

Syslog Messages 401001 to 450002

This chapter contains the following sections:

- Messages 401001 to 409023, on page 1
- Messages 410001 to 450002, on page 19

Messages 401001 to 409023

This chapter includes messages from 401001 to 409023.

401001

Error Message `%FTD-4-401001: Shuns cleared`

Explanation The **clear shun** command was entered to remove existing shuns from memory. An institution to keep a record of shunning activity was allowed.

Recommended Action None required.

401002

Error Message `%FTD-4-401002: Shun added: IP_address IP_address port  port`

Explanation A **shun** command was entered, where the first IP address is the shunned host. The other addresses and ports are optional and are used to terminate the connection if available. An institution to keep a record of shunning activity was allowed.

Recommended Action None required.

401003

Error Message `%FTD-4-401003: Shun deleted: IP_address`

ExplanationA single shunned host was removed from the shun database. An institution to keep a record of shunning activity was allowed.

Recommended Action None required.

401004

Error Message `%FTD-4-401004: Shunned packet: IP_address ==> IP_address on interface interface_name`

ExplanationA packet was dropped because the host defined by IP SRC is a host in the shun database. A shunned host cannot pass traffic on the interface on which it is shunned. For example, an external host on the Internet can be shunned on the outside interface. A record of the activity of shunned hosts was provided. This message and message %Firewall Threat Defense-4-401005 can be used to evaluate further risk concerning this host.

Recommended Action None required.

401005

Error Message `%FTD-4-401005: Shun add failed: unable to allocate resources for IP_address IP_address port port`

Explanation The Secure Firewall Threat Defense device is out of memory; a shun cannot be applied.

Recommended Action The Cisco IPS should continue to attempt to apply this rule. Try to reclaim memory and reapply a shun manually, or wait for the Cisco IPS to do this.

402114

Error Message `%FTD-4-402114: IPSEC: Received an protocol packet (SPI= spi, sequence number= seq_num) from remote_IP to local_IP with an invalid SPI.`

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq_num>— IPsec sequence number
- remote_IP>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local_IP>— IP address of the local endpoint of the tunnel

ExplanationAn IPsec packet was received that specifies an SPI that does not exist in the SA database. This may be a temporary condition caused by slight differences in aging of SAs between the IPsec peers, or it may be because the local SAs have been cleared. It may also indicate incorrect packets sent by the IPsec peer, which may be part of an attack. This message is rate limited to no more than one message every five seconds.

Recommended Action The peer may not acknowledge that the local SAs have been cleared. If a new connection is established from the local router, the two peers may then reestablish connection successfully. Otherwise, if the problem occurs for more than a brief period, either attempt to establish a new connection or contact the peer administrator.

402115

Error Message `%FTD-4-402115: IPSEC: Received a packet from remote_IP to local_IP containing act_prot data instead of exp_prot data.`

Explanation An IPsec packet was received that is missing the expected ESP header. The peer is sending packets that do not match the negotiated security policy, which may indicate an attack. This message is rate limited to no more than one message every five seconds.

- remote_IP>— IP address of the remote endpoint of the tunnel
- local_IP>— IP address of the local endpoint of the tunnel
- >*act_prot*— Received IPsec protocol
- >*exp_prot*— Expected IPsec protocol

Recommended Action Contact the administrator of the peer.

402116

Error Message `%FTD-4-402116: IPSEC: Received an protocol packet (SPI= spi, sequence number= seq_num) from remote_ip (user= username) to local_ip. The decapsulated inner packet doesn't match the negotiated policy in the SA. The packet specifies its destination as pkt_daddr, its source as pkt_saddr, and its protocol as pkt_prot. The SA specifies its local proxy as id_daddr/id_dmask/id_dprot/id_dport and its remote_proxy as id_saddr/id_smask/id_sprot/id_sport.`

Explanation: A decapsulated IPsec packet does not match the negotiated identity. The peer is sending other traffic through this security association, which may be caused by a security association selection error by the peer, or it may be part of an attack. This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq_num>— IPsec sequence number
- remote_ip>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local_ip>— IP address of the local endpoint of the tunnel
- pkt_daddr>— Destination address from the decapsulated packet
- pkt_saddr>— Source address from the decapsulated packet
- pkt_prot>— Transport protocol from the decapsulated packet
- id_daddr>— Local proxy IP address
- id_dmask>— Local proxy IP subnet mask
- id_dprot>— Local proxy transport protocol
- id_dport>— Local proxy port
- id_saddr>— Remote proxy IP address
- id_smask>— Remote proxy IP subnet mask
- id_sprot>— Remote proxy transport protocol
- id_sport>— Remote proxy port

Recommended Action Contact the administrator of the peer and compare policy settings.

402117

Error Message `%FTD-4-402117: IPSEC: Received a non-IPSec packet (protocol= protocol) from remote_IP to local_IP.`

ExplanationThe received packet matched the crypto map ACL, but it is not IPsec-encapsulated. The IPsec peer is sending unencapsulated packets. This error can occur because of a policy setup error on the peer. For example, the firewall may be configured to only accept encrypted Telnet traffic to the outside interface port 23. If you attempt to use Telnet without IPsec encryption to access the outside interface on port 23, this

message appears, but not with Telnet or traffic to the outside interface on ports other than 23. This error can also indicate an attack. This message is not generated except under these conditions (for example, it is not generated for traffic to the Secure Firewall Threat Defense interfaces themselves). This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- remote_IP>— IP address of the remote endpoint of the tunnel
- local_IP>— IP address of the local endpoint of the tunnel

Recommended Action Contact the administrator of the peer to compare policy settings.

402118

Error Message `%FTD-4-402118: IPSEC: Received an protocol packet (SPI= spi, sequence number= seq_num) from remote_IP (user= username) to local_IP containing an illegal IP fragment of length frag_len with offset frag_offset.`

Explanation A decapsulatd IPsec packet included an IP fragment with an offset less than or equal to 128 bytes. The latest version of the security architecture for IP RFC recommends 128 bytes as the minimum IP fragment offset to prevent reassembly attacks. This may be part of an attack. This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq_num>— IPsec sequence number
- remote_IP>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local_IP>— IP address of the local endpoint of the tunnel
- frag_len>— IP fragment length
- frag_offset>— IP fragment offset in bytes

Recommended Action Contact the administrator of the remote peer to compare policy settings.

402119

Error Message `%FTD-4-402119: IPSEC: Received an protocol packet (SPI= spi, sequence number= seq_num) from remote_IP (user= username) to local_IP that failed anti-replay checking.`

ExplanationAn IPsec packet was received with an invalid sequence number. The peer is sending packets including sequence numbers that may have been previously used. This message indicates that an IPsec packet has been received with a sequence number outside of the acceptable window. This packet will be dropped by IPsec as part of a possible attack. This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq_num>— IPsec sequence number
- remote_IP>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local_IP>— IP address of the local endpoint of the tunnel

Recommended Action Contact the administrator of the peer.

402120

Error Message `%FTD-4-402120: IPSEC: Received an protocol packet (SPI= spi, sequence number= seq_num) from remote_IP (user= username) to local_IP that failed authentication.`

Explanation An IPsec packet was received and failed authentication. The packet is dropped. The packet may have been corrupted in transit, or the peer may be sending invalid IPsec packets, which may indicate an attack if many of these packets were received from the same peer. This message is rate limited to no more than one message every five seconds.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq_num>— IPsec sequence number
- remote_IP>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- local_IP>— IP address of the local endpoint of the tunnel

Recommended Action Contact the administrator of the remote peer if many failed packets were received.

402121

Error Message `%FTD-4-402121: IPSEC: Received an protocol packet (SPI= spi, sequence number= seq_num) from peer_addr (user= username) to lcl_addr that was dropped by IPSec (drop_reason).`

Explanation An IPsec packet to be decapsulated was received and subsequently dropped by the IPsec subsystem. This may indicate a problem with the Secure Firewall Threat Defense configuration or with the Secure Firewall Threat Defense device itself.

- >*protocol*— IPsec protocol
- >*spi*— IPsec Security Parameter Index
- seq_num>— IPsec sequence number
- peer_addr>— IP address of the remote endpoint of the tunnel
- >*username*— Username associated with the IPsec tunnel
- lcl_addr>— IP address of the local endpoint of the tunnel
- drop_reason>— Reason that the packet was dropped

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

402122

Error Message `%FTD-4-402122: IPSEC: Received a cleartext packet from src_addr to dest_addr that was to be encapsulated in IPSec that was dropped by IPSec (drop_reason).`

Explanation A packet to be encapsulated in IPsec was received and subsequently dropped by the IPsec subsystem. This may indicate a problem with the Secure Firewall Threat Defense configuration or with the Secure Firewall Threat Defense device itself.

- *src_addr* >— Source IP address
- *dest_addr* >— Destination> IP address
- drop_reason>— Reason that the packet was dropped

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

402123

Error Message `%FTD-4-402123: CRYPTO: The accel_type hardware accelerator encountered an error (eror_type, code= error_string) while executing the command command_name (command).`

Explanation An error was detected while running a crypto command with a hardware accelerator, which may indicate a problem with the accelerator. This type of error may occur for a variety of reasons, and this message supplements the crypto accelerator counters to help determine the cause.

- accel_type—Hardware accelerator type
- >*error_string*— Code indicating the type of error
- command—Crypto command that generated the error

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

402124

Error Message-1 `%FTD-4-402124: CRYPTO: The platform hardware accelerator encountered an error (HWErrAddr= 0xerror_address, Core= error_core, HwErrCode= error_code, IstatReg= 0xIstat, PciErrReg= 0xPCI, CoreErrStat= 0xcore_error_stat, CoreErrAddr= 0xcore_err_address, Doorbell Size[0]= size, DoorBell Outstanding[0]= outstanding, Doorbell Size[1]= size, DoorBell Outstanding[1]= outstanding, SWReset= Reset_code)`

Error Message-2 `%FTD-4-402124: CRYPTO: The platform hardware accelerator encountered an error (HWErrAddr= 0xerror_address, Core= error_core, HwErrCode= error_code, Queue= queue_string (0), IstatReg= 0xIstat, Station= core_station, CoreRptr= 0xcore_pointer, CoreConfig= 0xcore_config_pointer, SWReset= Reset_code)`

Explanation The crypto hardware chip has reported a fatal error, indicating that the chip is inoperable. The information from this message captures the details to allow further analysis of the problem. The crypto chip is reset when this condition is detected to unobtrusively allow the Secure Firewall Threat Defense device to continue functioning. Also, the crypto environment at the time this issue is detected is written to a crypto archive directory on flash to provide further debugging information. Various parameters related to the crypto hardware are included in this message, as follows:

- HWErrAddr>— Hardware address (set by crypto chip)
- Core>— Crypto core experiencing the error
- HwErrCode>— Hardware error code (set by crypto chip)
- IstatReg>— Interrupt status register (set by crypto chip)
- PciErrReg>— PCI error register (set by crypto chip)
- CoreErrStat>— Core error status (set by crypto chip)
- CoreErrAddr>— Core error address (set by crypto chip)
- Doorbell Size>— Maximum crypto commands allowed
- DoorBell Outstanding>— Crypto commands outstanding
- SWReset>— Number of crypto chip resets since boot

Note The %Firewall Threat Defense-vpn-4-402124: CRYPTO: The Firewall Threat Defense hardware accelerator encountered an error (HWErrAddr= 0x40EE9800, Core= 0, HwErrCode= 23, IstatReg= 0x8, PciErrReg= 0x0, CoreErrStat= 0x41, CoreErrAddr= 0x844E9800, Doorbell Size[0]= 2048, DoorBell Outstanding[0]= 0, Doorbell Size[1]= 0, DoorBell Outstanding[1]= 0, SWReset= 99) error message indicates a AnyConnect problem and the workaround for this to upgrade to AnyConnect 3.1.x.

Recommended Action Forward the message information to the Cisco TAC for further analysis.

402125

Error Message-1 `%FTD-4-402125: CRYPTO: The platform hardware accelerator ring_string ring timed out (Desc= 0xdescriptor_address, CtrlStat= 0xcontrol_or_status value, ResultP= 0xsuccess_pointer, ResultVal= success_value, Cmd= 0xcrypto_command, CmdSize= command_size, Param= 0xcommand_parameters, Dlen= Data_length, DataP= 0xData_pointer, CtxtP= 0xVPN_context_pointer, SWReset= reset_number)`

Explanation The crypto driver has detected that either the IPSEC descriptor ring or SSL/Admin descriptor ring is no longer progressing, meaning the crypto chip no longer appears to be functioning. The crypto chip is reset when this condition is detected to unobtrusively allow the Secure Firewall Threat Defense device to continue functioning. Also, the crypto environment at the time this issue was detected was written to a crypto archive directory on flash to provide further debugging information.

- >*ring*— IPSEC or Admin ring
- *parameters* >— Include the following:

- Desc>— Descriptor address

- CtrlStat>— Control/status value

- ResultP>— Success pointer

- ResultVal>— Success value

- Cmd>— Crypto command

- CmdSize>— Command size

- Param>— Command parameters

- Dlen>— Data length

- DataP>— Data pointer

- CtxtP>— VPN context pointer

- SWReset>— Number of crypto chip resets since boot

Recommended Action Forward the message information to the Cisco TAC for further analysis.

402126

Error Message `%FTD-4-402126: CRYPTO: The platform created Crypto Archive File <Archive_Filename> as a Soft Reset was necessary. Please forward this archived information to Cisco`

Explanation A functional problem with the hardware crypto chip was detected (see syslog messages 402124 and 402125). To further debug the crypto problem, a crypto archive file was generated that included the current crypto hardware environment (hardware registers and crypto description entries). At boot time, a crypto_archive directory was automatically created on the flash file system (if it did not exist previously). A maximum of two crypto archive files are allowed to exist in this directory.

- >*Archive Filename*— The name of the crypto archive file name. The crypto archive file names are of the form, crypto_arch_x.bin, where x = (1 or 2).

Recommended Action Forward the crypto archive files to the Cisco TAC for further analysis.

402127

Error Message `%FTD-4-402127: CRYPTO: The platform is skipping the writing of latest Crypto Archive File as the maximum # of files ( max_number ) allowed have been written to <archive_directory>. Please archive remove files from < Archive Directory > if you want more Crypto Archive Files saved`

Explanation A functional problem with the hardware crypto chip was detected (see messages 4402124 and 4402125). This message indicates a crypto archive file was not written, because the maximum number of crypto archive files already existed.

- *max_number* >— Maximum number of files allowed in the archive directory; currently set to two
- >*archive_directory*— Name of the archive directory

Recommended Action Forward previously generated crypto archive files to the Cisco TAC. Remove the previously generated archive file(s) so that more can be written (if deemed necessary).

402128

Error Message `%FTD-5-402128: CRYPTO: An attempt to allocate a large memory block failed, size: size, limit: limit.`

Explanation An SSL connection is attempting to use more memory than allowed. The request has been denied.

- *size* —The size of the memory block being allocated
- *limit* —The maximum size of allocated memory permitted

Recommended Action If this message persists, an SSL denial of service attack may be in progress. Contact the remote peer administrator or upstream provider.

402129

Error Message `%FTD-6-402129: CRYPTO: An attempt to release a DMA memory block failed, location: address.`

Explanation An internal software error has occurred.

- *address* —The address being freed

Recommended Action Contact the Cisco TAC for assistance.

402130

Error Message `%FTD-6-402130: CRYPTO: Received an ESP packet (SPI = xxxxxxxxxx, sequence number=xxxx) from 172.16.0.1 (user=user) to 192.168.0.2 with incorrect IPsec padding.`

Explanation The Secure Firewall Threat Defense device crypto hardware accelerator detected an IPsec packet with invalid padding. The ATT VPN client sometimes pads IPsec packets incorrectly.

- *SPI* —The SPI associated with the packet
- *sequence number* —The sequence number associated with the packet
- *user* —Username string
- *padding* —Padding data from the packet

Recommended Action While this message is None required and does not indicate a problem with the Secure Firewall Threat Defense device, customers using the ATT VPN client may wish to upgrade their VPN client software.

402131

Error Message `%FTD-4-402131: CRYPTO: status changing the accel_instance hardware accelerator's configuration bias from old_config_bias to new_config_bias.`

Explanation The hardware accelerator configuration has been changed on the Secure Firewall Threat Defense device. Some Secure Firewall Threat Defense platforms have multiple hardware accelerators. One syslog message is generated for each hardware accelerator change.

- *status* —Indicates success or failure
- *accel_instance* —The instance of the hardware accelerator
- *old_config_bias* —The old configuration
- *new_config_bias* —The new configuration

Recommended Action If any of the accelerators fails when attempting to change its configuration, collect logging information and contact the Cisco TAC. If a failure occurs, the software will retry the configuration change multiple times. The software will fall back to the original configuration bias if the retry attempts fail. If multiple attempts to reconfigure the hardware accelerator fail, it may indicate a hardware failure.

402140

Error Message `%FTD-3-402140: CRYPTO: RSA key generation error: modulus len len`

Explanation An error occurred during an RSA public key pair generation.

- *len* —The prime modulus length in bits

Recommended Action Contact the Cisco TAC for assistance.

402141

Error Message `%FTD-3-402141: CRYPTO: Key zeroization error: key set 'type', reason 'reason'`

Explanation An error occurred during an RSA public key pair generation.

- *type* —The key set type, which can be any of the following: DH, RSA, DSA, or unknown
- *reason* —The unexpected crypto session type

Recommended Action Contact the Cisco TAC for assistance.

402142

Error Message `%FTD-3-402142: CRYPTO: Bulk data op error: algorithm 'alg', mode 'mode'`

Explanation An error occurred during a symmetric key operation.

- *op* —The operation, which can be either encryption or decryption
- *alg* —The encryption algorithm, which can be any of the following: DES, 3DES, AES, or RC4
- *mode* —The mode, which can be any of the following: CBC, CTR, CFB, ECB, stateful-RC4, or stateless-RC4

Recommended Action Contact the Cisco TAC for assistance.

402143

Error Message `%FTD-3-402143: CRYPTO: alg type key op error`

Explanation An error occurred during an asymmetric key operation.

- *alg* —The encryption algorithm, which can be either RSA or DSA
- *type* —The key type, which can be either public or private
- *op* —The operation, which can be either encryption or decryption

Recommended Action Contact the Cisco TAC for assistance.

402144

Error Message `%FTD-3-402144: CRYPTO: Digital signature error: signature algorithm 'sig', hash algorithm 'hash'`

Explanation An error occurred during digital signature generation.

- *sig* —The signature algorithm, which can be either RSA or DSA
- *hash* —The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512

Recommended Action Contact the Cisco TAC for assistance.

402145

Error Message `%FTD-3-402145: CRYPTO: Hash generation error: algorithm 'hash'`

Explanation A hash generation error occurred.

- *hash* —The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512

Recommended Action Contact the Cisco TAC for assistance.

402146

Error Message `%FTD-3-402146: CRYPTO: Keyed hash generation error: algorithm 'hash', key len len`

Explanation A keyed hash generation error occurred.

- *hash* —The hash algorithm, which can be any of the following: MD5, SHA1, SHA256, SHA384, or SHA512
- *len* —The key length in bits

Recommended Action Contact the Cisco TAC for assistance.

402147

Error Message `%FTD-3-402147: CRYPTO: HMAC generation error: algorithm 'alg'`

Explanation An HMAC generation error occurred.

- *alg* —The HMAC algorithm, which can be any of the following: HMAC-MD5, HMAC-SHA1, HMAC-SHA2, or AES-XCBC

Recommended Action Contact the Cisco TAC for assistance.

402148

Error Message `%FTD-3-402148: CRYPTO: Random Number Generator error`

Explanation A random number generator error occurred.

Recommended Action Contact the Cisco TAC for assistance.

402149

Error Message `%FTD-3-402149: CRYPTO: Weak encryption_type (length) provided. Operation disallowed. Not FIPS 140-2 compliant`

Explanation The Secure Firewall Threat Defense device tried to use an RSA key that is less than 2048 bits or DH groups 1, 2, or 5.

- *encryption type* —The encryption type
- *length* —The RSA key length or DH group number

Recommended Action Configure the Secure Firewall Threat Defense device or external application to use an RSA key that is at least 2048 bits, or to configure a DH group that is not 1, 2, or 5.

402150

Error Message `%FTD-3-402150: CRYPTO: Deprecated hash algorithm used for RSA operation (hash_alg). Operation disallowed. Not FIPS 140-2 compliant`

Explanation An unacceptable hashing algorithm has been used for digital certificate signing or verification for FIPS 140-2 certification.

- *operation* —Sign or verify

- *hash alg* —The name of the unacceptable hashing algorithm

Recommended Action Make sure that you use the minimum acceptable hashing algorithm for digital certificate signing or verification for FIPS 140-2 certification. These include SHA-256, SHA-384, and SHA-512.

403500

Error Message `%FTD-6-403500: PPPoE - Service name 'any' not received in interface_name. AC:ac_name.`

Explanation The Secure Firewall Threat Defense device requested the PPPoE service *any* from the access controller at the Internet service provider. The response from the service provider includes other services, but does not include the service *any* . This is a discrepancy in the implementation of the protocol. The PADO packet is processed normally, and connection negotiations continue.

Recommended Action None required.

403501

Error Message `%FTD-3-403501: PPPoE - Bad host-unique in PADO - packet dropped. AC:interface_name.`

Explanation The Secure Firewall Threat Defense device sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The Secure Firewall Threat Defense device was unable to identify the corresponding connection request for this response. The packet was dropped, and connection negotiations were discontinued.

Recommended Action Contact the Internet service provider. Either the access controller at the service provider is mishandling the host-unique value, or the PADO packet is being forged.

403502

Error Message `%FTD-3-403502: PPPoE - Bad host-unique in PADS - packet dropped. AC:interface_name.`

Explanation The Secure Firewall Threat Defense device sent an identifier called the host-unique value to the access controller. The access controller responded with a different host-unique value. The Secure Firewall Threat Defense device was unable to identify the corresponding connection request for this response. The packet was dropped, and connection negotiations were discontinued.

Recommended Action Contact the Internet service provider. Either the access controller at the service provider is mishandling the host-unique value, or the PADO packet is being forged.

403503

Error Message `%FTD-3-403503: Header_string:PPP link down[:reason string]`

Explanation The PPP link has gone down. There are many reasons why this can happen. The first format will display a reason if PPP provides one.

Recommended Action Check the network link to ensure that the link is connected. The access concentrator may be down. Make sure that your authentication protocol matches the access concentrator and that your name and password are correct. Verify this information with your ISP or network support person.

403504

Error Message `%FTD-3-403504: group_name:No 'vpdn group' for PPPoE has been created!`

Explanation PPPoE requires a dial-out configuration before starting a PPPoE session. In general, the configuration should specify a dialing policy, the PPP authentication, the username, and a password. The following example configures the Secure Firewall Threat Defense device for PPPoE dialout. The my-username and my-password commands are used to authenticate the access concentrator, using PAP if necessary.

For example:

```
ciscoftd# vpdn group my-pppoe request dialout pppoe
ciscoftd# vpdn group my-pppoe ppp authentication pap
ciscoftd# vpdn group my-pppoe localname my-username
ciscoftd# vpdn username my-username password my-password
ciscoftd# ip address outside pppoe setroute
```

Recommended Action Configure a VPDN group for PPPoE.

403505

Error Message `%FTD-4-403505: PPPoE:PPP - Unable to set default route to IP_address at interface_name. interface`

Explanation This message is usually followed by the message, default route already exists.

Recommended Action Remove the current default route or remove the *setroute* parameter so that there is no conflict between PPPoE and the manually configured route.

403506

Error Message `%FTD-4-403506: PPPoE: failed to assign PPP address IP_address netmask netmask at interface interface_name`

Explanation This message is followed by one of the followings messages: subnet is the same as interface, or on failover channel.

Recommended Action In the first case, change the address causing the conflict. In the second case, configure the PPPoE on an interface other than the failover interface.

403507

Error Message `%FTD-3-403507: PPPoE:PPPoE client on interface interface failed to locate PPPoE vpdn group group_name`

Explanation You can configure the PPPoE client on an interface to use a particular VPDN group by entering the **pppoe client vpdn group group_name** command. If a PPPoE VPDN group of the configured name was not located during system startup, this message is generated.

- *interface* —The interface on which the PPPoE client failed
- *group_name* —The VPDN group name of the PPPoe client on the interface

Recommended Action Perform the following steps:

1. Add the required VPDN group by entering the **vpdn group group_name** command. Request dialout PPPoE in global configuration mode, and add all the group properties.
2. Remove the **pppoe client vpdn group** *group_name* command from the interface indicated. In this case, the PPPoE client will attempt to use the first PPPoE VPDN group defined.



Note All changes take effect only after the PPPoE client on the interface is restarted by entering the **ip address pppoe** command.

405001

Error Message `%FTD-4-405001: Received ARP {request | response} collision from ip_address/MAC_address on interface interface_name with existing ARP entry ip_address/MAC_address`

Explanation The Secure Firewall Threat Defense device received an ARP packet, and the MAC address in the packet differs from the ARP cache entry.

Recommended Action This traffic might be legitimate, or it might indicate that an ARP poisoning attack is in progress. Check the source MAC address to determine where the packets are coming from and to see if they belong to a valid host.

405002

Error Message `%FTD-4-405002: Received mac mismatch packet from IP_address/{MAC_bytes|MAC_address} for authenticated host`

Explanation This packet appears for one of the following conditions:

- The Secure Firewall Threat Defense device received a packet with the same IP address, but a different MAC address from one of its uauth entries.
- You configured the **vpnclient mac-exempt** command on the Secure Firewall Threat Defense device, and the Secure Firewall Threat Defense device received a packet with an exempt MAC address, but a different IP address from the corresponding uauth entry.

Recommended Action This traffic might be legitimate, or it might indicate that a spoofing attack is in progress. Check the source MAC address and IP address to determine where the packets are coming from and if they belong to a valid host.

405003

Error Message `%FTD-4-405003: IP address collision detected between host ip_address at MAC_address and interface interface_name, MAC_address`

Explanation A client IP address in the network is the same as the Secure Firewall Threat Defense interface IP address.

Recommended Action Change the IP address of the client.

405101

Error Message-1 `%FTD-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for faddr foreign_ip_address to laddr local_ip_address/local_port`

Error Message-2 `%FTD-4-405101: Unable to Pre-allocate H225 Call Signalling Connection for faddr foreign_ip_address/foreign_port to laddr local_ip_address`

Explanation The module failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

Recommended Action If this message occurs periodically, it can be ignored. You can check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of translates and connections. This error message may also be caused by insufficient memory; try reducing the amount of memory usage, or purchasing additional memory. If the problem persists, contact the Cisco TAC.

405102

Error Message-1 `%FTD-4-405102: Unable to Pre-allocate H245 Connection for faddr foreign_ip_address to laddr local_ip_address/local_port`

Error Message-2 `%FTD-4-405102: Unable to Pre-allocate H245 Connection for faddr foreign_ip_address/foreign_port to laddr local_ip_address`

Explanation The Secure Firewall Threat Defense device failed to allocate RAM system memory while starting a connection or has no more address translation slots available.

Recommended Action Check the size of the global pool compared to the number of inside network clients. A PAT address may be necessary. Alternatively, shorten the timeout interval of translations and connections. In addition, reduce the amount of memory usage, or purchase additional memory. If this message occurs periodically, it can be ignored. If the problem persists, contact the Cisco TAC.

405103

Error Message `%FTD-4-405103: H225 message from source_address/source_port to dest_address/dest_port contains bad protocol discriminator hex`

Explanation The Secure Firewall Threat Defense device is expecting the protocol discriminator, 0x08, but it received something other than 0x08. The endpoint may be sending a bad packet, or received a message segment other than the first segment. The packet is allowed through.

Recommended Action None required.

405104

Error Message `%FTD-4-405104: H225 message string received from outside_address/outside_port to inside_address/inside_port before SETUP`

Explanation An H.225 message was received out of order, before the initial SETUP message, which is not allowed. The Secure Firewall Threat Defense device must receive an initial SETUP message for that H.225 call signalling channel before accepting any other H.225 messages.

Recommended Action None required.

405105

Error Message `%FTD-4-405105: H323 RAS message AdmissionConfirm received from source_address/source_port to dest_address/dest_port without an AdmissionRequest`

Explanation A gatekeeper has sent an ACF, but the Secure Firewall Threat Defense device did not send an ARQ to the gatekeeper.

Recommended Action Check the gatekeeper with the specified **source_address** to determine why it sent an ACF without receiving an ARQ from the Secure Firewall Threat Defense device.

406001

Error Message `%FTD-4-406001: FTP port command low port: IP_address/port to IP_address on interface interface_name`

Explanation A client entered an FTP port command and supplied a port less than 1024 (in the well-known port range usually devoted to server ports). This is indicative of an attempt to avert the site security policy. The Secure Firewall Threat Defense device drops the packet, terminates the connection, and logs the event.

Recommended Action None required.

406002

Error Message `%FTD-4-406002: FTP port command different address: IP_address(IP_address) to IP_address on interface interface_name`

Explanation A client entered an FTP port command and supplied an address other than the address used in the connection. An attempt to avert the site security policy occurred. For example, an attacker might attempt to hijack an FTP session by changing the packet on the way, and putting different source information instead of the correct source information. The Secure Firewall Threat Defense device drops the packet, terminates the connection, and logs the event. The address in parentheses is the address from the port command.

Recommended Action None required.

407001

Error Message `%FTD-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded`

Explanation The host limit was exceeded. An inside host is counted toward the limit when one of the following conditions is true:

- The inside host has forwarded traffic through the Secure Firewall Threat Defense device within the last five minutes.
- The inside host has reserved an xlate connection or user authentication at the Secure Firewall Threat Defense device.

Recommended Action The host limit is enforced on the low-end platforms. Use the **show version** command to view the host limit. Use the **show local-host** command to view the current active hosts and the inside users that have sessions at the Secure Firewall Threat Defense device. To forcefully disconnect one or more users, use the **clear local-host** command. To expire the inside users more quickly from the limit, set the xlate, connection, and uauth timeouts to the recommended values or lower as given in the table below:

Table 1: Timeouts and Recommended Values

Timeout	Recommended Value
xlate	00:05:00 (five minutes)
conn	00:01:00 (one hour)
uauth	00:05:00 (five minutes)

407002

Error Message `%FTD-4-407002: Embryonic limit for through connections exceeded` *`nconns/elimit. outside_address/outside_port`* `to` *`global_address`*`(`*`inside_address`*`)/`*`inside_port`* `on interface` *`interface_name`*

Explanation The number of connections from a specified foreign address over a specified global address to the specified local address exceeded the maximum embryonic limit for that static. The Secure Firewall Threat Defense device tries to accept the connection if it can allocate memory for that connection. It proxies on behalf of the local host and sends a SYN_ACK packet to the foreign host. The Secure Firewall Threat Defense device retains pertinent state information, drops the packet, and waits for the acknowledgment from the client. The message might indicate legitimate traffic or that a DoS attack is in progress.

Recommended Action Check the source address to determine where the packets are coming from and whether or not a valid host is sending them.

407003

Error Message `%FTD-4-407003: Established limit for RPC services exceeded`

Explanation The Secure Firewall Threat Defense device tried to open a new hole for a pair of RPC servers or services that have already been configured after the maximum number of holes has been met.

Recommended Action Wait for other holes to be closed (through associated timeout expiration), or limit the number of active pairs of servers or services.

408001

Error Message `%FTD-4-408001: IP route counter negative`

Explanation An attempt to decrement the IP route counter into a negative value failed.

Recommended Action Enter the **clear ip route** command to reset the route counter. If the problem persists, contact the Cisco TAC.

408101

Error Message `%FTD-4-408101: KEYMAN : Type` *`encrption_type`* `encryption unknown. Interpreting keystring as literal.`

Explanation The format type was not recognized by the system. A keystring format type value of 0 (unencrypted keystring) or 7 (hidden keystring), followed by a space, can precede the actual keystring to

indicate its format. An unknown type value will be accepted, but the system will consider the keystring as being unencrypted.

Recommended Action Use the correct format for the value type or remove the space following the value type.

408102

Error Message `%FTD-4-408102: KEYMAN : Bad encrypted keystring for key id key_id.`

Explanation The system could not successfully decrypt an encrypted keystring. The keystring may have been corrupted during system configuration.

Recommended Action Re-enter the key-string command, and reconfigure the key string.

409014

Error Message `%Firewall Threat Defense-4-409014: No valid authentication send key is available on interface nameif.`

Explanation The authentication key configured on the interface is not valid.

Recommended Action Configure a new key.

409015

Error Message `%Firewall Threat Defense-4-409015: Key ID key-id received on interface nameif.`

Explanation The ID is not found in the configured key chain.

Recommended Action Configure a new security association with the Key ID.

409016

Error Message `%Firewall Threat Defense-4-409016: Key chain name key-chain-name on nameif is invalid.`

Explanation The key-chain name configured under OSPF interface does not match global key chain configuration.

Recommended Action Fix configuration. Either remove OSPF authentication command or configure key chain in global configuration mode.

409017

Error Message `%Firewall Threat Defense-4-409017: Key ID key-id in key chain key-chain-name is invalid.`

Explanation The Key ID configured in the key chain is out of range for OSPF. This may happen because the key chain allows Key ID values of the range which is not acceptable for OSPF.

Recommended Action Configure a new security association with a Key ID that is in the range 1-255.

409023

Error Message `%FTD-4-409023: Attempting AAA Fallback method method_name for request_type request for user user : Auth-server group Auth-server unreachable`

Explanation An authentication or authorization attempt to an external server has failed and will be performed using the local user database.

- **aaa_operation**—Either authentication or authorization
- **username**—The user associated with the connection
- **server_group**—The name of the AAA server whose servers were unreachable

Recommended Action Investigate any connectivity problems with the AAA servers configured in the first method. Ping the authentication servers from the Secure Firewall Threat Defense device. Make sure that the daemons are running on the AAA server.

Messages 410001 to 450002

This chapter includes messages from 410001 to 450002.

410001

Error Message `%FTD-4-410001: Dropped UDP DNS request from source_interface:source_address/source_port to dest_interface:dest_address/dest_port; label|domain-name length number bytes exceeds remaining_packet_length limit of number bytes`

Explanation The label length exceeds bytes in a UDP DNS packet. See RFC 1035, section 2.3.4 for more information. .

Recommended Action Create the policy-map and add a custom DNS class-map to match traffic and exclude it from inspection to allow packets exceeding the label length.

411001

Error Message `%FTD-4-411001: Line protocol on Interface interface_name, changed state to up`

Explanation The status of the line protocol has changed from down to up . If **interface_name** is a logical interface name such as inside and outside, this message indicates that the logical interface line protocol has changed from down to up . If **interface_name** is a physical interface name such as Ethernet0 and GigabitEthernet0/1, this message indicates that the physical interface line protocol has changed from down to up .

Recommended Action None required.

411002

Error Message `%FTD-4-411002: Line protocol on Interface interface_name, changed state to down`

Explanation The status of the line protocol has changed from up to down. If **interface_name** is a logical interface name such as inside and outside, this message indicates that the logical interface line protocol has

changed from up to down. In this case, the physical interface line protocol status is not affected. If **interface_name** is a physical interface name such as Ethernet0 and GigabitEthernet0/1, this message indicates that the physical interface line protocol has changed from up to down.

Recommended Action If this is an unexpected event on the interface, check the physical line.

411003

Error Message `%FTD-4-411003: Interface interface_name, changed state to administratively up`

Explanation The configuration status of the interface has changed from down to up.

Recommended Action If this is an unexpected event, check the physical line.

411004

Error Message `%FTD-4-411004: Interface interface_name, changed state to administratively down`

Explanation The configuration status of the interface has changed from down to up.

Recommended Action None required.

411005

Error Message `%FTD-4-411005: Interface variable_1 experienced a hardware transmit hang. A software reset has been performed.`

Explanation The interface experienced a hardware transmit freeze that required a reset of the Ethernet controller to restore the interface to full operation.

- *variable 1* —The interface name, such as GigabitEthernet0/0

Recommended Action None required.

412001

Error Message `%FTD-4-412001: MAC MAC_address moved from interface_1 to interface_2`

Explanation A host move was detected from one module interface to another. In a transparent Secure Firewall Threat Defense, mapping between the host (MAC) and Secure Firewall Threat Defense port is maintained in a Layer 2 forwarding table. The table dynamically binds packet source MAC addresses to an Secure Firewall Threat Defense port. In this process, whenever movement of a host from one interface to another interface is detected, this message is generated.

Recommended Action The host move might be valid or might be an attempt to spoof host MACs on other interfaces. If it is a MAC spoof attempt, you can either locate vulnerable hosts on your network and remove them or configure static MAC entries, which will not allow MAC address and port binding to change. If it is a genuine host move, no action is required.

412002

Error Message `%FTD-4-412002: Detected bridge table full while inserting MAC MAC_address on interface interface. Number of entries = num`

Explanation The bridge table was full and an attempt was made to add one more entry. The Secure Firewall Threat Defense device maintains a separate Layer 2 forwarding table per context and the message is generated whenever a context exceeds its size limit. The MAC address will be added, but it will replace the oldest existing dynamic entry (if available) in the table. This might be an attempted attack.

Recommended Action Make sure that the new bridge table entries are valid. In case of attack, use EtherType ACLs to control access to vulnerable hosts.

413001

Error Message `%FTD-4-413001: Module module_id is not able to shut down. Module Error: errnum message`

Explanation The module identified by *module_id* was not able to comply with a request from the Secure Firewall Threat Defense system module to shut down. It may be performing a task that cannot be interrupted, such as a software upgrade. The **errnum** and **message** text describes the reason why the module cannot shut down, and the recommended corrective action.

Recommended Action Wait for the task on the module to complete before shutting down the module, or use the **session** command to access the CLI on the module, and stop the task that is preventing the module from shutting down.

413002

Error Message `%FTD-4-413002: Module module_id is not able to reload. Module Error: errnum message`

Explanation The module identified by *module_id* was not able to comply with a request from the Secure Firewall Threat Defense module to reload. It may be performing a task that cannot be interrupted, such as a software upgrade. The **errnum** and **message** text describes the reason why the module cannot reload, and the recommended corrective action.

Recommended Action Wait for the task on the module to complete before reloading the module, or use the **session** command to access the CLI on the module and stop the task that is preventing the module from reloading.

413003

Error Message `%FTD-4-413003: Module string_one is not a recognized type.`

Explanation A module was detected that is not recognized as a valid module type.

Recommended Action Upgrade to a version of Secure Firewall Threat Defense software that supports the module type installed.

413004

Error Message `%FTD-4-413004: Module in slot string_one failed to write software vnewver (currently vver), reason. Trying again.`

Explanation The module failed to accept a software version, and will be transitioned to an UNRESPONSIVE state. Another attempt will be made to update the module software.

- >*string one*— The text string that specifies the module
- >*newver* —The new version number of software that was not successfully written to the module (for example, 1.0(1)0)
- >*ver* —The current version number of the software on the module (for example, 1.0(1)0)
- >*reason* —The reason the new version cannot be written to the module. The possible values for >*reason* include the following:

- write failure

- failed to create a thread to write the image

Recommended Action None required. Subsequent attempts will either generate a message indicating a successful update or failure. You may verify the module transitions to UP after a subsequent update attempt by using the **show module** command.

413005

Error Message `%FTD-4-413005: Module module_id, application is not supported "app_name" version "app_vers" type app_type.`

Error Message `%FTD-4-413005: Module prod_id in slot slot_num , application is not supported app_name version app_vers type app_type`

Explanation The module installed in slot *slot_num* was running an unsupported application version or type.

- *module_id*— The name of the software services module
- *prod_id* —Product ID string
- *slot_num* —The slot number in which the module is installed. Slot 0 indicates the system main board, and slot 1 indicates the module installed in the expansion slot.
- *app_name* —Application name (string)
- *app_vers* —Application version (string)
- *app_type* —Application type (decimal)

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

413006

Error Message `%FTD-4-413006: prod-id Module software version mismatch; slot slot is "prod-id" version "running-vers". Slot slot "prod-id" requires version "required-vers"`

Explanation The version of software running on the module in slot *slot* was not the version required by another module.

- *slot* —Slot 0 indicates the system main board. Slot 1 indicates the module installed in the expansion slot.
- *prod_id* —Product ID string for the device installed in slot *slot*
- *running_vers* —Version of software currently running on the module installed in slot *slot*

- *required_vers* —Version of software required by the module in slot *slot*

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

413009

Error Message `%FTD-4-413009: internal_interface =current value`

Explanation The firewall checks the current value of an internal interface or a data ring every one minute. When the current value of the ring falls below 10, this message is generated.

```
%FTD-4-413009: Internal-Data0/1:RX[1]=[2]
```

In the above example, Internal-Data0/1 RX1 value went to 2, which is less than 10.

Recommended Action None.

414001

Error Message `%FTD-3-414001: Failed to save logging buffer to FTP server filename using filename ftp_server_address on interface interface_name: fail_reason`

Explanation The logging module failed to save the logging buffer to an external FTP server.

Recommended Action Take applicable actions based on the failed reason:

- Protocol error—Make sure no connectivity issue exists between the FTP server and Secure Firewall Threat Defense device, and that the FTP sever can accept the FTP port command and PUT requests.
- Invalid username or password—Make sure that the configured FTP client username and password are correct.
- All other errors—If the problem persists, contact the Cisco TAC.

414002

Error Message `%FTD-3-414002: Failed to save logging buffer to flash:/syslog directory using filename filename: fail_reason`

Explanation The logging module failed to save the logging buffer to system flash.

Recommended Action If the failed reason is caused by insufficient space, check the flash free space, and make sure that the configured limits of the **logging flash-size** command are set correctly. If the error is a flash file system I/O error, then contact the Cisco TAC for assistance.

414003

Error Message `%FTD-3-414003: TCP Syslog Server intf:IP_Address/port not responding, New connections are [permitted|denied] based on logging permit-hostdown policy`

Explanation The TCP syslog server for remote host logging was successful, is connected to the server, and new connections are permitted or denied based on the logging permit-hostdown policy. If the logging permit-hostdown policy is configured, a new connection is permitted. If not configured, a new connection is denied.

- *intf* —Interface of the Secure Firewall Threat Defense device to which the server is connected

- *IP_Address* —IP address of the remote TCP syslog server
- *port* —Port of the remote TCP syslog server

Recommended Action Validate that the configured TCP syslog server is up. To permit new connections, configure the logging permit-hostdown policy. To deny new connections, do not configure the logging permit-hostdown policy.

414005

Error Message `%FTD-3-414005: TCP Syslog Server intf : IP_Address /port connected, New connections are permitted based on logging permit-hostdown policy`

Explanation The TCP syslog server for remote host logging was successful, is connected to the server, and new connections are permitted based on the logging permit-hostdown policy. If the logging permit-hostdown policy is configured, a new connection is permitted.

- *intf* —Interface of the Secure Firewall Threat Defense device to which the server is connected
- *IP_Address* —IP address of the remote TCP syslog server
- *port* —Port of the remote TCP syslog server

Recommended Action None required.

414006

Error Message `%FTD-3-414006: TCP syslog server configured and logging queue is full. New connections denied based on logging permit-hostdown policy.`

Explanation The logging queue is close to reaching the configured limit, so there is a risk that syslog messages will be discarded.

Recommended Action See the "Configuring the Logging Queue" section in the CLI configuration guide for information about how to tune the queue size to avoid this situation. If you want to deny new connections in this case, use the **no logging permit-hostdown** command. If you want to allow new connections in this case, use the **logging permit-hostdown** command.

415020

Error Message `%FTD-5-415020: HTTP - matched matched_string in policy-map map_name, a non-ASCII character was matched connection_action int_type:IP_address/port_num to int_type:IP_address/port_num`

Explanation A non-ASCII character was found.

- **matched_string**—The matched string is one of the following:

- The class map ID, followed by the name of the class map. This string appears when the class map is user configured.

- The actual **match** command that initiated the message. This string appears when the class map is internal.

- *map_name* —The name of the policy map
- *connection_action* —Dropping the connection or resetting the connection
- *interface_type* —The type of interface (for example, DMZ or outside)
- *IP_address* —The IP address of the interface

- *port_num* —The port number

Recommended Action Enter the **match** {**request** | **response**} **header non-ascii** command to correct the problem.

417001

Error Message `%FTD-4-417001: Unexpected event received: number`

Explanation A process received a signal, but no handler was found for the event.

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

417004

Error Message `%FTD-4-417004: Filter violation error: conn number (string:string) in string`

Explanation A client tried to modify a route attribute that the client does not own.

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

417006

Error Message `%FTD-4-417006: No memory for string in string (warning)`

Explanation An operation failed because of low memory, but will be handled with another mechanism.

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

418001

Error Message `%FTD-4-418001: Through-the-device packet to/from management-only network is denied: protocol_string`

Explanation A packet from the specified source to the destination was dropped because it is traversing the Secure Firewall Threat Defense device to and from the management-only network.

- **protocol_string**—TCP, UDP, ICMP, or protocol ID as a number in decimal
- **interface_name**— Interface name
- **IP_address**—IP address
- **port**—Port number
- *sg_info* —Security group name or tag for the specified IP address

Recommended Action Determine who is generating this packet and why.

419001

Error Message `%FTD-4-419001: Dropping TCP packet from src_ifc:src_IP/src_port to dest_ifc:dest_IP/dest_port, reason: reason, MSS size, data size`

Explanation The length of the TCP packet exceeded the MSS advertised in the three-way handshake.

- >*src_ifc*— Input interface name
- >*src_IP*— The source IP address of the packet

- >*src_port*— The source port of the packet
- >*dest_ifc*— The output interface name
- >*dest_IP*— The destination IP address of the packet
- >*dest_port*— The destination port of the packet

Recommended Action If there is a need to allow packets that exceed the MSS, create a TCP map using the **exceed-mss** command, as in the following example:

```
ciscoftd# access-list http-list permit tcp any host server_ip eq 80
ciscoftd# class-map http
 ciscoftd# match access-list http-list
 ciscoftd# tcp-map tmap
ciscoftd# exceed-mss allow
ciscoftd# policy-map global_policy
ciscoftd# class http
ciscoftd# set connection advanced-options tmap
```

419002

Error Message `%FTD-4-419002: Duplicate TCP SYN from` *`in_interface`*`:`*`src_address`*`/`*`src_port`* `to` *`out_interface`*`:`*`dest_address`*`/`*`dest_port`* `with different initial sequence number`

Explanation A duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number from the SYN that opened the embryonic connection. This may indicate that SYNs are being spoofed. This message occurs in Release 7.0.4.1 and later.

- **in_interface**—The input interface
- **src_address**—The source IP address of the packet
- **src_port**—The source port of the packet
- **out_interface**—The output interface
- **dest_address**—The destination IP address of the packet
- **dest_port**—The destination port of the packet

Recommended Action None required.

419003

Error Message `%FTD-4-419003: Cleared TCP urgent flag from` *`out_ifc`*`:`*`src_ip`*`/`*`src_port`* `to` *`in_ifc`*`:`*`dest_ip`*`/`*`dest_port`*

Explanation A duplicate TCP SYN was received during the three-way-handshake that has a different initial sequence number from the SYN that opened the embryonic connection. This may indicate that SYNs are being spoofed. This message occurs in Release 7.0.4.1 and later.

- **in_ifc**—The input interface
- **src_ip**—The source IP address of the packet
- **src_port**—The source port of the packet
- **out_ifc**—The output interface
- **dest_ip**—The destination IP address of the packet
- **dest_port**—The destination port of the packet

Recommended Action If you need to keep the urgent flag in TCP headers, use the **urgent-flag allow** command in TCP map configuration mode.

Error Message `%FTD-7-419003: Cleared TCP urgent flag.`

Explanation This syslog is displayed when urgent flag or urgent pointer of tcp packet is cleared. This could be due to user configuration (tcp-map) or having some value for the urgent pointer in a tcp packet but the urgent flag is not set.

Recommended Action Verify if the tcp-map configurations whether the urget flag is set to clear.

419004

Error Message `%FTD-6-419004: TCP connection ID from src_ifc:src_ip/src_port (src_ip/src_port) to dst_ifc:dst_ip/dst_port (dst_ip/dst_port) is probed by DCD`

Explanation

A TCP connection was probed by Dead Connection Detection (DCD) to determine if connection was still valid.

Recommended Action None.

419005

Error Message `%FTD-6-419005: TCP connection ID from src_ifc:src_ip/src_port (src_ip/src_port) to dest_ifc:des_ip/des_port (des_ip/des_port) duration hh:mm:ss data bytes, is kept open by DCD as valid connection`

Explanation

A TCP connection was kept open by Dead Connection Detection (DCD) as a valid connection.

Recommended Action None.

419006

Error Message `%FTD-6-419006: Teardown TCP connection ID from src_ifc:src_ip/src_port (src_ip/src_port) to dst_ifc:dst_ip/dst_port (dst_ip/dst_port) duration hh:mm:ss data bytes, DCD probe was not responded from client/server interface ifc_name`

Explanation

A TCP connection was closed by Dead Connection Detection (DCD) as it is no longer required.

Recommended Action None.

421005

Error Message `%FTD-6-421005: interface_name:IP_address is counted as a user for application`

Explanation A host has been counted toward the license limit. The specified host was counted as a user of **application**. The total number of users in 24 hours is calculated at midnight for license validation.

- **interface_name**—The interface name
- **IP_address**—The IP address
- **application**—The CSC SSM

Recommended Action None required. However, if the overall count exceeds the user license that you have purchased, contact the Cisco TAC to upgrade your license.

421007

Error Message `%FTD-3-421007: TCP|UDP flow from interface_name :IP_address /port to interface_name :IP_address /port is skipped because application has failed.`

Explanation A flow was skipped because the service module application has failed. By default, this message is rate limited to 1 message every 10 seconds.

- **IP_address**—The IP address
- **port**—The port number
- **interface_name**—The name of the interface on which the policy is applied
- **application**—The CSC SSM

Recommended Action Determine the problem with the service module.

422004

Error Message `%FTD-4-422004: IP SLA Monitor number0: Duplicate event received. Event number number1`

Explanation The IP SLA monitor process has received a duplicate event. Currently, this message applies to destroy events. Only one destroy request will be applied. This is only a warning message.

- *number0* —The SLA operation number
- *number1* —The SLA operation event ID

Recommended Action If this recurs, enter the **show sla monitor configuration SLA_operation_id** command and copy the output of the command. Copy the message as it appears on the console or in the system log. Then contact the Cisco TAC and provide the representative with the information that you have, along with information about the application that is configuring and polling the SLA probes.

422005

Error Message `%FTD-4-422005: IP SLA Monitor Probe(s) could not be scheduled because clock is not set.`

Explanation One or more IP SLA monitor probes cannot be scheduled because the system clock was not set.

Recommended Action Make sure that the system clock is functional by using NTP or another mechanism.

422006

Error Message `%FTD-4-422006: IP SLA Monitor Probe number: string`

Explanation The IP SLA monitor probe cannot be scheduled. Either the configured starting time has already occurred or the starting time is invalid.

- *number* —The SLA operation ID
- *string* —A string describing the error

Recommended Action Reschedule the failed probe with a valid start time.

424001

Error Message `%FTD-4-424001: Packet denied: protocol_string. intf_in interface is in a backup state`

Explanation A packet was dropped because it was traversing the Secure Firewall Threat Defense device to or from a redundant interface. Interface functionality is limited on low-end platforms. The interface specified by the **backup interface** command can only be a backup for the primary interface configured. If the default route to the primary interface is up, any traffic through the Secure Firewall Threat Defense device from the backup interface will be denied. Conversely, if the default route to the primary interface is down, traffic through the Secure Firewall Threat Defense device from the primary interface will be denied.

- *protocol_string* —The protocol string; for example, TCP or protocol ID (a decimal number)
- *intf_in* —The input interface name
- *src_ip* —The source IP address of the packet
- *src_port* —The source port of the packet
- *intf_out* —The output interface name
- *dst_ip* —The destination IP address of the packet
- *dst_port* —The destination port of the packet
- *sg_info* —The security group name or tag for the specified IP address

Recommended Action Determine the source of the denied packet.

424002

Error Message `%FTD-4-424002: Connection to the backup interface is denied: protocol_string`

Explanation A connection was dropped because it is in a backup state. Interface functionality is limited on low-end platforms. The backup interface can only be a backup for the primary interface specified by the **backup interface** command. If the default route to the primary interface is up, any connection to the Secure Firewall Threat Defense device through the backup interface will be denied. Conversely, if the default route to the primary interface is down, connections to the Secure Firewall Threat Defense device through the primary interface will be denied.

- *protocol_string* —The protocol string; for example, TCP or protocol ID (a decimal number)
- *intf_in* —The input interface name
- *src_ip* —The source IP address of the packet
- *src_port* —The source port of the packet
- *intf_out* —The output interface name
- *dst_ip* —The destination IP address of the packet
- *dst_port* —The destination port of the packet

Recommended Action Determine the source of the denied packet.

425001

Error Message `%FTD-6-425001: Redundant interface redundant_interface_name created.`

Explanation The specified redundant interface was created in the configuration.

- *redundant_interface_name* —Redundant interface name

Recommended Action None required.

425002

Error Message `%FTD-6-425002: Redundant interface redundant_interface_name removed.`

Explanation The specified redundant interface was removed from the configuration.

- *redundant_interface_name* —Redundant interface name

Recommended Action None required.

425003

Error Message `%FTD-6-425003: Interface interface_name added into redundant interface redundant_interface_name`

Explanation The specified physical interface was added to the specified redundant interface as a member interface.

- *interface_name* —An interface name
- *redundant_interface_name* —Redundant interface name

Recommended Action None required.

425004

Error Message `%FTD-6-425004: Interface interface_name removed from redundant interface redundant_interface_name`

Explanation The specified redundant interface was removed from the specified redundant interface.

- *interface_name* —An interface name
- *redundant_interface_name* —Redundant interface name

Recommended Action None required.

425005

Error Message `%FTD-5-425005: Interface interface_name become active in redundant interface redundant_interface_name`

Explanation Within a redundant interface, one member interface is the active member. Traffic only passes through the active member interface. The specified physical interface became the active member of the specified redundant interface. Member interface switchover occurs when one of the following is true:

- The **redundant-interface interface-name active-member interface-name** command was executed.
- The active member interface is down, while the standby member interface is up.
- The standby member interface comes up (from down), while the active member interface remains down.

- *interface_name* —An interface name
- *redundant_interface_name* —Redundant interface name

Recommended Action Check the status of the member interfaces.

425006

Error Message `%FTD-3-425006: Redundant interface redundant_interface_name switch active member to interface_name failed`

Explanation An error occurred when member interface switchover was attempted.

- *redundant_interface_name* —Redundant interface name
- *interface_name* —An interface name

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

426001

Error Message `%FTD-6-426001: PORT-CHANNEL:Interface ifc_name bundled into EtherChannel interface num`

Explanation The **interface port-channel** *num* or the **channel-group** *num* **mode** *mode* command has been used on a nonexistent port channel.

- *ifc_name* —The EtherChannel interface name
- *num* —The port channel number

Recommended Action None required.

426002

Error Message `%FTD-6-426002: PORT-CHANNEL:Interface ifc_name unbundled from EtherChannel interface num`

Explanation The **no interface port-channel** *num* command has been used.

- *ifc_name* —The EtherChannel interface name
- *num*— The port channel number

Recommended Action None required.

426003

Error Message `%FTD-6-426003: PORT-CHANNEL:Interface ifc_name1 has become standby in EtherChannel interface num`

Explanation The **channel-group** *num* **mode** *mode* command has been used.

- *ifc_name1* —The EtherChannel interface name
- *num* —The port channel number

Recommended Action None required.

426004

Error Message 1 `%FTD-4-426004: PORT-CHANNEL:Interface ifc_name1 is not compatible with ifc_name and will be suspended (speed_of ifc_name1 is X_Mbps, Y is 1000_Mbps)`

Error Message 2 `%FTD-4-426004: Interface ifc_name1 is not compatible with ifc_name1 and will be suspended (ifc_name1 is Full-duplex, ifc_name1 is Half-duplex)`

Explanation The **channel-group** *num* **mode** *mode* command is executed on a physical interface and there is a speed or duplex mismatch of this physical interface with that of the port channel.

- *ifc_name* —The interface that is being added to the port channel
- *ifc_name1* —The interface that is already in the port channel and in a bundled state

Recommended Action Do one of the following:

- Change the speed of the physical interface to that of the port channel and execute the **channel-group** *num* **mode** *mode* command again.
- Leave the member interface in a suspended state. When the last active member is removed, then that member will try to reestablish LACP on the suspended member.

426101

Error Message `%FTD-6-426101: PORT-CHANNEL:Interface ifc_name is allowed to bundle into EtherChannel interface port-channel_id by CLACP.`

Explanation A port has been bundled in a span-cluster channel group.

Recommended Action None required.

426102

Error Message `%FTD-6-426102: PORT-CHANNEL:Interface ifc_name is moved to standby in EtherChannel interface port-channel_id by CLACP.`

Explanation A port has been moved to hot-standby state in a span-cluster channel group.

Recommended Action None required.

426103

Error Message `%FTD-6-426103: PORT-CHANNEL:Interface ifc_name is selected to move from standby to bundle in EtherChannel interface port-channel_id by CLACP.`

Explanation A standby port has been selected to move to bundled state in a span-cluster channel group.

Recommended Action None required.

426104

Error Message `%FTD-6-426104: PORT-CHANNEL:Interface ifc_name is unselected in EtherChannel interface port-channel_id by CLACP.`

Explanation A bundled port has been unbundled in a span-cluster channel group to obtain space for other ports to be bundled.

Recommended Action None required.

428002

Error Message `%FTD-6-428002: WAAS confirmed from in_interface :src_ip_addr/src_port to out_interface :dest_ip_addr/dest_port , inspection services bypassed on this connection.`

Explanation WAAS optimization was detected on a connection. All layer 7 inspection services, including IPS, are bypassed on WAAS-optimized connections.

Recommended Action No action is required if the network includes WAE devices; otherwise, the network administrator should investigate the use of the WAAS option on this connection.

429008

Error Message `%FTD-4-429008: Unable to respond to VPN query from CX for session 0x%x . Reason %s`

Explanation The CX sent a VPN session query to the Secure Firewall Threat Defense device, but it did not respond either because of an invalid session ID or another reason. Valid reasons can be any of the following:

- TLV length is invalid
- TLV memory allocation failed
- VPN session query message enqueue failed
- VPN session ID is invalid

Recommended Action None required.

430001

This message number was introduced in Release 6.3. It identifies an intrusion event.

For more information about this and other security event messages, see Security Event Syslog Messages.

430002

This message number was introduced in Release 6.3. It identifies a connection event logged at the beginning of the connection.

For more information about this and other security event messages, see Security Event Syslog Messages.

430003

This message number was introduced in Release 6.3. It identifies a connection event logged at the end of the connection.

For more information about this and other security event messages, see Security Event Syslog Messages.

430004

This message number was introduced in Release 6.4. It identifies a file event. See also 430005, on page 34 for file malware events.

For more information about this and other security event messages, see Security Event Syslog Messages.

430005

This message number was introduced in Release 6.4. It identifies a file malware event. See also 430004, on page 34 for file events.

For more information about this and other security event messages, see Security Event Syslog Messages.

431001

Message `%FTD-4-431001: HTTP event with fields: ts: timestamp, uid: connection_id, version: http_version, id.orig_h: source_ip_addr, id.orig_p: source_port, id.resp_h: destination_ip_address, id.resp_p: destination_port, pkt_num: packet_number, method: http_method_used, host: host, uri: uri_path, user_agent: user_agent, referrer: referrer, origin: origin_header, status_code: http_status_code, status_msg: http_status_message, trans_depth: requests_in_session, request_body_len: request_body_length, response_body_len: response_body_length, info_code: server_status_code, info_msg: server_status_message, proxied: proxy_headers, orig_filenames: uploaded_file_names, resp_filenames: downloaded_file_names, orig_mime_types: uploaded_file_types, resp_mime_types: downloaded_file_types`

Explanation This message records detailed HTTP request and response metadata for a connection, providing enhanced visibility into web traffic. Log records can be formatted as JSON, CSV, or TSV.

Recommended Action None.

431002

Message `%FTD-4-431002: FTP event with fields: ts: timestamp, uid: connection_id, id.orig_h: source_ip_addr, id.orig_p: source_port, id.resp_h: destination_ip_addr, id.resp_p: destination_port, pkt_num: packet_number, command: ftd_command, arg: command_argument, user: ftp_session_user_name, reply_code: reply_code, reply_msg: reply_message, file_size: file_size_in_bytes, data_channel.passive: passive_data_mode, data_channel.orig_h: data_channel_source_ip, data_channel.resp_h: data_channel_destination_ip, data_channel.resp_p: data_channel_destination_port`

Explanation This message logs FTP commands and responses within a session, including authentication attempts, file transfers, and directory operations. Log records can be formatted as JSON, CSV, or TSV.

Recommended Action None.

431003

Message `%FTD-4-431003: Connection event with fields: ts: timestamp, uid: unique_connection_id, id.orig_h: source_ip_addr, id.orig_p: source_port, id.resp_h: destination_ip_address, id.resp_p: destination_port, pkt_num: packet_number, proto: protocol,`

service: *service*, orig_pkts: *packets_sent*, resp_pkts: *packets_received*, duration: *duration*, orig_bytes: *bytes_sent*, resp_bytes: *bytes_received*, history: *connection_history*, conn_state: *connection_state*

Explanation This message logs connection-level details including source and destination IP addresses and ports, protocol, and connection duration. It serves as the foundational log for correlating protocol-specific events. Log records can be formatted as JSON, CSV, or TSV.

Recommended Action None.

431004

Message %FTD-4-431004: DNS event with fields: ts: *timestamp*, uid: *connection_id*, id.orig_h: *source_ip_addr*, id.orig_p: *source_port*, id.resp_h: *destination_ip_addr*, id.resp_p: *destination_port*, pkt_num: *packet_number*, proto: *protocol*, trans_id: *client_transaction_id*, query: *query_domain*, qclass: *query_class*, qclass_name: *query_class_name*, qtype: *query_type*, qtype_name: *query_class_name*, rcode: *response_code_value*, rcode_name: *response_code_name*, AA: *authoritative_answer_boolean*, TC: *truncated_message_boolean*, RD: *recursion_desired_boolean*, RA: *recursion_available_boolean*, Z: *reserved_bits*, answers: *response_answers*, TTLs: *ttls_for_each_answer*, rejected: *server_query*, auth: *authoritative_responses*, addl: *additional_responses*

Explanation This message records DNS queries and responses. It includes the queried domain, response code, and returned answers. It provides detailed DNS activity visibility. You can format log records as JSON, CSV, or TSV.

Recommended Action None.

431005

Message %FTD-4-431005: WEIRD event with fields: ts: *timestamp*, uid: *connection_id*, id.orig_h: *source_ip_addr*, id.orig_p: *source_port*, id.resp_h: *destination_ip_addr*, id.resp_p: *destination_port*, pkt_num: *packet_number*, sid: *snort_rule_id*, gid: *snort_inspector_id*, msg: *rule_message*, proto: *protocol*, source: *snort_inspector*

Explanation This message documents protocol anomalies detected by Snort inspectors. These anomalies indicate unusual or malformed network behavior. Log records can be formatted as JSON, CSV, or TSV.

Recommended Action None.

431006

Message %FTD-4-431006: NOTICE event with fields: ts: *timestamp*, uid: *connection_id*, id.orig_h: *source_ip_addr*, id.orig_p: *source_port*, id.resp_h: *destination_ip_addr*, id.resp_p: *destination_port*, pkt_num: *packet_number*, action: *action*, sid: *snort_rule_id*, gid: *snort_inspector_id*, rev: *snort_rule_revision*, msg: *rule_message*, refs: *references*, proto: *protocol*, source: *snort_inspector*

Explanation This message logs intrusion alerts triggered by IPS rules, including rule identifiers, messages, actions taken, and references. Log records can be formatted as JSON, CSV, or TSV.

Recommended Action None.

434001

Error Message `%FTD-4-434001: SFR card not up and fail-close mode used, dropping protocol packet from ingress:source/IP_address to source_port:egress_interface/destination_IP_address`

Explanation A packet has been dropped because of a fail-close configuration for the module. Your loss of connectivity for all the flows is caused by redirecting them to the module, because the fail-close configuration is designed to drop all the flows if the module is down.

Recommended Action Try to understand the reason for failure and restore services. Alternatively, you can use the fail-open option even if the card does not recover immediately. Note that in the fail-open configuration, all packets to the module are bypassed if the card status is down.

434004

Error Message `%FTD-5-434004: SFR requested device to bypass further packet redirection and process protocol flow from inside_ifc_name:src_ip/src_port to outside_ifc_name:dst_ip/dst_port locally`

Explanation SourceFire (SFR) has determined not to inspect more traffic of a flow and requests the Secure Firewall Threat Defense device to stop redirecting the flow of traffic to SFR.

Recommended Action None Required.

446003

Error Message `%FTD-4-446003: Denied TLS Proxy session from src_int :src_ip /src_port to dst_int :dst_ip /dst_port , UC-IME license is disabled.`

Explanation The UC-IME license is either on or off. Once enabled, UC-IME can use any number of available TLS sessions, according to the Secure Firewall Threat Defense limit and the K8 export limit.

- *src_int* —The source interface name (inside or outside)
- *src_ip* —The source IP address
- *src_port* —The source port
- *dst_int* —The destination interface name (inside or outside)
- *dst_ip* —The destination IP address
- *dst_port* —The destination port

Recommended Action Check to see if UC-IME is disabled. If so, activate it.

447001

Error Message `%FTD-4-447001: ASP DP to CP queue_name was full. Queue length length, limit limit`

Explanation This message indicates a particular data path (DP) to control point (CP) event queue is full, and one or more multiple enqueue actions have failed. If the event contains a packet block, such as for CP application inspection, the packet will be dropped by the DP, and a counter from the **show asp drop** command will increment. If the event is for punt to CP, a typical counter is the Punt no memory ASP-drop counter.

- *queue* —The name of the DP-CP event queue.
- *length* —The current number of events on the queue.

- *limit* —The maximum number of events that are allowed on the queue.

Recommended Action The queue-full condition reflects the fact that the load on the CP has exceeded the CP processing ability, which may or may not be a temporary condition. You should consider reducing the feature load on the CP if this message appears repeatedly. Use the **show asp event dp-cp** command to identify the features that contribute the most load on the event queue.

448001

Error Message `%FTD-4-448001: Denied SRTP crypto session setup on flow from src_int:src_ip/src_port to dst_int:dst_ip/dst_port, licensed K8 SRTP crypto session limit of limit exceeded`

Explanation For a K8 platform, the limit of 250 SRTP crypto sessions is enforced. Each pair of SRTP encrypt or decrypt sessions is counted as one SRTP crypto session. A call is counted toward this limit only when encryption or decryption is required for a medium, which means that if the pass-through is set for the call, even if both legs use SRTP, they are not counted toward this limit.

- *src_int* —The source interface name (inside or outside)
- *src_ip* —The source IP address
- *src_port* —The source port
- *dst_int* —The destination interface name (inside or outside)
- *dst_ip* —The destination IP address
- *dst_port* —The destination port
- *limit* —The K8 limit of SRTP crypto sessions (250)

Recommended Action None required. You can set up new SRTP crypto sessions only when existing SRTP crypto sessions have been released.

450002

Error Message `%FTD-4-450002: Teardown string connection connection for interface:address/port to interface:address/port duration hh:mm:ss bytes bytes reason reason_string`

Explanation Drop due to vPath license failure.

Recommended Action None required.