# show asp drop Command Usage

**First Published:** 2005-05-31

**Last Modified:** 2023-12-13

## 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. Use **?** to see a list of possible flow drop reasons. |
| **frame***frame_drop_reason* | (Optional) Shows the dropped packets. You can specify a particular reason by using the *frame_drop_reason* argument. Use **?** to see a list of possible frame drop reasons. |

### Command Default

No default behavior or values.

### Command Modes

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

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

### Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |
| 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 general operations 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, on page 2
- Flow Drop Reasons, on page 115


# 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: 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: ipsec-tun-need-swap
Needed to swap to another IPSEC tunnel:
    This counter will increment when the appliance receives a packet associated with an
IPSec connection that went down and needs to swapped to another IPSec connection.

 Recommendation:
    This is a normal condition when an IPSec tunnel goes down and the packet can be moved
to another IPSec Tunnel. If this happens frequently, investigate IPSec tunnel failures.

 Syslogs:
    None


----------------------------------------------------------------
Name: invalid-encryption-packet
Invalid encryption packet received:
    This counter will increment when the appliance receives a packet associated with an
IPSec connection on a flow that does not have encrypt flags 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 traffic disruption, then this may be
caused by a misconfiguration or a software defect.

 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-send-cp-fail
SVC Module send CP error failed:
    This counter will increment when the security appliance cannot send the error information
 to CP.

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-session-frag-fail
SVC Module failed to send frag fail:
    This counter will increment when the security appliance cannot generate ICMP error
message.

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-decompress-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-invalid-src-addr
SVC Module found invalid inner SRC address:
    This counter will increment when the security appliance is finds an invalid inner src
address 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:
    Use packet capture of type asp-drop to determine the direction of the packet. Most often
 this indicates that the client is unable to accept more data. On rare occasion, the counter
 can indicate the appliance cannot handle the inbound traffic if the packet direcion is
towards the appliance.

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: mp-svc-bad-compress
SVC Module unable to compress a packet:
    This counter is incremented when a packet to be sent to an AnyConnect client is not
able to be compressed.

Recommendation:
    Disable all compression for the AnyConnect client.

Syslogs:
    None.


-------------------------------------------------------------------
Name: mp-svc-bad-decompress
SVC Module unable to decompress a packet:
    This counter is incremented when a packet received from an AnyConnect client is not
able to be decompressed.

Recommendation:
    Disable all compression for the AnyConnect client.

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: 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: 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-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


----------------------------------------------------------------
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: 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; its 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: 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: ttl-exceeded
ttl exceeded:
    This counter is incremented when the security appliance receives an IP packet whose
value of ttl(time to live) has exceeded the allowed limit. Specifically if the packet has
ttl value of 1, when set connection decrement-ttl command is configured, or less than 1,
the packet is dropped.

Syslogs:
    None.


-----------------------------------------------------------------
Name: hop-limit-exceeded
hop-limit exceeded:
    This counter is incremented when the security appliance receives an IPv6 packet whose
value of hop-limit has exceeded the allowed limit. Specifically if the packet has hop-limit
 less than 1, the packet is dropped.

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: invalid-sctp-length
Invalid SCTP Length:
    This counter is incremented when the security appliance recieves a SCTP packet whose
common header size is less than the required common header size (12 bytes).

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

Syslog:
    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: invalid-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: no-v4-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: no-v6-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: no-paired-ifc
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 it's 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 thegenerated syslog.

Syslogs:
   110001.


----------------------------------------------------------------
Name: invalid-vxlan-segment-id
Invalid VXLAN segment-id:
    This counter is incremented when the security appliance decapsulates a VXLAN packet
which has an invalid segment-id.

Recommendation:
    No.

Syslogs:
   778001.


----------------------------------------------------------------
Name: invalid-geneve-segment-id
Invalid Geneve segment-id:
    This counter is incremented when the security appliance decapsulates a Geneve packet
which has an invalid segment-id.

Recommendation:
    No.

Syslogs:
   860001.


----------------------------------------------------------------
Name: invalid-vxlan-segment-id-tvi
Invalid VXLAN segment-id on TVI:
    This counter is incremented when the TVI interface processes a VXLAN packet which has
an invalid segment-id.

Recommendation:
    No.

Syslogs:
   No.


----------------------------------------------------------------
Name: sts-lookup-failure
STS lookup failure:
    This counter is incremented when the security appliance fails to lookup for the out tag
```

```
 for a given in tag when tag switching is enabled on the VNI interface.

Recommendation:
    Verify that an out tag exists for the in tag obtained from thegenerated syslog.

Syslogs:
   779001.


----------------------------------------------------------------
Name: no-valid-vni-ifc
No valid VNI interface:
    This counter is incremented when the security appliance fails to identify the VNI
interface by a given segment-id.

Recommendation:
    Verify that the segment-id in the syslog is configured on an interface.

Syslogs:
   778002.


----------------------------------------------------------------
Name: no-valid-nve-ifc
No valid NVE interface:
    This counter is incremented when the security appliance fails to identify the NVE
interface for a VNI interface.

Recommendation:
    Verify that the nve is configured for all interfaces.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-peer-nve
Invalid peer NVE:
    This counter is incremented when the security appliance fails to get IP and MAC address
 of a peer NVE.

Recommendation:
    Verify that peer nve is configured or learned for the nve.

Syslogs:
    None.


----------------------------------------------------------------
Name: vxlan-encap-error
Fail to encap with VXLAN:
    This counter is incremented when the security appliance fails to encapsulate a packet
with VXLAN.

Recommendation:
    No.

Syslogs:
    None.


----------------------------------------------------------------
Name: geneve-encap-error
Fail to encap with Geneve:
```

```
    This counter is incremented when the security appliance fails to encapsulate a packet
with Geneve.

Recommendation:
    No.

Syslogs:
    None.


----------------------------------------------------------------
Name: sts-nat-diff-egress
STS locates different egress from NAT:
   This counter is incremented when the security appliance locates different egress interface
 by STS and NAT.

Recommendation:
    Verify that the NAT configuration on interface shown in the syslog is correct.

Syslogs:
   779002.


----------------------------------------------------------------
Name: invalid-vxlan-segment-id-fp
Invalid VXLAN in-tag:
    This counter is incremented when the security appliance decapsulates a VXLAN packet in
 FP which has an invalid segment-id.

Recommendation:
    No.

Syslogs:
    778003.


----------------------------------------------------------------
Name: vxlan-invalid-header
Invalid VXLAN header format:
    This counter is increamented when the security appliance receives a UDP packet with
correct VXLAN destination port number but failed to decode the VXLAN header.

Recommendation:
    No.

Syslogs:
    778004.


----------------------------------------------------------------
Name: vxlan-invalid-header-thru-traffic
Invalid VXLAN header format for through-the-box traffic:
    This counter is increamented when the security appliance receives a through-the-box UDP
 packet with correct VXLAN destination port number but failed to decode the VXLAN header.

Recommendation:
    No.

Syslogs:
    778008.


----------------------------------------------------------------
Name: vxlan-invalid-udp-checksum
```

```
Invalid VXLAN header format:
    This counter is increamented when the security appliance receives a VXLAN packet with
incorrect checksum value in UDP header.

Recommendation:
    No.

Syslogs:
    778006.


----------------------------------------------------------------
Name: vxlan-invalid-nve-peer
VXLAN packet from an invalid NVE peer:
    This counter is increamented when the security appliance receives a VXLAN packet from
an NVE peer that is not configured.

Recommendation:
    No.

Syslogs:
    778007.


----------------------------------------------------------------
Name: no-route-to-peer-nve
No route to peer NVE:
    This counter is incremented when the security appliance fails to locate next hop to
peer NVE.

Recommendation:
    Verify peer NVE is reachable via source-interface.

Syslogs:
    None.


----------------------------------------------------------------
Name: vxlan-invalid-vni-mcast-ip
Invalid Multicast IP on VNI interface:
   This counter is incremented when the security appliance fails to get the multicast group
 IP from the VNI interface.

Recommendation:
    Verify that in the absence of a configured peer NVE, the VNI     interface has a valid
 multicast group IP configured on it.

Syslogs:
    None.


----------------------------------------------------------------
Name: vxlan-missing-peer-vtep-ip
Peer VTEP IP not found:
    This counter is incremented when the security appliance fails to find the peer VTEP IP
 for an inner destnation IP for VXLAN encapsulation.

Recommendation:
    Verify that in show arp vtep-mapping/show mac-address-table     vtep-mapping/show ipv6
 neighbor vtep-mapping, the VTEP IP is     present for the desired remote inner host.

Syslogs:
    None.
```

```
-----------------------------------------------------------------
Name: vxlan-ccl-inner-dip-not-found
Peer CCL inner IP not found:
    This counter is incremented when the security appliance fails to find Peer's CCL inner
 destination IP.

Recommendation:
    No.

Syslogs:
    None.


-----------------------------------------------------------------
Name: invalid-geneve-segment-id-fp
Invalid VXLAN in-tag:
    This counter is incremented when the security appliance decapsulates a VXLAN packet in
 FP which has an invalid segment-id.

Recommendation:
    No.

Syslogs:
    778003.


-----------------------------------------------------------------
Name: geneve-invalid-header
Invalid Geneve header format:
    This counter is increamented when the security appliance receives a UDP packet with
correct Geneve destination port number but failed to decode the Geneve header.

Recommendation:
    No.

Syslogs:
    860004.


-----------------------------------------------------------------
Name: geneve-invalid-header-thru-traffic
Invalid Geneve header format for through-the-box traffic:
    This counter is increamented when the security appliance receives a through-the-box UDP
 packet with correct Geneve destination port number but failed to decode the Geneve header.

Recommendation:
    No.

Syslogs:
    860008.


-----------------------------------------------------------------
Name: geneve-invalid-udp-checksum
Invalid GENEVE header format:
    This counter is increamented when the security appliance receives a Geneve packet with
 incorrect checksum value in UDP header.

Recommendation:
    No.

Syslogs:
    860006.
```

```
------------------------------------------------------------------
Name: geneve-invalid-nve-peer
Geneve packet from an invalid NVE peer:
    This counter is increamented when the security appliance receives a Geneve packet from
 an NVE peer that is not configured.

Recommendation:
    No.

Syslogs:
    860007.


------------------------------------------------------------------
Name: geneve-invalid-vni-mcast-ip
Invalid Multicast IP on Geneve VNI interface:
   This counter is incremented when the security appliance fails to get the multicast group
 IP from the VNI interface.

Recommendation:
    Verify that in the absence of a configured peer NVE, the VNI     interface has a valid
 multicast group IP configured on it.

Syslogs:
    None.


------------------------------------------------------------------
Name: geneve-missing-peer-vtep-ip
Geneve Peer VTEP IP not found:
    This counter is incremented when the security appliance fails to find the peer VTEP IP
 for an inner destnation IP for Geneve encapsulation.

Recommendation:
    Verify that in show arp vtep-mapping/show mac-address-table     vtep-mapping/show ipv6
 neighbor vtep-mapping, the VTEP IP is     present for the desired remote inner host.

Syslogs:
    None.


------------------------------------------------------------------
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: no-same-security-traffic
No same-security-traffic configured:
    This counter is incremented when the decrypt and encrypt tunnel is owned by the same
interface and same-security-traffic is not configured.

Recommendation:
    Configure "same-security-traffic permit intra-interface".

Syslogs:
    None.


----------------------------------------------------------------
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: permit-validate
Permit validation failed:
    This reason is given for dropping a packet during the initial connection establishment
 when the registered validation for this listener fails.

Recommendation:
```

```
    If this is incrementing rapidly, check syslogs to determine which host is failing
validation on the given listener.

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: sctp-no-association
SCTP no association:
    This counter is incremented and the packet is dropped when no matching association exist
 for this packet.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-pkt-too-small
SCTP packet size less than minimum length of 16:
    This counter is incremented and the packet is dropped when SCTP packet size is less
then the combined size of common header and chunk header.

Recommendations:
    None

Syslogs:
    None


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

```
Name: sctp-pkt-partial_chunk
SCTP packet has partial chunk:
   This counter is incremented and the packet is dropped when SCTP packet contains a partial
 chunk.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-too-small
SCTP chunk length value is smaller then chunk header size:
    This counter is incremented and the packet is dropped when the SCTP chunk length value
 is less then the size of chunk header.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-too-small
SCTP chunk length value is smaller then the INIT chunk size:
    This counter is incremented and the packet is dropped when the SCTP chunk length value
 is less then the size of INIT chunk.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-param-too-small
SCTP INIT chunk parameter length value is smaller then the parameter header size:
    This counter is incremented and the packet is dropped when the SCTP parameter length
value is less then the size of parameter header.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-new-addr
SCTP restart INIT chunk contains new address:
    This counter is incremented and the packet is dropped when SCTP restart INIT chunk
contains new address.

Recommendations:
    None

Syslogs:
    None
```

```
----------------------------------------------------------------
Name: sctp-chunk-initack-too-small
SCTP chunk length value is smaller then the INIT ACK chunk size:
    This counter is incremented and the packet is dropped when the SCTP chunk length value
 is less then the size of INIT ACK chunk.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-in-shutdown
SCTP INIT is seen in shutdown state:
    This counter is incremented and the packet is dropped when SCTP INIT chunk is received
 in SHUTDOWN state.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-initack-no-matching-init
SCTP INITACK chunk has no matching INIT:
    This counter is incremented and the packet is dropped when SCTP INIT ACK chunk is
received with no matching INIT.

Recommendations:
    This drop can happen in a scenarios like when there are     redundant paths between
client and server or due to some     congestion in the network which could cause INIT ACK
to be received     after the connection created for INIT is torn down. If this     error
occurs in large numbers, please use packet capture     feature to help isolate the issue.

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-0-tag
SCTP INIT contains 0 value initiate tag:
    This counter is incremented and the packet is dropped when SCTP INIT chunk contains 0
value initiate tag.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-initack-0-tag
SCTP INIT ACK contains 0 value initiate tag:
    This counter is incremented and the packet is dropped when SCTP INIT ACK chunk contains
 0 value initiate tag.

Recommendations:
    None
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-rwnd-too-small
SCTP INIT receive-window value is too small:
   This counter is incremented and the packet is dropped when SCTP INIT chunk receive-window
 value is too small (less than 1500).

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-initack-rwnd-too-small
SCTP INIT ACK receive-window value is too small:
    This counter is incremented and the packet is dropped when SCTP INIT ACK chunk
receive-window value is too small (less than 1500).

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-0-stream-cnt
SCTP INIT contains 0 value inbound/outbound stream count:
    This counter is incremented and the packet is dropped when SCTP INIT chunk contains 0
value inbound/outbound stream count.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-ack-0-stream-cnt
SCTP INIT ACK contains 0 value inbound/outbound stream count:
    This counter is incremented and the packet is dropped when SCTP INIT ACK chunk contains
 0 value inbound/outbound stream count.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-inv-param-len
SCTP INIT ACK contains invalid parameter length value:
    This counter is incremented and the packet is dropped when SCTP INIT ACK chunk contains
 invalid parameter length value.

Recommendations:
    None
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-inv-ipv4-param-len
SCTP INIT contains invalid ipv4 parameter length value:
    This counter is incremented and the packet is dropped when SCTP INIT chunk contains
invalid ipv4 parameter length value.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-ack-inv-ipv4-param-len
SCTP INIT ACK contains invalid ipv4 parameter length value:
    This counter is incremented and the packet is dropped when SCTP INIT ACK chunk contains
 invalid ipv4 parameter length value.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-inv-ipv6-param-len
SCTP INIT contains invalid ipv6 parameter length value:
    This counter is incremented and the packet is dropped when SCTP INIT chunk contains
invalid ipv6 parameter length value.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-ack-inv-ipv6-param-len
SCTP INIT ACK contains invalid ipv6 parameter length value:
    This counter is incremented and the packet is dropped when SCTP INIT ACK chunk contains
 invalid ipv6 parameter length value.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-cookie-echo-no-assoc
SCTP COOKIE ECHO is received with no association:
    This counter is incremented and the packet is dropped when SCTP COOKIE ECHO chunk is
received without an association.

Recommendations:
```

```
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-chunk-cookie-ack-no-assoc
SCTP COOKIE ACK is received with no association:
    This counter is incremented and the packet is dropped when SCTP COOKIE ACK chunk is
received without an association.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-chunk-cookie-echo-cookie-len
SCTP COOKIE ECHO contains cookie with different length:
    This counter is incremented and the packet is dropped when SCTP COOKIE ECHO chunk
contains an echoed cookie with a different length.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-chunk-cookie-echo-in-close
SCTP COOKIE ECHO is received in CLOSED state:
    This counter is incremented and the packet is dropped when SCTP COOKIE ECHO chunk is
received in association CLOSED state.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-chunk-cookie-echo-in-shut
SCTP COOKIE ECHO is received during shutdown:
    This counter is incremented and the packet is dropped when SCTP COOKIE ECHO chunk is
received during association shutdown.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-chunk-cookie-ack-in-invalid-state
SCTP COOKIE ACK is not received in COOKIE ECHOED state:
    This counter is incremented and the packet is dropped when SCTP COOKIE ACK chunk is not
 received in COOKIE ECHOED state.
```

```
Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-chunk-shutdown-too-small
SCTP SHUTDOWN length is too small:
    This counter is incremented and the packet is dropped when SCTP SHUTDOWN chunk length
is too small.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-chunk-shutdown-in-invalid-state
SCTP SHUTDOWN is not received in valid state:
    This counter is incremented and the packet is dropped when SCTP SHUTDOWN chunk is not
received in valid state.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-chunk-shutdown-ack-in-invalid-state
SCTP SHUTDOWN ACK is not received in valid state:
    This counter is incremented and the packet is dropped when SCTP SHUTDOWN ACK chunk is
not received in valid state.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-chunk-shutdown-complete-in-invalid-state
SCTP SHUTDOWN COMPLETE is not received in valid state:
    This counter is incremented and the packet is dropped when SCTP SHUTDOWN COMPLETE chunk
 is not received in valid state.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-chunk-sack-in-invalid-state
SCTP SACK is not received in valid state:
    This counter is incremented and the packet is dropped when SCTP SACK chunk is not
received in valid state.
```

```
Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-sack-too-small
SCTP SACK length is too small:
    This counter is incremented and the packet is dropped when SCTP SACK chunk length is
too small.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-fwd-tsn-in-invalid-state
SCTP FWD TSN is not received in valid state:
    This counter is incremented and the packet is dropped when SCTP FORWARD CUMULATIVE TSN
 chunk is not received in valid state.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-fwd-tsn-too-small
SCTP FWD TSN length is too small:
    This counter is incremented and the packet is dropped when SCTP FORWARD CUMULATIVE TSN
 chunk length is too small.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-fwd-tsn-gap-out-of-range
SCTP FWD TSN gap is out of range:
    This counter is incremented and the packet is dropped when SCTP FORWARD CUMULATIVE TSN
 gap is out of range (100).

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-restart-bad-ip
SCTP INIT (restart) contains IP address not in previous INIT:
    This counter is incremented and the packet is dropped when SCTP INIT (restart) chunk
```

```
contains IP address that is not in previous INIT.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-asconf-auth-inconsistent
SCTP INIT contains contains ASCONF support without AUTH support:
    This counter is incremented and the packet is dropped when SCTP INIT chunk contains
contains ASCONF support without AUTH support.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-redundancy-auth-inconsistent
SCTP INIT contains contains REDUNDANCY support without AUTH support:
    This counter is incremented and the packet is dropped when SCTP INIT chunk contains
REDUNDANCY support without AUTH support.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-invalid-bundle
SCTP chunk bundle included INIT, INIT_ACK, or SHUTDOWN_COMPLETE:
    This counter is incremented and the packet is dropped when SCTP chunk bundle included
INIT, INIT_ACK, or SHUTDOWN_COMPLETE.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-invalid-bundle
SCTP packet bundle has control chunks after data chunks:
    This counter is incremented and the packet is dropped when SCTP packet has control
chunks present after data chunks and is dropped.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-unrec-param
SCTP chunk contains unrecognizable parameter:
```

```
    This counter is incremented and the packet is dropped when SCTP chunk contains
unrecognizable parameter.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-param-supaddrlen-inv
SCTP chunk parameter SUPPORTED ADDRESS contains invalid length:n    This counter is
incremented and the packet is dropped when SCTP INIT/INIT ACK chunk parameter SUPPORTED
ADDRESS contains invalid length (< 4).

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-pkt-auth-chunk-extra
SCTP packets contains more than one AUTH chunk:
    This counter is incremented and the packet is dropped when SCTP packet contains more
than one AUTH chunk.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-pkt-auth-chunk-no-data
SCTP packets contains only AUTH chunks:
    This counter is incremented and the packet is dropped when SCTP packet contains only
AUTH chunks.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-initack-chunk-inv-state
Received SCTP INIT ACK chunk in non-COOKIE-WAIT state:
    This counter is incremented and the packet is dropped when SCTP packet containing INIT
 ACK chunk is received in non-cookie-wait state.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-zero-ver-tag
```

```
Received SCTP non-INIT/ABORT chunk with zero verification tag:
    This counter is incremented and the packet is dropped when packet containing INIT/ABORT
 chunk has zero verification tag.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-inva-ver-tag
Received SCTP chunk with invalid verification tag:
    This counter is incremented and the packet is dropped when packet contains verification
 tag that does not match association tag.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-abort-chunk-unexpected
Received SCTP ABORT chunk unexpectedly:
    This counter is incremented and the packet is dropped when SCTP chunk is received
unexpectedly.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-shutack-chunk-unexpected
Received SCTP SHUTDOWN ACK chunk unexpectedly:
    This counter is incremented and the packet is dropped when SHUTDOWN ACK is received
unexpectedly.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-shutcomplete-chunk-unexpected
Received SCTP SHUTDOWN COMPLETE chunk unexpectedly:
    This counter is incremented and the packet is dropped when SHUTDOWN COMPLETE is received
 unexpectedly.

Recommendations:
    None

Syslogs:
    None


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

```
Name: sctp-chunk-unexpected
Received SCTP chunk unexpectedly:
    This counter is incremented and the packet is dropped when chunk is received unexpectedly.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-data-chunk-in-invalid-state
SCTP DATA chunk in invalid state:
    This counter is incremented and the packet is dropped when SCTP DATA chunk is received
 in invalid state.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-descriptor-unavailable
SCTP DATA chunk descriptor unavailable:
    This counter is incremented and the packet is dropped when SCTP chunk descriptor is
unavailable.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-dgram-header-unavailable
SCTP Datagram header unavailable:
    This counter is incremented and the packet is dropped when SCTP datagram header is
unavailable.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-stream-id-invalid
SCTP DATA chunk contains invalid stream id:
    This counter is incremented and the packet is dropped when SCTP DATA chunk contains
invalid stream id.

Recommendations:
    None

Syslogs:
    None


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

```
Name: sctp-data-chunk-len-invalid
SCTP DATA chunk length is invalid:
    This counter is incremented and the chunk is dropped when SCTP DATA chunk has invalid
chunk length.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-data-chunk-len-too-small
SCTP DATA chunk length is too small:
    This counter is incremented and the packet is dropped when SCTP DATA chunk length is
too small.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-data-chunk-len-exceeds-rwnd
SCTP DATA chunk length greater than receive window:
    This counter is incremented and the packet is dropped when SCTP DATA chunk length is
greater than receive window.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-duplicate-data-stream
Received duplicate SCTP DATA stream:
    This counter is incremented and the packet is dropped when a duplicate SCTP DATA stream
 is received.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name:  sctp queue-limit
SCTP Out-of-order queue full:
    This counter is incremented and the packet is dropped when the SCTP out of order packet
 queue exceeds the default limit 20.

Recommendations:
    None

Syslogs:
    None
```

```
----------------------------------------------------------------
Name:  sctp-reorder-queue-timeout
SCTP Reorder queue timeout:
    This counter is incremented and the data chunk is dropped when an out of order SCTP
data chunk has been held in the buffer for 30 seconds.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-drop-fixme
SCTP drop fixme:
    This counter is incremented when the security appliance recieves a SCTP packet with a
fixme drop reason

Recommendation:
    None.

Syslog:
    None.


----------------------------------------------------------------
Name: sctp-reorder-queue-limit
SCTP Reorder queue limit exceeded:
    This counter is incremented and the chunk is dropped when number of out of order chunks
 exceeds the limit(50/stream) for the stream.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-reassembly-queue-timeout
SCTP Reassembly queue timeout:
    This counter is incremented and the fragmented chunks are deleted from the reassembly
queue when those fragmented chunks has been held in the reassembly queue for 30 seconds.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-reassembly-queue-limit
SCTP Reassembly queue limit exceeded:
    This counter is incremented and the fragmented chunks are deleted from the reassembly
queue after the number of fragments in reassembly queue reaches its maximum(6).

Recommendations:
    None

Syslogs:
    None
```

```
-----------------------------------------------------------------
Name: sctp-reassembly-buffer-size-limit
SCTP Reassembly Datagram queue bytesize limit exceeded:
     This counter is incremented and the reassembly datagram is deleted from the stream
reassembly queue(all fragments) after the total bytesize of chunks in the dgram reassembly
 queue reaches its maximum(8192bytes).

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-reorder-stream-limit
SCTP Number of streams in reorder exceeded limit:
    This counter is incremented and the chunk is dropped when first out of order chunk is
received after the number ofStreams in Reorder reaches its maximum(64*number of cpu cores).

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-reassembly-system-limit
SCTP Reassembly Datagram queue limit exceeded:
    This counter is incremented and the reassembly datagram will not be created for the new
 incoming fragments after the number of datagrams in reassembly queues in ASA reaches its
maximum(125/core) We do repacking if the fragment is bundled else we drop the whole packet.


Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-invalid-fragments
SCTP invalid fragments received:
     This counter is incremented and all fragments in reassembly queue will be deleted
including the fragment which is not yet been queued.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: sctp-chunk-shutdown-no-assoc
SCTP SHUTDOWN is received with no association:
    This counter is incremented and the packet is dropped when SCTP SHUTDOWN chunk is
received without an association.

Recommendations:
    None
```

```
Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-shutdown-ack-no-assoc
SCTP SHUTDOWN ACK is received with no association:
    This counter is incremented and the packet is dropped when SCTP SHUTDOWN ACK chunk is
received without an association.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-shutdown-comp-no-assoc
SCTP SHUTDOWN COMPLETE is received with no association:
    This counter is incremented and the packet is dropped when SCTP SHUTDOWN COMPLETE chunk
 is received without an association.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-sack-no-assoc
SCTP SACK is received with no association:
    This counter is incremented and the packet is dropped when SCTP SACK chunk is received
 without an association.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-heartbeat-no-assoc
SCTP HEARTBEAT is received with no association:
    This counter is incremented and the packet is dropped when SCTP HEARTBEAT chunk is
received without an association.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-heartbeat-ack-no-assoc
SCTP HEARTBEAT ACK is received with no association:
    This counter is incremented and the packet is dropped when SCTP HEARTBEAT ACK chunk is
 received without an association.

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: tcp-bad-option-length
TCP option length invalid:
    This counter is incremented and the packet is dropped when the     appliance receives
a TCP packet with TCP option length 0, which is invalid     for non-NOP option.
Recommendation:
    None.

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: ssl-first-record-invalid
SSL first record invalid:
    The minimal length of SSL first handshake record should be 11 bytes. If the first record
 is less than 11 bytes, the packet will be dropped.
 Recommendation:
    This counter is incremented for invalid SSL record type that has first SSL record less
 than 11 bytes. This invalid type received from the remote peer is treated as a fatal error
 and the SSL packets that encounter this error must be dropped.

 Syslogs:
    None


-----------------------------------------------------------------
Name: ssl-record-length-invalid
SSL record length invalid:
    The minimal length of SSL handshake record should be 4 bytes. If the handshake record
is less than 4 bytes, the packet will be dropped.
 Recommendation:
    This counter is incremented for invalid SSL record type that has SSL record less than
4 bytes. This invalid type received from the remote peer is treated as a fatal error and
the SSL packets that encounter this error must be dropped.

 Syslogs:
    None


-----------------------------------------------------------------
Name: ssl-alert-length-invalid
SSL alert length invalid:
    The minimal length of SSL handshake alert should be 2 bytes. If the handshake record
is less than 2 bytes, the packet will be dropped.
 Recommendation:
```

```
    This counter is incremented for invalid SSL record type that has SSL alert less than 2
 bytes. This invalid type received from the remote peer is treated as a fatal error and the
 SSL packets that encounter this error must be dropped.

 Syslogs:
    None


----------------------------------------------------------------
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: policy-params-failed
Unable to create policy params:
    This counter is incremented and every packet is dropped  when data-plane does not have
```

```
 a valid policy     installed in the security context

Recommendation:
    If this is incrementing check the data plane logs to see why there was a policy install
 failure.
Syslogs:
    None


-----------------------------------------------------------------
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
       - Destination IP address host part equal to all 0'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: 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 Layer 2 switching 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 Layer 2 switching. You
 can also execute (show mac-address-table) to list the L2 MAC address locations currently
discovered by the appliance.

 Syslogs:
    None


----------------------------------------------------------------
Name: bvi-missing-nameif
Bridge interface missing nameif:
    This counter will be incremented when the ingress interface belongs to a bridge-group
and leaving via an interface which belongs to a different bridge-group or a L3 interface
without nameif configured on the ingress BVI interface.

 Recommendation:
    For traffic to leave the BVI interface, nameif has to be configured on the ingress BVI
 interface.

 Syslogs:
    None


----------------------------------------------------------------
Name: bvi-unsupported-packet
Unsupported packet on Bridge interface:
   This counter will be incremented when the unsupported packets are punted on BVI interface.


 Recommendation:
    Analyze the packets to determine source of unsuported packets that are tried to punt
on BVI interface.

 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: pmtu-reinject-fail
Dispatch PMTU Reinject Fail:
ICMP PMTU 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: flow-expired-drop
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: meta-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: connection-q-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: reinject-fail
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-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-icmp-invalid-pak
ICMP Inspect invalid packet:
    This counter will increment when the appliance detects an invalid ICMPv4 or ICMPv6
packet.  Examples: Incomplete ICMP header; malformed ICMP Next Header; invalid hop-limit
for ICMPv6 NS (neighbor solicitation); etc.

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-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-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-stun-out-of-trans-id
STUN Inspect out of Trans ID:
   This counter will increment when the STUN inspection engine fails to allocate an 'Trans
 ID' data structure.  The structure is used to store the transaction id of the STUN packet.

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

Syslogs:
```

```
    None.


----------------------------------------------------------------
Name: inspect-stun-out-of-memory
STUN Inspect out of Memory:
    This counter will increment when the STUN inspection engine fails to allocate memory.

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

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-stun-trans-id-no-match
STUN Inspect trans id not matched:
   This counter will increment when the transaction id in the STUN successful/error response
 message does not match any STUN request 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-stun-invalid-pak
STUN Inspect invalid packet:
    This counter will increment when the appliance detects an invalid STUN packet.

Examples: Incomplete STUN header; malformed STUN Header; etc.

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-stun-pinhole-fail
STUN Inspect failed to open pinhole:
    This counter will increment when the appliance fails to open a pinhole after a STUN
request and successful response message exchange.

Recommendation:
    Check the system memory usage.  This event normally happens when the system runs short
 of memory.
Syslog:
    None.


----------------------------------------------------------------
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-opt-format-error
DNS Inspect Multiple OPT Record:
    This counter will increment when multiple OPT records were found In a single DNS packet


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: inspect-dns-umbrella-no-memory
DNS Inspect Umbrella memory allocation failure:
    This counter will increment when Umbrella was unable to allocate new memory The current
 packet being processed was dropped.

Recommendation:
    Check system load. CHeck memory usage.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-umbrella-flow-exp
Umbrella DNS packet delay. Flow expired:
    This counter will increment when a dns response from Umbrella was unable to find pairing
 client flow to redirect the packet.Packet will be dropped

Recommendation:
    Check reachabiliy to Umbrella resolvers or network delays.

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-umbrella-appid-fail
Umbrella DNS Transaction Id entry creation or lookup fail:
    Non Matching Response to Request transaction id. app-id table was not updated.

Recommendation:
    Check dns flows, system load, memory usage.

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

Recommendations:
    Check syslogs and alerts on 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 CXSC module when
 the packet has bad TLV's.

Recommendations:
    Check syslogs and alerts on CXSC module.

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: 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 card is down:
    This counter is incremented and the packet is dropped when CXSC card is down and
fail-close option was used in CXSC action.

Recommendations:
    Check and bring up the CXSC card.

Syslogs:
    429001


----------------------------------------------------------------
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-bad-handle-received
Received Bad flow handle in a packet from CXSC Module, thus dropping flow.
    This counter is incremented, flow and packet are dropped on ASA as the handle for CX
flow has changed in flow duration.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    None


-----------------------------------------------------------------
Name: cxsc-rx-monitor-only
CXSC invalid monitor-only receive drop:
    This counter is incremented when the security appliance receives a CXSC packet when in
 monitor-only mode, and the packet is dropped.

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

Syslogs:
    None.


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

Recommendations:
    Check syslogs and alerts on SFR module.

Syslogs:
    434002


-----------------------------------------------------------------
Name: sfr-request-ssl-decrypt
SFR Module SSL decryption requested drop:
    This counter is incremented and the packet is dropped as requested by SFR module SSL
decryption when the packet is decrypted.

Recommendations:
    Check syslogs and alerts on SFR module.

Syslogs:
    None


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

Recommendations:
    Check syslogs and alerts on SFR module.

Syslogs:
    None
```

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

Recommendations:
    Check syslogs and alerts on SFR module.

Syslogs:
    None


------------------------------------------------------------------
Name: sfr-fail-close
SFR card is down:
   This counter is incremented and the packet is dropped when SFR card is down and fail-close
 option was configured in SFR action.

Recommendations:
    Check and bring up the SFR card.

Syslogs:
    434001


------------------------------------------------------------------
Name: sfr-no-flow
SFR config removed for connection:
    This counter is incremented and the packet is dropped when SFR configuration is not
found for a particular connection.

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

Syslogs:
   None


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

Recommendation:
    This could happen occasionally when SFR 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 SFR and ASA are out of sync. If that happens, contact Cisco TAC for assistance.

Syslogs:
    None.


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

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

```
Syslogs:
    None.


-----------------------------------------------------------------
Name: sfr-bad-handle-received
Received Bad flow handle in a packet from SFR Module, thus dropping flow.
    This counter is incremented, flow and packet are dropped on ASA as the handle for SFR
flow has changed in flow duration.

Recommendations:
    Check syslogs and alerts on SFR module.

Syslogs:
    None


-----------------------------------------------------------------
Name: sfr-rx-monitor-only
SFR invalid monitor-only receive drop:
    This counter is incremented when the security appliance receives a SFR packet when in
monitor-only mode, and the packet is dropped.

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

Syslogs:
    None.


-----------------------------------------------------------------
Name: inspect-dp-out-of-memory
Inspect Datapath out of memory:
    This counter is incremented when the inspect datapath fails to allocate memory.

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

Syslogs:
    None.


-----------------------------------------------------------------
Name: app-recv-queue-not-ready
Inspect Datapath peer index not ready:
    This counter is incremented when the application receiving queue is not ready.

Recommendations:
    This event only happens when the system is in the transient state, such as the system
is booting, or Snort is in the middle of becoming up or down.

Syslogs:
    None.


-----------------------------------------------------------------
Name: snort-drop
Snort requested to drop the frame:
    This counter is incremented and the packet is dropped as requested by Snort module.

Recommendations:
    Review Snort policies for any such rule denying the flow.
```

```
Syslogs:
    None.


----------------------------------------------------------------
Name: snort-down
Drop the frame as the SNORT instance is down:
    This counter is incremented and the packet is dropped as the Snort module is down.

Recommendations:
    Review Snort statistics for the reason behind SNORT instance down.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-down-no-app-info
Drop the frame as the SNORT instance is down:
    This counter is incremented and the packet is dropped as the Snort module is down and
unable to find app info or flow.

Recommendations:
    Review Snort statistics for the reason behind SNORT instance down.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-down-inline-flow
Drop the frame as the SNORT instance is down:
    This counter is incremented and the packet is dropped as the Snort module is down and
flow in either inline or passive.

Recommendations:
    Review Snort statistics for the reason behind SNORT instance down.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-down-in-fp
Drop the frame as the SNORT instance is down:
    This counter is incremented and the packet is dropped as the Snort module is down and
unable to handle in full proxy mode.

Recommendations:
    Review Snort statistics for the reason behind SNORT instance down.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-down-not-fp
Drop the frame as the SNORT instance is down:
    This counter is incremented and the packet is dropped as the Snort module is down and
unable to handle when it is not in full proxy mode.

Recommendations:
    Review Snort statistics for the reason behind SNORT instance down.
```

```
Syslogs:
    None.


----------------------------------------------------------------
Name: snort-busy
Drop the frame as SNORT instance is busy and can not handle:
    This counter is incremented and the packet is dropped as the Snort module is busy and
unable to handle the frame.

Recommendations:
    Review Snort statistics for the reason behind high load on SNORT instance.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-busy-no-app-info
Drop the frame as SNORT instance is busy and can not handle:
    This counter is incremented and the packet is dropped as the Snort module is busy and
unable to find app info or flow.

Recommendations:
    Review Snort statistics for the reason behind high load on SNORT instance.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-busy-inline-flow
Drop the frame as SNORT instance is busy and can not handle:
    This counter is incremented and the packet is dropped as the Snort module is busy and
flow in either inline or passive.

Recommendations:
    Review Snort statistics for the reason behind high load on SNORT instance.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-busy-in-fp
Drop the frame as SNORT instance is busy and can not handle:
    This counter is incremented and the packet is dropped as the Snort module is busy and
unable to handle in full proxy mode.

Recommendations:
    Review Snort statistics for the reason behind high load on SNORT instance.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-busy-not-fp
Drop the frame as SNORT instance is busy and can not handle:
    This counter is incremented and the packet is dropped as the Snort module is busy and
unable to handle when it is not in full proxy mode.

Recommendations:
    Review Snort statistics for the reason behind high load on SNORT instance.
```

```
Syslogs:
    None.


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

Recommendations:
    Please apply an activiation key that has the IPS Module License enabled.

Syslogs:
    420008


----------------------------------------------------------------
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-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-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.

    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: l2_acl_vxlan
FP L2 rule VXLAN drop:
    This counter will increment when the appliance denies a packet because it fails to
locate VXLAN out_tag when applying layer-2 ACL checks.

 Recommendation:
   This only happens under VXLAN based tag-switching use case.  Please make sure VXLAN
segment-id configuration and tag switching table are correct.

 Syslogs:
    None


----------------------------------------------------------------
Name: punt_action
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.

    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-full-reassembly-failed
Fragment full reassembly failed:
    This counter is incremented when the appliance fails to allocate memory     while
reassembling a chain of fragmented packets into a single packet.     All the fragment packets
 in the chain are dropped.
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: service-interface-down
Service interface is down:
    ASA 1000V will drop any vPath tagged traffic if the service-interface has     not been
 configured.

Recommendation:
   Ensure that all security profile interfaces are associated with the inside    interface
 using
    service-interface security-profile all <inside_interface_name>
    (only needed in ASDM mode)
```

```
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: passenger-flow-handling-failed
Passenger flow processing error mishandling:
    This counter is incremented when the security appliance receives a supported tunnel IP
 packet and a handling error is encountered during the passenger IP packet processing.The
packet is dropped.

Recommendation:
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: passenger-flow-invalid-encap-request
Passenger flow processing error invalid tunnel encap request:
    This counter is incremented when the security appliance attempts to encapsulate an IP
packet and an error is encountered because the requested tunnel encapsulation is invalid.The
 packet is dropped.

Recommendation:
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: passenger-flow-malformed-packet
Passenger flow processing error malformed tunnel encap:
    This counter is incremented when the security appliance receives a supported tunnel IP
 packet and an error is encountered because the tunnel encapsulation is malformed.The packet
 is dropped.

Recommendation:
    No action required.

Syslogs:
    None


----------------------------------------------------------------
Name: passenger-flow-no-encap-info
Passenger flow processing error missing tunnel encap info:
    This counter is incremented when the security appliance attempts to encapsulate an IP
packet and an error is encountered because the necessary tunnel encapsulation information
is missing.The packet is dropped.

Recommendation:
    No action required.

Syslogs:
```

```
    None


-----------------------------------------------------------------
Name: passenger-flow-unsupported-encap
Passenger flow processing error unsupported tunnel encap:
    This counter is incremented when the security appliance recieves a unsupported tunnel
IP packet and an error is encountered because passenger flow processing bypass fails.The
packet is dropped.

Recommendation:
    No action required.

Syslogs:
    None


-----------------------------------------------------------------
Name: passenger-flow-unsupported-payload
Passenger flow processing error unsupported tunnel encap:
    This counter is incremented when the security appliance recieves a supported tunnel IP
 packet and an error is encountered because the tunnel payload is unsupported and passenger
 flow processing bypass fails.The packet is dropped.

Recommendation:
    No action required.

Syslogs:
    None


-----------------------------------------------------------------
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-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
Dispatch 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
it's 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: 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: security-profile-not-used
Security-profile not used:
    This traffic does not use a security-profile. Traffic through ASA 1000V     is expected
 to use a security-profile configured on Nexus 1000V.
Recommendation:
    Check the port-profile configuration on the Nexus 1000V with     "show port-profile"
and verify that a security-profile is configured for     each port-profile redirecting
traffic to ASA 1000V, and that     security-profile names match between Nexus 1000V and ASA
 1000V. Verify     that security-profiles are associated with the inside interface using
   "service-interface security-profile all <inside_interface_name>"     on ASA 1000V. Use
"show vsn port" on Nexus 1000V and     "show vsn security-profile" on ASA 1000V to verify
that     security-profiles have matching ID values on both devices.
Syslogs:
    None.


----------------------------------------------------------------
Name: security-profile-not-matched
Security-profile not matched:
```

```
    This traffic contains a security-profile ID that does not match     a security-profile
 on ASA 1000V.
Recommendation:
    Check the port-profile configuration on the Nexus 1000V with     "show port-profile"
and verify that a security-profile is configured for     each port-profile redirecting
traffic to ASA 1000V, and that     security-profile names match between Nexus 1000V and ASA
 1000V.     Verify that security-profiles are associated with the inside interface     using
 "service-interface security-profile all <inside_interface_name>"     on ASA 1000V. Use
"show vsn port" on Nexus 1000V and     "show vsn security-profile" on ASA 1000V to verify
that     security-profiles have matching ID values on both devices.
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 interface 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     Technical 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     Technical 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 interface, 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: packet-infinite-looping
```

```
Infinite looping of packet:
    This counter is incremented and the packet is dropped when the packet attempts to queue
 to the loopback queue and its egress interface will trigger infinite looping.

Recommendations:
    Should never happen, possible wrong internal processing of packet.     The packet is
entering an infinite loop in the interface.

Syslogs:
    None


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

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


 Syslogs:
    None


----------------------------------------------------------------
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: unable-to-replicate-packets
Packet dropped and not replicated due to resource limitation:
    In case of shared interface, we need to loopback multicast and broadcast traffic. When
 system resource 'packet block extension memory' limitation is reached, this counter will
be incremented, the packet will be droppped and the packet will not be replicated to other
 contexts.

Recommendation:
    - Observe if free system memory is low.
```

```
 Syslogs:
    None


-----------------------------------------------------------------
Name: inspect-scansafe-server-not-reachable
Scansafe server not reachable:
    This counter is incremented when the security appliance finds scansafe cloud down. The
 packet is dropped and the connection isclosed.

Recommendation:
    Verify if the configured scansafe servers are reachable from the security appliance.

Syslogs:
    775002.


-----------------------------------------------------------------
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: 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: same-physical-interface
Same input and output physical interface:
    A flow cannot use the same physical interface for input and output     on ASA 1000V.
Recommendation:
    Check the NAT and routing policies configured on ASA 1000V. Use ASA 1000V
"packet-tracer" command to determine which security-profiles are used     based on the NAT
 and routing policies configured.    Use "show running-config service-interface" to display
 the association     between the physical interfaces and the configured security-profiles.

Syslogs:
    None.


----------------------------------------------------------------
Name: vPath-license-failure
Packet dropped due to vPath license failure:
```

```
    Traffic is dropped due to licensing failure for ASA 1000V.
Recommendation:
    Check Nexus 1000V and verify that there are sufficient ASA 1000V licenses     installed
 to support all ASA 1000V virtual machines in use.     Use "show license" to check the
available licenses for ASA 1000V and     use "show license usage" to check the status of
them.
Syslogs:
    4450002.


----------------------------------------------------------------
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: zta-src-translation-failure
ZeroTrustAccess SRC NAT POOL exhaustion
    This counter is incremented and the packet is dropped when source     translation is
configured for zero-trust traffic but pool is exhausted

Recommendation:
    This may be due to insufficient IPs configured to translate source of the     traffic
destined to zero-trust applications. Consider adding more IPs to     source translation
pool

Syslogs:
    None.


----------------------------------------------------------------
Name: cmd-invalid-encap
Invalid Encapsulation:
    This counter is incremented when the security appliance receives a invalid CMD packet.
 The packet is dropped.

Recommendation:
    Verify that directly connected CMD supported devices have proper CMD settings.

Syslogs:
    None.


----------------------------------------------------------------
Name: ifc-not-cmd-enabled
Interface not CMD configured
    This counter is incremented when the security appliance receives a CMD packet on an
interface not configured to recieve one. The packet is dropped.

Recommendation:
    Verify that interface under consideration has proper CMD settings.

Syslogs:
   None.
```

```
-----------------------------------------------------------------
Name: cluster-not-supported
Cluster not supported:
    Cluster not supported on this platform.
Recommendation:
    Remove cluster config
Syslogs:
    None.


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


-----------------------------------------------------------------
Name: cluster-invalid-owner
Cluster invalid owner:
    A Cluster data packet was received when the owner is not in the cluster.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-stub-uninterested
Cluster stub uninterested:
    A Cluster data packet was received when there is no owner or director.
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-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-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-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 may be oversubscribed because cluster is under high pressure     to send out
cluster logic update (CLU) message.
Recommendation:
    This behavior is expected as cluster is oversubscribed and is under     high pressure
to send out cluster logic update (CLU) message.     Please avoid oversubscribing the cluster.
Syslogs:
    None.


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

```
Name: cluster-data-node-ignored
Flow matched a cluster drop-on-data node classify rule:
    A multicast routing packet was received on a L3 cluster     interface when the unit was
 a data node. Only a control node     is permitted to process these packets.
Recommendation:
    This counter is informational and the behavior expected. The packet is    processed by
 control node.
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-xlate-pool-exhausted
NAT failed due to pool exhaustion:
   Failed to create an xlate to translate an IP or transport header due to pool exhaustion.

Recommendation:
    Check "show nat pool" to see how the NAT pool is allocated for xlate creation.

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 if access is desired.
Syslogs:
    None.


----------------------------------------------------------------
Name: pat-port-block-state-mismatch
PAT port block state mismatch:
    There is a mismatch between port block state and configuration across     cluster. This
 usually happens when a dynamic PAT rule is converted     from "block-allocation" to regular
 or vice-versa with active translations.
Recommendation:
    Please execute the following recommended steps -     1. Remove the current policy which
 resulted in this inconsistent state     2. Clear the active translations established by
the removed policy         as "cluster exec clear xlate global <ip1[-ip2]>"     3. Make
sure there are no active translations using previous global IPs,         through "cluster
exec show xlate global <ip1[-ip2]>"     4. Add back the policy with needed pat-pool options.
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-data-node-data-ifc-not-ready
Cluster data interface on data node unit is not ready (some data interfaces are     in
```

```
different state from the control node). For a L3 interface that is not     management-only,
 before the data interface is ready the data node cannot own     any connection on this L3
 interface. Packets must be owned by the data node     are dropped. From the box packets
are also dropped before data node's data     interface becomes ready. This drop will not
occur after data node's data     interface is ready and the data node fully joins the
cluster.
Recommendation:
    This counter is informational and the behavior expected. The packet will     be dropped.
Syslogs:
    None.


----------------------------------------------------------------
Name: nat-cluster-pool-update-fail
Cluster control node failed to send NAT pool update to data node:
    Cluster control node has failed to send NAT pool update to data node. 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.


----------------------------------------------------------------
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:
    Thsi 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 Systems in such case.Syslogs:
    None.


----------------------------------------------------------------
Name: platform-unlicensed
ASAv platform is unlicensed:
    The ASAv is not licensed.  All data traffic traversing the appliance will be     dropped
 until the ASAv is licensed.
Recommendation:
    Check the platform license state with "show activation-key" and     install the
appropriate ASAv platform license.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-forward-error
Cluster member failed to send data packet over CCL:
    Cluster member failed to transmit control packet over the CCL link.
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-tp-version-incompatible
The packet contains an incompatible transport protocol:
    The transport protocol of the packet contains a transport protocol that     is not
compatible.
Recommendation:
```

```
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-ip-version-error
IP version mismatch between layer-2 and layer-3 headers:
    The IP protocol versions in layer-2 and layer-3 headers mismatch
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-tp-sender-myself
DP message over CCL from a unit with same ID as myself:
    The sender information in the transport header indicates that the sender     is myself,
 which could happen if two clusters (with overlapping IDs) exist     on the same network
segment.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-ttl-expired
TTL of the packet has expired:
    Maximum TTL value has exceeded for this packet.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-ttl-invalid
TTL of the packet is invalid:
    The TTL value of the packet is not a valid value.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-non-ip-pkt
Layer 3 protocol of the packet is not IP:
    The packet is not IPv4, IPv6 or an ARP packet.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-bad-tp-pkt
Failed to fetch the transport layer header of the packet:
    Fetching the transport layer header of the packet failed.
    This occurs when TTL is 254 and it matches ANY of the following conditions:
    1. Cluster is disabled.
    2. The packet is not UDP.
```

```
    3. Destination port is not 4193.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-bad-trailer
Failed to fetch the trailer of the packet:
    Fetching the trailer of the packet failed.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-frag-owner-query-error
Cluster fragment failed to query flow director for flow owner:
    A failure either when forwarding first fragment to flow director or     fragment chain
 reinsert failure.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-frag-error
The fragment is not formatted correctly:
    The fragment is not formatted correctly and cannot be processed or     forwarding to
the Fragment Owner failed.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-bad-ifc-goid-in-trailer
Failed to find ifc from goid in the trailer:
    The goid extracted from the trailer does not yield a     valid real ifc.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-bad-trailer-tlv
Cluster CCL packet trailer has incorrect tlv:
    Packet received on the Cluster CCL interface has incorrect     trailer tlv option.
 Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: rule-transaction-in-progress
Initial rule transaction compiling in progress:
    This reason is given for dropping a packet when the transactional     commit mode is
used and the initial rule transaction compiling is still    in progress.  All through-the-box
```

```
 traffic is dropped when the ASA is     in this state.
Recommendation:
    This is a temporal condition that happens once during the system     initialization or
 the security context initialization.  The duration of     this condition depends on the
number of rules, such as ACLs or NAT     rules, in the configuration.
Syslogs:
    None.


-----------------------------------------------------------------
Name: mcast-in-nonactive-device
The device in HA mode received a multicast packet when it is not in active state:
    This reason is given for dropping a packet when the device is in HA mode     and is
currently not in active state and a multicast packet is received.     As the HA device can
 only process the  multicast in the active state, the received packet     will be dropped.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-semi-scale-not-ready
Semi scalable owner flow is not ready yet:
    Bulk sync has not elected a valid new owner     for this semi-scalable flow yet.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-app-no-forward
Application packet not allowed to be forwarded:
    Some applications might have problems if their packets are     forwarded.
Recommendation:
    None.
Syslogs:
    None.


-----------------------------------------------------------------
Name: block-no-prepend
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 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: tcp-proxy-no-inspection
TCP proxy no inspection:
    This counter is incremented and the packet is dropped when tcp proxy couldn't pass the
 packets for inspection.

Recommendations:
    None

Syslogs:
    None
```

```
----------------------------------------------------------------
Name: inspect-gtp
GTP inspection:
    This counter is incremented and the packet is dropped when GTP inspection found validation
 or internal errors, or performed policy drop.

Recommendations:
    Use this ASP drop reason to capture dropped GTP packets for trouble shooting.

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-proxy-3whs-failed
TCP proxy three way handshake failed:
    This counter is incremented and the packet is dropped when the TCP proxy encounters a
error during three way handshake.
Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-proxy-mixed-mode-failed
TCP proxy mixed mode failed:
    This counter is incremented and the packet is dropped when the TCP proxy encounters a
error during mixed mode operation, transitioning from light weight TCP proxy to full mode
TCP proxy.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-proxy-mixed-mode-drop
TCP proxy mixed mode drop:
    This counter is incremented and the light weight proxy tx queue is cleared when the TCP
 proxy is transitioning from light weight TCP proxy to full TCP proxy.We enqueue a FIN
segment when inspection is in progress When we trigger full proxy, this queue should be
cleared.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: tcp-proxy-ooo-drop
TCP proxy OOO:
    This counter is incremented and the packet is dropped when the TCP proxyreceives out
of order packets for processing in lightweight mode.

Recommendations:
    None
```

```
Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-retransmit-drop
TCP proxy retransmit:
   This counter is incremented and the packet is dropped when tcp proxy received a retransmit
 packet that is still being inspected.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: pdts-snort-info-missing
Flow missing pdts snort info:
    This counter is incremented and the packet is dropped when a flow to be inspected by
the Snort is missing relevant info to capture Snort data.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-fp2lw-enqueue-limit-drop
TCP proxy FP2LW enqueue limit:
    This counter is incremented and the packet is dropped when tcp proxy receives a packet
 while trying to bypass Full Proxy and proxy layer has reached its enqueue limit.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-null-flow-drop
TCP proxy NULL flow:
    This counter is incremented and the packet is dropped when tcp proxy received a packet
 for a non-existant flow.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-copy-failed-drop
TCP proxy packet copy failed:
    This counter is incremented and the packet is dropped when the tcp proxy was unable to
 copy a packet since it was unable to allocate a new one.

Recommendations:
```

```
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-l2-copy-failed-drop
TCP proxy L2 copy failed:
    This counter is incremented and the packet is dropped when the tcp proxy was unable to
 copy L2 header to a packet in Full Proxy mode.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-l2-no-header-room
TCP proxy L2 no header room:
    This counter is incremented and the packet is dropped when there was no header room
left for L2 header of a packet in Full Proxy mode.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-l2-not-initialized
TCP proxy L2 not initialized:
    This counter is incremented and the packet is dropped when the L2 header of a packet
was not initialized in Full Proxy mode.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-invalid-tcp-state-drop
TCP proxy invalid TCP state:
    This counter is incremented and the packet is dropped when the TCB is in an invalid
state.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-invalid-tcp-checksum-drop
TCP proxy invalid TCP checksum:
    This counter is incremented and the packet is dropped when the RST/FIN with data packet
 received with invalid checksum.
```

```
Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-probe-rst-injected
TCP proxy reset injected during probe:
    This counter is incremented and the packet is dropped when the RESET is injected by
snort after server hello is done.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-probe-tcp-probe-drop
TCP proxy probe reply:
   This counter is incremented and the packet is dropped when the reply to the probe message
 is received.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-fp-flow-null-drop
TCP proxy full proxy NULL flow:
    This counter is incremented and the packet is dropped when the flow is NULL in full
proxy mode.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-probe-client-conn-collision
TCP proxy client connection matches probe tuple:
    This counter is incremented and the packet is dropped when packet from client matches
the probe's tuple.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-probe-blk-alloc-failed
TCP proxy block allocation during collision:
   This counter is incremented and the packet is dropped when the TCP proxy block allocation
 fails during collision.
```

```
Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-probe-inject-pkt
TCP proxy inject probe packet:
    This counter is incremented and the packet is dropped when the TCP Proxy probe injected
 packet.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-probe-max-port-collision
TCP proxy maximum port collision:
    This counter is incremented and the packet is dropped when the TCP Proxy connection
reaches maximum port collision.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-probe-server-rst
Server intitated reset message to TCP proxy probe:
    This counter is incremented and the packet is dropped when the server inititated reset
 message is received to TCP Proxy probe.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-probe-invalid-tcp
Invalid TCP while processing FIN on TCP proxy probe:
    This counter is incremented and the packet is dropped when the invalid TCP while
processing FIN on TCP proxy probe.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-probe-lock-fin-fail
Unable to lock TCP during FIN processing on TCP proxy probe:
    This counter is incremented and the packet is dropped when the TCP proxy probe is unable
```

```
 to lock TCP during FIN processing.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-probe-server-fin
Server initiated FIN to TCP proxy probe:
    This counter is incremented and the packet is dropped when the server initiated fin is
 received to TCP proxy probe.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-proxy-probe-fin-ack-rcv
ACK received in response to FIN-ACK for probe:
    This counter is incremented and the packet is dropped when the ACK is received in
response to FIN-ACK to TCP proxy probe.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: quic-proxy-null-flow-drop
QUIC Proxy NULL flow:
    This counter is incremented and the packet is dropped when QUIC proxy receives a packet
 for a non-existent flow.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: quic-proxy-only-ack-drop
QUIC Proxy only Ack received:
    This counter is incremented and the packet is dropped when  QUIC proxy receives a packet
 with only ACK in it.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: quic-proxy-destroy-tx-queue-drop
QUIC Proxy destroy queue packet drop:
```

```
    This counter is incremented and the packet is dropped when tx queue is destroyed.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: quic-proxy-alloc-drop
QUIC Proxy Allocation failure packet drop:
    This counter is incremented and the packet is dropped when memory allocation fails.

Recommendations:
    None

Syslogs:
    None


-----------------------------------------------------------------
Name: pdts-punt-limit-exceeded
PDTS Punt limit exceeded:
     This counter is incremented and the packet dropped when datapath punts packets to
inspectors and the no. of packets queued exceeded the maximum limit.

Recommendations:
      None
Syslogs:
      None


-----------------------------------------------------------------
Name: monitor-only-mode-hdr-mismatch
Monitor-only mode packets:
     This counter is incremented and the packet dropped if there is a mismatch in monitor-only
 mode config and the AFBP header flag.

Recommendations:
      None
Syslogs:
      None


-----------------------------------------------------------------
Name: ids-pkts-processed
Packets processed in IDS modes:
   This counter is incremented after packet processing is complete in inline-tap and passive
 modes, the packet is dropped after this.

Recommendations:
    Expected behavior in these modes, no action required.

Syslogs:
    None.


-----------------------------------------------------------------
Name: snort-blist-full
Snort flow block list limit reached:
     This counter is incremented and the packet dropped when datapath buffers packets to
avoid out-of-order on fast-forwarded flows and the no. of packets queued exceeded the maximum
 limit.
```

```
Recommendations:
      None
Syslogs:
      None


------------------------------------------------------------------
Name: snort-blist-full-failopen
Snort flow block list limit reached:
     This counter is incremented and the packet dropped when datapath buffers packets to
avoid out-of-order on fail-open flows and the no. of packets queued exceeded the maximum
limit.

Recommendations:
      None
Syslogs:
      None


------------------------------------------------------------------
Name: pbr-next-hop-same
Drop the packet if next hop of pbr is self:
    This counter is incremented and the packet is dropped as the next hop configured on pbr
 is of connected IP.

Recommendations:
    Do Not add connected ip as next hop in PBR .

Syslogs:
    None.


------------------------------------------------------------------
Name: object-group-search-threshold-exceeded
object group search threshold exceeded:
    This counter is incremented when a packet is checked against an access-list and the
number of access-list object-groups that matched the packet exceeds 10000. If this occurs,
 the packet is dropped. Access-list checks can negatively impact the performance of the
device when a packet matches an excessive number of object-groups when object-group-search
 access-control feature is enabled.

Recommendations:
    Reconfigure the access-list and object-group configuration to ensure that traffic will
 not match an excess number of object-groups. Usually this problem is triggered by a large
 number of overlapping or duplicated objects. Examine the traffic being dropped with 'capture
 asp type asp-drop ogs-match-limit-exceeded', then 'show capture asp'.

Syslogs:
    None.


------------------------------------------------------------------
Name: memif-non-ip-pkt
MEMIF Non IP Packet:
    This counter is incremented when any non IP packet is received on Memif for policy
lookup. Non IP packets are dropped in that case.

Recommendation:
    Investigate why a NON IP packet is being sent by the sender for policy lookup.

Syslogs:
    None.
```

```
-----------------------------------------------------------------
Name: memif-non-policy-pkt
MEMIF No Policy Packet:
    This counter is incremented when any packet is received on Memif not tagged for policy
 lookup. Such packets are dropped in that case.

Recommendation:
    Investigate why a NON IP packet is being sent by the sender for policy lookup.

Syslogs:
    None.


-----------------------------------------------------------------
Name: reason-info
Preprocessor sending packet info to tracer:
    This counter is used internally by snort.

Recommendations:
    None.

Syslogs:
    None.


-----------------------------------------------------------------
Name: session-string
Session debug info:
    This counter is used internally by snort.

Recommendations:
    None.

Syslogs:
    None.


-----------------------------------------------------------------
Name: none
Not a Blocking Packet:
    This counter is incremented when the packet is not blocked.

Recommendations:
    None.

Syslogs:
    None.


-----------------------------------------------------------------
Name: a-module
Packet is unknown or traced:
   This counter is incremented when the packet blocked by an unknown preprocessor.

Recommendations:
    None.

Syslogs:
    None.


-----------------------------------------------------------------
Name: daq-retry
```

```
Wait for re-transmitted packet from DAQ:
    This counter is incremented when a packet re-transmission is needed from DAQ.

Recommendations:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-module
Blocked or blacklisted by snort:
    This counter is incremented and the packet is dropped as requested by snort.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: appid
Blocked or blacklisted by the AppID preprocessor:
    This counter is incremented and the packet is dropped as requested by the AppID
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: ssl-preproc
Blocked or blacklisted by the SSL preprocessor:
    This counter is incremented and the packet is dropped as requested by the SSL
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: firewall
Blocked or blacklisted by the firewall preprocessor:
    This counter is incremented and the packet is dropped as requested by the firewall
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: captive-portal
Blocked or blacklisted by the captive portal preprocessor:
```

```
   This counter is incremented and the packet is dropped as requested by the captive portal
 preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: safe-search
Blocked or blacklisted by the safe search preprocessor:
    This counter is incremented and the packet is dropped as requested by the safe search
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: si
Blocked or blacklisted by the SI preprocessor:
   This counter is incremented and the packet is dropped as requested by the SI preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: prefilter
Blocked or blacklisted by the prefilter preprocessor:
    This counter is incremented and the packet is dropped as requested by the prefilter
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: ftp
Blocked or blacklisted by the FTP preprocessor:
    This counter is incremented and the packet is dropped as requested by the FTP
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: stream
Blocked or blacklisted by the stream preprocessor:
```

```
    This counter is incremented and the packet is dropped as requested by the stream
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: session-preproc
Blocked or blacklisted by the session preprocessor:
    This counter is incremented and the packet is dropped as requested by the session
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: defragmentation
Blocked or blacklisted by the defragmentation preprocessor:
   This counter is incremented and the packet is dropped as requested by the defragmentation
 preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-react
Blocked or blacklisted by the snort react preprocessor:
    This counter is incremented and the packet is dropped as requested by the snort react
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-response
Blocked or blacklisted by the snort response preprocessor:
   This counter is incremented and the packet is dropped as requested by the snort response
 preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: reputation
```

```
Blocked or blacklisted by the reputation preprocessor:
    This counter is incremented and the packet is dropped as requested by the reputation
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: x-link2state
Blocked or blacklisted by the x-link2state preprocessor:
    This counter is incremented and the packet is dropped as requested by the x-link2state
 preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: back-orifice
Blocked or blacklisted by the back orifice preprocessor:
    This counter is incremented and the packet is dropped as requested by the back orifice
 preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: smb
Blocked or blacklisted by the SMB preprocessor:
    This counter is incremented and the packet is dropped as requested by the SMB
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: file-process
Blocked or blacklisted by the file process preprocessor:
    This counter is incremented and the packet is dropped as requested by thefile process
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


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

```
Name: ips-preproc
Blocked or blacklisted by the IPS preprocessor:
    This counter is incremented and the packet is dropped as requested by the IPS
preprocessor.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: eve-handler
Blocked or blacklisted by the eve-handler:
    This counter is incremented and the packet is dropped as requested by the eve-handler.

Recommendations:
    Review the snort output in packet tracer or capture with trace enabled.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-ccl-bad-unxlate-redirect
Cluster member dropped an unexpected NAT untranslate redirect packet from peer:
    Dynamic PAT pool owner received a NAT untranslate packet from peer. However it
matches a director stub flow.
Recommendation:
    This counter is a temporal condition after a cluster member failure.     However, if
this counter is incremented continuously, there could be a     timing issue that caused the
 error. Contact Cisco Systems in such case.Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-ccl-bad-unxlate-redirect-backup
Cluster member dropped an unexpected NAT untranslate redirect packet from peer:
    Dynamic PAT pool owner received a NAT untranslate packet from peer. However it
matches a backup stub flow.
Recommendation:
    This counter is a temporal condition after a cluster member failure.     However, if
this counter is incremented continuously, there could be a     timing issue that caused the
 error. Contact Cisco Systems in such case.Syslogs:
    None.


----------------------------------------------------------------
Name: unsupported_8021q_vlan_tags
Unsupported 802.1Q VLAN tags:
    This counter is incremented and the packet dropped when the security appliance receives
 a packet with too many layers of VLAN tags.

Recommendations:
    None
Syslogs:
    None


----------------------------------------------------------------
Name: fragment-reassembly-failed
Fragment reassembly failed:
    This counter is incremented when the appliance fails to reassemble the fragmented IP
```

```
packets. All the fragment packets in the chain are dropped.

Recommendation:
    Use 'show fragment' command to check all the failure counters.

Syslogs:
    None


-----------------------------------------------------------------
Name: df-bit-set
Egress fragmentation needed, DF bit is set:
    This counter is incremented when a packet requires egress fragmentation     but the IP
 header DF bit is set. The packet is dropped and an ICMP error     message is sent to the
source.

Recommendation:
    Review the MTU configuration on egress interface.

Syslogs:
    None


-----------------------------------------------------------------
Name: vpn-cflow-fail-due-to-full-flow
Packet dropped due to a conflicting full flow:
    This counter is incremented when we fail to create a cluster stub flow in the peer
receiving a forwarded VPN decoded packet, because there is already a full flow.

Recommendations:
    None.

Syslogs:
    None.


-----------------------------------------------------------------
Name: unable-to-create-vpn-fwd-cflow
Packet dropped due to resource limitation:
    This counter is incremented when we fail to create a cluster stub flow in the peer
receiving a forwarded VPN decoded packet.

Recommendations:
    None.

Syslogs:
    None.


-----------------------------------------------------------------
Name: unable-to-find-vpn-context
Packet dropped due to failure to find the VPN context:
    This counter is incremented when a cluster peer tries to encrypt a packet but fails to
 get the VPN context.

Recommendations:
    None.

Syslogs:
    None.


-----------------------------------------------------------------
Name: unable-to-find-owner
```

```
Packet dropped due to failure to find the owner:
   This counter is incremented when a cluster node fails to find the onwer for the connection
 from VPN director

Recommendations:
    Check whether the Director node is ready to process queries.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-onwer-id-received
Packet dropped as invalid owner id received :
    This counter is incremented when a cluster node gets a invalid owner id  from the VPN
director.

Recommendations:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: unable-to-add-to-owner-table
Packet dropped due to failure to add an entry to the owner table:
    This counter is incremented when a cluster node fails to add the onwer entry for the
connection

Recommendations:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: ike-spi-corrupted-value
IKE packet containing corrupted SPI:
    This counter is incremented and the packet is dropped when SPI consistency checks fail
 indicating the packet  might have been altered in transit.

Recommendations:
     Check the syslog to get more information about the origin of packet. This situation
can be normal and transient. If the drops persist, call TAC to investigate further.

Syslogs:
    753001


----------------------------------------------------------------
Name: ike-spi-cookie-expired
IKE packet with expired SPI cookie:
    This counter is incremented and the packet is dropped when the SPI received in the
incoming packet is considered expired.

Recommendations:
    Check the syslog to get more information about the origin of packet. If this is a valid
 peer connection, this may be the result of a very long network delay that should be
eliminated. If the drops persist, call TAC to investigate further.

Syslogs:
    753001
```

```
------------------------------------------------------------------
Name: snort-invalid-verdict
Received invalid verdict from snort:
    This counter is incremented and the packet is dropped as verdict is invalid and cannot
 be acted up on.

Recommendations:
    Enable and review the module specific snort/pdts debug messages.

Syslogs:
    None.


------------------------------------------------------------------
Name: snort-blacklist
Packet is blacklisted by snort:
    This counter is incremented and the packet is dropped as flow is     blacklisted by
snort.
Recommendations:
    Review Snort policies for any such rule denying the flow.
Syslogs:
    None.


------------------------------------------------------------------
Name: snort-block
Packet is blocked as requested by snort:
    This counter is incremented and the packet is dropped as requested by snort.

Recommendations:
    Review Snort policies for any such rule denying the flow.
Syslogs:
    None.


------------------------------------------------------------------
Name: snort-silent-drop
Packet is dropped silently as requested by snort:
    This counter is incremented and the packet is dropped as requested by snort.

Recommendations:
    Enable and review the module specific snort/pdts debug messages.

Syslogs:
    None.


------------------------------------------------------------------
Name: snort-invalid-msg
Received an invalid message from snort:
    This counter is incremented when the packet framed by snort is incorrect and needs to
be dropped.

Recommendations:
    Enable and review the module specific snort/pdts debug messages.

Syslogs:
    None.


------------------------------------------------------------------
Name: snort-flow-mismatch
```

```
Received an different flow from snort:
    This counter is incremented as the flow received from snort is different and needs to
be dropped.

Recommendations:
    Enable and review the module specific snort/pdts debug messages.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-inject-data-pkt
Inject a new data packet after being received from from snort:
    This counter is incremented as a new data packet is injected and needs to be dropped.

Recommendations:
    Enable and review the module specific snort/pdts debug messages.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-inject-data-pkt-l2-hdr
Inject a new data L2 header packet after being received from from snort:
    This counter is incremented as a new L2 header data packet is injected and needs to be
 dropped.

Recommendations:
    Enable and review the module specific snort/pdts debug messages.

Syslogs:
    None.


----------------------------------------------------------------
Name: snort-replace-data-pkt
Replace fixed length of data packet after being received from from snort:
    This counter is incremented as the fixed length of data is replaced and needs to be
dropped.

Recommendations:
    Enable and review the module specific snort/pdts debug messages.

Syslogs:
    None.


----------------------------------------------------------------
Name: pdts-reassembly-err
Error during reassembling of packets received from snort:
    This counter is incremented when there is an error encountered during reassembling of
packets received from snort.

Recommendations:
    Enable and review the module specific snort/pdts debug messages.

Syslogs:
    None.


----------------------------------------------------------------
Name: failed-to-setup-pdts-flow-param
```

```
Failure during setting up pdts flow paramters:
    This counter is incremented when there is failure in setting up pdts flow parameters.

Recommendations:
    Enable and review the module specific snort/pdts debug messages.

Syslogs:
    None.


----------------------------------------------------------------
Name: ha-nlp-invalid-fragments
NLP sending invalid fragments in failover link:
     This counter is incremented and the packet is dropped when NLP tries to send a fragmented
 packet with invalid size through failover link.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: ha-nlp-lu-link-not-ready
Failover link is not ready for processing NLP packets:
     This counter is incremented and the packet is dropped when NLP tries to send or receive
 a packet however failover link lu status is down.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: ha-nlp-send-ha-msg-err
Send NLP packet over HA failover link failed:
     This counter is incremented and the packet is dropped when NLP failed to send packet
through failover link.

Recommendations:
    Check the show counter result to get more information about the failure.

Syslogs:
    None


----------------------------------------------------------------
Name: invalid-map-address-port
Invalid MAP address/port combination:
    A packet with an address that matches a MAP (Mapping of Address and Port) domain Basic
 Mapping Rule has inconsistent encoding or the port number used is not within the allotted
 range.

Recommendation:
    Check MAP BR and CE configurations to ensure they are consistent within the same MAP
domain. Note that this can also be caused by a rouge MAP CE that maliciously tries to use
an unallotted port.

Syslogs:
    305019, 305020
```

```
----------------------------------------------------------------
Name: snort-detain
Packet is detained as requested by snort:
    This counter is incremented and the packet is detained as requested by snort.

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

Syslogs:
    None.


----------------------------------------------------------------
Name: vti-channel
Vti channel drop:
    This counter is incremented when the security appliance has tried to forward the packet
 through vti interface channel. The packet is dropped.

Recommendation:
    Expected scenario, packets forwarded to vti interface       will get dropped. cases
like icmp, mcast etc.

Syslogs:
   None.


----------------------------------------------------------------
Name: vtemplate-channel
Vtemplate channel drop:
    This counter is incremented when the security appliance has tried to forward the packet
 through virtual template interface channel. The packet is dropped.

Recommendation:
    Expected scenario, packets forwarded to virtual template interface     will get dropped.
 cases like icmp, mcast etc.

Syslogs:
   None.


----------------------------------------------------------------
Name: vaccess-channel
Vaccess channel drop:
    This counter is incremented when the security appliance has tried to forward the packet
 through vaccess interface channel. The packet is dropped.

Recommendation:
    Expected scenario, packets forwarded to vaccess interface     will get dropped. cases
like icmp, mcast etc.

Syslogs:
   None.


----------------------------------------------------------------
Name: snp-ha-udp-lu-link-resource-alloc-failure
Failover dropped packet due to resource limitation:
    This counter is incremented and the packet is dropped when block extension allocation
fails due to a system resource limitation.  The resource limit may be either:
       1) system memory
       2) packet block extension memory

Recommendation:
```

```
    - Observe if free system memory is low.

Syslogs:
    None


-----------------------------------------------------------------
Name: snp-ha-udp-lu-link-unexpected-packet
Failover UDP trans received an unexpected packet:
    This counter is incremented and the packet is dropped when NP HA UDP transport receives
 a packet destined for a different entity.

Recommendation:
    Verify if the appliance is under attack. If there are no suspicious packets, 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: dispatch-queue-limit
Dispatch queue limit reached:
    There are 32K load balancer queues that a packet could be hashed to. Each     queue has
 a limit of 1000 packets. When more packets are attempted, tail     drop occurs and this
counter is incremented.
Recommendation:
    If this happens excessively, find out which queues are affected and the     connections
 hashing to that queue. Send this information to development
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; its 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 commands to
gather more information about this counter and contact 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 operation, 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 commands to
gather more information about this counter and contact 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: ipsec-detunnel-fail
IPsec detunnel processing failed:
  This counter will increment when a clear text flow fails IPSec tunnel flow processing.

Recommendation:
    Use the following command to look at more specific packet drops.

    show asp drop

Syslogs:
    None


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


----------------------------------------------------------------
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: vpn-reclassify_failed
The flow could not be reclassified according to existing VPN policies:
    When VPN policies change, flows that no longer match those policies are     freed as
packets arrive for those flows.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    No new syslogs accompany this event.


----------------------------------------------------------------
Name: vpn-missing-decrypt
The flow could not be created because its decryption policy was not available:
    A VPN flow creation was attempted before its decryption policy was     fully initialized.
 This is a transient condition and will be resolved once the     decryption policy completes
 its installation.

Recommendations:
It is possible to see this counter increment as part of normal operation. However, if the
counter is rapidly incrementing and there is a traffic disruption, then this may be caused
 by a misconfiguration or a software defect. Use the following commands to gather more
information about this counter and contact the Cisco TAC to investigate the issue further.

    capture <name> type asp-drop vpn-missing-decrypt
    show asp table classify
    show asp drop
    show tech-support

Syslogs:
    No new syslogs accompany this event.
```

```
----------------------------------------------------------------
Name: vpn-bad-decrypt-rule
The flow could not be created because a wrong decryption policy was hit:
    This is a transient condition when clustering is enabled and vpn-mode is     set to
distributed.

Recommendations:
It is possible to see this counter increment as part of normal operation. However, if the
counter is rapidly incrementing and there is a traffic disruption, then this may be caused
 by a misconfiguration or a software defect. Use the following commands to gather more
information about this counter and contact the Cisco TAC to investigate the issue further.

    show asp drop
    show tech-support

Syslogs:
    No new syslogs accompany this event.


----------------------------------------------------------------
Name: vpn-invalid-encryption
The flow is dropped because encryption flag was not set:

Recommendations:
It is possible to see this counter increment as part of normal operation. However, if the
counter is rapidly incrementing and there is a traffic disruption, then this may be caused
 by a misconfiguration or a software defect. Use the following commands to gather more
information about this counter and contact the Cisco TAC to investigate the issue further.

    show asp drop
    show tech-support

Syslogs:
    No new syslogs accompany this event.


----------------------------------------------------------------
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: acl-drop-reclassify
Flow is denied by access rule after reclassification:
     This counter is incremented when a drop rule is hit by the packet during reclassification
 of ACL rules.

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: ips-syn-timeout
IPS SYN Timeout:
    This reason is given for closing an optimised state track lite 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: ips-conn-timeout
IPS CONN Timeout:
    This reason is given for closing an optimised state track lite TCP flow due to expiry
of connection 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: sctp-init-0-tag
SCTP INIT contains 0 value initiate tag:
    This counter is incremented and the flow is dropped when sctp INIT chunk contains 0
value initiate tag.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-initack-0-tag
SCTP INIT ACK contains 0 value initiate tag:
    This counter is incremented and the flow is dropped when sctp INIT ACK chunk contains
0 value initiate tag.

Recommendations:
```

```
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-0-stream-cnt
SCTP INIT contains 0 value inbound/outbound stream count:
    This counter is incremented and the packet is dropped when sctp INIT chunk contains 0
value inbound/outbound stream count.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-timeout
SCTP INIT timed out (not receiving INIT ACK):
    This counter is incremented and the flow is dropped when sctp INIT chunk timeout count
 reaches limit.

Recommendations:
    This drop can happen in a scenarios like when the receiver     of INIT chunk is not
responding INIT ACK or there could be     redundant path between client and server where
INIT goes in     one path and INIT ACK comes in another path. If this error     occurs in
large numbers, please use packet capture feature     to help isolate the issue.

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-cookie-timeout
SCTP cookie timed out:
    This counter is incremented and the flow is dropped when sctp cookie state (after
received INIT ACK or COOKIE ECHO) timeout count reaches limit.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-endpoint-abort
SCTP received ABORT from endpoint:
    This counter is incremented and the flow is dropped when sctp ABORT chunk is received.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-chunk-init-ack-0-stream-cnt
SCTP INIT ACK contains 0 value inbound/outbound stream count:
    This counter is incremented and the packet is dropped when sctp INIT ACK chunk contains
```

```
 0 value inbound/outbound stream count.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
Name: sctp-shutdown-timeout
SCTP SHUTDOWN timed out (not receiving SHUTDOWN ACK):
    This counter is incremented and the flow is dropped when sctp SHUTDOWN timeout count
reaches limit.

Recommendations:
    None

Syslogs:
    None


----------------------------------------------------------------
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: cxsc-bad-hdl
Flow terminated by ASA due to bad handle from CX
    Since the handle received from CX is invalid, dropping flow.

Recommendations:
    Check syslogs and alerts on CXSC module.

Syslogs:
    421004


----------------------------------------------------------------
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: sfr-request
Flow terminated by SFR:
    This reason is given for terminating a flow as requested by SFR module.

Recommendations:
    Check syslogs and alerts on SFR module.

Syslogs:
    434002


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

Recommendations:
    Check and bring up SFR card

Syslogs:
    434001


----------------------------------------------------------------
Name: sfr-bad-hdl
Flow terminated by ASA due to bad handle from SFR
    Since the handle received from SFR is invalid, dropping flow.

Recommendations:
    Check syslogs and alerts on SFR module.

Syslogs:
    421004


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

Recommendations:
    Check syslogs and alerts on SFR module.

Syslogs:
    434003


----------------------------------------------------------------
Name: snort-flow-drop
Flow terminated by SNORT:
    This reason is given for terminating a flow as requested by SNORT module.

Recommendations:
```

```
    Review Snort policies for any such rule denying the flow.

Syslogs:
    None.


----------------------------------------------------------------
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: 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: ips-license-disabled-fail-close
IPS module license disabled:
    This reason is given for terminating a flow when the IPS module license is disabled and
 the fail-close option was used in IPS inspection.

Recommendations:
    Please apply an activiation key that has the IPS Module License enabled.

Syslogs:
    420008


----------------------------------------------------------------
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: 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: dtls-hello-close
DTLS hello close:
    This counter is incremented when the UDP connection is dropped after the DTLS client
hello message processing is finished. This does not indicatean error.
```

```
Recommendation:
    None.
Syslogs:
    None.


----------------------------------------------------------------
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 remidiation     steps to
remove the infection.

Syslogs:
    None.


----------------------------------------------------------------
Name: asa-teardown
ASA requested flow to be torndown:
    ASA requested the flow to be removed
Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: punt-limit
No. of segments queued to an inspector reached limit:
    For this flow, no. of packets queued to the inspector reached     the limit. Thus,
terminating the flow
Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: pdts-rule-meta-failed
PDTS rule-meta allocation failed:
    This counter is incremented when rule-meta allocation failed,     thus terminating the
 flow

Recommendation:
    None.

Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: tcp-full-proxy-required
Full TCP proxy is required, but not available in monitor-only mode:
    This flow requires full TCP proxy, but this feature is not available in     monitor-only
 mode.
Recommendation:
    None.

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: vPath-license-failure
Flow terminated due to vPath license failure:
    The flow is dropped due to licensing failure for ASA 1000V.

Recommendation:
    Check Nexus 1000V and verify that there are sufficient ASA 1000V licenses     installed
 to support all ASA 1000V virtual machines in use.     Use "show license" to check the
available licenses for ASA 1000V and     use "show license usage" to check the status of
them.

 Syslogs:
    4450002.


----------------------------------------------------------------
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-nat-pool-removed
Cluster flow is removed due to non-existent nat pool:
    Deleting a director/backup flow as it is referring to a NAT pool IP which is already
removed.

Recommendation:
    This counter is informational.

Syslogs:
    None.


-----------------------------------------------------------------
Name: cluster-cflow-stale-clu-closed
Cluster flow with CLU removed due to stale owner:
    A cluster flow was removed because it has stale owner info. Stale info can  happen due
```

```
 to missing CLU_DELETE as normally this is not a reliable msg.

Recommendation:
    This counter is informational.

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

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

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: cluster-mobility-owner-removed
Flow mobility has old owner removed:
    Flow mobility moved this flow to another unit. This old owner     will be removed.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-mobility-fwder-removed
Flow mobility has old fwder removed:
   Flow mobility moved this flow to another unit. This old fwder     will be removed because
 it's turning into a backup.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-mobility-backup-removed
Flow mobility has backup removed:
    Flow mobility moved this flow to another unit. This backup     will be removed because
 new owner and director are on difference nodes.

Recommendations:
    This counter is informational and the behavior expected.

Syslogs:
    None.


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

```
Name: cluster-mobility-owner-2-dir
Flow mobility has old owner/director changed to director only:
    Flow mobility moved this flow to another unit. This unit used     to be both owner and
 director, now will host director flow     only.

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-owner-2-dir
Another owner overrides me, and I will become a director later:
    Another unit owns the flow, and asks me to delete my flow in order     to create a
director flow in its place later.

Recommendations:
    This counter is informational and the behavior is expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-owner-2-fwd
Another owner overrides me, and I will become a forwarder later:
    Another unit owns the flow, and asks me to delete my flow in order     to create a
forwarder flow in its place later.

Recommendations:
    This counter is informational and the behavior is 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-control-node-change
Control node only pinhole flow removed at bulk sync due to control node change:
    Control node only pinhole flow is removed during bulk sync becase cluster control node
     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 control node may have just left the cluster. And there might be     packet
 drops on the Cluster Control Link.

Syslogs:
    302014


----------------------------------------------------------------
Name: invalid-vxlan-segment-id
Invalid VXLAN segment-id:
   This counter is incremented when the security appliance sees an invalid VXLAN segment-id
 attached to a flow.

Recommendation:
    No.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-geneve-segment-id
Invalid Geneve segment-id:
   This counter is incremented when the security appliance sees an invalid Geneve segment-id
 attached to a flow.

Recommendation:
    No.

Syslogs:
```

```
    None.


----------------------------------------------------------------
Name: no-valid-nve-ifc
No valid NVE interface:
    This counter is incremented when the security appliance fails to identify the NVE
interface of a VNI interface for a flow.

Recommendation:
    Verify that the nve is configured for all interfaces.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-peer-nve
Invalid peer NVE:
    This counter is incremented when the security appliance fails to get IP and MAC address
 of a peer NVE for a flow.

Recommendation:
    Verify that peer nve is configured or learned for the nve.

Syslogs:
    None.


----------------------------------------------------------------
Name: vxlan-encap-error
Fail to encap with VXLAN:
    This counter is incremented when the security appliance fails to encapsulate a packet
with VXLAN for a flow.

Recommendation:
    No.

Syslogs:
    None.


----------------------------------------------------------------
Name: geneve-encap-error
Fail to encap with Geneve:
    This counter is incremented when the security appliance fails to encapsulate a packet
with Geneve for a flow.

Recommendation:
    No.

Syslogs:
    None.


----------------------------------------------------------------
Name: no-route-to-peer-nve
No route to peer NVE:
    This counter is incremented when the security appliance fails to locate next hop to
peer NVE.

Recommendation:
    Verify peer NVE is reachable via source-interface.
```

```
Syslogs:
    None.


----------------------------------------------------------------
Name: vxlan-invalid-vni-mcast-ip
Invalid Multicast IP on VNI interface:
   This counter is incremented when the security appliance fails to get the multicast group
 IP from the VNI interface.

Recommendation:
    Verify that in the absence of a configured peer NVE, the VNI     interface has a valid
 multicast group IP configured on it.

Syslogs:
    None.


----------------------------------------------------------------
Name: vxlan-missing-peer-vtep-ip
Peer VTEP IP not found:
    This counter is incremented when the security appliance fails to find the peer VTEP IP
 for an inner destnation IP for VXLAN encapsulation.

Recommendation:
    Verify that in show arp vtep-mapping/show mac-address-table     vtep-mapping/show ipv6
 neighbor vtep-mapping, the VTEP IP is     present for the desired remote inner host.

Syslogs:
    None.


----------------------------------------------------------------
Name: vxlan-ccl-inner-dip-not-found
Peer CCL inner IP not found:
    This counter is incremented when the security appliance fails to find peer's CCL inner
 destination IP.

Recommendation:
    No.

Syslogs:
    None.


----------------------------------------------------------------
Name: ifc-zn-chg
Interface experienced a zone change:
    This reason is given for terminating a flow because the parent interface has joined or
 left a zone.

Recommendations:
    No action required.

Syslogs:
    302014, 302016, 302018, 302021, 302304


----------------------------------------------------------------
Name: flow-missing-snort-info
Snort inspected flow missing pdts snort info:
    This reason is given for terminating a flow because the connection lacks snort related
 structure.
```

```
Recommendations:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: ifc-vrf-chg
Interface experienced a VRF change:
    This reason is given for terminating a flow because the parent interface has moved from
 one VRF to another..

Recommendations:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: ifc-addr-chg
Stale Ike flow with incorrect outbound ifc, cleared as part of Address change/removal on
tunnel src interface(vti):
This reason is given for terminating stale ike flow with incorrect outbound ifc, which are
 created because tunnel src interface experienced ip/ipv6 address change/removal.

Recommendations:
    No action required.

Syslogs:
    None.


----------------------------------------------------------------
Name: clean_for_vpn_stub
Clean up for creation of a new VPN stub:
    This reason is given for tearing down a conflicting connection in preparation for a new
 vpn stub connection.

Recommendations:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-cflow-isakmp-owner-closed
Cluster flow closed on ISAKMP owner:
    Director/backup unit received an isakmp redirected packet from a forwarding     unit
and terminated the flow.

Recommendation:
    This counter should increment for every cflow torn down by isakmp redirected packet on
     the isakmp owner unit.

Syslogs:
    None.


----------------------------------------------------------------
Name: vpn-context-association-failure
VPN context association failure:
```

```
    This counter is increased whenever we fail to associate the VPN context with a
cluster flow.

Recommendation:
    None.

Syslogs:
    None.


----------------------------------------------------------------
Name: ike-pkt-with-bad-spi
Flow removed for IKE packet with corrupted or expired SPI:
    This counter is incremented and the flow is dropped when the IKE packet in this flow
gets dropped due to corrupted or expired SPI.

Recommendations:
    Check the syslog to get more information about the origin of the packet. This situation
 can be normal and transient. If the drops persist, call TAC to investigate further.

Syslogs:
    753001


----------------------------------------------------------------
Name: max-retries-of-retransmission-exceeded
Maximum retries of retransmission exceeded:
    The connection was torn down because the TCP packet exceeded maximum retries of
retransmission,     no reply from peer, tearing down connection.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: probe-max-retries-of-retransmission-exceeded
Probe maximum retries of retransmission exceeded:
    The connection was torn down because the TCP packet exceeded maximum probe retries of
retransmission,     no reply from peer, tearing down connection.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: probe-max-retransmission-time-elapsed
Probe maximum retransmission time elapsed:
    The connection was torn down because the maximum probing time for TCP packet has elapsed,
     no reply from peer, tearing down connection.

Recommendation:
    None.

Syslogs:
    302014


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

```
Name: probe-retransmit-invalid-timeout
Probe retransmit has invalid timeout:
    The connection was torn down because flow moved to Full proxy,     with invalid probe
timeout.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: probe-received-tcp-reset
Probe received RST:
    The connection was torn down because the probe connection received RST from server,
  tearing down connection.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: probe-received-tcp-fin
Probe received FIN:
    The connection was torn down because the probe connection received FIN from server,
  tearing down connection.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: probe-complete
Probe completed:
    The connection was torn down because the probe connection is successful,     tearing
down connection.

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: cluster-dup-owner-to-dir
Duplicated owner flow detected, and I will become a director later:
    Another unit owns the flow, so need to delete my flow in order     to create a director
 flow in its place later.

Recommendations:
    This counter is informational and the behavior is expected.

Syslogs:
    None.
```

```
----------------------------------------------------------------
Name: cluster-dir-removed-dup-owner
Duplicated owner flow removed by director:
    Another unit owns the flow, so director deleted the flow on this unit.

Recommendations:
    This counter is informational and the behavior is expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: cluster-removed-stale-stub
Stale stub flow removed by owner:
    This is a stale stub flow, so owner deleted the flow on this unit.

Recommendations:
    This counter is informational and the behavior is expected.

Syslogs:
    None.


----------------------------------------------------------------
Name: invalid-map-address-port
Invalid MAP address/port combination:
    A packet with an address that matches a MAP (Mapping of Address and Port) domain Basic
 Mapping Rule has inconsistent encoding or the port number used is not within the allotted
 range.

Recommendation:
    Check MAP BR and CE configurations to ensure they are consistent within the same MAP
domain. Note that this can also be caused by a rouge MAP CE that maliciously tries to use
an unallotted port.

Syslogs:
    305019, 305020


----------------------------------------------------------------
Name: closed-by-block-reset
Flow is cleared on receiving block with reset:
     Snort sends a block with reset
Recommendation:
    This counter is informational and the behavior is expected.

Syslogs:
    None.


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

# Examples

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

```
ciscoasa# 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. |