CHAPTER 45

show asp cluster counter through show asp table vpn-context Commands

show asp cluster counter

To debug global or context-specific information in a clustering environment, use the **show asp cluster counter** command in privileged EXEC mode.

show asp cluster counter

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

The **show asp cluster counter** command shows the global and context-specific DP counters, which might help you troubleshoot a problem. This information is used for debugging purposes only, and the information output is subject to change. Consult the Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp cluster counter** command:

```
hostname# show asp cluster counter

Global dp-counters:


Context specific dp-counters:

MCAST_FP_TO_SP                  361136
MCAST_SP_TOTAL                  361136
MCAST_SP_PKTS                   143327
MCAST_SP_PKTS_TO_CP             143327
MCAST_FP_CHK_FAIL_NO_HANDLE     217809
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC 81192
MCAST_FP_CHK_FAIL_NO_FP_FWD     62135
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show asp drop

To debug the accelerated security path dropped packets or connections, use the **show asp drop** command in privileged EXEC mode.

show asp drop [**flow** [*flow_drop_reason*] | **frame** [*frame_drop_reason*]]

Syntax Description

flow [*flow_drop_reason*]	(Optional) Shows the dropped flows (connections). You can specify a particular reason by using the *flow_drop_reason* argument. Valid values for the *flow_drop_reason* argument are listed in the "Usage Guidelines" section.
frame [*frame_drop_reason*]	(Optional) Shows the dropped packets. You can specify a particular reason by using the *frame_drop_reason* argument. Valid values for the *frame_drop_reason* argument are listed in the "Usage Guidelines" section.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
7.0(8)/7.2(4)/8.0(4)	Output includes a timestamp indicating when the counters were last cleared (see the **clear asp drop** command). It also displays the drop reason keywords next to the description, so you can easily use the **capture asp-drop** command with the associated keyword.

Usage Guidelines

The **show asp drop** command shows the packets or connections dropped by the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. This information is used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

The following sections include each drop reason name and description, including recommendations:

- Frame Drop Reasons, page 45-5
- Flow Drop Reasons, page 45-60

Frame Drop Reasons

```
------------------------------------------------------------------
Name: natt-keepalive
NAT-T keepalive message:
    This counter will increment when the appliance receives an IPSec NAT-T keepalive
message.  NAT-T keepalive messages are sent from the IPSec peer to the appliance to keep
NAT/PAT flow information current in network devices between the NAT-T IPSec peer and the
appliance.

 Recommendation:
    If you have configured IPSec NAT-T on your appliance, this indication is normal and
doesn't indicate a problem.  If NAT-T is not configured on your appliance, analyze your
network traffic to determine the source of the NAT-T traffic.

 Syslogs:
    None


------------------------------------------------------------------
Name: ipsecudp-keepalive
IPSEC/UDP keepalive message:
    This counter will increment when the appliance receives an IPSec over UDP keepalive
message. IPSec over UDP keepalive messages are sent from the IPSec peer to the appliance
to keep NAT/PAT flow information current in network devices between the IPSec over UDP
peer and the appliance. Note - These are not industry standard NAT-T keepalive messages
which are also carried over UDP and addressed to UDP port 4500.
 Recommendation:
    If you have configured IPSec over UDP on your appliance, this indication is normal and
doesn't indicate a problem.  If IPSec over UDP is not configured on your appliance,
analyze your network traffic to determine the source of the IPSec over UDP traffic.

 Syslogs:
    None


------------------------------------------------------------------
Name: bad-ipsec-prot
IPSec not AH or ESP:
    This counter will increment when the appliance receives a packet on an IPSec
connection which is not an AH or ESP protocol. This is not a normal condition.

 Recommendation:
    If you are receiving many IPSec not AH or ESP indications on your appliance, analyze
your network traffic to determine the source of the traffic.

 Syslogs:
    402115


------------------------------------------------------------------
Name: ipsec-ipv6
IPSec via IPV6:
    This counter will increment when the appliance receives an IPSec ESP packet, IPSec
NAT-T ESP packet or an IPSec over UDP ESP packet encapsulated in an IP version 6 header.
The appliance does not currently support any IPSec sessions encapsulated in IP version 6.

 Recommendation:
    None

 Syslogs:
    None
```

```
------------------------------------------------------------------
Name: bad-ipsec-natt
BAD IPSec NATT packet:
    This counter will increment when the appliance receives a packet on an IPSec
connection which has negotiated NAT-T but the packet is not addressed to the NAT-T UDP
destination port of 4500 or had an invalid payload length.

 Recommendation:
    Analyze your network traffic to determine the source of the NAT-T traffic.

 Syslogs:
    None


------------------------------------------------------------------
Name: bad-ipsec-udp
BAD IPSec UDP packet:
    This counter will increment when the appliance receives a packet on an IPSec
connection which has negotiated IPSec over UDP but the packet has an invalid payload
length.

 Recommendation:
    Analyze your network traffic to determine the source of the NAT-T traffic.

 Syslogs:
    None


------------------------------------------------------------------
Name: inspect-srtp-encrypt-failed
Inspect SRTP Encryption failed:
    This counter will increment when SRTP encryption fails.

Recommendation:
    If error persists even after a reboot please call TAC to see why SRTP encryption is
failing in the hardware crypto accelerator.

Syslogs:
    337001.


------------------------------------------------------------------
Name: inspect-srtp-decrypt-failed
Inspect SRTP Decryption failed:
    This counter will increment when SRTP decryption fails.

Recommendation:
    If error persists even after a reboot please call TAC to see why SRTP decryption is
failing in the hardware crypto accelerator.

Syslogs:
    337002.


------------------------------------------------------------------
Name: inspect-srtp-validate-authtag-failed
Inspect SRTP Authentication tag validation failed:
    This counter will increment when SRTP authentication tag validation fails.

Recommendation:
    No action is required. If error persists SRTP packets arriving at the firewall are
being tampered with and the administrator has to identify the cause.

Syslogs:
```

```
    337003.


----------------------------------------------------------------
Name: inspect-srtp-generate-authtag-failed
Inspect SRTP Authentication tag generation failed:
    This counter will increment when SRTP authentication tag generation fails.

Recommendation:
    No action is required.

Syslogs:
    337004.


----------------------------------------------------------------
Name: inspect-srtp-no-output-flow
Inspect SRTP failed to find output flow:
    This counter will increment when the flow from the Phone proxy could not be created or
if the flow has been torn down

Recommendation:
    No action is required. The flow creation could have failed because of low memory
conditions.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-setup-srtp-failed
Inspect SRTP setup in CTM failed:
    This counter will increment when SRTP setup in the CTM fails.

Recommendation:
    No action is required. If error persists call TAC to see why the CTM calls are
failing.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-one-part-no-key
Inspect SRTP failed to find keys for both parties:
    This counter will increment when Inspect SRTP finds only one party's keys populated in
the media session.

Recommendation:
    No action is required. This counter could increment in the beginning phase of the call
but eventually when the call signaling exchange completes both parties should know their
respective keys.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-no-media-session
Inspect SRTP Media session lookup failed:
    This counter will increment when SRTP media session lookup fails.

Recommendation:
```

```
    No action is required. The media session is created by Inspect SIP or Skinny when the
IP address is parsed as part of the signaling exchange. Debug the signaling messages to
figure out the cause.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-no-remote-phone-proxy-ip
Inspect SRTP Remote Phone Proxy IP not populated:
    This counter will increment when remote phone proxy IP is not populated

Recommendation:
    No action is required. The remote phone proxy IP address is populated from the
signaling exchange. If error persists debug the signaling messages to figure out if ASA is
seeing all the signaling messages.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-srtp-client-port-not-present
Inspect SRTP client port wildcarded in media session:
    This counter will increment when client port is not populated in media session

Recommendation:
    No action is required. The client port is populated dynamically when the media stream
comes in from the client. Capture the media packets to see if the client is sending media
packets.

Syslogs:
    None.


----------------------------------------------------------------
Name: ipsec-need-sa
IPSec SA not negotiated yet:
    This counter will increment when the appliance receives a packet which requires
encryption but has no established IPSec security association. This is generally a normal
condition for LAN-to-LAN IPSec configurations. This indication will cause the appliance to
begin ISAKMP negotiations with the destination peer.

 Recommendation:
    If you have configured IPSec LAN-to-LAN on your appliance, this indication is normal
and doesn't indicate a problem.  However, if this counter increments rapidly it may
indicate a crypto configuration error or network error preventing the ISAKMP negotiation
from completing. Verify that you can communicate with the destination peer and verify your
crypto configuration via the 'show running-config' command.

 Syslogs:
    None


----------------------------------------------------------------
Name: ipsec-spoof
IPSec spoof detected:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not. The packet matched the inner header security policy check of a
configured and established IPSec connection on the appliance but was received unencrypted.
This is a security issue.

 Recommendation:
```

```
    Analyze your network traffic to determine the source of the spoofed IPSec traffic.

 Syslogs:
    402117


----------------------------------------------------------------
Name: ipsec-clearpkt-notun
IPSec Clear Pkt w/no tunnel:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not.  The packet matched the inner header security policy check of
a configured and established IPSec connection on the appliance but was received
unencrypted. This is a security issue.

 Recommendation:
    Analyze your network traffic to determine the source of the spoofed IPSec traffic.

 Syslogs:
    402117


----------------------------------------------------------------
Name: ipsec-tun-down
IPSec tunnel is down:
    This counter will increment when the appliance receives a packet associated with an
IPSec connection which is in the process of being deleted.

 Recommendation:
    This is a normal condition when the IPSec tunnel is torn down for any reason.

 Syslogs:
    None


----------------------------------------------------------------
Name: mp-svc-delete-in-progress
SVC Module received data while connection was being deleted:
    This counter will increment when the security appliance receives a packet associated
with an SVC connection that is in the process of being deleted.

Recommendation:
    This is a normal condition when the SVC connection is torn down for any reason. If
this error occurs repeatedly or in large numbers, it could indicate that clients are
having network connectivity issues.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-svc-bad-framing
SVC Module received badly framed data:
    This counter will increment when the security appliance receives a packet from an SVC
or the control software that it is unable to decode.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
    722037 (Only for SVC received data).


----------------------------------------------------------------
```

```
Name: mp-svc-bad-length
SVC Module received bad data length:
    This counter will increment when the security appliance receives a packet from an SVC
or the control software where the calculated and specified lengths do not match.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
    722037 (Only for SVC received data).


----------------------------------------------------------------
Name: mp-svc-unknown-type
SVC Module received unknown data frame:
    This counter will increment when the security appliance receives a packet from an SVC
where the data type is unknown.

Recommendation:
    Validate that the SVC being used by the client is compatible with the version of
security appliance software.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-addr-renew-response
SVC Module received address renew response data frame:
    This counter will increment when the security appliance receives an Address Renew
Response message from an SVC. The SVC should not be sending this message.

Recommendation:
    This indicates that an SVC software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-prepend
SVC Module does not have enough space to insert header:
    This counter will increment when there is not enough space before the packet data to
prepend a MAC header in order to put the packet onto the network.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-channel
SVC Module does not have a channel for reinjection:
    This counter will increment when the interface that the encrypted data was received
upon cannot be found in order to inject the decrypted data.

Recommendation:
    If an interface is shut down during a connection, this could happen; re-enable/check
the interface. Otherwise, this indicates that a software error should be reported to the
Cisco TAC.
```

```
Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-session
SVC Module does not have a session:
    This counter will increment when the security appliance cannot determine the SVC
session that this data should be transmitted over.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-session-lock-failure
SVC Module failed to acquire the session lock:
    This counter will increment when the security appliance cannot grab the lock for the
SVC session that this data should be transmitted over.

Recommendation:
    This condition should never be encountered during normal operation and     may
indicate a software problem with the appliance.  Contact the Cisco     Technical
Assistance Center (TAC) if this error occurs.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-svc-decompres-error
SVC Module decompression error:
    This counter will increment when the security appliance encounters an error during
decompression of data from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
   722037.


----------------------------------------------------------------
Name: mp-svc-compress-error
SVC Module compression error:
    This counter will increment when the security appliance encounters an error during
compression of data to an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC. The SVC or
security appliance could be at fault.

Syslogs:
   722037.


----------------------------------------------------------------
Name: mp-svc-no-mac
SVC Module unable to find L2 data for frame:
```

```
    This counter will increment when the security appliance is unable to find an L2 MAC
header for data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-invalid-mac
SVC Module found invalid L2 data in the frame:
    This counter will increment when the security appliance is finds an invalid L2 MAC
header attached to data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-invalid-mac-len
SVC Module found invalid L2 data length in the frame:
    This counter will increment when the security appliance is finds an invalid L2 MAC
length attached to data received from an SVC.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-flow-control
SVC Session is in flow control:
    This counter will increment when the security appliance needs to drop data because an
SVC is temporarily not accepting any more data.

Recommendation:
    This indicates that the client is unable to accept more data. The client should reduce
the amount of traffic it is attempting to receive.

Syslogs:
   None.


----------------------------------------------------------------
Name: mp-svc-no-fragment
SVC Module unable to fragment packet:
    This counter is incremented when a packet to be sent to the SVC is not permitted to be
fragmented or when there are not enough data buffers to fragment the packet.

Recommendation:
    Increase the MTU of the SVC to reduce fragmentation. Avoid using applications that do
not permit fragmentation. Decrease the load on the device to increase available data
buffers.

Syslogs:
    None.
```

```
------------------------------------------------------------------
Name: vpn-handle-error
VPN Handle Error:
    This counter is incremented when the appliances is unable to create a VPN handle
because the VPN handle already exists.

 Recommendation:
    It is possible to see this counter increment as part of normal operation However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

 Syslogs:
    None.


------------------------------------------------------------------
Name: ipsec-lock-error
IPSec locking error:
    This counter is incremented when an IPSec operation is attempted but fails due to an
internal locking error.

Recommendation:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance. Contact the Cisco Technical Assistance Center (TAC)
if this error occurs.

Syslogs:
    None.


------------------------------------------------------------------
Name: vpn-handle-mismatch
VPN Handle Mismatch:
    This counter is incremented when the appliance wants to forward a block and the flow
referred to by the VPN Handle is different than the flow associated with the block.

 Recommendation:
    This is not a normal occurrence. Please perform a "show console-output" and forward
that output to CISCO TAC for further analysis.

 Syslogs:
    None.


------------------------------------------------------------------
Name: vpn-reclassify-failed
VPN Reclassify Failed:
    This counter is incremented when a packet for a VPN flow is dropped due to the flow
failing to be reclassified after a VPN state change.

 Recommendation:
    This counter is incremented when a packet for a VPN flow arrives that requires
reclassification due to VPN CLI or Tunnel state changes. If the flow no longer matches the
existing policies, then the flow is freed and the packet dropped.

 Syslogs:
    No new syslogs accompany this event.


------------------------------------------------------------------
Name: punt-rate-limit
Punt rate limit exceeded:
```

```
    This counter will increment when the appliance attempts to forward a layer-2 packet to
a rate-limited control point service routine and the rate limit (per/second) is now being
exceeded. Currently, the only layer-2 packets destined for a control point service routine
which are rate limited are ARP packets. The ARP packet rate limit is 500 ARPs per second
per interface.

Recommendation:
    Analyze your network traffic to determine the reason behind the high rate of ARP
packets.

 Syslogs:
    322002, 322003


----------------------------------------------------------------
Name: punt-no-mem
Punt no memory:
    This counter is incremented and the packet is dropped when there is no memory to
create data structure for punting a packet to Control Point.

Recommendation:
    No action needs to be taken if this condition is transient. If this condition persists
due to low memory, then system upgrade might be necessary.

Syslogs:
    None


----------------------------------------------------------------
Name: punt-queue-limit
Punt queue limit exceeded:
    This counter is incremented and the packet is dropped when punt queue limit is
exceeded, an indication that a bottle-neck is forming at Control Point.

Recommendation:
    No action needs to be taken.  This is a design limitation.

Syslogs:
    None


----------------------------------------------------------------
Name: flow-being-freed
Flow is being freed:
    This counter is incremented when the flow is being freed and all packets queued for
inspection are dropped.

Recommendation:
    No action needs to be taken.

Syslogs:
    None


----------------------------------------------------------------
Name: invalid-encap
Invalid Encapsulation:
    This counter is incremented when the security appliance receives a frame belonging to
an unsupported link-level protocol or if the L3type specified in the frame is not
supported by the appliance. The packet is dropped.

Recommendation:
    Verify that directly connected hosts have proper link-level protocol settings.
```

```
Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-ip-header
Invalid IP header:
    This counter is incremented and the packet is dropped when the appliance receives an
IP packet whose computed checksum of the IP header does not match the recorded checksum in
the header.

Recommendation:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a peer is sending corrupted packets and an attack is in progress. Please use the
packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: unsupported-ip-version
Unsupported IP version:
    This counter is incremented when the security appliance receives an IP packet that has
an unsupported version in version field of IP header. Specifically, if the packet does not
belong to version 4 or version 6. The packet is dropped.

Recommendation:
    Verify that other devices on connected network are configured to send IP packets
belonging to versions 4 or 6 only.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-ip-length
Invalid IP Length:
    This counter is incremented when the security appliance receives an IPv4 or IPv6
packet in which the header length or total length fields in IP header are not valid or do
not conform to the received packet length.

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-ethertype
Invalid Ethertype:
    This counter is incremented when the fragmentation module on the security appliance
receives or tries to send a fragmented packet that does not belong IP version 4 or version
6. The packet is dropped.

Recommendation:
    Verify mtu of device and other devices on connected network to determine why the
device is processing such fragments.

Syslogs:
    None.
```

```
------------------------------------------------------------------
Name: invalid-tcp-hdr-length
Invalid TCP Length:
    This counter is incremented when the security appliance receives a TCP packet whose
size is smaller than minimum-allowed header length or does not conform to the received
packet length.

Recommendation:
    The invalid packet could be a bogus packet being sent by an attacker.
Investigate the traffic from source in the following syslog.

Syslogs:
    500003.


------------------------------------------------------------------
Name: invalid-udp-length
Invalid UDP Length:
    This counter is incremented when the security appliance receives a UDP packet whose
size as calculated from the fields in header is different from the measured size of packet
as received from the network.

Recommendation:
    The invalid packet could be a bogus packet being sent by an attacker.

Syslogs:
    None.


------------------------------------------------------------------
Name: no-adjacency
No valid adjacency:
    This counter is incremented when the security appliance has tried to obtian an
adjacency and could not obtain mac-address for next hop. The packet is dropped.

Recommendation:
    Configure a capture for this drop reason and check if a host with specified
destination address exists on connected network or is routable from the device.

Syslogs:
   None.


------------------------------------------------------------------
Name: unexpected-packet
Unexpected packet:
    This counter is incremented when the appliance in transparent mode receives a non-IP
packet, destined to its MAC address, but there is no corresponding service running on the
appliance to process the packet.

Recommendation:
    Verify if the appliance is under attack. If there are no suspicious packets, or the
device is not in transparent mode, this counter is most likely being incremented due to a
software error. Attempt to capture the traffic that is causing the counter to increment
and contact the Cisco TAC.

Syslogs:
    None


------------------------------------------------------------------
Name: no-route
No route to host:
```

```
    This counter is incremented when the security appliance tries to send a packet out of
an interface and does not find a route for it in routing table.

Recommendation:
    Verify that a route exists for the destination address obtained from the generated
syslog.

Syslogs:
   110002, 110003.


----------------------------------------------------------------
Name: rpf-violated
Reverse-path verify failed:
    This counter is incremented when ip-verify is configured on an interface and the
security appliance receives a packet for which the route lookup of source-ip did not yield
the same interface as the one on which the packet was received.

Recommendation:
    Trace the source of traffic based on source-ip printed in syslog below and investigate
why it is sending spoofed traffic.

Syslogs:
    106021.


----------------------------------------------------------------
Name: acl-drop
Flow is denied by configured rule:
    This counter is incremented when a drop rule is hit by the packet and gets dropped.
This rule could be a default rule created when the box comes up, when various features are
turned on or off, when an acl is applied to interface or any other feature etc. Apart from
default rule drops, a packet could be dropped because of:
     1) ACL configured on an interface
     2) ACL configured for AAA and AAA denied the user
     3) Thru-box traffic arriving at management-only ifc
     4) Unencrypted traffic arriving on a ipsec-enabled interface

Recommendation:
    Note if one of ACLs listed below are fired.

Syslogs:
    106023, 106100, 106004


----------------------------------------------------------------
Name: unable-to-create-flow
Flow denied due to resource limitation:
    This counter is incremented and the packet is dropped when flow creation fails due to
a system resource limitation.  The resource limit may be either:
       1) system memory
       2) packet block extension memory
       3) system connection limit
    Causes 1 and 2 will occur simultaneously with flow drop reason "No memory to complete
flow".

Recommendation:
    - Observe if free system memory is low.
    - Observe if flow drop reason "No memory to complete flow" occurs.
    - Observe if connection count reaches the system connection limit with the command
"show resource usage".

Syslogs:
    None
```

```
----------------------------------------------------------------
Name: unable-to-add-flow
Flow hash full:
    This counter is incremented when a newly created flow is inserted into flow hash table
and the insertion failed because the hash table was full. The flow and the packet are
dropped. This is different from counter that gets incremented when maximum connection
limit is reached.

Recommendation:
    This message signifies lack of resources on the device to support an operation that
should have been successful. Please check if the connections in the 'show conn' output
have exceeded their configured idle timeout values. If so, contact the Cisco Technical
Assistance Center (TAC).

Syslogs:
    None.


----------------------------------------------------------------
Name: np-sp-invalid-spi
Invalid SPI:
    This counter will increment when the appliance receives an IPSec ESP packet addressed
to the appliance which specifies a SPI (security parameter index) not currently known by
the appliance.

 Recommendation:
    Occasional invalid SPI indications are common, especially during rekey processing.
Many invalid SPI indications may suggest a problem or DoS attack. If you are experiencing
a high rate of invalid SPI indications, analyze your network traffic to determine the
source of the ESP traffic.

 Syslogs:
    402114


----------------------------------------------------------------
Name: unsupport-ipv6-hdr
Unsupported IPv6 header:
    This counter is incremented and the packet is dropped if an IPv6 packet is received
with an unsupported IPv6 extension header. The supported IPv6 extension headers are: TCP,
UDP, ICMPv6, ESP, AH, Hop Options, Destination Options, and Fragment. The IPv6 routing
extension header is not supported, and any extension header not listed above is not
supported.  IPv6 ESP and AH headers are supported only if the packet is through-the-box.
To-the-box IPv6 ESP and AH packets are not supported and will be dropped.

Recommendation:
    This error may be due to a misconfigured host. If this error occurs repeatedly or in
large numbers, it could also indicate spurious or malicious activity such as an attempted
DoS attack.

Syslogs:
    None.


----------------------------------------------------------------
Name: tcp-not-syn
First TCP packet not SYN:
    Received a non SYN packet as the first packet of a non intercepted and non nailed
connection.

Recommendation:
```

```
    Under normal conditions, this may be seen when the appliance has already closed a
connection, and the client or server still believe the connection is open, and continue to
transmit data.  Some examples where this may occur is just after a 'clear local-host' or
'clear xlate' is issued. Also, if connections have not been recently removed, and the
counter is incrementing rapidly, the appliance may be under attack. Capture a sniffer
trace to help isolate the cause.

Syslogs:
    6106015


----------------------------------------------------------------
Name: bad-tcp-cksum
Bad TCP checksum:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet whose computed TCP checksum does not match the recorded checksum in TCP header.

Recommendation:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet. To allow
packets with incorrect TCP checksum disable checksum-verification feature under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: bad-tcp-flags
Bad TCP flags:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with invalid TCP flags in TCP header. Example a packet with SYN and FIN TCP
flags set will be dropped.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-reserved-set
TCP reserved flags set:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with reserved flags set in TCP header.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet. To allow such
TCP packets or clear reserved flags and then pass the packet use reserved-bits
configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-bad-option-list
TCP option list invalid:
```

```
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with a non-standard TCP header option.

Recommendations:
    To allow such TCP packets or clear non-standard TCP header options and then allow the
packet, use tcp-options configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-mss-exceeded
TCP data exceeded MSS:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with data length greater than the MSS advertized by peer TCP endpoint.

Recommendations:
    To allow such TCP packets use exceed-mss configuration under tcp-map

Syslogs:
    4419001


----------------------------------------------------------------
Name: tcp-synack-data
TCP SYNACK with data:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP SYN-ACK packet with data.

Recommendations:
    The packet corruption may be caused by a bad cable or noise on the line. It may also
be that a TCP endpoint is sending corrupted packets and an attack is in progress. Please
use the packet capture feature to learn more about the origin of the packet.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-syn-data
TCP SYN with data:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP SYN packet with data.

Recommendations:
    To allow such TCP packets use syn-data configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-dual-open
TCP Dual open denied:
    This counter is incremented and the packet is dropped when the appliance recevies a
TCP SYN packet from the server, when an embryonic TCP connection is already open.

Recommendations:
    None

Syslogs:
    None
```

```
------------------------------------------------------------------
Name: tcp-data-past-fin
TCP data send after FIN:
    This counter is incremented and the packet is dropped when the appliance recevies new
TCP data packet from an endpoint which had sent a FIN to close the connection.

Recommendations:
    None

Syslogs:
    None


------------------------------------------------------------------
Name: tcp-3whs-failed
TCP failed 3 way handshake:
    This counter is incremented and the packet is dropped when appliance receives an
invalid TCP packet during three-way-handshake. Example SYN-ACK from client will be dropped
for this reason.

Recommendations:
    None

Syslogs:
    None


------------------------------------------------------------------
Name: tcp-rstfin-ooo
TCP RST/FIN out of order:
    This counter is incremented and the packet is dropped when appliance receives a RST or
a FIN packet with incorrect TCP sequence number.

Recommendations:
    None

Syslogs:
    None


------------------------------------------------------------------
Name: tcp-seq-syn-diff
TCP SEQ in SYN/SYNACK invalid:
    This counter is incremented and the packet is dropped when appliance receives a SYN or
SYN-ACK packet during three-way-handshake with incorrect TCP sequence number.

Recommendations:
    None

Syslogs:
    None


------------------------------------------------------------------
Name: tcp-ack-syn-diff
TCP ACK in SYNACK invalid:
    This counter is incremented and the packet is dropped when appliance receives a
SYN-ACK packet during three-way-handshake with incorrect TCP acknowledgement number.

Recommendations:
    None

Syslogs:
```

```
    None


-------------------------------------------------------------------
Name: tcp-syn-ooo
TCP SYN on established conn:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN packet on an established TCP connection.

Recommendations:
    None

Syslogs:
    None


-------------------------------------------------------------------
Name: tcp-synack-ooo
TCP SYNACK on established conn:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN-ACK packet on an established TCP connection.

Recommendations:
    None

Syslogs:
    None


-------------------------------------------------------------------
Name: tcp-seq-past-win
TCP packet SEQ past window:
    This counter is incremented and the packet is dropped when appliance receives a TCP
data packet with sequence number beyond the window allowed by the peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


-------------------------------------------------------------------
Name: tcp-invalid-ack
TCP invalid ACK:
    This counter is incremented and the packet is dropped when appliance receives a TCP
packet with acknowledgement number greater than data sent by peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


-------------------------------------------------------------------
Name: tcp-fo-drop
TCP replicated flow pak drop:
    This counter is incremented and the packet is dropped when appliance receives a TCP
packet with control flag like SYN, FIN or RST on an established connection just after the
appliance has taken over as active unit.

Recommendations:
    None
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: tcp-discarded-ooo
TCP ACK in 3 way handshake invalid:
    This counter is incremented and the packet is dropped when appliance receives a TCP
ACK packet from client during three-way-handshake and the sequence number is not next
expected sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-buffer-full
TCP Out-of-Order packet buffer full:
    This counter is incremented and the packet is dropped when appliance receives an
out-of-order TCP packet on a connection and there is no buffer space to store this packet.
Typically TCP packets are put into order on connections that are inspected by the
appliance or when packets are sent to SSM for inspection. There is a default queue size
and when packets in excess of this default queue size are received they will be dropped.

Recommendations:
    On ASA platforms the queue size could be increased using queue-limit configuration
under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-global-buffer-full
TCP global Out-of-Order packet buffer full:
    This counter is incremented and the packet is dropped when the security appliance
receives an out-of-order TCP packet on a connection and there are no more global buffers
available. Typically TCP packets are put into order on connections that are inspected by
the security appliance or when packets are sent to the SSM for inspection. When the global
Out-of-Order buffer queue is full, the packet will be dropped and this counter will
increment.

Recommendations:
    This is a temporary condition when all global buffers are used. If this counter is
constantly incrementing, then please check your network for large amounts of Out-of-Order
traffic, which could be caused by traffic of the same flow taking different routes through
the network.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-buffer-timeout
TCP Out-of-Order packet buffer timeout:
    This counter is incremented and the packet is dropped when a queued out of order TCP
packet has been held in the buffer for too long.Typically, TCP packets are put into order
on connections that are inspected by the security appliance or when packets are sent to
the SSM for inspection. When the next expected TCP packet does not arrive within a certain
period, the queued out of order packet is dropped.
```

```
Recommendations:
    The next expected TCP packet may not arrive due to congestion in the network which is
normal in a busy network. The TCP retransmission mechanism in the end host will retransmit
the packet and the session will continue.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-rst-syn-in-win
TCP RST/SYN in window:
    This counter is incremented and the packet is dropped when appliance receives a TCP
SYN or TCP RST packet on an established connection with sequence number within window but
not next expected sequence number.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-acked
TCP DUP and has been ACKed:
    This counter is incremented and the packet is dropped when appliance receives a
retransmitted data packet and the data has been acknowledged by the peer TCP endpoint.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-dup-in-queue
TCP dup of packet in Out-of-Order queue:
    This counter is incremented and the packet is dropped when appliance receives a
retransmitted data packet that is already in our out of order packet queue.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-paws-fail
TCP packet failed PAWS test:
    This counter is incremented and the packet is dropped when TCP packet with timestamp
header option fails the PAWS (Protect Against Wrapped Sequences) test.

Recommendations:
    To allow such connections to proceed, use tcp-options configuration under tcp-map to
clear timestamp option.

Syslogs:
    None
```

```
------------------------------------------------------------------
Name: tcp-conn-limit
TCP connection limit reached:
    This reason is given for dropping a TCP packet during TCP connection establishment
phase when the connection limit has been exceeded. The connection limit is configured via
the 'set connection conn-max' action command.

Recommendation:
    If this is incrementing rapidly, check the syslogs to determine which host's
connection limit is reached. The connection limit may need to be increased if the traffic
is normal, or the host may be under attack.

Syslogs:
    201011


------------------------------------------------------------------
Name: conn-limit
Connection limit reached:
    This reason is given for dropping a packet when the connection limit or host
connection limit has been exceeded. If this is a TCP packet which is dropped during TCP
connection establishment phase due to connection limit, the drop reason 'TCP connection
limit reached' is also reported.

Recommendation:
    If this is incrementing rapidly, check the syslogs to determine which host's
connection limit is reached. The connection limit may need to be increased if the traffic
is normal, or the host may be under attack.

Syslogs:
    201011


------------------------------------------------------------------
Name: tcp_xmit_partial
TCP retransmission partial:
    This counter is incremented and the packet is dropped when check-retranmission feature
is enabled and a partial TCP retransmission was received.

Recommendations:
    None

Syslogs:
    None


------------------------------------------------------------------
Name: tcpnorm-rexmit-bad
TCP bad retransmission:
    This counter is incremented and the packet is dropped when check-retranmission feature
is enabled and a TCP retranmission with different data from the original packet was
received.

Recommendations:
    None

Syslogs:
    None


------------------------------------------------------------------
Name: tcpnorm-win-variation
TCP unexpected window size variation:
```

```
    This counter is incremented and the packet is dropped when window size advertized by
TCP endpoint is drastically changed without accepting that much data.

Recommendations:
    In order to allow such packet, use the window-variation configuration under tcp-map.

Syslogs:
    None


----------------------------------------------------------------
Name: rate-exceeded
QoS rate exceeded:
    This counter is incremented when rate-limiting (policing) is configured on an
egress/ingress interface and the egress/ingress traffic rate exceeds the burst rate
configured. The counter is incremented for each packet dropped.

Recommendation:
    Investigate and determine why the rate of traffic leaving/entering the interface is
higher than the configured rate. This may be normal, or could be an indication of virus or
attempted attack.

Syslogs:
    None.


----------------------------------------------------------------
Name: queue-removed
Rate-limiter queued packet dropped:
    When QoS config is changed or removed, the existing packets in the output queues
awaiting transmission are dropped and this counter is incremented.

Recommendation:
    Under normal conditions, this may be seen when the QoS configuration has been changed
by the user. If this occurs when no changes to QoS config were performed, please contact
Cisco Technical Assistance Center (TAC).

Syslogs:
   None.


----------------------------------------------------------------
Name: bad-crypto
Bad crypto return in packet:
    This counter will increment when the appliance attempts to perform a crypto operation
on a packet and the crypto operation fails. This is not a normal condition and could
indicate possible software or hardware problems with the appliance

 Recommendation:
    If you are receiving many bad crypto indications your appliance may need servicing.
You should enable syslog 402123 to determine whether the crypto errors are hardware or
software errors. You can also check the error counter in the global IPSec statistics with
the 'show ipsec stats' CLI command. If the IPSec SA which is triggering these errors is
known, the SA statistics from the 'show ipsec sa detail' command will also be useful in
diagnosing the problem.

 Syslogs:
    402123


----------------------------------------------------------------
Name: ctm-error
CTM returned error:
```

```
    This counter will increment when the appliance attempts to perform a crypto operation
on a packet and the crypto operation fails. This is not a normal condition and could
indicate possible software or hardware problems with the appliance.

 Recommendation:
    If you are receiving many bad crypto indications your appliance may need servicing.
You should enable syslog 402123 to determine whether the crypto errors are hardware or
software errors. You can also check the error counter in the global IPSec statistics with
the 'show ipsec stats' CLI command. If the IPSec SA which is triggering these errors is
known, the SA statistics from the 'show ipsec sa detail' command will also be useful in
diagnosing the problem.

 Syslogs:
    402123


----------------------------------------------------------------
Name: send-ctm-error
Send to CTM returned error:
    This counter is obsolete in the appliance and should never increment.

 Recommendation:
    None

 Syslogs:
    None


----------------------------------------------------------------
Name: security-failed
Early security checks failed:
    This counter is incremented and packet is dropped when the security appliance :
    - receives an IPv4 multicast packet when the packets multicast MAC address doesn't
match the packets multicast destination IP address
    - receives an IPv6 or IPv4 teardrop fragment containing either small offset or
fragment overlapping
    - receives an IPv4 packet that matches an IP audit (IPS) signature

Recommendation:
    Contact the remote peer administrator or escalate this issue according to your
security policy
    For detailed description and syslogs for IP audit attack checks please refer the ip
audit signature section of command reference guide

Syslogs:
    106020
    400xx in case of ip audit checks


----------------------------------------------------------------
Name: sp-security-failed
Slowpath security checks failed:
    This counter is incremented and packet is dropped when the security appliance is:
    1) In routed mode receives a through-the-box:
       - L2 broadcast packet
       - IPv4 packet with destination IP address equal to 0.0.0.0
       - IPv4 packet with source IP address equal to 0.0.0.0
    2) In routed or transparent mode and receives a through-the-box IPv4 packet with:
       - first octet of the source IP address equal to zero
       - source IP address equal to the loopback IP address
       - network part of source IP address equal to all 0's
       - network part of the source IP address equal to all 1's
       - source IP address host part equal to all 0's or all 1's
```

```
    3) In routed or transparent mode and receives an IPv4 or IPv6 packet with same source
and destination IP addresses

Recommendation:
    1 and 2) Determine if an external user is trying to compromise the protected network.
Check for misconfigured clients.
    3) If this message counter is incrementing rapidly, an attack may be in progress. Use
the packet capture feature to capture type asp packets, and check the source MAC address
in the packet to see where they are coming from.

Syslogs:
    1 and 2) 106016
    3) 106017


-------------------------------------------------------------------
Name: ipv6_sp-security-failed
IPv6 slowpath security checks failed:
    This counter is incremented and the packet is dropped for one of the following
reasons:
1) IPv6 through-the-box packet with identical source and destination address.
2) IPv6 through-the-box packet with linklocal source or destination address.
3) IPv6 through-the-box packet with multicast destination address.

Recommendation:
    These packets could indicate malicious activity, or could be the result of a
misconfigured IPv6 host.  Use the packet capture feature to capture type asp packets, and
use the source MAC address to identify the source.

Syslogs:
    For identical source and destination address, syslog 106016, else none.


-------------------------------------------------------------------
Name: invalid-ip-option
IP option drop:
    This counter is incremented when any unicast packet with ip options or a multicast
packet with ip-options that have not been configured to be accepted, is received by the
security appliance. The packet is dropped.

Recommendation:
    Investigate why a packet with ip options is being sent by the sender.

Syslogs:
    None.


-------------------------------------------------------------------
Name: lu-invalid-pkt
Invalid LU packet:
    Standby unit received a corrupted Logical Update packet.

Recommendation:
    The packet corruption could be caused by a bad cable, interface card, line noise, or
software defect. If the interface appears to be functioning properly, then report the
problem to Cisco TAC.

Syslogs:
    None


-------------------------------------------------------------------
Name: fo-standby
Dropped by standby unit:
```

```
    If a through-the-box packet arrives at an appliance or context in a Standby state and
a flow is created, the packet is dropped and the flow removed. This counter will increment
each time a packet is dropped in this manner.

Recommendation:
    This counter should never be incrementing on the Active appliance or context. However,
it is normal to see it increment on the Standby appliance or context.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: dst-l2_lookup-fail
Dst MAC L2 Lookup Failed:
    This counter will increment when the appliance is configured for transparent mode and
the appliance does a Layer 2 destination MAC address lookup which fails. Upon the lookup
failure, the appliance will begin the destination MAC discovery process and attempt to
find the location of the host via ARP and/or ICMP messages.

 Recommendation:
    This is a normal condition when the appliance is configured for transparent mode. You
can also execute (show mac-address-table) to list the L2 MAC address locations currently
discovered by the appliance.

 Syslogs:
    None


----------------------------------------------------------------
Name: l2_same-lan-port
L2 Src/Dst same LAN port:
    This counter will increment when the appliance/context is configured for transparent
mode and the appliance determines that the destination interface's L2 MAC address is the
same as its ingress interface.

 Recommendation:
    This is a normal condition when the appliance/context is configured for transparent
mode.  Since the appliance interface is operating in promiscuous mode, the
appliance/context receives all packets on the local LAN seqment.

 Syslogs:
    None


----------------------------------------------------------------
Name: flow-expired
Expired flow:
    This counter is incremented when the security appliance tries to inject a new or
cached packet belonging to a flow that has already expired.It is also incremented when the
appliance attempts to send an rst on a tcp flow that has already expired or when a packet
returns from IDS blade but the flow had already expired. The packet is dropped

Recommendation:
    If valid applications are getting pre-empted, investigate if a longer timeout is
needed.

Syslogs:
   None.


----------------------------------------------------------------
Name: inspect-icmp-out-of-app-id
ICMP Inspect out of App ID:
```

```
    This counter will increment when the ICMP inspection engine fails to allocate an 'App
ID' data structure. The structure is used to store the sequence number of the ICMP packet.

Recommendation:
    Check the system memory usage. This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-icmp-bad-code
ICMP Inspect bad icmp code:
    This counter will increment when the ICMP code in the ICMP echo request or reply
message is non-zero.

Recommendation:
    No action required if it is an intermittent event.  If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313009.


----------------------------------------------------------------
Name: inspect-icmp-seq-num-not-matched
ICMP Inspect seq num not matched:
    This counter will increment when the sequence number in the ICMP echo reply message
does not match any ICMP echo message that passed across the appliance earlier on the same
connection.

Recommendation:
    No action required if it is an intermittent event. If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313004


----------------------------------------------------------------
Name: inspect-icmp-error-no-existing-conn
ICMP Error Inspect no existing conn:
    This counter will increment when the appliance is not able to find any established
connection related to the frame embedded in the ICMP error message.

Recommendation:
    No action required if it is an intermittent event.  If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmp-error-nat64-error
ICMP NAT64 Error Inspect XLATE Error:
    This counter will increment when the appliance is unable to translate ICMP error
messages between IPv6 and IPv4.

Recommendation:
    No action required if it is an intermittent event.  If the cause is an attack, you can
deny the host using the ACLs.
```

```
Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmp-nat64-frag
ICMP NAT64 Inspect Fragmentation Error:
    This counter will increment when the appliance is unable to translate ICMP messages
between IPv6 and IPv4 due to fragmentation.  Per RFC-6145, ICMP packet fragments will not
be translated.

Recommendation:
    No action required.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmp-error-different-embedded-conn
ICMP Error Inspect different embedded conn:
    This counter will increment when the frame embedded in the ICMP error message does not
match the established connection that has been identified when the ICMP connection is
created.

Recommendation:
    No action required if it is an intermittent event.  If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-icmpv6-error-invalid-pak
ICMPv6 Error Inspect invalid packet:
    This counter will increment when the appliance detects an invalid frame embedded in
the ICMPv6 packet. This check is the same as that on IPv6 packets. Examples: Incomplete
IPv6 header; malformed IPv6 Next Header; etc.

Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-icmpv6-error-no-existing-conn
ICMPv6 Error Inspect no existing conn:
    This counter will increment when the appliance is not able to find any established
connection related to the frame embedded in the ICMPv6 error message.

Recommendation:
    No action required if it is an intermittent event. If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313005


----------------------------------------------------------------
Name: inspect-dns-invalid-pak
DNS Inspect invalid packet:
```

```
    This counter will increment when the appliance detects an invalid DNS packet.
Examples: A DNS packet with no DNS header; the number of DNS resource records not matching
the counter in the header; etc.

Recommendation:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-invalid-domain-label
DNS Inspect invalid domain label:
    This counter will increment when the appliance detects an invalid DNS domain name or
label. DNS domain name and label is checked per RFC 1035.

Recommendation:
    No action required. If the domain name and label check is not desired, disable the
protocol-enforcement parameter in the DNS inspection policy-map (in supported releases).

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-pak-too-long
DNS Inspect packet too long:
    This counter is incremented when the length of the DNS message exceeds the configured
maximum allowed value.

Recommendation:
    No action required.  If DNS message length checking is not desired, enable DNS
inspection without the 'maximum-length' option, or disable the 'message-length maximum'
parameter in the DNS inspection policy-map (in supported releases).

Syslogs:
    410001


----------------------------------------------------------------
Name: inspect-dns-out-of-app-id
DNS Inspect out of App ID:
    This counter will increment when the DNS inspection engine fails to allocate a data
structure to store the identification of the DNS message.
Recommendation:
    Check the system memory usage. This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-id-not-matched
DNS Inspect ID not matched:
    This counter will increment when the identification of the DNS response message does
not match any DNS queries that passed across the appliance earlier on the same connection.

Recommendation:
    No action required if it is an intermittent event. If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
```

```
    None.


----------------------------------------------------------------
Name: dns-guard-out-of-app-id
DNS Guard out of App ID:
    This counter will increment when the DNS Guard function fails to allocate a data
structure to store the identification of the DNS message.

Recommendation:
    Check the system memory usage.  This event normally happens when the system runs short
of memory.

Syslogs:
    None.


----------------------------------------------------------------
Name: dns-guard-id-not-matched
DNS Guard ID not matched:
    This counter will increment when the identification of the DNS response message does
not match any DNS queries that passed across the appliance earlier on the same connection.
This counter will increment by the DNS Guard function.

Recommendation:
    No action required if it is an intermittent event.  If the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtp-invalid-length
Invalid RTP Packet length:
    This counter will increment when the UDP packet length is less than the size of the
RTP header.

Recommendation:
    No action required. A capture can be used to figure out which RTP source is sending
the incorrect packets and you can deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtp-invalid-version
Invalid RTP Version field:
    This counter will increment when the RTP version field contains a version other than
2.

Recommendation:
    The RTP source in your network does not seem to be sending RTP packets conformant with
the RFC 1889. The reason for this has to be identified and you can deny the host using
ACLs if required.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-invalid-payload-type
Invalid RTP Payload type field:
```

```
    This counter will increment when the RTP payload type field does not contain an audio
payload type when the signalling channel negotiated an audio media type for this RTP
secondary connection. The counter increments similarly for the video payload type.

Recommendation:
    The RTP source in your network is using the audio RTP secondary connection to send
video  or vice versa. If you wish to prevent this you can deny the host using ACLs.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-ssrc-mismatch
Invalid RTP Synchronization Source field:
    This counter will increment when the RTP SSRC field in the packet does not match the
SSRC which the inspect has been seeing from this RTP source in all the RTP packets.

Recommendation:
    This could be because the RTP source in your network is rebooting and hence changing
the SSRC or it could be because of another host on your network trying to use the opened
secondary RTP connections on the firewall to send RTP packets. This should be investigated
further to confirm if there is a problem.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-sequence-num-outofrange
RTP Sequence number out of range:
    This counter will increment when the RTP sequence number in the packet is not in the
range expected by the inspect.

Recommendation:
    No action is required because the inspect tries to recover and start tracking from a
new sequence number after a lapse in the sequence numbers from the RTP source.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtp-max-outofseq-paks-probation
RTP out of sequence packets in probation period:
    This counter will increment when the out of sequence packets when the RTP source is
being validated exceeds 20. During the probation period, the inspect looks for 5
in-sequence packets to consider the source validated.

Recommendation:
    Check the RTP source to see why the first few packets do not come in sequence and
correct it.

Syslogs:
    431001.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-length
Invalid RTCP Packet length:
    This counter will increment when the UDP packet length is less than the size of the
RTCP header.

Recommendation:
```

```
    No action required. A capture can be used to figure out which RTP source is sending
the incorrect packets and you can deny the host using the ACLs.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-version
Invalid RTCP Version field:
    This counter will increment when the RTCP version field contains a version other than
2.

Recommendation:
    The RTP source in your network does not seem to be sending RTCP packets conformant
with the RFC 1889. The reason for this has to be identified and you can deny the host
using ACLs if required.

Syslogs:
    431002.


----------------------------------------------------------------
Name: inspect-rtcp-invalid-payload-type
Invalid RTCP Payload type field:
    This counter will increment when the RTCP payload type field does not contain the
values 200 to 204.

Recommendation:
    The RTP source should be validated to see why it is sending payload types outside of
the range recommended by the RFC 1889.

Syslogs:
    431002.


----------------------------------------------------------------
Name: cxsc-request
Flow terminated by CXSC:
This reason is given for terminating a flow as requested by CXSC module. Recommendations:
Check syslogs and alerts on CXSC module.
Syslogs: 429002


----------------------------------------------------------------
Name: cxsc-fail
CXSC config removed for connection:
    This counter is incremented and the packet is dropped when CXSC configuration is not
found for a particular connection.

Recommendations:
   check if any configuration changes have been done for CXSC.

Syslogs:
   None


----------------------------------------------------------------
Name: cxsc-fail-close
CXSC fail-close:
    This reason is given for terminating a flow since CXSC card is down and fail-close
option was used with CXSC action.

Recommendations:
```

```
    Check and bring up CXSC card.

Syslogs:
    429001


----------------------------------------------------------------
Name: cxsc-bad-tlv-received
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by CXSC module when
the packet has bad TLV's.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    None


----------------------------------------------------------------
Name: cxsc-ha-request
CXSC HA replication drop:
    This counter is incremented when the security appliance receives a CXSC HA request
packet, but could not process it and the packet is dropped.

Recommendation:
    This could happen occasionally when CXSC does not have the latest ASA HA state, like
right after ASA HA state change. If the counter is constantly increasing however, then it
can be because CXSC and ASA are out of sync. If that happens, contact Cisco TAC for
assistance.

Syslogs:
    None.


----------------------------------------------------------------
Name: cxsc-invalid-encap
CXSC invalid header drop:
    This counter is incremented when the security appliance receives a CXSC packet with
invalid messsage header, and the packet is dropped.

Recommendation:
    This should not happen. Contact Cisco TAC for assistance.

Syslogs:
    None.


----------------------------------------------------------------
Name: cxsc-malformed-packet
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by CXSC module when
the packet is malformed.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    None


----------------------------------------------------------------
Name: ips-request
IPS Module requested drop:
```

```
    This counter is incremented and the packet is dropped as requested by IPS module when
the packet matches a signature on the IPS engine.

Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420002


----------------------------------------------------------------
Name: ips-fail-close
IPS card is down:
    This counter is incremented and the packet is dropped when IPS card is down and
fail-close option was used in IPS inspection.

Recommendations:
    Check and bring up the IPS card.

Syslogs:
    420001


----------------------------------------------------------------
Name: ips-fail
IPS config removed for connection:
    This counter is incremented and the packet is dropped when IPS configuration is not
found for a particular connection.

Recommendations:
   check if any configuration changes have been done for IPS.

Syslogs:
   None


----------------------------------------------------------------
Name: ips-no-ipv6
Executing IPS software does not support IPv6:
    This counter is incremented when an IPv6 packet, configured to be directed toward IPS
SSM, is discarded since the software executing on IPS SSM card does not support IPv6.

Recommendations:
   Upgrade the IPS software to version 6.2 or later.

Syslogs:
   None


----------------------------------------------------------------
Name: l2_acl
FP L2 rule drop:
    This counter will increment when the appliance denies a packet due to a layer-2 ACL.
By default, in routed mode the appliance will PERMIT:
    1) IPv4 packets
    2) IPv6 packets
    3) ARP packets
    4) L2 Destination MAC of FFFF:FFFF:FFFF (broadcast)
    5) IPv4 MCAST packet with destination L2 of 0100:5E00:0000-0100:5EFE:FFFF
    6) IPv6 MCAST packet with destination L2 of 3333:0000:0000-3333:FFFF:FFFF

    By default, in Transparent mode permits the routed mode ACL and PERMITS:

    1) BPDU packets with destination L2 of 0100:0CCC:CCCD
```

```
    2) Appletalk packets with destination L2 of 0900:0700:0000-0900:07FF:FFFF

    The user can also configure ethertype ACL(s) and apply them to an interface to permit
other types of L2 traffic.

    The default L2 ACL can be seen in routed and transparent mode with the show asp table
classify domain permit command.

    Note - Packets permitted by L2 ACLs may still be dropped by L3-L4 ACLs.

 Recommendation:
    If your running the appliance/context in transparent mode and your non-IP packets are
dropped by the appliance, you can configure an ethertype ACL and apply the ACL to an
access group. Note - the appliance ethertype CLI only supports protocol types and not L2
destination MAC addresses.

 Syslogs:
    106026, 106027


----------------------------------------------------------------
Name: intercept-unexpected
Intercept unexpected packet:
    Either received data from client while waiting for SYNACK from server or received a
packet which cannot be handled in a particular state of TCP intercept.

Recommendation:
    If this drop is causing the connection to fail, please have a sniffer trace of the
client and server side of the connection while reporting the issue. The box could be under
attack and the sniffer traces or capture would help narrowing down the culprit.

Syslogs:
    None.


----------------------------------------------------------------
Name: no-mcast-entry
FP no mcast entry:
    A packet has arrived that matches a multicast flow, but the multicast service is no
longer enabled, or was re-enabled after the flow was built.
    - OR -
    A multicast entry change has been detected after a packet was punted to the CP, and
the NP can no longer forward the packet since no entry is present.

Recommendation:
    Reenable multicast if it is disabled.
    - OR -
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: no-mcast-intrf
FP no mcast output intrf:
    All output interfaces have been removed from the multicast entry.
    - OR -
    The multicast packet could not be forwarded.

Recommendation:
    Verify that there are no longer any receivers for this group.
    - OR -
    Verify that a flow exists for this packet.
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: fragment-reassembly-failed
Fragment reassembly failed:
    This counter is incremented when the appliance fails to reassemble a chain of
fragmented packets into a single packet. All the fragment packets in the chain are
dropped. This is most probably because of failure while allocating memory for the
reassembled packet.

Recommendation:
    Use the show blocks command to monitor the current block memory.

Syslogs:
    None


----------------------------------------------------------------
Name: ifc-classify
Virtual firewall classification failed:
    A packet arrived on a shared interface, but failed to classify to any specific context
interface.

Recommendation:
    For software versions without customizable mac-address support, use the "global" or
"static" command to specify the IPv4 addresses that belong to each context interface.  For
software versions with customizable mac-address support, enable "mac-address auto" in
system context.  Alternatively, configure unique MAC addresses for each context interfaces
residing over a shared interface with "mac-address" command under each context interface
submode.

Syslogs:
    None.


----------------------------------------------------------------
Name: connection-lock
Connection locking failed:
    While the packet was waiting for processing, the flow that would be usedwas destroyed.

Recommendation:
    The message could occur from user interface command to remove connection in an device
that is actively processing packet.  Otherwise, investigate flow drop counter.  This
message may occur if the flow are forced dropped from error.

Syslogs:
    None.


----------------------------------------------------------------
Name: interface-down
Interface is down:
    This counter will increment for each packet received on an interface that is shutdown
via the 'shutdown' interface sub-mode command. For ingress traffic, the packet is dropped
after security context classification and if the interface associated with the context is
shut down. For egress traffic, the packet is dropped when the egress interface is shut
down.

Recommendation:
    No action required.
```

```
Syslogs:
    None.


-----------------------------------------------------------------
Name: invalid-app-length
Invalid App length:
    This counter will increment when the appliance detects an invalid length of the Layer
7 payload in the packet.  Currently, it counts the drops by the DNS Guard function only.
Example: Incomplete DNS header.

Recommendation:
    No action required.

Syslogs:
    None.


-----------------------------------------------------------------
Name: loopback-buffer-full
Loopback buffer full:
    This counter is incremented and the packet is dropped when packets are sent from one
context of the appliance to another context through a shared interface and there is no
buffer space in loopback queue.

Recommendations:
    Check system CPU to make sure it is not overloaded.

Syslogs:
    None


-----------------------------------------------------------------
Name: non-ip-pkt-in-routed-mode
Non-IP packet received in routed mode:
    This counter will increment when the appliance receives a packet which is not IPv4,
IPv6 or ARP and the appliance/context is configured for routed mode. In normal operation
such packets should be dropped by the default L2 ACL configuration.

 Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

 Syslogs:
    106026, 106027


-----------------------------------------------------------------
Name: host-move-pkt
FP host move packet:
    This counter will increment when the appliance/context is configured for transparent
and source interface of a known L2 MAC address is detected on a different interface.

 Recommendation:
    This indicates that a host has been moved from one interface (i.e. LAN segment) to
another. This condition is normal while in transparent mode if the host has in fact been
moved. However, if the host move toggles back and forth between interfaces, a network loop
may be present.

 Syslogs:
    412001, 412002, 322001


-----------------------------------------------------------------
Name: tfw-no-mgmt-ip-config
```

```
No management IP address configured for TFW:
    This counter is incremented when the security appliance receives an IP packet in
transparent mode and has no management IP address defined. The packet is dropped.

Recommendation:
    Configure the device with management IP address and mask values.

Syslogs:
    322004


----------------------------------------------------------------
Name: shunned
Packet shunned:
    This counter will increment when a packet is received which has a source IP address
that matches a host in the shun database.

Recommendation:
    No action required.

Syslogs:
    401004


----------------------------------------------------------------
Name: rm-conn-limit
RM connection limit reached:
    This counter is incremented when the maximum number of connections for a context or
the system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001


----------------------------------------------------------------
Name: rm-conn-rate-limit
RM connection rate limit reached:
    This counter is incremented when the maximum connection rate for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321002


----------------------------------------------------------------
Name: np-socket-closed
Dropped pending packets in a closed socket:
    If a socket is abruptly closed, by the user or software, then any pending packets in
the pipeline for that socket are also dropped. This counter is incremented for each packet
in the pipeline that is dropped.

Recommendation:
```

```
    It is common to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-pf-queue-full
Port Forwarding Queue Is Full:
       This counter is incremented when the Port Forwarding application's internal queue
is full and it receives another packet  for transmission.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-dpp-invalid
Invalid packet received from SSM card:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the security appliance receives a packet from the internal data plane
interface but could not find the proper driver to parse it.

Recommendation:
    The data plane driver is dynamically registered depending on the type of SSM installed
in the system. So this could happen if data plane packets arrive before the security
appliance is fully initialized. This counter is usually 0. You should not be concerned if
there are a few drops. However, if this counter keeps rising when system is up and
running, it may indicate a problem. Please contact Cisco Technical Assistance Center (TAC)
if you suspect it affects the normal operation of your the security appliance.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-asdp-invalid
Invalid ASDP packet received from SSM card:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the security appliance receives an ASA SSM Dataplane Protocol (ASDP)
packet from the internal data plane interface, but the driver encountered a problem when
parsing the packet. ASDP is a protocol used by the security appliance to communicate with
certain types of SSMs, like the CSC-SSM. This could happen for various reasons, for
example ASDP protocol version is not compatible between the security appliance and SSM, in
which case the card manager process in the control plane issues system messages and CLI
warnings to inform you of the proper version of images that need to be installed; the ASDP
packet belongs to a connection that has already been terminated on the security appliance;
the security appliance has switched to the standby state (if failover is enable) in which
case it can no longer pass traffic; or any unexpected value when parsing the ASDP header
and payload.

Recommendation:
    The counter is usually 0 or a very small number. But user should not be concerned if
the counter slowly increases over the time, especially when there has been a failover, or
you have manually cleared connections on the security appliance via CLI. If the counter
increases drastically during normal operation, please contact Cisco Technical Assistance
Center (TAC).
```

```
Syslogs:
    421003
    421004


------------------------------------------------------------------
Name: ssm-app-request
Service module requested drop:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the application running on the SSM requests the security appliance to
drop a packet.

Recommendation:
    More information could be obtained by querying the incident report or system messages
generated by the SSM itself. Please consult the documentation that comes with your SSM for
instructions.

Syslogs:
    None.


------------------------------------------------------------------
Name: ssm-app-fail
Service module is down:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when a packet to be inspected by the SSM is dropped because the SSM has become
unavailable. Some examples of this are: software or hardware failure, software or
signature upgrade, or the module being shut down.

Recommendation:
    The card manager process running in the security appliance control plane would have
issued system messages and CLI warning to inform you of the failure. Please consult the
documentation that comes with the SSM to trouble shoot the SSM failure. Contact Cisco
Technical Assistance Center (TAC) if needed.

Syslog:
    None.


------------------------------------------------------------------
Name: wccp-return-no-route
No route to host for WCCP returned packet:
    This counter is incremented when a packet is returned from the Cache Engine and the
security appliance does not find a route for the original source of the packet.

Recommendation:
    Verify that a route exists for the source ip address of the packet returned from Cache
Engine.

Syslogs:
    None.


------------------------------------------------------------------
Name: wccp-redirect-no-route
No route to Cache Engine:
    This counter is incremented when the security appliance tries to redirect a packet and
does not find a route to the Cache Engine.

Recommendation:
    Verify that a route exists for Cache Engine.

Syslogs:
   None.
```

```
------------------------------------------------------------------
Name: telnet-not-permitted
Telnet not permitted on least secure interface:
    This counter is incremented and packet is dropped when the appliance receives a TCP
SYN packet attempting to establish a TELNET session to the appliance and that packet was
received on the least secure interface.

 Recommendation:
    To establish a Telnet session to the appliance via the least secure interface, first
establish an IPSec tunnel to that interface and then connect the Telnet session over that
tunnel.

 Syslogs:
    402117


------------------------------------------------------------------
Name: ipv6-sp-security-failed
IPv6 slowpath security checks failed:
    This counter is incremented and the packet is dropped for one of the following
reasons:
1) IPv6 through-the-box packet with identical source and destination address.
2) IPv6 through-the-box packet with linklocal source or destination address.
3) IPv6 through-the-box packet with multicast destination address.

Recommendation:
    These packets could indicate malicious activity, or could be the result of a
misconfigured IPv6 host.  Use the packet capture feature to capture type asp packets, and
use the source MAC address to identify the source.
Syslogs:
    For identical source and destination address, syslog 106016, else none.


------------------------------------------------------------------
Name: ipv6-eh-inspect-failed
IPv6 extension header is detected and denied:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet but extension header could not be inspected due to memory allocation failed.

 Recommendation:
Also check 'show memory' output to make sure appliance has enough memory to operate.

 Syslogs:
    None


------------------------------------------------------------------
Name: ipv6-bad-eh
Bad IPv6 extension header is detected and denied:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with bad extension header.

 Recommendation:
Check 'verify-header type' of 'parameters' in 'policy-map type ipv6'. Remove
'verify-header type' if the header conformance can be skipped.

 Syslogs:
    325005


------------------------------------------------------------------
Name: ipv6-bad-eh-order
```

```
IPv6 extension headers not in proper order is detected and denied:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with extension headers not in proper order.

 Recommendation:
Check 'verify-header order' of 'parameters' in 'policy-map type ipv6'. Remove
'verify-header order' if the header order can be arbitrary.

 Syslogs:
    325005


----------------------------------------------------------------
Name: ipv6-mobility-denied
IPv6 mobility extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with mobility extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header mobility' in 'policy-map type ipv6'. Remove action
'drop' if mobility should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-mobility-type-denied
IPv6 mobility type extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with mobility type extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header mobility type' in 'policy-map type ipv6'. Remove action
'drop' if mobility should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-fragment-denied
IPv6 fragmentation extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with fragmentation extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header fragmentation' in 'policy-map type ipv6'. Remove action
'drop' if fragmentation should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-routing-address-denied
IPv6 routing extension header exceeding configured maximum routing addresses is denied:
routing count is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with too many routing addresses in routing extension header whichis denied by the
user configuration rule.

 Recommendation:
```

```
    Check action of 'match header routing-address count' in 'policy-map type ipv6'. Remove
action 'drop' or increase <count> if <count> routing addresses should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-routing-type-denied
routing type is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with routing type extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header routing-type' in 'policy-map type ipv6'. Remove action
'drop' if routing-type should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-eh-count-denied
IPv6 extension headers exceeding configured maximum extension headers is denied:
extension header count is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with fragmentation extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header fragmentation' in 'policy-map type ipv6'. Remove action
'drop' if fragmentation should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-dest-option-denied
destination-option is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with destination-option extension header which is denied by the user configuration
rule.

 Recommendation:
    Check action of 'match header destination-option' in 'policy-map type ipv6'. Remove
action 'drop' if destination-option should be allowed.

 Syslogs:
    325004


----------------------------------------------------------------
Name: ipv6-hop-by-hop-denied
IPv6 hop-by-hp extension header is denied by user configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with hop-by-hop extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header hop-by-hop' in 'policy-map type ipv6'. Remove action
'drop' if hop-by-hop should be allowed.

 Syslogs:
    325004
```

```
------------------------------------------------------------------
Name: ipv6-esp-denied
ESP is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with ESP extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header esp' in 'policy-map type ipv6'. Remove action 'drop' if
ESP should be allowed.

 Syslogs:
    325004


------------------------------------------------------------------
Name: ipv6-ah-denied
AH is denied by IPv6 extension header configuration:
    This counter is incremented and packet is dropped when the appliance receives a IPv6
packet with AH extension header which is denied by the user configuration rule.

 Recommendation:
    Check action of 'match header ah' in 'policy-map type ipv6'. Remove action 'drop' if
AH should be allowed.

 Syslogs:
    325004


------------------------------------------------------------------
Name: channel-closed
Data path channel closed:
    This counter is incremented when the data path channel has been closed before the
packet attempts to be sent out through this channel.

Recommendation:
    It is normal in multi-processor system when one processor closes the channel (e.g.,
via CLI), and another processor tries to send a packet through the channel.

 Syslogs:
    None


------------------------------------------------------------------
Name: dispatch-decode-err
Diapatch decode error:
    This counter is incremented when the packet dispatch module finds an error when
decoding the frame.  An example is an unsupported packet frame.
Recommendation:
    Verify the packet format with a capture tool.

 Syslogs:
    None


------------------------------------------------------------------
Name: cp-event-queue-error
CP event queue error:
    This counter is incremented when a CP event queue enqueue attempt has failed due to
queue length exceeded. This queue is used by the data-path to punt packets to the
control-point for additional processing. This condition is only possible in a
multi-processor enviroment. The module that attempted to enqueue the packet may issue its
own packet specific drop in response to this error.
```

```
Recommendation:
    While this error does indicate a failure to completely process a packet, it may not
adversely affect the connection. If the condition persists or connections are adversely
affected contact the Cisco Technical Assistance Center (TAC).

Syslogs:
    None


----------------------------------------------------------------
Name: host-limit
Host limit exceeded:
    This counter is incremented when the licensed host limit is exceeded.

Recommendation:
    None.

Syslogs:
    450001


----------------------------------------------------------------
Name: cp-syslog-event-queue-error
CP syslog event queue error:
    This counter is incremented when a CP syslog event queue enqueue attempt has failed
due to queue length exceeded. This queue is used by the data-path to punt logging events
to the control-point when logging destinations other than to a UDP server are configured.
This condition is only possible in a multi-processor environment.

Recommendation:
    While this error does indicate a failure to completely process a logging event,
logging to UDP servers should not be affected. If the condition persists consider lowering
the logging level and/or removing logging destinations or contact the Cisco Technical
Assistance Center (TAC).

Syslogs:
    None


----------------------------------------------------------------
Name: dispatch-block-alloc
Dispatch block unavailable:
     This counter is incremented and the packet is dropped when the appliance could not
allocate a core local block to process the packet that was received by the interface
driver.

Recommendation:
    This may be due to packets being queued for later processing or a block leak. Core
local blocks may also not be available if they are not replenished on time by the free
resource rebalancing logic. Please use "show blocks core" to further diagnose the problem.

Syslogs:
    None


----------------------------------------------------------------
Name: async-lock-queue-limit
Async lock queue limit exceeded:
    Each async lock working queue has a limit of 1000. When more SIP packets are attempted
to be dispatch to the work queue, packet will be dropped.

Recommendation:
```

```
    Only SIP traffic may be dropped. When SIP packets have the same parent lock and they
can be queued into the same async lock queue, thus may result into blocks depletion,
becasue only single core is handling all the media. If a SIP packet attempts to be queued
when the size of the async lock queue exceeds the limit, the packet will be dropped.

Syslogs:
    None.


----------------------------------------------------------------
Name: loopback-lock-failed
Loopback lock failed
    This counter is incremented and the packet is dropped when packets are sent from one
context of the appliance to another context through a shared intrface and the loopback
queue has failed to acquire a lock.

Recommendations:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance. Contact the Cisco Techncial Assistance Center (TAC)
if this error occurs.

Syslogs:
    None

----------------------------------------------------------------
Name: loopback-ifc-not-found
Loopback output interface not found
    This counter is incremented and the packet is dropped when packets are sent from one
context of the appliance to another context through a shared interface, and the output
interface is not found by the loopback queue.

Recommendations:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance. Contact the Cisco Techncial Assistance Center (TAC)
if this error occurs.

Syslogs:
    None


----------------------------------------------------------------
Name: loopback-count-exceeded
Loopback count exceeded
    This counter is incremented and the packet is dropped when a packet is sent from one
context of the appliance to another context through a shared intreface, but this packet
has exceeded the number of times it is allowed to queue to the loopback queue.

Recommendations:
    Check the context configuration for each context. The packet is entering a loop in the
context configurations so that it is stuck between contexts, and is repeatedly put into
the loopback queue.

Syslogs:
    None


----------------------------------------------------------------
Name: ips-license-disabled-fail-close
IPS module license disabled
    The IPS module license has been disabled and when the fail-close mode is configured,
all traffic destined for the IPS module will be dropped. The status of the license can be
checked using the "show activation-key" command.

Recommendation:
```

```
    Please apply an activation key using the "activation-key" command that has the IPS
license enabled.

Syslogs:
    420008


------------------------------------------------------------------
Name: backplane-channel-null
Backplane channel null:
The card backplane channel was NULL. This may happen because the channel
was not initialized correctly and had to be closed. ASA will drop the packet.
Recommendation:
    This should not happen. Contact Cisco TAC for assistance.

Syslogs:
    None.


------------------------------------------------------------------


------------------------------------------------------------------
Name: svc-conn-timer-cb-fail
SVC connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.

 Recommendation:
    None.

 Syslogs:
    None.


------------------------------------------------------------------
Name: svc-udp-conn-timer-cb-fail
SVC UDP connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.

 Recommendation:
    None.

 Syslogs:
    None.


------------------------------------------------------------------
Name: nat64/46-conversion-fail
IPv6 to IPv4 or vice-versa conversion failure:
    This condition occurs when there is a failure in coversion of IPv6 traffic to IPv4 or
vice-versa.

 Recommendation:
    None.

 Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-cflow-clu-closed
Cluster flow with CLU closed on owner:
```

```
    Director/backup unit received a cluster flow clu delete message from the owner unit
and terminated the flow.

Recommendation:
    This counter should increment for every replicated clu that is torn down on the owner
unit.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-cflow-clu-timeout
Cluster flow with CLU removed from due to idle timeout:
    A cluster flow with CLU is considered idle if the director/backup unit no longer
receives periodic updates from the owner, which is supposed to happen at fixed intervals
when the flow is alive.

Recommendation:
    This counter is informational.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-redirect
Flow matched a cluster redirect classify rule:
    A stub forwarding flow will thereafter forward packets to the cluster unit that owns
the flow.

Recommendations:
    This counter is informational and the behavior expected. The packet was forwarded to
the owner over the Cluster Control Link.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-drop-on-slave
Flow matched a cluster drop-on-slave classify rule:
    This is for cases that the packets from L3 subnet are seen by all units and only
master unit need to process them.

Recommendations:
    This counter is informational and the behavior expected. The packet is processed by
master.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-director-change
The flow director changed due to a cluster join event:
    A new unit joined the cluster and is now the director for the flow. The old
director/backup has removed it's flow and the flow owner will update the new director.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.
```

```
------------------------------------------------------------------
Name: cluster-mcast-owner-change
The multicast flow owner changed due to a cluster join or leave event:
     This flow gets created on a new owner unit.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-convert-to-dirbak
Forwarding or redirect flow converted to director or backup flow:
    Forwarding or redirect flow is removed, so that director or  backup flow can be
created.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


------------------------------------------------------------------
Name: inspect-scansafe-server-not-reachable
Scansafe server is not configured or the cloud is down:
    Either the scansafe server IP is not specified in the scansafe general options or the
scansafe server is not reachable.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


------------------------------------------------------------------
Name: inspect-scansafe-public_key_not_configured
Scansafe public key not configured:
    This counter is incremented when the scansafe public key is not configured. The packet
is dropped and the connection isclosed.

Recommendation:
    Verify if the configured scansafe public key is configured on the security appliance.

Syslogs:
    775002.


------------------------------------------------------------------
Name: inspect-scansafe-license-key-not-configured
Scansafe license key not configured:
    This counter is incremented when the scansafe licnese key is not configured. The
packet is dropped and the connection isclosed.

Recommendation:
    Verify if the configured scansafe license key is configured on the security appliance.

Syslogs:
    775002.
```

```
------------------------------------------------------------------
Name: inspect-scansafe-encoding-failed
Inspect  scansafe header encoding failed :
    This counter is incremented when the base64 encoding of user and group name is failed.
The packet is dropped and connection is closed.

Syslogs:
    775002.


------------------------------------------------------------------
Name: inspect-scansafe-hdr-encryption-failed
Inspect  scansafe header encryption failed:
    This counter is incremented when the encryption of scansafe header is failed. The
packet is dropped and connection is closed.

Syslogs:
    775002.


------------------------------------------------------------------
Name: inspect-scansafe-max-conn-reached
Inspect  scansafe max allowed connections reached:
    This counter is incremented when we get a new connection and the maximum allowed
concurrent scansafe connection for the platform is already reached. The packet is dropped
and connection is closed.

Syslogs:
    775002.


------------------------------------------------------------------
Name: inspect-scansafe-duplicate-conn
Inspect scansafe duplicate connection:
     This counter is incremented when duplicate connection with the same source ip address
and port. This packet will be dropped and connection will be closed.

Syslogs:
    775002.


------------------------------------------------------------------
Name: cluster-director-closed
Flow removed due to director flow closed:
    Owner unit received a cluster flow clu delete message from the director unit and
terminated the flow.

Recommendation:
    This counter should increment for every replicated clu that is torn down on the
director unit.

Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-pinhole-master-change
Master only pinhole flow removed at bulk sync due to master change:
    Master only pinhole flow is removed during bulk sync becase cluster master has
changed.

Recommendation:
```

```
    This counter is informational and the behavior expected.

Syslogs:
    302014


----------------------------------------------------------------
Name: np-socket-lock-failure
Dropped pending packets due to a failed attempt to get an internal socket lock:
    This error occurs if an attempt to grab an internal socket lock fails.

Recommendation:
    This condition should never be encountered during normal operation and     may
indicate a software problem with the appliance.  Contact the Cisco     Technical
Assistance Center (TAC) if this error occurs.

Syslogs:
    None.


----------------------------------------------------------------
Name: mp-service-inject-failed
SERVICE Module failed to inject a packet:
    This error occurs if an attempt to inject a packet via the SERVICE     Module fails.

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: nat-64-or-46-conversion-fail
IPv6 to IPv4 or vice-versa conversion failure:
    This condition occurs when there is a failure in coversion of     IPv6 traffic to IPv4
or vice-versa.

Recommendation:
    Verify if the NAT64 or NAT46 policies are configured properly.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-not-owner
Cluster not owner:
    A Cluster data packet was received without a flow.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-ccl-cfull-sent
CLU FULL sent:
    A Cluster data packet was received over CCL and full flow is built on a new owner.
This packet is no longer needed.
Recommendation:
    None.
Syslogs:
    None.
```

```
------------------------------------------------------------------
Name: cluster-ccl-backup
Cluster CCL backup:
    A Cluster data packet was received over CCL on a backup unit, when it should have been
received on the owner+director unit.
Recommendation:
    None.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-ccl-unknown-stub
Cluster CCL unknown stub:
    A Cluster data packet was received over CCL and a matching stub flow found, but unit
has unknown role.
Recommendation:
    None.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-stub-to-full
Cluster stub to full flow:
    A Cluster packet was received on director, stub flow was converted to full flow. Drop
this packet and wait for retransmission.
Recommendation:
    None.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-ccl-unknown
Cluster CCL unknown role:
    A Cluster data packet was received over CCL and no matching flow is found, and unit
has unknown role.
Recommendation:
    None.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-owner-update
Cluster owner update:
    A Cluster data packet was received updating the flow owner.
Recommendation:
    None.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-invalid-pkt
Cluster rcvd invalid packet:
    An invalid cluster packet was received.
Recommendation:
    None.
Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: cluster-no-msgp
Cluster unit is out of message descriptor:
    Cluster unit is out of message descriptor.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-slave-ignored
Flow matched a cluster drop-on-slave classify rule:
    A multicast routing packet was received on a L3 cluster     interface when the unit
was a slave. Only a master unit     is permitted to process these packets.
Recommendation:
    This counter is informational and the behavior expected. The packet is    processed by
master.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-non-owner-ignored
Flow matched a cluster drop-on-non-owner classify rule:
    A multicast data packet was received on a L3 cluster     interface when the unit was
not an elected owner unit.     Only an elected owner unit is permitted to process
these packets.
Recommendation:
    This counter is informational and the behavior expected. The packet is    processed by
one elected owner unit.
Syslogs:
    None.


----------------------------------------------------------------
Name: nat-xlate-failed
NAT failed:
    Failed to create an xlate to translate an IP or transport header.

Recommendation:
    If NAT is not desired, disable "nat-control".  Otherwise, use the "static", "nat" or
"global" command to configure NAT policy for the dropped flow.  For dynamic NAT, ensure
that each "nat" command is paired with at least one "global" command.  Use "show nat" and
"debug pix process" to verify NAT rules.

Syslogs:
    305005, 305006, 305009, 305010, 305011, 305012


----------------------------------------------------------------
Name: nat-rpf-failed
NAT reverse path failed:
    Rejected attempt to connect to a translated host using the translated host's real
address.

Recommendation:
    When not on the same interface as the host undergoing NAT, use the mapped address
instead of the real address to connect to the host. Also, enable the appropriate inspect
command if the application embeds IP address.

Syslogs:
```

```
    305005


------------------------------------------------------------------
Name: nat-cluster-input
NAT invalid input:
    An input value for clustering communication contains an unexpected or invalid value.
Recommendation:
    This could be an internal software error.  Contact Cisco Systems.
Syslogs:
    None.


------------------------------------------------------------------
Name: nat-no-xlate-to-pat-pool
NAT no xlate to pat pool:
    No pre-existing xlate found for a connection with a destination matching a mapped
address in a PAT pool.
Recommendation:
    Configure static PAT is access is desired.
Syslogs:
    None.


------------------------------------------------------------------
Name: nat--xlate-create-failed
NAT xlate creation failed:
    Creation of a PAT xlate failed.
Recommendation:
    Check system memory. Configure at least one backup PAT address. Configure a NAT
address to translate non-overload IP address. Only TCP, UDP, ICMP echo, and PPTP GRE
overloadable.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-peer-mcast-ignored
Flow matched a cluster peer mcast data traffic classify rule:
    A multicast data packet was received on a L3 cluster interface when it is from a
cluster peer unit corresponding interface. This is a packet flooded back from L3 subnet.
Recommendation:
    This counter is informational and the behavior expected. The packet has been forwarded
out of the cluster and should be ignored by cluster.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-dispatch-queue-fail
Cluster failed to enqueue into global dispatch work queue:
    A forwarded data packet failed to enqueue into global dispatch work queue.
Recommendation:
    This could be an internal software error.  Contact Cisco Systems.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-dir-flow-create-fail
Cluster director failed to create director flow:
    Director is trying to create a stub flow but failed due to resource     limitation.
The resource limit may be either:
       1) system memory
```

```
       2) packet block extension memory
       3) system connection limit
    Causes 1 and 2 will occur simultaneously with flow drop reason "No     memory to
complete flow".
Recommendation:
    - Observe if free system memory is low.
    - Observe if flow drop reason "No memory to complete flow" occurs.
    - Observe if connection count reaches the system connection limit with     the command
"show resource usage".
Syslogs:
    None


------------------------------------------------------------------
Name: cluster-early-sec-chk-fail
Cluster early security check has failed:
    Director applied early security check has failed due to ACL, WCCP     redirect,
TCP-intercept or IP option.
Recommendation:
    This counter is informational and the behavior expected. The packet will     be
dropped.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-queued-ccl-unknown
Cluster CCL unknown stub:
    A queued cluster data packet received over ccl was processed but unit has     unknown
role.
Recommendation:
    None.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-dir-nat-changed
Cluster director NAT action changed:
    Cluster director NAT action has changed due to NAT policy change, update     or
expiration before queued ccl data packet can be processed.Recommendation:
    This counter is informational and the behavior expected. The packet will     be
dropped.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-dir-invalid-ifc
Cluster director has packet with invalid ingress/egress interface:
    Cluster director has processed a previously queued packet with invalid     ingress
and/or egress interface. This is a result of interface removal     (through CLI) before
the packet can be processed.
Recommendation:
    This counter is informational and the behavior expected. The packet will     be
dropped.
Syslogs:
    None.


------------------------------------------------------------------
Name: cluster-parent-owner-left
Flow removed at bulk sync becasue parent flow is gone:
    Flow is removed during bulk sync because the parent flow's owner has left the cluster.
```

```
Recommendation:
    This counter is informational and the behavior expected.

Syslogs:
    302014


----------------------------------------------------------------
Name: cluster-ctp-punt-channel-missing
Flow removed at bulk sync becasue CTP punt channel is missing:
    Flow is removed during bulk sync because CTP punt channel is missing in cluster
restored flow.

Recommendation:
    The cluster master may have just left the cluster, and there might be packet drops on
the Cluster Control Link.

Syslogs:
    302014


----------------------------------------------------------------
Name: ike-sa-rate-limit
IKE need SA indication per SA rule rate limit exceeded:
     This counter will increment when the appliance attempts to send a message,indicating
that a new SA is needed for a rate-limited control point service routine and the rate
limit (per/second) is now being exceeded. The current rate is one message every two
seconds.

Recommendation:
     This counter is informational and the behavior expected. The packet will be dropped.

Syslogs:
     None


----------------------------------------------------------------
Name: ike-sa-global-rate-limit
IKE new SA global limit exceeded:
     This counter will increment when the appliance attempts to send a message,indicating
that a new SA is needed for a rate-limited control point service routine and the global
rate limit (per/second) is now being exceeded. The current rate is ten messages per
second.

Recommendation:
     This counter is informational and the behavior expected. The packet will be dropped.

Syslogs:
     None


----------------------------------------------------------------
Name: nat-cluster-invalid-unxlate-redirect
Cluster member dropped an invalid NAT untranslate redirect packet from peer:
    Cluster member received a NAT untranslate packet from peer. However this member does
not own the NAT address pool the packet belongs to.

Recommendation:
    This counter is a temporal condition after a cluster member failure. However, if this
counter is incremented continuously, it could be an internal software error. Contact Cisco
TAC in this case.

Syslogs:
```

```
    None.


----------------------------------------------------------------
Name: nat-cluster-pool-update-fail
Cluster master failed to send NAT pool update to slave:
    Cluster master has failed to send NAT pool update to slave unit. This drop will
increase if system resources is low.

Recommendation:
    - Observe if free system memory is low.
    - Observe if "SEC_NAT_SEND_NO_BUFFER" counter is increasing.

Syslogs:
    None.


----------------------------------------------------------------
```

Flow Drop Reasons

```
----------------------------------------------------------------
Name: tunnel-torn-down
Tunnel has been torn down:
    This counter will increment when the appliance receives a packet associated with an
established flow whose IPSec security association is in the process of being deleted.

Recommendation:
    This is a normal condition when the IPSec tunnel is torn down for any reason.

Syslogs:
    None


----------------------------------------------------------------
Name: no-ipv6-ipsec
IPSec over IPv6 unsupported:
    This counter will increment when the appliance receives an IPSec ESP packet, IPSec
NAT-T ESP packet or an IPSec over UDP ESP packet encapsulated in an IP version 6 header.
The appliance does not currently support any IPSec sessions encapsulated in IP version 6.

Recommendation:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tunnel-pending
Tunnel being brought up or torn down:
    This counter will increment when the appliance receives a packet matching an entry in
the security policy database (i.e. crypto map) but the security association is in the
process of being negotiated; it’s not complete yet.

    This counter will also increment when the appliance receives a packet matching an
entry in the security policy database but the security association has been or is in the
process of being deleted. The difference between this indication and the 'Tunnel has been
torn down' indication is that the 'Tunnel has been torn down' indication is for
established flows.

Recommendation:
```

```
    This is a normal condition when the IPSec tunnel is in the process of being negotiated
or deleted.

Syslogs:
    None


------------------------------------------------------------------
Name: need-ike
Need to start IKE negotiation:
    This counter will increment when the appliance receives a packet which requires
encryption but has no established IPSec security association. This is generally a normal
condition for LAN-to-LAN IPSec configurations. This indication will cause the appliance to
begin ISAKMP negotiations  with the destination peer.

Recommendation:
    If you have configured IPSec LAN-to-LAN on your appliance, this indication is normal
and does not indicate a problem.  However, if this counter increments rapidly it may
indicate a crypto configuration error or network error preventing the ISAKMP negotiation
from completing.

    Verify that you can communicate with the destination peer and verify your crypto
configuration via the 'show running-config' command.

Syslogs:
    None


------------------------------------------------------------------
Name: vpn-handle-error
VPN handle error:
    This counter is incremented when the appliance is unable to create a VPN handle
because the VPN handle already exists.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect. Use the following command sto
gather more information about this counter and ontact the Cisco TAC to investigate the
issue further.

    capture <name> type asp-drop vpn-handle-error
    show asp table classify crypto
    show asp table vpn-context detail

Syslogs:
    None


------------------------------------------------------------------
Name: vpn-handle-not-found
VPN handle not found:
    This counter is incremented when a datagram hits an encrypt or decrypt rule, and no
VPN handle is found for the flow the datagram is on.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of vpn-based
applications, then this may be caused by a software defect. Use the following command sto
gather more information about this counter and ontact the Cisco TAC to investigate the
issue further.

    capture <name> type asp-drop vpn-handle-not-found
    show asp table classify crypto
```

```
    show asp table vpn-context detail

Syslogs:
    None


------------------------------------------------------------------
Name: ipsec-spoof-detect
IPSec spoof packet detected:
    This counter will increment when the appliance receives a packet which should have
been encrypted but was not.  The packet matched the inner header security policy check of
a configured and established IPSec connection on the appliance but was received
unencrypted.  This is a security issue.

Recommendation:
    Analyze your network traffic to determine the source of the spoofed IPSec traffic.

Syslogs:
    402117


------------------------------------------------------------------
Name: svc-spoof-detect
SVC spoof packet detected:
    This counter will increment when the security appliance receives a packet which should
have been encrypted but was not. The packet matched the inner header security policy check
of a configured and established SVC connection on the security appliance but was received
unencrypted. This is a security issue.

Recommendation:
    Analyze your network traffic to determine the source of the spoofed SVC traffic.

Syslogs:
    None


------------------------------------------------------------------
Name: svc-failover
An SVC socket connection is being disconnected on the standby unit:
    This counter is incremented for each new SVC socket connection that is disconnected
when the active unit is transitioning into standby state as part of a failover transition.

Recommendation:
    None. This is part of a normal cleanup of a SVC connection when the current device is
transitioning from active to standby. Existing SVC connections on the device are no longer
valid and need to be removed.

Syslogs:
    None.


------------------------------------------------------------------
Name: svc-replacement-conn
SVC replacement connection established:
    This counter is incremented when an SVC connection is replaced by a new connection.

Recommendation:
    None. This may indicate that users are having difficulty maintaining connections to
the ASA. Users should evaluate the quality of their home network and Internet connection.

Syslog:
    722032
```

```
------------------------------------------------------------------
Name: ipsec-selector-failure
IPSec VPN inner policy selector mismatch detected:
    This counter is incremented when an IPSec packet is received with an inner IP header
that does not match the configured policy for the tunnel.

 Recommendation:
    Verify that the crypto ACLs for the tunnel are correct and that all acceptable packets
are included in the tunnel identity.  Verify that the box is not under attack if this
message is repeatedly seen.

 Syslogs:
    402116


------------------------------------------------------------------
Name: vpn-context-expired
Expired VPN context:
    This counter will increment when the security appliance receives a packet that
requires encryption or decryption, and the ASP VPN context required to perform the
operation is no longer valid.

 Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

 Syslogs:
    None


------------------------------------------------------------------
Name: vpn-lock-error
IPSec locking error:
    This counter is incremented when VPN flow cannot be created due to an internal locking
error.

Recommendation:
    This condition should never be encountered during normal operation and may indicate a
software problem with the appliance. Contact the Cisco Technical Assistance Center (TAC)
if this error occurs.

Syslogs:
    None.


------------------------------------------------------------------
Name: out-of-memory
No memory to complete flow:
    This counter is incremented when the appliance is unable to create a flow because of
insufficient memory.

Recommendation:
    Verify that the box is not under attack by checking the current connections. Also
verify if the configured timeout values are too large resulting in idle flows residing in
memory longer. Check the free memory available by issuing 'show memory'.  If free memory
is low, issue the command 'show processes memory' to determine which processes are
utilizing most of the memory.

Syslogs:
    None


------------------------------------------------------------------
Name: parent-closed
Parent flow is closed:
```

```
    When the parent flow of a subordinating flow is closed, the subordinating flow is also
closed.  For example, an FTP data flow (subordinating flow) will be closed with this
specific reason when its control flow (parent flow) is terminated.  This reason is also
given when a secondary flow (pin-hole) is closed by its controlling application.  For
example, when the BYE messaged is received, the SIP inspection engine (controlling
application) will close the corresponding SIP RTP flows (secondary flow).

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: closed-by-inspection
Flow closed by inspection:
    This reason is given for closing a flow due to an error detected during application
inspection.  For example, if an error is detected during inspecting an H323 message, the
corresponding H323 flow is closed with this reason.

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: fo-primary-closed
Failover primary closed:
    Standby unit received a flow delete message from the active unit and terminated the
flow.

Recommendation:
    If the appliance is running stateful failover, then this counter should increment for
every replicated connection that is torn down on the standby appliance.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: fo-standby
Flow closed by failover standby:
    If a through-the-box packet arrives at an appliance or context is in a Standby state,
and a flow is created, the packet is dropped and the flow removed. This counter will
increment each time a flow is removed in this manner.

Recommendation:
    This counter should never be incrementing on the Active appliance or context. However,
it is normal to see it increment on the Standby appliance or context.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: fo_rep_err
Standby flow replication error:
    Standby unit failed to replicate a flow.

Recommendation:
```

```
    If appliance is processing VPN traffic, then this counter could be constantly
increasing on the standby unit because of the flow could be replicated before the IKE SA
info. No action is required in this case. If the appliance is not processing VPN traffic,
then this indicate a software detect, turn on the debug: "debug fover fail" on the standby
unit, collect the debug output, and report the problem to Cisco TAC.

Syslogs:
    302014, 302016, 302018


----------------------------------------------------------------
Name: loopback
Flow is a loopback:
    This reason is given for closing a flow due to the following conditions: 1) when
U-turn traffic is present on the flow, and, 2) 'same-security-traffic permit
intra-interface' is not configured.

Recommendation:
    To allow U-turn traffic on an interface, configure the interface with
'same-security-traffic permit intra-interface'.

Syslogs:
    None.


----------------------------------------------------------------
Name: acl-drop
Flow is denied by access rule:
     This counter is incremented when a drop rule is hit by the packet and flow creation
is denied. This rule could be a default rule created when the box comes up, when various
features are turned on or off, when an acl is applied to interface or any other feature
etc. Apart from default rule drops, a flow could be denied because of:
     1) ACL configured on an interface
     2) ACL configured for AAA and AAA denied the user
     3) Thru-box traffic arriving at management-only ifc
     4) Unencrypted traffic arriving on a ipsec-enabled interface
     5) Implicity deny 'ip any any' at the end of an ACL

Recommendation:
    Observe if one of syslogs related to packet drop are fired. Flow drop results in the
corresponding packet-drop that would fire requisite syslog.

Syslogs:
    None.


----------------------------------------------------------------
Name: pinhole-timeout
Pinhole timeout:
    This counter is incremented to report that the appliance opened a secondary flow, but
no packets passed through this flow within the timeout interval, and hence it was removed.
An example of a secondary flow is the FTP data channel that is created after successful
negotiation on the FTP control channel.

Recommendation:
    No action required.

Syslogs:
    302014, 302016


----------------------------------------------------------------
Name: host-removed
Host is removed:
```

```
    Flow removed in response to "clear local-host" command.

Recommendation:
    This is an information counter.

Syslogs:
    302014, 302016, 302018, 302021, 305010, 305012, 609002


----------------------------------------------------------------
Name: xlate-removed
Xlate Clear:
    Flow removed in response to "clear xlate" or "clear local-host" command.

Recommendation:
    This is an information counter.

Syslogs:
    302014, 302016, 302018, 302021, 305010, 305012, 609002


----------------------------------------------------------------
Name: connection-timeout
Connection timeout:
    This counter is incremented when a flow is closed because of the expiration of it's
inactivity timer.

Recommendation:
    No action required.

Syslogs:
    302014, 302016, 302018, 302021


----------------------------------------------------------------
Name: conn-limit-exceeded
Connection limit exceeded:
    This reason is given for closing a flow when the connection limit has been exceeded.
The connection limit is configured via the 'set connection conn-max' action command.

Recommendation:
    None.

Syslogs:
    201011


----------------------------------------------------------------
Name: tcp-fins
TCP FINs:
    This reason is given for closing a TCP flow when TCP FIN packets are received.

Recommendations:
    This counter will increment for each TCP connection that is terminated normally with
FINs.

Syslogs:
    302014


----------------------------------------------------------------
Name: syn-timeout
SYN Timeout:
    This reason is given for closing a TCP flow due to expiry of embryonic timer.
```

```
Recommendations:
    If these are valid session which take longer to establish a connection increase the
embryonic timeout.

Syslogs:
    302014


----------------------------------------------------------------
Name: fin-timeout
FIN Timeout:
    This reason is given for closing a TCP flow due to expiry of half-closed timer.

Recommendations:
    If these are valid session which take longer to close a TCP flow, increase the
half-closed timeout.

Syslogs:
    302014


----------------------------------------------------------------
Name: reset-in
TCP Reset-I:
    This reason is given for closing an outbound flow (from a low-security interface to a
same- or high-security interface) when a TCP reset is received on the flow.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: reset-out
TCP Reset-O:
    This reason is given for closing an inbound flow (from a high-security interface to
low-security interface) when a TCP reset is received on the flow.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: reset-appliance
TCP Reset-APPLIANCE:
    This reason is given for closing a flow when a TCP reset is generated by appliance.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: recurse
Close recursive flow:
```

```
    A flow was recursively freed. This reason applies to pair flows, multicast slave
flows, and syslog flows to prevent syslogs being issued for each of these subordinate
flows.

Recommendation:
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-intecept-no-response
TCP intercept, no response from server:
    SYN retransmission timeout after trying three times, once every second. Server
unreachable, tearing down connection.

Recommendation:
    Check if the server is reachable from the ASA.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-intercept-unexpected
TCP intercept unexpected state:
    Logic error in TCP intercept module, this should never happen.

Recommendation:
    Indicates memory corruption or some other logic error in the TCP intercept module.

Syslogs:
    None


----------------------------------------------------------------
Name: tcpnorm-rexmit-bad
TCP bad retransmission:
    This reason is given for closing a TCP flow when check-retranmission feature is
enabled and the TCP endpoint sent a retranmission with different data from the original
packet.

Recommendations:
    The TCP endpoint maybe attacking by sending different data in TCP retransmits. Please
use the packet capture feature to learn more about the origin of the packet.

Syslogs:
    302014


----------------------------------------------------------------
Name: tcpnorm-win-variation
TCP unexpected window size variation:
    This reason is given for closing a TCP flow when window size advertized by TCP
endpoint is drastically changed without accepting that much data.

Recommendations:
    In order to allow this connection, use the window-variation configuration under
tcp-map.

Syslogs:
    302014
```

```
----------------------------------------------------------------
Name: tcpnorm-invalid-syn
TCP invalid SYN:
    This reason is given for closing a TCP flow when the SYN packet is invalid.

Recommendations:
    SYN packet could be invalid for number of reasons, like invalid checksum, invalid TCP
header. Please use the packet capture feature to understand why the SYN packet is invalid.
If you would like to allow these connection use tcp-map configurations to bypass checks.

Syslogs:
    302014


----------------------------------------------------------------
Name: mcast-intrf-removed
Multicast interface removed:
    An output interface has been removed from the multicast entry.
    - OR -
    All output interfaces have been removed from the multicast entry.

Recommendation:
    No action required.
    - OR -
    Verify that there are no longer any receivers for this group.

Syslogs:
    None


----------------------------------------------------------------
Name: mcast-entry-removed
Multicast entry removed:
    A packet has arrived that matches a multicast flow, but the multicast service is no
longer enabled, or was re-enabled after the flow was built.
    - OR -
    The multicast entry has been deleted so the flow is being cleaned up, but the packet
will be reinjected into the data path.

Recommendation:
    Reenable multicast if it is disabled.
    - OR -
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-intercept-kill
Flow terminated by TCP Intercept:
    TCP intercept would teardown a connection if this is the first SYN, a connection is
created for the SYN, and TCP intercept replied with a SYN cookie, or after seeing a valid
ACK from client, when TCP intercept sends a SYN to server, server replies with a RST.

Recommendation:
    TCP intercept normally does not create a connection for first SYN, except when there
are nailed rules or the packet comes over a VPN tunnel or the next hop gateway address to
reach the client is not resolved. So for the first SYN this indicates that a connection
got created. When TCP intercept receives a RST from server, its likely the corresponding
port is closed on the server.

Syslogs:
```

```
    None


-------------------------------------------------------------
Name: audit-failure
Audit failure:
    A flow was freed after matching an "ip audit" signature that had reset as the
associated action.

Recommendation:
    If removing the flow is not the desired outcome of matching this signature, then
remove the reset action from the "ip audit" command.

Syslogs:
    None


-------------------------------------------------------------
Name: cxsc-request
Flow terminated by CXSC:
    This reason is given for terminating a flow as requested by CXSC module.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    429002


-------------------------------------------------------------
Name: cxsc-fail-close
CXSC fail-close:
    This reason is given for terminating a flow since CXSC card is down and fail-close
option was used with CXSC action.

Recommendations:
    Check and bring up CXSC card.

Syslogs:
    429001


-------------------------------------------------------------
Name: reset-by-cx
Flow reset by CXSC:
    This reason is given for terminating a TCP flow as requested by the CXSC module.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    429003


-------------------------------------------------------------
Name: ips-request
Flow terminated by IPS:
    This reason is given for terminating a flow as requested by IPS module.

Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420002
```

```
------------------------------------------------------------------
Name: cxsc-request
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by the CXSC module
when the packet matches a signature on the CXSC engine.

Recommendations:
    Check syslogs and alerts on the CXSC module.

Syslogs:
    429002


------------------------------------------------------------------
Name: cxsc-bad-tlv-received
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by the CXSC module
when the packet has bad TLVs.

Recommendations:
    Check syslogs and alerts on the CXSC module.
Syslogs:
    None


------------------------------------------------------------------
Name: cxsc-malformed-packet
CXSC Module requested drop:
    This counter is incremented and the packet is dropped as requested by the CXSC module
when the packet is malformed.

Recommendations:
    Check syslogs and alerts on the CXSC module.

Syslogs:
    None


------------------------------------------------------------------
Name: cxsc-fail
CXSC config removed for connection:
    This counter is incremented and the packet is dropped when the CXSC configuration is
not found for a particular connection.

Recommendations:
    Check if any configuration changes have been made for CXSC.

Syslogs:
    None


------------------------------------------------------------------
Name: cxsc-ha-request
CXSC HA replication drop:
    This counter is incremented when the security appliance receives a CXSC HA request
packet, but could not process it and the packet is dropped.

Recommendation:
    This could happen occasionally when CXSC does not have the latest ASA HA state, such
as right after an ASA HA state change. If the counter is constantly increasing however, it
may be because CXSC and ASA are out of sync. If that happens, contact Cisco TAC for
assistance.
```

```
Syslogs:
    None.


-----------------------------------------------------------------
Name: cxsc-invalid-encap
CXSC invalid header drop:
    This counter is incremented when the security appliance receives a CXSC packet with an
invalid messsage header, and the packet is dropped.

Recommendation: This should not happen. Contact Cisco TAC for assistance.

Syslogs:
    None.


-----------------------------------------------------------------
Name: ips-fail-close
IPS fail-close:
    This reason is given for terminating a flow since IPS card is down and fail-close
option was used with IPS inspection.

Recommendations:
    Check and bring up IPS card.

Syslogs:
    420001


-----------------------------------------------------------------
Name: reinject-punt
Flow terminated by punt action:
    This counter is incremented when a packet is punted to the exception-path for
processing by one of the enhanced services such as inspect, aaa etc and the servicing
routine, having detected a violation in the traffic flowing on the flow, requests that the
flow be dropped. The flow is immediately dropped.

Recommendation:
    Please watch for syslogs fired by servicing routine for more information. Flow drop
terminates the corresponding connection.

Syslogs:
    None.


-----------------------------------------------------------------
Name: shunned
Flow shunned:
    This counter will increment when a packet is received which has a source IP address
that matches a host in the shun database.  When a shun command is applied, it will be
incremented for each existing flow that matches the shun command.

Recommendation:
    No action required.

Syslogs:
    401004


-----------------------------------------------------------------
Name: host-limit
host-limit
```

```
---------------------------------------------------------------
Name: nat-failed
NAT failed:
    Failed to create an xlate to translate an IP or transport header.

Recommendation:
    If NAT is not desired, disable "nat-control".  Otherwise, use the "static", "nat" or
"global" command to configure NAT policy for the dropped flow.  For dynamic NAT, ensure
that each "nat" command is paired with at least one "global" command.  Use "show nat" and
"debug pix process" to verify NAT rules.

Syslogs:
    305005, 305006, 305009, 305010, 305011, 305012


---------------------------------------------------------------
Name: nat-rpf-failed
NAT reverse path failed:
    Rejected attempt to connect to a translated host using the translated host's real
address.

Recommendation:
    When not on the same interface as the host undergoing NAT, use the mapped address
instead of the real address to connect to the host. Also, enable the appropriate inspect
command if the application embeds IP address.

Syslogs:
    305005


---------------------------------------------------------------
Name: inspect-fail
Inspection failure:
    This counter will increment when the appliance fails to enable protocol inspection
carried out by the NP for the connection. The cause could be memory allocation failure, or
for ICMP error message, the appliance not being able to find any established connection
related to the frame embedded in the ICMP error message.

Recommendation:
    Check system memory usage.  For ICMP error message, if the cause is an attack, you can
deny the host using the ACLs.

Syslogs:
    313004 for ICMP error.


---------------------------------------------------------------
Name: no-inspect
Failed to allocate inspection:
    This counter will increment when the security appliance fails to allocate a run-time
inspection data structure upon connection creation. The connection will be dropped.

Recommendation:
    This error condition is caused when the security appliance runs out of system memory.
Please check the current available free memory by executing the "show memory" command.

Syslogs:
    None


---------------------------------------------------------------
Name: reset-by-ips
Flow reset by IPS:
    This reason is given for terminating a TCP flow as requested by IPS module.
```

```
Recommendations:
    Check syslogs and alerts on IPS module.

Syslogs:
    420003


----------------------------------------------------------------
Name: flow-reclaimed
Non-tcp/udp flow reclaimed for new request:
    This counter is incremented when a reclaimable flow is removed to make room for a new
flow.  This occurs only when the number of flows through the appliance equals the maximum
number permitted by the software imposed limit, and a new flow request is received. When
this occurs, if the number of reclaimable flows exceeds the number of VPN tunnels
permitted by the appliance, then the oldest reclaimable flow is removed to make room for
the new flow.  All flows except the following are deemed to be reclaimable:
    1. TCP, UDP, GRE and Failover flows
    2. ICMP flows if ICMP stateful inspection is enabled
    3. ESP flows to the appliance

Recommendation:
    No action is required if this counter is incrementing slowly. If this counter is
incrementing rapidly, it could mean that the appliance is under attack and the appliance
is spending more time reclaiming and rebuilding flows.

Syslogs
    302021


----------------------------------------------------------------
Name: non_tcp_syn
non-syn TCP:
    This reason is given for terminating a TCP flow when the first packet is not a SYN
packet.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: rm-xlate-limit
RM xlate limit reached:
    This counter is incremented when the maximum number of xlates for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001


----------------------------------------------------------------
Name: rm-host-limit
RM host limit reached:
    This counter is incremented when the maximum number of hosts for a context or the
system has been reached and a new connection is attempted.
```

```
 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321001


----------------------------------------------------------------
Name: rm-inspect-rate-limit
RM inspect rate limit reached:
    This counter is incremented when the maximum inspection rate for a context or the
system has been reached and a new connection is attempted.

 Recommendation:
    The device administrator can use the commands 'show resource usage' and 'show resource
usage system' to view context and system resource limits and 'Denied' counts and adjust
resource limits if desired.

 Syslogs:
    321002


----------------------------------------------------------------
Name: tcpmod-connect-clash
A TCP connect socket clashes with an existing listen connection. This is an internal
system error.  Contact TAC.

----------------------------------------------------------------
Name: ssm-app-request
Flow terminated by service module:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when the application running on the SSM requests the security appliance to
terminate a connection.

Recommendation:
    You can obtain more information by querying the incident report or system messages
generated by the SSM itself. Please consult the documentation that comes with comes with
the SSM for instructions.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssm-app-fail
Service module failed:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when a connection that is being inspected by the SSM is terminated because the
SSM has failed.

Recommendation:
    The card manager process running in the security appliance control plane issued system
messages and CLI warning to inform you of the failure. Please consult the documentation
that comes with the SSM to trouble shoot the SSM failure. Contact Cisco Technical
Assistance Center (TAC) if needed.

Syslog:
    421001.


----------------------------------------------------------------
Name: ssm-app-incompetent
```

```
Service module incompetent:
    This counter only applies to the ASA 5500 series adaptive security appliance. It is
incremented when a connection is supposed to be inspected by the SSM, but the SSM is not
able to inspect it. This counter is reserved for future use. It should always be 0 in the
current release.

Recommendation:
    None.

Syslog:
    None.


-----------------------------------------------------------------
Name: ssl-bad-record-detect
SSL bad record detected:
    This counter is incremented for each unknown SSL record type received from the remote
peer. Any unknown record type received from the peer is treated as a fatal error and the
SSL connections that encounter this error must be terminated.

Recommendation:
    It is not normal to see this counter increment at any time. If this counter is
incremented, it usually means that the SSL protocol state is out of sync with the client
software. The most likely cause of this problem is a software defect in the client
software. Contact the Cisco TAC with the client software or web browser version and
provide a network trace of the SSL data exchange to troubleshoot this problem.

Syslogs:
    None.


-----------------------------------------------------------------
Name: ssl-handshake-failed
SSL handshake failed:
    This counter is incremented when the TCP connection is dropped because the SSL
handshake failed.

Recommendation:
    This is to indicate that the TCP connection is dropped because the SSL handshake
failed. If the problem cannot be resolved based on the syslog information generated by the
handshake failure condition, please include the related syslog information when contacting
the Cisco TAC.

Syslogs:
    725006.
    725014.


-----------------------------------------------------------------
Name: ssl-malloc-error
SSL malloc error:
    This counter is incremented for each malloc failure that occurs in the SSL lib. This
is to indicate that SSL encountered a low memory condition where it can't allocate a
memory buffer or packet block.

Recommendation:
    Check the security appliance memory and packet block condition and contact Cisco the
TAC with this memory information.

Syslogs:
    None.


-----------------------------------------------------------------
```

```
Name: ctm-crypto-request-error
CTM crypto request error:
    This counter is incremented each time CTM cannot accept our crypto request. This
usually means the crypto hardware request queue is full.

Recommendation:
    Issue the show crypto protocol statistics ssl command and contact the Cisco TAC with
this information.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssl-record-decrypt-error
SSL record decryption failed:
    This counter is incremented when a decryption error occurs during SSL data receive.
This usually means that there is a bug in the SSL code of the ASA or peer, or an attacker
may be modifying the data stream. The SSL connection has been closed.

Recommendation:
    Investigate the SSL data streams to and from your ASA. If there is no attacker, then
this indicates a software error that should be reported to the Cisco TAC.

Syslogs:
    None.


----------------------------------------------------------------
Name: np-socket-conn-not-accepted
A new socket connection was not accepted:
    This counter is incremented for each new socket connection that is not accepted by the
security appliance.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-failure
NP socket failure:
    This is a general counter for critical socket processing errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


----------------------------------------------------------------
Name: np-socket-relay-failure
NP socket relay failure:
    This is a general counter for socket relay processing errors.

Recommendation:
```

```
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

Syslog:
    None.


-------------------------------------------------------------
Name: np-socket-data-move-failure
NP socket data movement failure:
    This counter is incremented for socket data movement errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


-------------------------------------------------------------
Name: np-socket-new-conn-failure
NP socket new connection failure:
    This counter is incremented for new socket connection failures.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


-------------------------------------------------------------
Name: np-socket-transport-closed
NP socket transport closed:
    This counter is incremented when the transport attached to the socket is abruptly
closed.

Recommendation:
    It is possible to see this counter increment as part of normal operation. However, if
the counter is rapidly incrementing and there is a major malfunction of socket-based
applications, then this may be caused by a software defect. Contact the Cisco TAC to
investigate the issue further.

Syslog:
    None.


-------------------------------------------------------------
Name: np-socket-block-conv-failure
NP socket block conversion failure:
    This counter is incremented for socket block conversion failures.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


-------------------------------------------------------------
Name: ssl-received-close-alert
SSL received close alert:
```

```
    This counter is incremented each time the security appliance receives a close alert
from the remote client. This indicates that the client has notified us they are going to
drop the connection. It is part of the normal disconnect process.

Recommendation:
    None.

Syslog:
    725007.


----------------------------------------------------------------
Name: children-limit
Max per-flow children limit exceeded:
    The number of children flows associated with one parent flow exceeds the internal
limit of 200.

Recommendation:
    This message indicates either a misbehaving application or an active attempt to
exhaust the firewall memory. Use "set connection per-client-max" command to further fine
tune the limit. For FTP, additionally enable the "strict" option in "inspect ftp".

Syslogs:
    210005


----------------------------------------------------------------
Name: tracer-flow
packet-tracer traced flow drop:
    This counter is internally used by packet-tracer for flow freed once tracing is
complete.

Recommendation:
    None.

Syslog:
    None.


----------------------------------------------------------------
Name: sp-looping-address
looping-address:
    This counter is incremented when the source and destination addresses in a flow are
the same. SIP flows where address privacy is enabled are excluded, as it is normal for
those flows to have the same source and destination address.

 Recommendation:
    There are two possible conditions when this counter will increment. One is when the
appliance receives a packet with the source address equal to the destination. This
represents a type of DoS attack.  The second is when the NAT configuration of the
appliance NATs a source address to equal that of the destination.  One should examine
syslog message 106017 to determine what IP address is causing the counter to increment,
then enable packet captures to capture the offending packet, and perform additional
analysis.

 Syslogs:
    106017


----------------------------------------------------------------
Name: no-adjacency
No valid adjacency:
```

```
    This counter will increment when the security appliance receives a packet on an
existing flow that no longer has a valid output adjacency. This can occur if the nexthop
is no longer reachable or if a routing change has occurred typically in a dynamic routing
environment.

 Recommendation:
    No action required.

 Syslogs:
    None


------------------------------------------------------------------
Name: np-midpath-service-failure
NP midpath service failure:
    This is a general counter for critical midpath service errors.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


------------------------------------------------------------------
Name: np-midpath-cp-event-failure
NP midpath CP event failure:
    This is counter for critical midpath events that could not be sent to the CP.

Recommendation:
    This indicates that a software error should be reported to the Cisco TAC.

Syslog:
    None.


------------------------------------------------------------------
Name: np-context-removed
NP virtual context removed:
    This counter is incremented when the virtual context with which the flow is going to
be associated has been removed. This could happen in multi-core environment when one CPU
core is in the process of destroying the virtual context, and another CPU core tries to
create a flow in the context.

Recommendation:
    No action is required.

Syslog:
    None.


------------------------------------------------------------------
Name: fover-idle-timeout
Flow removed from standby unit due to idle timeout:
    A flow is considered idle if standby unit no longer receives periodical update from
active which is supposed to happen to at fixed internal when flow is alive. This counter
is incremented when such flow is removed from standby unit.

Recommendation:
    This counter is informational.

Syslogs:
    None.
```

```
------------------------------------------------------------------
Name: dynamic-filter
Flow matched dynamic-filter blacklist:
    A flow matched a dynamic-filter blacklist or greylist entry with a threat-level higher
than the threat-level threshold configured to drop traffic.

Recommendation:
    Use the internal IP address to trace the infected host. Take remediation steps to
remove the infection.

Syslogs:
    None.


------------------------------------------------------------------

Name: route-change
Flow terminated due to route change:
    When the system adds a lower cost (better metric) route, incoming packets that match
the new route will cause their existing connection to be torn down after the user
configured timeout (floating-conn) value. Subsequent packets will rebuild the connection
out the interface with the better metric.

Recommendation:
    To prevent the addition of lower cost routes from affecting active flows, the
'floating-conn' configuration timeout value can be set to 0:0:0.

Syslogs:
    None.


------------------------------------------------------------------
Name: svc-selector-failure
SVC VPN inner policy selector mismatch detected:
    This counter is incremented when an SVC packet is received with an inner IP header
that does not match the policy for the tunnel.

 Recommendation:
    None. This packet will be discarded automatically.

 Syslogs:
    None.


------------------------------------------------------------------
Name: dtls-hello-close
DTLS hello processed and closed:
     This counter is incremented when the UDP connection is dropped after the DTLS client
hello message processing is finished. This does not indicate an error.

Recommendation:
None.

 Syslogs:
    None.


------------------------------------------------------------------
Name: svc-conn-timer-cb-fail
SVC connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.
```

```
 Recommendation:
    None.

 Syslogs:
    None.


-----------------------------------------------------------------
Name: svc-udp-conn-timer-cb-fail
SVC UDP connection timer callback failure:
    This condition occurs when there is a failed attempt to place an event on the async
lock queue for that connection.

 Recommendation:
    None.

 Syslogs:
    None.


-----------------------------------------------------------------
Name: nat64/46-conversion-fail
IPv6 to IPv4 or vice-versa conversion failure:
    This condition occurs when there is a failure in coversion of IPv6 traffic to IPv4 or
vice-versa.

 Recommendation:
    None.

 Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-cflow-clu-closed
Cluster flow with CLU closed on owner:
    Director/backup unit received a cluster flow clu delete message from the owner unit
and terminated the flow.

Recommendation:
    This counter should increment for every replicated clu that is torn down on the owner
unit.

Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-cflow-clu-timeout
Cluster flow with CLU removed from due to idle timeout:
    A cluster flow with CLU is considered idle if director/backup unit no longer receives
periodical update from owner which is supposed to happen at fixed interval when flow is
alive.

Recommendation:
    This counter is informational.

Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-redirect
Flow matched a cluster redirect classify rule:
```

```
    A stub forwarding flow will thereafter forward packets to the cluster unit that owns
the flow.

Recommendations:
    This counter is informational and the behavior expected. The packet was forwarded to
the owner over the Cluster Control Link.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-drop-on-slave
Flow matched a cluster drop-on-slave classify rule:
    This is for cases that the packets from L3 subnet are seen by all units and only
master unit need to process them.

Recommendations:
    This counter is informational and the behavior expected. The packet is processed by
master.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-director-change
The flow director changed due to a cluster join event:
    A new unit joined the cluster and is now the director for the flow. The old
director/backup has removed it's flow and the flow owner will update the new director.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-mcast-owner-change
The multicast flow owner changed due to a cluster join or leave event:
     This flow gets created on a new owner unit.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-convert-to-dirbak
Forwarding or redirect flow converted to director or backup flow:
    Forwarding or redirect flow is removed, so that director or backup flow can be
created.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
```

```
Name: inspect-scansafe-server-not-reachable
Scansafe server is not configured or the cloud is down:
    Either the scansafe server IP is not specified in the scansafe general options or the
scansafe server is not reachable.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-director-closed
Flow removed due to director flow closed:
    Owner unit received a cluster flow clu delete message from the director unit and
terminated the flow.

Recommendation:
    This counter should increment for every replicated clu that is torn down on the
director unit.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-pinhole-master-change
Master only pinhole flow removed at bulk sync due to master change:
    Master only pinhole flow is removed during bulk sync because cluster master has
changed.

Recommendation:
    This counter is informational and the behavior expected.

Syslogs:
    302014


----------------------------------------------------------------
Name: cluster-parent-owner-left
Flow removed at bulk sync becasue parent flow is gone:
    Flow is removed during bulk sync becasue the parent flow's owner has left the cluster.

Recommendation:
    This counter is informational and the behavior expected.

Syslogs:
    302014


----------------------------------------------------------------
Name: cluster-ctp-punt-channel-missing
Flow removed at bulk sync becasue CTP punt channel is missing:
    Flow is removed during bulk sync because CTP punt channel is missing in cluster
restored flow.

Recommendation:
    The cluster master may have just left the cluster. And there might be packet drops on
the Cluster Control Link.

Syslogs:
    302014
```

```
------------------------------------------------------------------
Name: vpn-overlap-conflict

VPN Network Overlap Conflict:
When a packet is decrypted, the inner packet is examined against the crypto map
configuration.  If the packet matches a different crypto map entry than the one it was
received on, it will be dropped and this counter will increment.  A common cause for this
is two crypto map entries containing similar/overlapping address spaces.

Recommendation:
    Check your VPN configuration for overlapping networks. Verify the
    order of your crypto maps and use of deny rules in ACLs.

Syslogs:
    None


------------------------------------------------------------------
```

Examples

The following is sample output from the **show asp drop** command, with the timestamp indicating the last time the counters were cleared:

```
hostname# show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                           3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                       4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                          760
  Expired flow (flow-expired)                                            1

Last clearing: Never

Flow drop:
  Flow is denied by access rule (acl-drop)                              24
  NAT failed (nat-failed)                                            28739
  NAT reverse path failed (nat-rpf-failed)                           22266
  Inspection failure (inspect-fail)                                  19433

Last clearing: 17:02:12 UTC Jan 17 2012 by enable_15
```

Related Commands

Command	Description
capture	Captures packets, including the option to capture packets based on an ASP drop code.
clear asp drop	Clears drop statistics for the accelerated security path.
show conn	Shows information about connections.

show asp event dp-cp

To debug the data path or control path event queues, use the **show asp event dp-cp** command in privileged EXEC mode.

show asp event dp-cp [**cxsc msg**]

Syntax Description

cxsc msg	(Optional) Identifies the CXSC event messages that are sent to the CXSC event queue.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
9.0(1)	This command was introduced.
9.1(3)	A routing event queue entry was added.

Usage Guidelines

The **show asp event dp-cp** command shows the contents of the data path and control path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the data path and control path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp event dp-cp** command:

```
hostname# show asp event dp-cp

DP-CP EVENT QUEUE                 QUEUE-LEN  HIGH-WATER
Punt Event Queue                          0        2048
Routing Event Queue                       0           1
Identity-Traffic Event Queue              0          17
General Event Queue                       0           0
Syslog Event Queue                        0        3192
Non-Blocking Event Queue                  0           4
Midpath High Event Queue                  0           0
Midpath Norm Event Queue                  0           0
SRTP Event Queue                          0           0
HA Event Queue                            0           3
Threat-Detection Event Queue              0           3
```

```
ARP Event Queue                          0           3
IDFW Event Queue                         0           0
CXSC Event Queue                         0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt              4005920          0   935295  3070625  4005920       4372
  inspect-sunrp   4005920          0   935295  3070625  4005920       4372
routing              77          0       77        0       77          0
arp-in              618          0      618        0      618          0
identity-traffic   1519          0     1519        0     1519          0
syslog             5501          0     5501        0     5501          0
threat-detection     12          0       12        0       12          0
ips-cplane         1047          0     1047        0     1047          0
ha-msg              520          0      520        0      520          0
cxsc-msg            127          0      127        0      127          0
```

show asp load-balance

To display a histogram of the load balancer queue sizes, use the **show asp load-balance** command in privileged EXEC mode.

show asp load-balance [**detail**]

Syntax Description

detail	(Optional) Shows detailed information about hash buckets.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
8.1(1)	This command was introduced.

Usage Guidelines

The **show asp load-balance** command might help you troubleshoot a problem. Normally a packet will be processed by the same core that pulled it in from the interface receive ring. However, if another core is already processing the same connection as the packet just received, then the packet will be queued to that core. This queuing can cause the load balancer queue to grow while other cores are idle. See the **asp load-balance per-packet** command for more information.

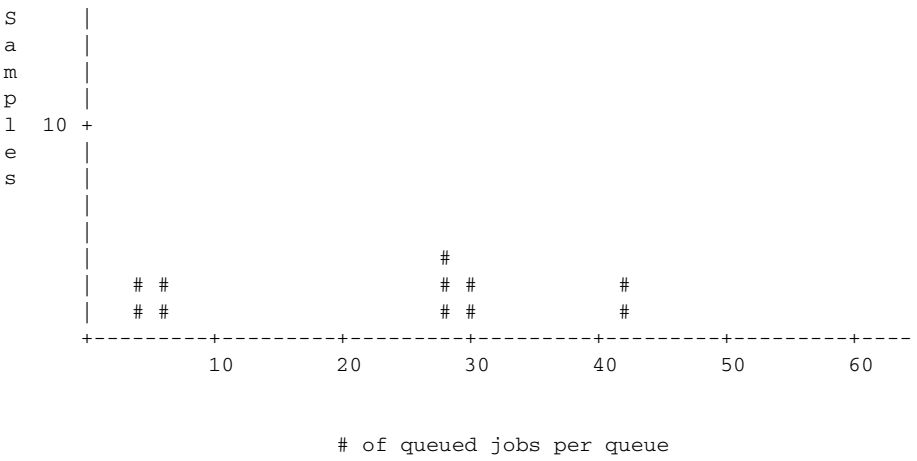
Examples

The following is sample output from the **show asp load-balance** command. The X-axis represents the number of packets queued in different queues. The Y-axis represents the number of load balancer hash buckets (not to be confused with the bucket in the histogram title, which refers to the histogram bucket) that has packets queued. To know the exact number of hash buckets having the queue, use the **detail** keyword.

```
hostname# show asp load-balance

Histogram of 'ASP load balancer queue sizes'
  64 buckets sampling from 1 to 65 (1 per bucket)
  6 samples within range (average=23)
                     ASP load balancer queue sizes

  100 +
      |
      |
      |
```



The following is sample output from the **show asp load-balance detail** command.

```
hostname# show asp load-balance detail

<Same histogram output as before with the addition of the following values for the
histogram>

Data points:
<snip>
  bucket[1-1] = 0 samples
  bucket[2-2] = 0 samples
  bucket[3-3] = 0 samples
  bucket[4-4] = 1 samples
  bucket[5-5] = 0 samples
  bucket[6-6] = 1 samples
<snip>
  bucket[28-28] = 2 samples
  bucket[29-29] = 0 samples
  bucket[30-30] = 1 samples
<snip>
  bucket[41-41] = 0 samples
  bucket[42-42] = 1 samples
```

RelatedCommands

Command	Description
asp load-balance per-packet	Changes the core load balancing method for multi-core ASA models.

show asp table arp

To debug the accelerated security path ARP tables, use the **show asp table arp** command in privileged EXEC mode.

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

Syntax Description

address *ip_address*	(Optional) Identifies an IP address for which you want to view ARP table entries.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the ARP table.
netmask *mask*	(Optional) Sets the subnet mask for the IP address.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show arp** command shows the contents of the control plane, while the **show asp table arp** command shows the contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table arp** command:

```
hostname# show asp table arp

Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0

Context: single_vf, Interface: identity
```

```
::                                      Active   0000.0000.0000 hits 0
0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

Related Commands

Command	Description
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.

show asp table classify

To debug the accelerated security path classifier tables, use the **show asp table classify** command in privileged EXEC mode.

s**how asp table classify** [**interface** *interface_name*] [**crypto** | **domain** *domain_name*] [**hits**] [**match** *regexp*] [**user-statistics**]

Syntax Description

crypto	(Optional) Shows the encrypt, decrypt, and ipsec tunnel flow domains only.
domain *domain_name*	(Optional) Shows entries for a specific classifier domain. See the "Usage Guidelines" section for a list of domains.
hits	(Optional) Shows classifier entries that have non-zero hits values.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the classifier table.
match *regexp*	(Optional) Shows classifier entries that match the regular expression. Use quotes when regular expressions include spaces.
user-statistics	(Optional) Specifies user and group information.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(4)	Added the **hits** option and the timestamp to indicate the last time the ASP table counters were cleared.
8.0(2)	A new counter was added to show the number of times a match compilation was aborted. This counter is shown only if the value is greater than 0.
8.2(2)	Added the **match** *regexp* option.
8.4(4.1)	Added the **csxc** and **cxsc-auth-proxy** domains for the ASA CX module.
9.0(1)	The **user-statistics** keyword was added. The output was updated to add security group names and source and destination tags.

Usage Guidelines

The **show asp table classify** command shows the classifier contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. The classifier examines properties of incoming packets, such as protocol, and source and destination address, to match each packet to an appropriate classification rule. Each rule is labeled with a classification domain that determines what types of actions are performed, such as dropping a packet or allowing it through. The information shown is used for debugging purposes only, and the output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Classifier domains include the following:

```
aaa-acct
aaa-auth
aaa-user
accounting
app-redirect
arp
autorp
backup interface CLI (Apply backup interface rule)
capture
cluster-drop-mcast-from-peer
cluster-drop-on-non-owner
cluster-drop-on-slave
cluster-mark-mcast-from-peer
cluster-redirect
conn-nailed
conn-set
ctcp
cxsc
cxsc-auth-proxy
debug-icmp-trace
decrypt
dhcp
dynamic-filter
eigrp
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
flow-export
host
host-limit
hqf
ids
inspect-ctiqbe
inspect-dcerpc
inspect-dns-cp
inspect-dns-ids
inspect-dns-np
inspect-ftp
inspect-ftp-data
inspect-gtp
inspect-h323
inspect-http
inspect-icmp
inspect-icmp-error
inspect-ils
inspect-im
inspect-ip-options
```

```
inspect-ipsec-pass-thru
inspect-ipv6
inspect-mgcp
inspect-mmp
inspect-netbios
inspect-phone-proxy
inspect-pptp
inspect-rsh
inspect-rtsp
inspect-scansafe
inspect-sip
inspect-skinny
inspect-smtp
inspect-snmp
inspect-sqlnet
inspect-sqlnet-plus
inspect-srtp
inspect-sunrpc
inspect-tftp
inspect-waas
inspect-xdmcp
ipsec-natt
ipsec-tunnel-flow
ipv6
l2tp
l2tp-ppp
limits
lu
mgmt-lockdown
mgmt-tcp-intercept
multicast
nat
nat-per-session
nat-reverse
no forward CLI (Apply no forward interface rule)
null
ospf
permit
permit-ip-option
permit-ip-option-explicit
pim
ppp
priority-q
punt
punt-root (soft NP)
qos
qos-per-class (soft NP)
qos-per-dest  (soft NP)
qos-per-flow  (soft NP)
qos-per-source (soft NP)
rip
sal-relay
shun
soft-np-tcp-module
soft-np-udp-module
splitdns
ssm
ssm-app-capacity
ssm-isvw
ssm-isvw-capable
svc-ib-tunnel-flow
svc-ob-tunnel-flow
tcp-intercept
tcp-ping
```

```
udp-unidirectional
user-statistics
vpn-user
wccp
```

Examples

The following is sample output from the **show asp table classify** command:

```
hostname# show asp table classify

Interface test:
No. of aborted compiles for input action table 0x33b3d70: 29
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=10.86.194.60, mask=255.255.255.255, port=0
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
...
```

The following is sample output from the **show asp table classify hits** command with a record of the last clearing hits counters:

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
       hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
       hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000,
       mask=0000.0000.0000 dst mac=0000.0000.0000, mask=0000.0000.0000
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
```

The following is sample output from the **show asp table classify hits** command that includes Layer 2 information:

```
Input Table
in  id=0x7fff2de10ae0, priority=120, domain=permit, deny=false
    hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1
    src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=identity in  id=0x7fff2de135c0, priority=0,
domain=inspect-ip-options, deny=true
    hits=41, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
```

```
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=any

.
.
.

Output Table:

L2 - Output Table:

L2 - Input Table:
in  id=0x7fff2de0e080, priority=1, domain=permit, deny=false
    hits=30, user_data=0x0, cs_id=0x0, l3_type=0x608
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0000.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e580, priority=1, domain=permit, deny=false
    hits=382, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0100.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e800, priority=1, domain=permit, deny=false
    hits=312, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=ffff.ffff.ffff, mask=ffff.ffff.ffff
    input_ifc=LAN-SEGMENT, output_ifc=any
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show asp table cluster chash-table

To debug the accelerated security path cHash tables for clustering, use the **show asp table cluster chash-table** command in privileged EXEC mode.

show asp table cluster chash-table

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

The **show asp table cluster chash-table** command shows the contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table cluster chash-table** command:

```
hostname# show asp table cluster chash-table
Cluster current chash table:

00003333
21001200
22000033
02222223
33331111
21110000
00133103
22222223
30000102
11222222
23222331
00002223
33111111
```

```
11000112
22332000
00231121
11222220
33330223
31013211
11101111
13111111
11023133
30001100
00000111
12022222
00133333
33222000
00022222
33011333
11110002
33333322
13333030
```

Related Commands

Command	Description
show asp cluster counter	Shows cluster datapath counter information.

show asp table cts sgt-map

To show the IP address-security group table mapping from the IP address-security group table database that is maintained in the data path for Cisco TrustSec, use the **show asp table cts sgt-map** command in privileged EXEC mode.

show asp table cts sgt-map [**address** *ipv4* | **address** *ipv6* | **ipv4** | **ipv6** | **sgt** *sgt*]

Syntax Description

address *ipv4*	(Optional) Shows the IP address-security group table mapping for the specified IPv4 addresses.
address *ipv6*	(Optional) Shows the IP address-security group table mapping for the specified IPv6 addresses.
ipv4	(Optional) Shows all of the IP address-security group table mapping for IPv4 addresses.
ipv6	(Optional) Shows all of the IP address-security group table mapping for IPv6 addresses.
sgt *sgt*	(Optional) Shows the IP address-security group table mapping for the specified security group table.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

If the address is not specified, then all the entries in the the IP address-security group table database in the data path appear. The address can be an exact address or a subnet-based address. In addition, the security group names appear when available.

Examples

The following is sample output from the **show asp table cts sgt-map** command:

```
hostname# show asp table cts sgt-map

IP Address                      SGT
================================================
10.10.10.5                      1234:Marketing
```

```
55.67.89.12                         5:Engineering
56.34.0.0                           338:HR
192.4.4.4                           345:Finance

Total number of entries shown = 4
```

The following is sample output from the **show asp table cts sgt-map address** command:

```
hostname# show asp table cts sgt-map address 10.10.10.5

IP Address                          SGT
================================================
10.10.10.5                          1234:Marketing

Total number of entries shown = 1
```

The following is sample output from the **show asp table cts sgt-map ipv6** command:

```
hostname# show asp table cts sgt-map ipv6

IP Address                                SGT
============================================================
FE80::A8BB:CCFF:FE00:110                  17:Marketing-Servers
FE80::A8BB:CCFF:FE00:120                  18:Eng-Servers

Total number of entries shown = 2
```

The following is sample output from the **show asp table cts sgt-map sgt** command:

```
hostname# show asp table cts sgt-map sgt 17

IP Address                                SGT
============================================
FE80::A8BB:CCFF:FE00:110                  17

Total number of entries shown = 1
```

Related Commands

Command	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts environment	Shows the health and status of the environment data refresh operation.

show asp table dynamic-filter

To debug the accelerated security path Botnet Traffic Filter tables, use the **show asp table dynamic-filter** command in privileged EXEC mode.

show asp table dynamic-filter [**hits**]

Syntax Description

hits	(Optional) Shows classifier entries which have non-zero hits values.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

The **show asp table dynamic-filter** command shows the Botnet Traffic Filter rules in the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table dynamic-filter** command:

```
hostname# show asp table dynamic-filter

Context: admin
 Address 10.246.235.42 mask 255.255.255.255 name: example.info
flags: 0x44 hits 0
 Address 10.40.9.250 mask 255.255.255.255 name: bad3.example.com
flags: 0x44 hits 0
 Address 10.64.147.20 mask 255.255.255.255 name: bad2.example.com flags: 0x44
hits 0
 Address 10.73.210.121 mask 255.255.255.255 name: bad1.example.com flags:
0x44 hits 0
 Address 10.34.131.135 mask 255.255.255.255 name: bad.example.com flags:
0x44 hits 0
 Address 10.64.147.16 mask 255.255.255.255 name:
1st-software-downloads.com flags: 0x44 hits 2
 Address 10.131.36.158 mask 255.255.255.255 name: www.example.com flags: 0x41 hits 0
```

```
 Address 10.129.205.209 mask 255.255.255.255 flags: 0x1 hits 0
 Address 10.166.20.10 mask 255.255.255.255 flags: 0x1 hits 0
...
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

show asp table filter

To debug the accelerated security path filter tables, use the **show asp table filter** command in privileged EXEC mode.

show asp table filter [**access-list** *acl-name*] [**hits**] [**match** *regexp*]

Syntax Description

acl-name	(Optional) Specifies the installed filter for a specified access list.
hits	(Optional) Specifies the filter rules that have non-zero hits values.
match *regexp*	(optional) Shows classifier entries that match the regular expression. Use quotes when regular expressions include spaces.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
8.2(2)	This command was introduced.

Usage Guidelines

When a filter has been applied to a VPN tunnel, the filter rules are installed into the filter table. If the tunnel has a filter specified, then the filter table is checked before encryption and after decryption to determine whether the inner packet should be permitted or denied.

Examples

The following is sample output from the **show asp table filter** command before a user1 connects. Only the implicit deny rules are installed for IPv4 and IPv6 in both the inbound and outbound directions.

```
hostname# show asp table filter

Global Filter Table:
 in  id=0xd616ef20, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd613ea60, filter_id=0x0(-implicit deny-), protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f420, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd615ef70, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
 out id=0xd616f1a0, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd614d900, filter_id=0x0(-implicit deny-), protocol=0
```

```
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd616f6d0, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd6161638, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
```

The following is sample output from the **show asp table filter** command after a user1 has connected. VPN filter ACLs are defined based on the inbound direction—the source represents the peer and the destination represents inside resources. The outbound rules are derived by swapping the source and destination for the inbound rule.

```
hostname# show asp table filter

Global Filter Table:
 in  id=0xd682f4a0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd682f460, filter_id=0x2(vpnfilter), protocol=6
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=21
 in  id=0xd68366a0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd6d89050, filter_id=0x2(vpnfilter), protocol=6
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=5001
 in  id=0xd45d5b08, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d5ac8, filter_id=0x2(vpnfilter), protocol=17
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=5002
 in  id=0xd6244f30, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd6244ef0, filter_id=0x2(vpnfilter), protocol=1
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=95.1.224.100, mask=255.255.255.255, port=0
 in  id=0xd64edca8, priority=12, domain=vpn-user, deny=true
        hits=0, user_data=0xd64edc68, filter_id=0x2(vpnfilter), protocol=1
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f018, priority=11, domain=vpn-user, deny=true
        hits=43, user_data=0xd613eb58, filter_id=0x0(-implicit deny-), protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f518, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd615f068, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
 out id=0xd7395650, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd7395610, filter_id=0x2(vpnfilter), protocol=6
        src ip=95.1.224.100, mask=255.255.255.255, port=21
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d49b8, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d4978, filter_id=0x2(vpnfilter), protocol=6
        src ip=95.1.224.100, mask=255.255.255.255, port=5001
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d5cf0, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd45d5cb0, filter_id=0x2(vpnfilter), protocol=17
        src ip=95.1.224.100, mask=255.255.255.255, port=5002
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd6245118, priority=12, domain=vpn-user, deny=false
        hits=0, user_data=0xd62450d8, filter_id=0x2(vpnfilter), protocol=1
        src ip=95.1.224.100, mask=255.255.255.255, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd64ede90, priority=12, domain=vpn-user, deny=true
        hits=0, user_data=0xd64ede50, filter_id=0x2(vpnfilter), protocol=1
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
```

```
out id=0xd616f298, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd614d9f8, filter_id=0x0(-implicit deny-), protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
out id=0xd616f7c8, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd6161730, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.
show asp table classifier	**S**hows the classifier contents of the accelerated security path.

show asp table interfaces

To debug the accelerated security path interface tables, use the **show asp table interfaces** command in privileged EXEC mode.

show asp table interfaces

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show asp table interfaces** command shows the interface table contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table interfaces** command:

```
hostname# show asp table interfaces

** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20

Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20
```

```
Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show asp table routing

To debug the accelerated security path routing tables, use the **show asp table routing** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

show asp table routing [**input** | **output**] [**address** *ip_address* [**netmask** *mask*] | **interface** *interface_name*]

Syntax Description

address *ip_address*	Sets the IP address for which you want to view routing entries. For IPv6 addresses, you can include the subnet mask as a slash (/) followed by the prefix (0 to 128). For example, enter the following: `fe80::2e0:b6ff:fe01:3b7a/128`
input	Shows the entries from the input route table.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the routing table.
netmask *mask*	For IPv4 addresses, specifies the subnet mask.
output	Shows the entries from the output route table.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **show asp table routing** command shows the routing table contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Note Invalid entries may appear in the show asp table routing command output on the ASA 5505.

Examples

The following is sample output from the **show asp table routing** command:

```
hostname# show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

Note Invalid entries in the **show asp table routing** command output may appear on the ASA 5505 platform. Ignore these entries; they have no effect.

Related Commands

Command	Description
show route	Shows the routing table in the control plane.

show asp table socket

To help debug the accelerated security path socket information, use the **show asp table socket** command in privileged EXEC mode.

show asp table socket [**socket handle**] [**stats**]

Syntax Description

socket handle	Specifies the length of the socket.
stats	Shows the statistics from the accelerated security path socket table.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **show asp table socket** command shows the accelerated security path socket information, which might help in troubleshooting accelerated security path socket problems. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table socket** command:

```
TCP Statistics:
  Rcvd:
     total14794
     checksum errors0
     no port0
  Sent:
     total0

UDP Statistics:
  Rcvd:
     total0
     checksum errors0
  Sent:
     total0
```

```
     copied0

NP SSL System Stats:
  Handshake Started:33
  Handshake Complete:33
  SSL Open:4
  SSL Close:117
  SSL Server:58
  SSL Server Verify:0
  SSL Client:0
```

TCP/UDP statistics are packet counters representing the number of packets sent or received that are directed to a service that is running or listening on the ASA, such as Telnet, SSH, or HTTPS. Checksum errors are the number of packets dropped because the calculated packet checksum did not match the checksum value stored in the packet (that is, the packet was corrupted). The NP SSL statistics indicate the number of each type of message received. Most indicate the start and completion of new SSL connections to either the SSL server or SSL client.

Related Commands

Command	Description
show asp table vpn-context	Shows the accelerated security path VPN context tables.

show asp table vpn-context

To debug the accelerated security path VPN context tables, use the **show asp table vpn-context** command in privileged EXEC mode.

show asp table vpn-context [**detail**]

Syntax Description

detail	(Optional) Shows additional detail for the VPN context tables.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.
8.0(4)	Added +PRESERVE flag for each context that maintains stateful flows after the tunnel drops.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **show asp table vpn-context** command shows the VPN context contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table vpn-context** command:

```
hostname# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

The following is sample output from the **show asp table vpn-context** command when the persistent IPsec tunneled flows feature is enabled, as shown by the PRESERVE flag:

```
hostname(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

The following is sample output from the **show asp table vpn-context detail** command:

```
hostname# show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

The following is sample output from the **show asp table vpn-context detail** command when the persistent IPsec tunneled flows feature is enabled, as shown by the PRESERVE flag.:

```
hostname(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54

Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
```

```
VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
hostname(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.