ip for user "username", with session ID audit-session-id, changing authorization attributes.`

**Explanation** The Secure Firewall Threat Defense device has successfully processed the CoA policy update request from *coa-source-ip* for user *username* with session id *audit-session-id* . This syslog message is generated after a change of authorization policy update has been received by the Secure Firewall Threat Defense device, validated and applied. In a non-error case, this is the only syslog message that is generated when a change of authorization is received and processed.

- *coa-source-ip* —Originating IP address of the change of authorization request
- *username* —User whose session is being changed
- *audit-session-id* —The global ID of the session being modified

**Recommended Action** None required.

# 109101

**Error Message** `%FTD-6-109101: Received CoA disconnect request from coa-source-ip for user "username", with session ID: audit-session-id.`

**Explanation** The Secure Firewall Threat Defense device has received a correctly formatted Disconnect-Request for an active VPN session and has successfully terminated the connection.

- *coa-source-ip* —Originating IP address of the change of authorization request
- *username* —User whose session is being changed
- *audit-session-id* —The global ID of the session being modified

**Recommended Action** None required.

# 109102

**Error Message** `%FTD-4-109102: Received CoA action-type from coa-source-ip, but cannot find named session audit-session-id.`

**Explanation** The Secure Firewall Threat Defense device has received a valid change of authorization request, but the session ID specified in the request does not match any active sessions on the Secure Firewall Threat Defense device. This could be the result of the change of authorization server attempting to issue a change of authorization on a session that has already been closed by the user.

- *action-type* —The requested change of authorization action (update or disconnect)
- *coa-source-ip* —Originating IP address of the change of authorization request
- *audit-session-id* —The global ID of the session being modified

**Recommended Action** None required.

# 109103

**Error Message** `%FTD-3-109103: CoA action-type from coa-source-ip failed for user "username", with session ID: audit-session-id.`

**Explanation** The Secure Firewall Threat Defense device has received a correctly formatted change of authorization request, but was unable to process it successfully.

- *action-type* —The requested change of authorization action (update or disconnect)
- *coa-source-ip* —Originating IP address of the change of authorization request
- *username* —User whose session is being changed
- *audit-session-id* —The global ID of the session being modified

**Recommended Action** Investigate the relevant VPN subsystem logs to determine why the updated attributes could not be applied or why the session could not be terminated.

# 109104

**Error Message** `%FTD-3-109104: CoA (Action type: action-type) from coa-source-ip failed for user "username", with session ID: audit-session-id. Action not supported.`

**Explanation** The Secure Firewall Threat Defense device has received a correctly formatted change of authorization request, but did not process it because the indicated action is not supported by the Secure Firewall Threat Defense device.

- *action-type* —The requested change of authorization action (update or disconnect)
- *coa-source-ip* —Originating IP address of the change of authorization request
- *username* —User whose session is being changed
- *audit-session-id* —The global ID of the session being modified

**Recommended Action** None required.

# 109105

**Error Message** `%FTD-3-109105: Failed to determine the egress interface for locally generated traffic destined to protocol IP:port.`

**Explanation** It is necessary for Secure Firewall Threat Defense device to log a syslog if no routes are present when the interface is BVI. Apparently, if default route is present and it does not route packet to the correct interface then it becomes impossible to track it. In case of Secure Firewall Threat Defense, management routes are looked first following the data interface. So if default route is routing packets to different destination, then it is difficult to track it.

**Recommended Action** It is highly recommended to add default route for correct destination or add static routes.

# 109201

**Error Message** `%FTD-5-109201: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Succeeded adding entry.`

**Explanation** When a VPN user is sucessfully added, this message is generated.

**Recommended Action** None.

# 109202

**Error Message** `%FTD-6-109202: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Succeeded incrementing entry use`

**Explanation** The VPN user account already exists and successfully incremented the reference count.

**Recommended Action** None.

# 109203

**Error Message** `%FTD-3-109203: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Failed adding entry.`

**Explanation** This message is generated when the device failed to apply ACL rules for newly created user entry.

**Recommended Action** Try to reconnect.

# 109204

**Error Message** `%FTD-5-109204: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Succeeded applying filter.`

**Explanation** This message is generated when the device failed to apply ACL rules for newly created user entry.

**Recommended Action** None.

# 109205

**Error Message** `%FTD-3-109205: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Failed applying filter.`

**Explanation** This message is generated when the user entry already exists and failed to apply new rules to session on interface.

**Recommended Action** Try to reconnect.

# 109206

**Error Message** `%FTD-3-109206: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Removing stale entry added hours ago.`

**Explanation** This message is generated when the device failed to add user entry due to collision and has removed stale entry.

**Recommended Action** Try to reconnect.

# 109207

**Error Message** `%FTD-5-109207: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Succeeded updating entry.`

**Explanation** This message is generated when the device has successfully applied rules for user on interface.

**Recommended Action** None.

# 109208

**Error Message** `%FTD-3-109208: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Failed updating entry - no entry.`

**Explanation** This message is generated when the device has failed to update user entry with new rules.

**Recommended Action** Try to reconnect again.

# 109209

**Error Message** `%FTD-3-109209: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Failed updating filter for entry. Entry was allocated to Session=session, User=username hours ago.`

**Explanation** This message is generated when the device has failed to update the rules in user entry due to collision.

**Recommended Action** Try to reconnect again.

## 109210

**Error Message** `%FTD-5-109210: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Succeeded removing entry.`

**Explanation** This message is generated when the device has successfully removed the rules for user during tunnel torn down.

**Recommended Action** None.

## 109211

**Error Message** `%FTD-6-109211: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Succeeded decrementing entry use.`

**Explanation** This message is generated when the reference count decremented successfully after tunnel removal.

**Recommended Action** None.

## 109212

**Error Message** `%FTD-3-109212: UAUTH: Session=session, User=user_name, Assigned IP=ip_address, Failed removing entry - reason_string.`

**Explanation** This message is generated when the device fails to delete due to invalid address, missing entry, or bad entry.

**Recommended Action** Try to disconnect again.

## 109213

**Error Message** `%FTD-3-109213: UAUTH: Session=session, User=username, Assigned IP=IP_Address, Failed removing entry. Address was allocated to Session=session, User=username hours ago.`

**Explanation** This message is generated when the device fails to delete due to collision in user entry.

**Recommended Action** Try to disconnect again.

# Messages 110002 to 113045

This section includes messages from 110002 to 113045.

# 110002

**Error Message** `%FTD-6-110002: Failed to locate egress interface for protocol from src_interface:src_ip/src_port to dest_ip/dest_port`

**Explanation** An error occurred when the Secure Firewall Threat Defense device tried to find the interface through which to send the packet.

- *protocol* —The protocol of the packet
- *src_interface* —The interface from which the packet was received
- *src_ip* —The source IP address of the packet
- *src_port* —The source port number
- *dest_ip* —The destination IP address of the packet
- *dest_port* —The destination port number

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC.

# 110003

**Error Message** `%FTD-6-110003: Routing failed to locate next hop for protocol from src_interface:src_ip/src_port to dest_interface:dest_ip/dest_port`

**Explanation** An error occurred when the Secure Firewall Threat Defense device tried to find the next hop on an interface routing table.

- *protocol* —The protocol of the packet
- *src_interface* —The interface from which the packet was received
- *src_ip* —The source IP address of the packet
- *src_port* —The source port number
- *dest_ip* —The destination IP address of the packet
- *dest_port* —The destination port number

**Recommended Action** Copy the error message, the configuration, and any details about the events leading up to the error, and contact Cisco TAC. During debugging, use the **show asp table routing** command to view the routing table details.

# 110004

**Error Message** `%FTD-6-110004: Egress interface changed from old_active_ifc to new_active_ifc on ip_protocol connection conn_id for outside_zone/parent_outside_ifc:outside_addr/outside_port (mapped_addr/mapped_port) to inside_zone/parent_inside_ifc:inside_addr/inside_port (mapped_addr/mapped_port)`

**Explanation** A flow changed on the egress interface.

**Recommended Action** None required.

# 110005

**Error Message** `%FTD-6-110005: Routing failed to locate next hop for protocol from interface:address/port to interface:address/port`

**Explanation** A flow not found during output route lookup.

**Recommended Action** None.

# 111001

**Error Message** `%FTD-5-111001: Begin configuration: IP_address writing to device`

**Explanation** You have entered the **write** command to store your configuration on a device (either floppy, flash memory, TFTP, the failover standby unit, or the console terminal). The **IP_address** indicates whether the login was made at the console port or with a Telnet connection.

**Recommended Action** None required.

# 111002

**Error Message** `%FTD-5-111002: Begin configuration: ip_address reading from device`

**Explanation** You have entered the **read** command to read your configuration from a device (either floppy disk, flash memory, TFTP, the failover standby unit, or the console terminal). The **ip_address** indicates whether the login was made at the console port or with a Telnet connection.

**Recommended Action** None required.

# 111003

**Error Message** `%FTD-5-111003: IP_address Erase configuration.`

**Explanation** You have erased the contents of flash memory by entering the **write erase** command at the console. The **IP_address** value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** After erasing the configuration, reconfigure the Secure Firewall Threat Defense device and save the new configuration. Alternatively, you can restore information from a configuration that was previously saved, either on a floppy disk or on a TFTP server elsewhere on the network.

# 111004

**Error Message** `%FTD-5-111004: IP_address end configuration: {FAILED|OK}`

**Explanation** You have entered the **config floppy/memory/ network** command or the **write floppy/memory/network/standby** command. The **IP_address** value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None required if the message ends with OK. If the message indicates a failure, try to fix the problem. For example, if writing to a floppy disk, ensure that the floppy disk is not write protected; if writing to a TFTP server, ensure that the server is up.

# 111005

**Error Message** `%FTD-5-111005: IP_address end configuration: OK`

**Explanation** You have exited the configuration mode. The **IP_address** value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None required.

# 111007

**Error Message** `%FTD-5-111007: Begin configuration: IP_address reading from device`

**Explanation** You have entered the **reload** or **configure** command to read in a configuration. The device text can be floppy, memory, net, standby, or terminal. The **IP_address** value indicates whether the login was made at the console port or through a Telnet connection.

**Recommended Action** None required.

# 111008

**Error Message** `%FTD-5-111008: User 'user' executed the 'string' command.`

**Explanation** The user entered any command, with the exception of a **show** command.

**Recommended Action** None required.



**Note** There is an exception for this syslog ID. Syslogs will be seen in logging <destination> even though global syslog is disabled.

# 111009

**Error Message** `%FTD-7-111009: User 'user' executed cmd: string`

**Explanation** The user entered a command that does not modify the configuration. This message appears only for **show** commands.

**Recommended Action** None required.

# 111010

**Error Message** `%FTD-5-111010: User 'username', running 'application-name' from IP ip_addr, executed 'cmd'`

**Explanation** A user made a configuration change.

- *username* —The user making the configuration change
- *application-name* —The application that the user is running
- *ip addr* —The IP address of the management station
- *cmd* —The command that the user has executed

**Recommended Action** None required.

**Note** There is an exception for this syslog ID. Syslogs will be seen in logging <destination> even though global syslog is disabled.

# 111111

**Error Message** `%FTD-1-111111: error_message`

**Explanation** A system or infrastructure error has occurred.

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

# 112001

**Error Message** `%FTD-2-112001: Clear finished`

**Explanation** A request to clear the module configuration was completed. The source file and line number are identified.

**Recommended Action** None required.

# 113001

**Error Message** `%FTD-3-113001: Unable to open AAA session. Session limit [limit] reached`

**Explanation** The AAA operation on an IPsec tunnel or WebVPN connection cannot be performed because of the unavailability of AAA resources. The **limit** value indicates the maximum number of concurrent AAA transactions.

**Recommended Action** Reduce the demand for AAA resources, if possible.

# 113003

**Error Message** `%FTD-6-113003: AAA group policy for user user is being set to policy_name`

**Explanation** The group policy that is associated with the tunnel group is being overridden with a user-specific policy, *policy_name* . The *policy_name* is specified using the **username** command when LOCAL authentication is configured or is returned in the RADIUS CLASS attribute when RADIUS authentication is configured.

**Recommended Action** None required.

# 113004

**Error Message** `%FTD-6-113004: AAA user aaa_type Successful : server = server_IP_address : user = user`

**Explanation** The AAA operation on an IPsec or WebVPN connection has been completed successfully. The AAA types are authentication, authorization, or accounting. The **server_IP_address** is the IP address of the relevant AAA server. The **user** is the user name associated with the connection.

**Recommended Action** None required.

# 113005

**Error Message-1** `%FTD-6-113005: AAA user authentication Rejected : reason = reason : server = ip_address : user =user_name : user IP = ip_address`

**Explanation** The AAA authentication on a connection has failed. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

**Recommended Action** Retry the authentication.

**Error Message-2** `%FTD-6-113005: AAA user authorization Rejected : reason = reason : server = ip_address : user =user_name : user IP = ip_address`

**Explanation** The AAA authorization on a connection has failed. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

**Recommended Action** Retry the authorization.

# 113006

**Error Message** `%FTD-6-113006: User 'user' locked out on exceeding 'number' successive failed authentication attempts`

**Explanation** A locally configured user is being locked out. This happens when a configured number of consecutive authentication failures have occurred for this user and indicates that all future authentication attempts by this user will be rejected until an administrator unlocks the user using the **clear aaa local user lockout** command. The **user** is the user that is now locked, and the **number** is the consecutive failure threshold configured using the **aaa local authentication attempts max-fail** command.

**Recommended Action** Try unlocking the user using the **clear_aaa_local_user_lockout** command or adjusting the maximum number of consecutive authentication failures that are tolerated.

# 113007

**Error Message** `%FTD-6-113007: User 'user' unlocked by 'administrator'`

**Explanation** A locally configured user that was locked out after exceeding the maximum number of consecutive authentication failures set by using the **aaa local authentication attempts max-fail** command has been unlocked by the indicated administrator.

**Recommended Action** None required.

# 113008

**Error Message** `%FTD-6-113008: AAA transaction status ACCEPT : user = user`

**Explanation** The AAA transaction for a user associated with an IPsec or WebVPN connection was completed successfully. The user is the username associated with the connection.

**Recommended Action** None required.

# 113009

**Error Message** `%FTD-6-113009: AAA retrieved default group policy (policy) for user = username`

**Explanation** The authentication or authorization of an IPsec or WebVPN connection has occurred. The attributes of the group policy that were specified with the **tunnel-group** or **webvpn** commands have been retrieved.

**Recommended Action** None required.

# 113010

**Error Message** `%FTD-6-113010: AAA challenge received for user user from server server_IP_address.`

**Explanation** The authentication of an IPsec connection has occurred with a SecurID server. The user will be prompted to provide further information before being authenticated.

- **user**—The username associated with the connection
- **server _IP_address**—The IP address of the relevant AAA server

**Recommended Action** None required.

# 113011

**Error Message** `%FTD-6-113011: AAA retrieved user specific group policy (policy) for user = user`

**Explanation** The authentication or authorization of an IPsec or WebVPN connection has occurred. The attributes of the group policy that was specified with the **tunnel-group** or **webvpn** commands have been retrieved.

**Recommended Action** None required.

# 113012

**Error Message** `%FTD-6-113012: AAA user authentication Successful : local database : user = user`

**Explanation** The user associated with a IPsec or WebVPN connection has been successfully authenticated to the local user database.

- **user**—The username associated with the connection

**Recommended Action** None required.

# 113013

**Error Message** `%FTD-6-113013: AAA unable to complete the request Error : reason = reason : user = user`

**Explanation** The AAA transaction for a user associated with an IPsec or WebVPN connection has failed because of an error or has been rejected because of a policy violation.

- **reason—**The reason details
- **user**—The username associated with the connection

**Recommended Action** None required.

# 113014

**Error Message** `%FTD-6-113014: AAA authentication server not accessible : server = server_IP_address : user = user`

**Explanation** The device was unable to communicate with the configured AAA server during the AAA transaction associated with an IPsec or WebVPN connection. This may or may not result in a failure of the user connection attempt depending on the backup servers configured in the **aaa-server** group and the availability of those servers. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

**Recommended Action** Verify connectivity with the configured AAA servers.

# 113015

**Error Message** `%FTD-6-113015: AAA user authentication Rejected : reason = reason : local database : user = user: : user IP = xxx.xxx.xxx.xxx`

**Explanation** A request for authentication to the local user database for a user associated with an IPsec or WebVPN connection has been rejected. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- **reason—**The details of why the request was rejected
- **user**—The username associated with the connection
- **user_ip** —The IP address of the user who initiated the authentication or authorization request<915CLI>

**Recommended Action** None required.

# 113016

**Error Message** `%FTD-6-113016: AAA credentials rejected : reason = reason : server = server_IP_address : user = user<915CLI>: : user IP = xxx.xxx.xxx.xxx`

**Explanation** The AAA transaction for a user associated with an IPsec or WebVPN connection has failed because of an error or rejected due to a policy violation. The username is hidden when invalid or unknown, but appears when valid or the **no logging hide username** command has been configured.

- **reason—**The details of why the request was rejected
- **server_IP_address**—The IP address of the relevant AAA server
- **user**—The username associated with the connection
- *<915CLI>user_ip* —The IP address of the user who initiated the authentication or authorization request

**Recommended Action** None required.

# 113017

**Error Message** `%FTD-6-113017: AAA credentials rejected : reason = reason : local database : user = user: : user IP = xxx.xxx.xxx.xxx`

**Explanation** The AAA transaction for a user associated with an IPsec or WebVPN connection has failed because of an error or rejected because of a policy violation. This event only appears when the AAA transaction is with the local user database rather than with an external AAA server.

- **reason—**The details of why the request was rejected

- **user**—The username associated with the connection
- **user_ip** —The IP address of the user who initiated the authentication or authorization request

**Recommended Action** None required.

# 113018

**Error Message** `%FTD-3-113018: User: 'user', Unsupported downloaded ACL Entry: 'ACL_entry', Action: 'action'`

**Explanation** An ACL entry in unsupported format was downloaded from the authentication server. The following list describes the message values:

- **user**—User trying to log in
- **ACL_entry**—Unsupported ACL entry downloaded from the authentication server
- **action**—Action taken when encountering the unsupported ACL entry

**Recommended Action** The ACL entry on the authentication server has to be changed by the administrator to conform to the supported ACL entry formats.

# 113019

**Error Message** `%FTD-4-113019: Group = group, Username = username, IP = peer_address, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason`

**Explanation** An indication of when and why the longest idle user is disconnected.

- **group**—Group name
- **username**—Username
- **IP**—Peer address
- **Session Type**—Session type (for example, IPsec or UDP)
- **duration**—Connection duration in hours, minutes, and seconds
- **Bytes xmt**—Number of bytes transmitted
- *Bytes rcv* —Number of bytes received
- **reason**—Reason for disconnection

User Requested. Indicates a disconnection from client.

Lost Carrier

Lost Service. The service loss could be due to an issue from ISP during a SSL session establishment.

Idle Timeout

Max time exceeded

Administrator Reset- Indicates disconnection from secure gateway through vpn-sessiondb logoff

Administrator Reboot

Administrator Shutdown

Port Error

NAS Error

NAS Request

NAS Reboot

Port unneeded

Connection preempted. Indicates that the allowed number of simultaneous (same user) logins has been exceeded. To resolve this problem, increase the number of simultaneous logins or have users only log in once with a given username and password.

Port Suspended

Service Unavailable

Callback

User error

Host Requested

SA Expired

IKE Delete

Bandwidth Management Error

Certificate Expired

Phase 2 Mismatch

Firewall Mismatch

Peer Address Changed

ACL Parse Error

Phase 2 Error

Configuration Error

Peer Reconnected

Internal Error

Crypto map policy not found

L2TP initiated

VLAN Mapping Error

NAC-Policy Error

Dynamic Access Policy terminate

Client type not supported

Unknown

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

# 113020

**Error Message** `%FTD-3-113020: Kerberos error : Clock skew with server` *`ip_address`* `greater than` *`time_in_seconds`* `seconds`

**Explanation** Authentication for an IPsec or WebVPN user through a Kerberos server has failed because the clocks on the Secure Firewall Threat Defense device and the server are more than five minutes (300 seconds) apart. When this occurs, the connection attempt is rejected.

- *ip_address* —The IP address of the Kerberos server

**Recommended Action** Synchronize the clocks on the Secure Firewall Threat Defense device and the Kerberos server.

# 113021

**Error Message** `%FTD-3-113021: Attempted console login failed user 'username' did NOT have appropriate Admin Rights.`

**Explanation** A user has tried to access the management console and was denied.

- *username* —The username entered by the user

**Recommended Action** If the user is a newly added admin rights user, check that the service type (LOCAL or RADIUS authentication server) for that user is set to allow access:

- nas-prompt—Allows login to the console and exec privileges at the required level, but not enable (configuration modification) access
- admin—Allows all access and can be further constrained by command privileges

Otherwise, the user is inappropriately trying to access the management console; the action to be taken should be consistent with company policy for these matters.

# 113022

**Error Message** `%FTD-2-113022: AAA Marking protocol server {IP_address | hostname} in aaa-server group tag as FAILED`

**Explanation** The Secure Firewall Threat Defense device has tried an authentication, authorization, or accounting request to the AAA server and did not receive a response within the configured timeout window. The AAA server will be marked as failed and has been removed from service.

- *protocol* —The type of authentication protocol, which can be one of the following:

- RADIUS

- TACACS+

- NT

- RSA SecurID

- Kerberos

- LDAP

- *ip-addr* —The IP address of the AAA server
- *tag* —The server group name

**Recommended Action** Verify that the AAA server is online and is accessible from the Secure Firewall Threat Defense device.

# 113023

**Error Message** `%FTD-2-113023: AAA Marking protocol server ip-addr in aaa-server group tag as ACTIVE`

**Explanation** The Secure Firewall Threat Defense device has reactivated the AAA server that was previously marked as failed. The AAA server is now available to service AAA requests.

- *protocol* —The type of authentication protocol, which can be one of the following:

- RADIUS

- TACACS+

- NT

- RSA SecurID

- Kerberos

- LDAP

- *ip-addr* —The IP address of the AAA server
- *tag* —The server group name

**Recommended Action** None required.

# 113024

**Error Message** `%FTD-5-113024: Group tg: Authenticating type connection from ip with username, user_name, from client certificate`

**Explanation** The prefill username feature overrides the username with one derived from the client certificate for use in AAA.

- *tg* —The tunnel group
- *type* —The type of connection (ssl-client or clientless)
- *ip* —The IP address of the connecting user
- *user_name* —The name extracted from the client certificate for use in AAA

**Recommended Action** None required.

# 113025

**Error Message** `%FTD-5-113025: Group tg: fields Could not authenticate connection_type connection from ip`

**Explanation** A username cannot be successfully extracted from the certificate.

- *tg* —The tunnel group
- *fields* —The DN fields being searched for
- *connection type* —The type of connection (SSL client or clientless)
- *ip* —The IP address of the connecting user

**Recommended Action** The administrator should check that the **authentication aaa certificate**, **ssl certificate-authentication**, and **authorization-dn-attributes** keywords have been set correctly.

# 113026

**Error Message** `%FTD-4-113026: Error error while executing Lua script for group tunnel_group`

**Explanation** An error occurred while extracting a username from the client certificate for use in AAA. This message is only generated when the username-from-certificate use-script option is enabled.

- *error* —Error string returned from the Lua environment
- *tunnel group* —The tunnel group attempting to extract a username from a certificate

**Recommended Action** Examine the script being used by the username-from-certificate use-script option for errors.

# 113027

**Error Message** `%FTD-2-113027: Error activating tunnel-group scripts`

**Explanation** The script file cannot be loaded successfully. No tunnel groups using the username-from-certificate use-script option work correctly.

**Recommended Action** The administrator should check the script file for errors using ASDM. Use the **debug aaa** command to obtain a more detailed error message that may be useful.

# 113028

**Error Message** `%FTD-7-113028: Extraction of username from VPN client certificate has string.. [Request num]`

**Explanation** The processing request of a username from a certificate is running or has finished.

- *num* —The ID of the request (the value of the pointer to the fiber), which is a monotonically increasing number.
- *string* —The status message, which can one of the following:
  - been requested
  - started
  - finished with error
  - finished successfully
  - completed

**Recommended Action** None required.

# 113029

**Error Message** `%FTD-4-113029: Group group User user IP ipaddr Session could not be established: session limit of num reached.`

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

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

# 113030

**Error Message** `%FTD-4-113030: Group group User user IP ipaddr User ACL acl from AAA doesn't exist on the device, terminating connection.`

**Explanation** The specified ACL was not found on the Secure Firewall Threat Defense device.

- **group—**The name of the group
- **user—**The name of the user
- **ipaddr—**The IP address
- **acl—**The name of the ACL

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

# 113031

**Error Message** `%FTD-4-113031: Group group User user IP ipaddr AnyConnect 'vpn-filter filter' is an IPv6 ACL; ACL not applied.`

**Explanation** The type of ACL to be applied is incorrect. An IPv6 ACL has been configured as an IPv4 ACL through the **vpn-filter** command.

- *group* —The group policy name of the user
- *user* —The username
- *ipaddr* —The public (not assigned) IP address of the user
- *filter* —The name of the VPN filter

**Recommended Action** Validate the VPN filter and IPv6 VPN filter configurations on the Secure Firewall Threat Defense device, and the filter parameters on the AAA (RADIUS) server. Make sure that the correct type of ACL is specified.

# 113032

**Error Message** `%FTD-4-113032: Group group User user IP ipaddr AnyConnect 'ipv6-vpn-filter filter' is an IPv4 ACL; ACL not applied.`

**Explanation** The type of ACL to be applied is incorrect. An IPv4 ACL has been configured as an IPv6 ACL through the **ipv6-vpn-filter** command.

- *group* —The group policy name of the user
- *user* —The username
- *ipaddr* —The public (not assigned) IP address of the user
- *filter* —The name of the VPN filter

**Recommended Action** Validate the VPN filter and IPv6 VPN filter configurations on the Secure Firewall Threat Defense device and the filter parameters on the AAA (RADIUS) server. Make sure that the correct type of ACL is specified.

# 113033

**Error Message** `%FTD-6-113033: Group group User user IP ipaddr AnyConnect session not allowed. ACL parse error.`

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

- *group* —The group policy name of the user
- *user* —The username
- *ipaddr* —The public (not assigned) IP address of the user

**Recommended Action** Correct the WebVPN ACL.

# 113034

**Error Message** `%FTD-4-113034: Group group User user IP ipaddr User ACL acl from AAA ignored, AV-PAIR ACL used instead.`

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

- **group—**The name of the group
- **user—**The name of the user
- **ipaddr—**The IP address
- **acl—**The name of the ACL

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

# 113035

**Error Message** `%FTD-4-113035: Group <group> User <user> IP <ip_address> Session terminated: AnyConnect not enabled or invalid AnyConnect image on the device_name`

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

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

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

# 113036

**Error Message** `%FTD-4-113036: Group group User user IP ipaddr AAA parameter name value invalid.`

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

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

**Recommended Action** Modify the configuration to correct the indicated parameter.

# 113037

**Error Message** `%FTD-6-113037: Group <group> User <user> IP <ip_address> Reboot pending, new sessions disabled. Denied user login.`

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

**Recommended Action** None required.

# 113038

**Error Message** `%FTD-4-113038: Group group User user IP ipaddr Unable to create AnyConnect_parent session.`

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

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

**Recommended Action** None required.

# 113039

**Error Message** `%FTD-6-113039: Group group User user IP ipaddr AnyConnect_parent session started.`

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

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

**Recommended Action** None required.

# 113040

**Error Message** `%FTD-4-113040: Group group User user IP ipaddr Terminating the VPN connection attempt from attempted_group. Reason: This connection is group locked to locked_group..`

**Explanation** The tunnel group over which the connection is attempted is not the same as the tunnel group set in the group lock.

- *attempted group* —The tunnel group over which the connection came in
- *locked group* —The tunnel group for which the connection is locked or restricted

**Recommended Action** Check the group-lock value in the group policy or the user attributes.

## 113041

**Error Message** `%FTD-4-113041: Redirect ACL configured for assigned_IP does not exist on the device.`

**Explanation** An error occurred when the redirect URL was installed and the ACL was received from the ISE, but the redirect ACL does not exist on the Secure Firewall Threat Defense device.

- *assigned IP* —The IP address that is assigned to the client

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

## 113042

**Error Message** `%FTD-4-113042: Non-HTTP connection from src_if:src_ip/src_port to dest_if:dest_ip/dest_port denied by redirect filter; only HTTP connections are supported for redirection.`

**Explanation** For the CoA feature, the redirect ACL filter drops the matching non-HTTP traffic during the redirect processing and provides information about the terminated traffic flow.

- *src_if* , *src_ip* , *src_port* —The source interface, IP address, and port of the flow
- *dest_if* , *dest_ip* , *dest_port* —The destination interface, IP address, and port of the flow
- *username* —The name of the user
- *client_IP* —The IP address of the client

**Recommended Action** Validate the redirect ACL configuration on the Secure Firewall Threat Defense device. Make sure that the correct filter is used to match the traffic to redirect and does not block the flow that is intended to be allowed through.

# Messages 114001 to 199021

This section includes messages from 114001 to 199021.

## 114001

**Error Message** `%FTD-1-114001: Failed to initialize card-type I/O card due to error_string.`

**Explanation** The system failed to initialize a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- *syslog_id* —Message identifier
- *>error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114002

**Error Message** `%FTD-1-114002: Failed to initialize SFP in card-type I/O card due to error_string.`

**Explanation** The system failed to initialize an SFP connector in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114003

**Error Message** `%FTD-1-114003: Failed to run cached commands in card-type I/O card due to error_string.`

**Explanation** The system failed to run cached commands in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier

- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114004

**Error Message** `%FTD-6-114004: 4GE_SSM I/O card Initialization is started.`

**Explanation** The user has been notified that a 4GE SSM I/O initialization is starting.

- >*syslog_id* —Message identifier

**Recommended Action** None required.

# 114005

**Error Message** `%FTD-6-114005: 4GE_SSM I/O card Initialization has completed.`

**Explanation** The user has been notified that an 4GE SSM I/O initialization is finished.

- >*syslog_id* —Message identifier

**Recommended Action** None required.

# 114006

**Error Message** `%FTD-3-114006: Failed to get port statistics in card-type I/O card due to error_string.`

**Explanation** The Secure Firewall Threat Defense device failed to obtain port statistics in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114007

**Error Message** `%FTD-3-114007: Failed to get current msr in card-type I/O card due to error_string.`

**Explanation** The Secure Firewall Threat Defense device failed to obtain the current module status register information in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:
  - 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114008

**Error Message** `%FTD-3-114008: Failed to enable port after link is up in card-type I/O card due to error_string.`

**Explanation** The Secure Firewall Threat Defense device failed to enable a port after the link transition to Up state is detected in a 4GE SSM I/O card because of either an I2C serial bus access error or a switch access error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114009

**Error Message** `%FTD-3-114009: Failed to set multicast address in card-type I/O card due to error_string.`

**Explanation** The Secure Firewall Threat Defense device failed to set the multicast address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114010

**Error Message** `%FTD-3-114010: Failed to set multicast hardware address in card-type I/O card due to error_string.`

**Explanation** The Secure Firewall Threat Defense device failed to set the multicast hardware address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - 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
  - I2C_DATA_PTR_ERROR

**Recommended Action** Perform the following steps:

1. Log and review the messages and the errors associated with the event.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114011

**Error Message** `%FTD-3-114011: Failed to delete multicast address in card-type I/O card due to error_string.`

**Explanation** The Secure Firewall Threat Defense device failed to delete the multicast address in a 4GE SSM I/O card because of either an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier

- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114012

**Error Message** `%FTD-3-114012: Failed to delete multicast hardware address in` *`card-type`* `I/O card due to` *`error_string`*`.`

**Explanation** The Secure Firewall Threat Defense device failed to delete the multicast hardware address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:
  - 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114013

**Error Message** `%FTD-3-114013: Failed to set mac address table in card-type I/O card due to error_string.`

**Explanation** The Secure Firewall Threat Defense device failed to set the MAC address table in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:

- 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114014

**Error Message** `%FTD-3-114014: Failed to set mac address in card-type I/O card due to error_string.`

**Explanation** The Secure Firewall Threat Defense device failed to set the MAC address in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:

- 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114015

**Error Message** `%FTD-3-114015: Failed to set mode in card-type I/O card due to error_string.`

**Explanation** The Secure Firewall Threat Defense device failed to set individual or promiscuous mode in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are I2C serial bus errors:

- 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114016

**Error Message** `%FTD-3-114016: Failed to set multicast mode in card-type I/O card due to error_string.`

**Explanation**The Secure Firewall Threat Defense device failed to set the multicast mode in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114017

**Error Message** `%FTD-3-114017: Failed to get link status in` *`card-type`* `I/O card due to` *`error_string`*`.`

**Explanation** The Secure Firewall Threat Defense device failed to obtain link status in a 4GE SSM I/O card because of an I2C serial bus access error or a switch access error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- 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. Notify the system administrator.
2. Log and review the messages and the errors associated with the event.
3. Reboot the software running on the Secure Firewall Threat Defense device.
4. Power cycle the device. When you turn off the power, make sure you wait several seconds before turning the power on.
5. If the problem persists, contact the Cisco TAC.

# 114018

**Error Message** `%FTD-3-114018: Failed to set port speed in card-type I/O card due to error_string.`

**Explanation** The Secure Firewall Threat Defense device failed to set the port speed in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier
- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114019

**Error Message** `%FTD-3-114019: Failed to set media type in card-type I/O card due to error_string.`

**Explanation** The Secure Firewall Threat Defense device failed to set the media type in a 4GE SSM I/O card because of an I2C error or a switch initialization error.

- >*syslog_id* —Message identifier

- >*error_string* —An I2C serial bus error or a switch access error, which is a decimal error code. The following are the I2C serial bus errors:

- 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.
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 you wait several seconds before turning the power on.
4. If the problem persists, contact the Cisco TAC.

# 114020

**Error Message** `%FTD-3-114020: Port link speed is unknown in 4GE_SSM I/O card.`

**Explanation** The Secure Firewall Threat Defense device cannot detect the port link speed in a 4GE SSM I/O card.

**Recommended Action** Perform the following steps:

1. Log and review the messages associated with the event.
2. Reset the 4GE SSM I/O card and observe whether or not the software automatically recovers from the event.
3. If the software does not recover automatically, power cycle the device. When you turn off the power, make sure you wait several seconds before you turn the power on.
4. If the problem persists, contact the Cisco TAC.

# 114021

**Error Message** `%FTD-3-114021: Failed to set multicast address table in 4GE_SSM I/O card due to error.`

**Explanation**The Secure Firewall Threat Defense device failed to set the multicast address table in the 4GE SSM I/O card because of either an I2C serial bus access error or a switch access error.

- **error**—A switch access error (a decimal error code) or an I2C serial bus error. Possible I2C serial bus errors include:

- 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 associated with the event.
2. Try to reboot the Secure Firewall Threat Defense device.
3. If the software does not recover automatically, power cycle the device. When you turn off the power, make sure you wait several seconds before you turn the power on.
4. If the problem persists, contact the Cisco TAC.

# 114023

**Error Message** `%FTD-3-114023: Failed to cache/flush mac table in` *`4GE_SSM`* `I/O card due to` *`error_string`*`.`

**Explanation** A failure to cache or flush the MAC table in a 4GE SSM I/O card occurred because of an I2C serial bus access error or a switch access error. This message rarely occurs.

- **error_string**— Either an I2C serial bus error (see the second bullet for possible values) or a switch access error (which is a decimal error code).
- I2C serial bus errors are as follows:

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 the syslog message and the errors surrounding the event.
2. Try to software reboot the Secure Firewall Threat Defense device.
3. Power cycle the Secure Firewall Threat Defense device.

**Note** When you turn off the power, make sure that you wait several seconds before powering on again. After you complete steps 1-3, if the problem persists, contact the Cisco TAC and provide the information described in step 1. You may need to RMA the Secure Firewall Threat Defense device.

# 115000

**Error Message** `%FTD-2-115000: Critical assertion in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

**Explanation**The critical assertion has gone off and is used during development in checked builds only, but never in production builds.

- **process name**— The name of the process
- *fiber name* —The name of the fiber
- *component name* —The name of the specified component
- *subcomponent name* —The name of the specified subcomponent
- *filename* —The name of the specified file
- *line number* —The line number for the specified line
- *condition* —The specified condition

**Recommended Action** A high priority defect should be filed, the reason for the assertion should be investigated, and the problem corrected.

# 115001

**Error Message** `%FTD-3-115001: Error in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

**Explanation** An error assertion has gone off and is used during development in checked builds only, but never in production builds.

- **process name**— The name of the process
- *fiber name* —The name of the fiber
- *component name* —The name of the specified component
- *subcomponent name* —The name of the specified subcomponent
- *filename* —The name of the specified file
- *line number* —The line number for the specified line
- *condition* —The specified condition

**Recommended Action** A defect should be filed, the reason for the assertion should be investigated, and the problem fixed.

# 115002

**Error Message** `%FTD-4-115002: Warning in process: process name fiber: fiber name , component: component name , subcomponent: subcomponent name , file: filename , line: line number , cond: condition`

**Explanation** A warning assertion has gone off and is used during development in checked builds only, but never in production builds.

- **process name**— The name of the process
- *fiber name* —The name of the fiber
- *component name* —The name of the specified component
- *subcomponent name* —The name of the specified subcomponent
- *filename* —The name of the specified file
- *line number* —The line number for the specified line
- *condition* —The specified condition

**Recommended Action** The reason for the assertion should be investigated and if a problem is found, a defect should be filed, and the problem corrected.

# 199001

**Error Message** `%FTD-5-199001: Reloaded at time by user. Reload reason: reload reason`

**Explanation** The address of the host that is initiating an Secure Firewall Threat Defense device reboot with the **reload** command has been recorded.

**Recommended Action** None required.

# 199002

**Error Message** `%FTD-6-199002: Startup completed. Beginning operation.`

**Explanation** The Secure Firewall Threat Defense device finished its initial boot and the flash memory reading sequence, and is ready to begin operating normally.

**Note** You cannot block this message by using the no logging message command.

**Recommended Action** None required.

# 199003

**Error Message** `%FTD-6-199003: Reducing Link MTU dec`

**Explanation** The Secure Firewall Threat Defense device received a packet from the outside network that uses a larger MTU than the inside network. The Secure Firewall Threat Defense device then sent an ICMP message to the outside host to negotiate an appropriate MTU. The log message includes the sequence number of the ICMP message.

**Recommended Action** None required.

# 199005

**Error Message** `%FTD-6-199005: Startup begin`

**Explanation** The Secure Firewall Threat Defense device started.

**Recommended Action** None required.

# 199010

**Error Message** `%FTD-1-199010: Signal number caught in process/fiber (rtcli_async_executor_process)/(rtcli_async_executor) at address ip_address, corrective action at ip_address`

**Explanation** The system has recovered from a serious error.

**Recommended Action** Contact the Cisco TAC.

# 199011

**Error Message** `%FTD-2-199011: Close on bad channel in process/fiber process_name/fiber_name, channel ID p, channel state channel_state`

**Explanation** An unexpected channel close condition has been detected.

- *p*—The channel ID
- *process/fiber* —The name of the process/fiber that caused the bad channel close operation
- *s*—The channel state

**Recommended Action** Contact the Cisco TAC and attach a log file.

# 199012

**Error Message** `%FTD-1-199012: Stack overflow during new_stack_call in process/fiber process_name/fiber_name, call target f, stack size s`

**Explanation** A stack overflow condition has been detected.

- *f*—The target of the new_stack_call
- *process/fiber* —The name of the process/fiber that caused the stack overflow
- *s*—The new stack size specified in new_stack_call

**Recommended Action** Contact the Cisco TAC and attach the log file.

# 199013

**Error Message** `%FTD-1-199013: syslog`

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The alert syslog passed verbatim from an external process

**Recommended Action** Contact the Cisco TAC.

# 199014

**Error Message** `%FTD-2-199014: syslog`

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The critical syslog passed verbatim from an external process

**Recommended Action** Contact the Cisco TAC.

# 199015

**Error Message** `%FTD-3-199015: syslog`

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The error syslog passed verbatim from an external process.

  Example of syslog messages generated:



**Note** These logs do not indicate any issues. They are populated only to provide information.

- `port-manager: PHYREG debug list for if_index = value is empty`
- `port-manager: mrvlGetEpmPhyPortNumfromSlotInterfaceAggrPort finding interfaceName = Ethernet 1/5`
- `port-manager: mrvlGetEpmPhyPortNumfromSlotInterfaceAggrPort: portNum was not found for slot 0 port = port interfaceName = Ethernet 1/16`
- `port-manager: mrvlGetPortNumFromSrcId: port was not found for src_id number`

**Recommended Action** Contact the Cisco TAC.

# 199016

**Error Message** `%FTD-4-199016:` *syslog*

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The warning syslog passed verbatim from an external process

In some instances, the message may appear to be an issue that is internal to the device platform process. For example, in the following message though it indicates to be an internal device issue, it is related to an internal virtual device which is not used on the device platform, and it does not cause any functionality impact.

```
%FTD-4-199016: mm dd HH:MM:SS acpid: input device has been disconnected, fd 4
```

**Recommended Action** Contact the Cisco TAC.

# 199017

**Error Message** `%FTD-5-199017: syslog`

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The notification syslog passed verbatim from an external process

**Recommended Action** None required.

# 199018

**Error Message** `%FTD-6-199018: syslog`

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The informational syslog passed verbatim from an external process

**Recommended Action** None required.

# 199019

**Error Message** `%FTD-7-199019: syslog`

**Explanation** A variable syslog was generated by an assistive process.

- **syslog**—The debugging syslog passed verbatim from an external process

**Recommended Action** None required.

# 199020

**Error Message** `%FTD-2-199020: System memory utilization has reached X %. System will reload if memory usage reaches the configured trigger level of Y %.`

**Explanation** The system memory utilization has reached 80% of the system memory watchdog facility's configured value.

**Recommended Action** Reduce system memory utilization by reducing traffic load, removing traffic inspections, reducing the number of ACL entries, and so on. If a memory leak is suspected, contact Cisco TAC.

# 199021

**Error Message** `%FTD-1-199021: System memory utilization has reached the configured threshold of Y%. System will now reload.`

**Explanation** The system memory utilization has reached 100% of the system memory watchdog facility's configured value. The system will automatically reload.

**Recommended Action** Reduce system memory utilization by reducing traffic load, removing traffic inspections, reducing the number of ACL entries, and so on. If a memory leak is suspected, contact Cisco TAC.