show asp drop through show curpriv Commands

show asp drop

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.0(8)/7.2(4)	Output now 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 using the 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. It also indicates when the last time the asp drop counters were cleared. See the *Cisco Security Appliance Command Line Configuration Guide* for more information about the accelerated security path. This information is used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

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

- Frame Drop Reasons, page 25-3
- Flow Drop Reasons, page 25-35

Frame Drop Reasons

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

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

Syslogs:
    None.


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

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

Syslogs:
    None


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

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

Syslogs:
    None.
```

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

Recommendation:
    None.

Syslogs:
    None.


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

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

Syslogs:
    None.


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

Recommendation:
    The invalid packet could be a bogus packet being sent by an attacker.
Investigate the traffic from source in the following syslog.
Syslogs:
    500003.


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

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

Syslogs:
    None.


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

Recommendation:
```

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

Syslogs:
   None.

Name: unexpected-packet
Unexpected packet:
   This counter is incremented when the appliance in transparent mode receives a non-IP
packet, destined to 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: 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

Cisco Security Appliance Command Reference 7.2(2)

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

Syslogs:
    106023, 106100, 106004


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

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

Syslogs:
    None


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

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

Syslogs:
    None.


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

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

 Syslogs:
    402114
```

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

Recommendation:
    This error may be due to a misconfigured host.  If this error occurs repeatedly or in
large numbers, it could also indicate spurious or malicious activity such as an attempted
DoS attack.
Syslogs:
    None.


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

Recommendation:
    Under normal conditions, this may be seen when the appliance has already closed a
connection, and the client or server still believe the connection is open, and continue to
transmit data.  Some examples where this may occur is just after a 'clear local-host' or
'clear xlate' is issued. Also, if connections have not been recently removed, and the
counter is incrementing rapidly, the appliance may be under attack. Capture a sniffer
trace to help isolate the cause.
Syslogs:
    6106015


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

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

```
Syslogs:
    None


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

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

Syslogs:
    None


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

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

Syslogs:
    None


-----------------------------------------------------------------
Name: tcp-bad-option-list
TCP option list invalid:
    This counter is incremented and the packet is dropped when the appliance receives a
TCP packet with a non-standard TCP header option.

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

Syslogs:
    None


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

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

Syslogs:
    4419001
```

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

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

Syslogs:
     None


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

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

Syslogs:
     None


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

Recommendations:
     None

Syslogs:
     None


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

Recommendations:
     None

Syslogs:
     None


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

Recommendations:
     None
```

```
Syslogs:
    None



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

Recommendations:
    None

Syslogs:
    None



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

Recommendations:
    None

Syslogs:
    None



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

Recommendations:
    None

Syslogs:
    None



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

Recommendations:
    None

Syslogs:
    None



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

Recommendations:
    None
```

```
          Syslogs:
              None


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

          Recommendations:
              None

          Syslogs:
              None


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

          Recommendations:
              None

          Syslogs:
              None


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

          Recommendations:
              None

          Syslogs:
              None


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

          Recommendations:
              None

          Syslogs:
              None


          ----------------------------------------------------------------
          Name: tcp-buffer-full
          TCP Out-of-Order packet buffer full:
```

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

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

Syslogs:
      None

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

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

Syslogs:
      None

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

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

Syslogs:
      None

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

Recommendations:
      None

Syslogs:
      None

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

          Recommendations:
              None

          Syslogs:
              None


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

          Recommendations:
              None

          Syslogs:
              None


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

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

          Syslogs:
              None


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

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

          Syslogs:
              201011


          ----------------------------------------------------------------
          Name: conn-limit
          Connection limit reached:
```

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

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

Syslogs:
    201011

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

Recommendations:
    None

Syslogs:
    None

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

Recommendations:
    None

Syslogs:
    None

Name: tcpnorm-win-variation
TCP unexpected window size variation:
    This counter is incremented and the packet is dropped when window size advertized by
TCP endpoint is drastically changed without accepting that much data.

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

Syslogs:
    None

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

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

Syslogs:
    106020
    400xx in case of ip audit checks


---------------------------------------------------------------
Name: sp-security-failed
Slowpath security checks failed:
    This counter is incremented and packet is dropped when the security appliance is:
    1) In routed mode receives a through-the-box:
        - L2 broadcast packet
        - IPv4 packet with destination IP address equal to 0.0.0.0
        - IPv4 packet with source IP address equal to 0.0.0.0
    2) In routed or transparent mode and receives a through-the-box IPv4 packet with:
        - first octet of the source IP address equal to zero
        - source IP address equal to the loopback IP address
        - network part of source IP address equal to all 0's
        - network part of the source IP address equal to all 1's
        - source IP address host part equal to all 0's or all 1's
    3) In routed or transparent mode and receives an IPv4 or IPv6 packet with same source
and destination IP addresses

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

Syslogs:
    1 and 2) 106016
    3) 106017
```

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

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


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

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

Syslogs:
     None.


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

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

Syslogs:
     None


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

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

Syslogs:
     302014, 302016, 302018


-----------------------------------------------------------------
Name: dst-l2_lookup-fail
Dst MAC L2 Lookup Failed:
```

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

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

 Syslogs:
    None

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

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

 Syslogs:
    None

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

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

Syslogs:
    None.

Name: inspect-icmp-out-of-app-id
ICMP Inspect out of App ID:
    This counter will increment when the ICMP inspection engine fails to allocate an 'App ID' data structure. The structure is used to store the sequence number of the ICMP packet.

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

Syslogs:
    None.

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

        Recommendation:
            No action required.

        Syslogs:
            None.

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

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

```
Syslogs:
    313005


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

Recommendation:
    No action required.

Syslogs:
    None.


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

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

Syslogs:
    None.


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

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

Syslogs:
    410001


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

Syslogs:
    None.


----------------------------------------------------------------
Name: inspect-dns-id-not-matched
DNS Inspect ID not matched:
```

This counter will increment when the identification of the DNS response message does
not match any DNS queries that passed across the appliance earlier on the same connection.

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

Syslogs:
    None.

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

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

Syslogs:
    None.

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

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

Syslogs:
    None.

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

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

Syslogs:
    None.

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

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

Syslogs:
    431001.

Name: inspect-rtp-invalid-payload-type
Invalid RTP Payload type field:
    This counter will increment when the RTP payload type field does not contain an audio
payload type when the signalling channel negotiated an audio media type for this RTP
secondary connection. The counter increments similarly for the video payload type.

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

Syslogs:
    431001.

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

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

Syslogs:
    431001.

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

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

Syslogs:
    431001.

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

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

Syslogs:
    431001.

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

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

Syslogs:
     None.


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

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

Syslogs:
     431002.


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

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

Syslogs:
     431002.


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

Recommendations:
     Check syslogs and alerts on IPS module.

Syslogs:
     420002


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

Recommendations:
```

```
        Check and bring up the IPS card.

    Syslogs:
        420001


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

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

    Syslogs:
        None


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

    Recommendation:
        If this drop is causing the connection to fail, please have a sniffer trace of the
    client and server side of the connection while reporting the issue. The box could be under
    attack and the sniffer traces or capture would help narrowing down the culprit.
    Syslogs:
        None.
```

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

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

                 Syslogs:
                     None


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

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

                 Syslogs:
                     None


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

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

                 Syslogs:
                     None


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

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

Syslogs:
        None.


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

Recommendation:
    No action required.

Syslogs:
        None.


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

Recommendation:
    No action required.

Syslogs:
        None.


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

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

Syslogs:
        None


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

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

 Syslogs:
    106026, 106027


----------------------------------------------------------------
Name: host-move-pkt
```

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

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

 Syslogs:
    412001, 412002, 322001


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

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

Syslogs:
    322004


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

Recommendation:
    No action required.

Syslogs:
    401004


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

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

 Syslogs:
    321001


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

 Recommendation:
```

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

      Syslogs:
         321002

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

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

    Syslogs:
         None.

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

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

    Syslogs:
         None.

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

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

    Syslogs:
         None.

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

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

    Syslogs:

```
        722037 (Only for SVC received data).


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

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

        Syslogs:
            722037 (Only for SVC received data).


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

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

        Syslogs:
            None.


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

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

        Syslogs:
            None.


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

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

        Syslogs:
            None.


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

        Recommendation:
```

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

Syslogs:
   None.



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

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

Syslogs:
   None.



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

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

Syslogs:
   722037.



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

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

Syslogs:
   722037.



----------------------------------------------------------------
Name: mp-svc-no-mac
SVC Module unable to find L2 data for frame:
     This counter will increment when the security appliance is unable to find an L2 MAC
header for data received from an SVC.

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

Syslogs:
   None.



----------------------------------------------------------------
Name: mp-svc-invalid-mac
```

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

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

Syslogs:
    None.
```

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

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

Syslogs:
    None.
```

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

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

Syslogs:
    None.
```

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

Recommendation:
    None.

Syslogs:
    450001


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

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: 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.

Cisco Security Appliance Command Reference 7.2(2)

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

Recommendation:
     No action required.

Syslogs:
     302014, 302016


----------------------------------------------------------------
Name: host-removed
Host is removed:
     Flow removed in response to "clear local-host" command.

Recommendation:
     This is an information counter.

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


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

Recommendation:
     This is an information counter.

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


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

Recommendation:
     No action required.

Syslogs:
     302014, 302016, 302018, 302021


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

Recommendation:
     None.

Syslogs:
     201011
```

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

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

                    Syslogs:
                         302014


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

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

                    Syslogs:
                         302014


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

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

                    Syslogs:
                         302014


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

                    Recommendation:
                         None.

                    Syslogs:
                         302014


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

                    Recommendation:
                         None.

                    Syslogs:
```

302014

Name: recurse
Close recursive flow:
    A flow was recursively freed. This reason applies to pair flows and multicast slave
flows, and serves 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 retransmission 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 advertised by TCP
endpoint is drastically changed without accepting that much data.

Recommendations:

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

Syslogs:
    302014

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

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

Syslogs:
    302014

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

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

Syslogs:
    None

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

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

Syslogs:
    None

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

Recommendation:

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

Syslogs:
    None

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

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

Syslogs:
    None

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

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

Syslogs:
    None.

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

                Recommendation:
                    No action required.

                Syslogs:
                    401004


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


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

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

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


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

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

                Syslogs:
                    305005


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

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

          Syslogs:
              None.


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

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

          Syslog:
              421001.


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

          Recommendation:
```

```
                         None.


              Syslog:
                         None.



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

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

              Syslogs:
                         None.



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

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

              Syslogs:
                         725006.
                         725014.



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

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

              Syslogs:
                         None.



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

              Recommendation:
```

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

Syslogs:
    None.

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

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

Syslogs:
    None.

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

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

Syslog:
    None.

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

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

Syslog:
    None.

Name: np-socket-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

Cisco Security Appliance Command Reference 7.2(2)

```
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: 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: 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: 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: 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



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

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

```
hostname# show asp drop

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

Last clearing: Never

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

Last clearing: 17:02:12 UTC Jan 17 2008 by enable_15
```

Related Commands

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

show asp table arp

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

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

Syntax Description

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

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(4)	Added a timestamp indicating when the last time the asp table counters were cleared.

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

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

```
hostname# show asp table arp

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

```
Context: single_vf, Interface: identity
 ::                                         Active   0000.0000.0000 hits 0
 0.0.0.0                                    Active   0000.0000.0000 hits 50208
```

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

```
hostname# show asp table arp

Context: single_vf, Interface: inside
  10.0.72.1                                 Active   0003.fecf.501c hits 0
Context: single_vf, Interface: mgmt
  10.0.8.1                                  Active   0003.fecf.501c hits 35
Context: single_vf, Interface: identity
  ::                                        Active   0000.0000.0000 hits 0
  0.0.0.0                                   Active   0000.0000.0000 hits 2
Last clearing of hits counters: Never
```

Related Commands

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

show asp table classify

To debug the accelerated security path classifier tables, use the **show asp table classify** command in privileged EXEC mode. The classifier examines properties of incoming packets, such as protocol, and source and destination address, to match each packet to an appropriate classification rule. Each rule is labeled with a classification domain that determines what types of actions are performed, such as dropping a packet or allowing it through.

   show asp table classify [**hit** | **crypto** | **domain** *domain_name* | **interface** *interface_name*]

Syntax Description

crypto	(Optional) Shows the encrypt, decrypt, and ipsec tunnel flow domains only.
domain *domain_name*	(Optional) Shows entries for a specific classifier domain. See "Usage Guidelines" for a list of domains.
hits	(Optional) Shows classifier entries which have non-zero hits values
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the classifier table.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(4)	Added the **hits** option, and the timestamp indicating when the last time the asp table counters were cleared.

Usage Guidelines   The **show asp table classifier** command shows the classifier contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco Security Appliance Command Line Configuration Guide* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Classifier domains include the following:

```
aaa-acct
aaa-auth
aaa-user
accounting
arp
```

```
capture
capture
conn-nailed
conn-set
ctcp
decrypt
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
host
ids
inspect
inspect-ctiqbe
inspect-dns
inspect-dns-ids
inspect-ftp
inspect-ftp-data
inspect-gtp
inspect-h323
inspect-http
inspect-icmp
inspect-icmp-error
inspect-ils
inspect-mgcp
inspect-netbios
inspect-pptp
inspect-rsh
inspect-rtsp
inspect-sip
inspect-skinny
inspect-smtp
inspect-snmp
inspect-sqlnet
inspect-sqlnet-plus
inspect-sunrpc
inspect-tftp
inspect-xdmcp
ipsec-natt
ipsec-tunnel-flow
ipsec-user
limits
lu
mac-permit
mgmt-lockdown
mgmt-tcp-intercept
multicast
nat
nat-exempt
nat-exempt-reverse
nat-reverse
null
permit
permit-ip-option
permit-log
pim
ppp
priority-q
punt
punt-l2
punt-root
```

```
qos
qos-per-class
qos-per-dest
qos-per-flow
qos-per-source
shun
tcp-intercept
```

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

```
hostname# show asp table classify

Interface test:
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=10.86.194.60, mask=255.255.255.255, port=0
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
...
```

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

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

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

Related Commands

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

show asp table interfaces

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

> **show asp table interfaces**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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

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

```
hostname# show asp table interfaces

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

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

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

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

Related Commands

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

show asp table routing

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

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

Syntax Description

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

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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

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

```
hostname# show asp table routing

in   255.255.255.255 255.255.255.255 identity
```

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

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

show asp table vpn-context

To debug the accelerated security path VPN context tables, use the **show asp table vpn-context** command in privileged EXEC mode.

> **show asp table vpn-context** [**detail**]

Syntax Description	detail	(Optional) Shows additional detail for the VPN context tables.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines   The **show asp table vpn-context** command shows the VPN context contents of the accelerated security path, which might help you troubleshoot a problem. See the *Cisco Security Appliance Command Line Configuration Guide* for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples   The following is sample output from the **show asp table vpn-context** command:

```
hostname# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

The following is sample output from the **show asp table vpn-context detail** command:

```
hostname# show asp table vpn-context detail
```

```
VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

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

show blocks

To show the packet buffer utilization, use the **show blocks** command in privileged EXEC mode.

show blocks [{**address** *hex* | **all** | **assigned** | **free** | **old** | **pool** *size* [**summary**]} [**diagnostics** | **dump** | **header** | **packet**] | **queue history** [**detail**]]

Syntax Description		
address *hex*	(Optional) Shows a block corresponding to this address, in hexadecimal.
all	(Optional) Shows all blocks.
assigned	(Optional) Shows blocks that are assigned and in use by an application.
detail	(Optional) Shows a portion (128 bytes) of the first block for each unique queue type.
dump	(Optional) Shows the entire block contents, including the header and packet information. The difference between dump and packet is that dump includes additional information between the header and the packet.
diagnostics	(Optional) Shows block diagnostics.
free	(Optional) Shows blocks that are available for use.
header	(Optional) Shows the header of the block.
old	(Optional) Shows blocks that were assigned more than a minute ago.
packet	(Optional) Shows the header of the block as well as the packet contents.
pool *size*	(Optional) Shows blocks of a specific size.
queue history	(Optional) Shows where blocks are assigned when the security appliance runs out of blocks. Sometimes, a block is allocated from the pool but never assigned to a queue. In that case, the location is the code address that allocated the block.
summary	(Optional) Shows detailed information about block usage sorted by the program addresses of applications that allocated blocks in this class, program addresses of applications that released blocks in this class, and the queues to which valid blocks in this class belong.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	The **pool summary** option was added.

Usage Guidelines   The **show blocks** command helps you determine if the security appliance is overloaded. This command lists preallocated system buffer utilization. A full memory condition is not a problem as long as traffic is moving through the security appliance. You can use the **show conn** command to see if traffic is moving. If traffic is not moving and the memory is full, there may be a problem.

You can also view this information using SNMP.

The information shown in a security context includes the system-wide information as well as context-specific information about the blocks in use and the high water mark for block usage.

See the "Examples" section for a description of the display output.

Examples   The following is sample output from the **show blocks** command in single mode:

```
hostname# show blocks
  SIZE    MAX     LOW     CNT
     4   1600    1598    1599
    80    400     398     399
   256   3600    3540    3542
  1550   4716    3177    3184
 16384     10      10      10
  2048   1000    1000    1000
```

Table 25-1 shows each field description.

Table 25-1   show blocks Fields

Field	Description
SIZE	Size, in bytes, of the block pool. Each size represents a particular type. Examples are shown below.
4	Duplicates existing blocks in applications such as DNS, ISAKMP, URL filtering, uauth, TFTP, and TCP modules.
80	Used in TCP intercept to generate acknowledgment packets and for failover hello messages.
256	Used for Stateful Failover updates, syslogging, and other TCP functions.
	These blocks are mainly used for Stateful Failover messages. The active security appliance generates and sends packets to the standby security appliance to update the translation and connection table. In bursty traffic, where high rates of connections are created or torn down, the number of available blocks might drop to 0. This situation indicates that one or more connections were not updated to the standby security appliance. The Stateful Failover protocol catches the missing translation or connection the next time. If the CNT column for 256-byte blocks stays at or near 0 for extended periods of time, then the security appliance is having trouble keeping the translation and connection tables synchronized because of the number of connections per second that the security appliance is processing.
	Syslog messages sent out from the security appliance also use the 256-byte blocks, but they are generally not released in such quantity to cause a depletion of the 256-byte block pool. If the CNT column shows that the number of 256-byte blocks is near 0, ensure that you are not logging at Debugging (level 7) to the syslog server. This is indicated by the logging trap line in the security appliance configuration. We recommend that you set logging at Notification (level 5) or lower, unless you require additional information for debugging purposes.

Table 25-1   show blocks Fields (continued)

Field	Description
1550	Used to store Ethernet packets for processing through the security appliance.
	When a packet enters a security appliance interface, it is placed on the input interface queue, passed up to the operating system, and placed in a block. The security appliance determines whether the packet should be permitted or denied based on the security policy and processes the packet through to the output queue on the outbound interface. If the security appliance is having trouble keeping up with the traffic load, the number of available blocks will hover close to 0 (as shown in the CNT column of the command output). When the CNT column is zero, the security appliance attempts to allocate more blocks, up to a maximum of 8192. If no more blocks are available, the security appliance drops the packet.
16384	Only used for the 64-bit, 66-MHz Gigabit Ethernet cards (i82543).
	See the description for 1550 for more information about Ethernet packets.
2048	Control or guided frames used for control updates.
MAX	Maximum number of blocks available for the specified byte block pool. The maximum number of blocks are carved out of memory at bootup. Typically, the maximum number of blocks does not change. The exception is for the 256- and 1550-byte blocks, where the security appliance can dynamically create more when needed, up to a maximum of 8192.
LOW	Low-water mark. This number indicates the lowest number of this size blocks available since the security appliance was powered up, or since the last clearing of the blocks (with the **clear blocks** command). A zero in the LOW column indicates a previous event where memory was full.
CNT	Current number of blocks available for that specific size block pool. A zero in the CNT column means memory is full now.

The following is sample output from the **show blocks all** command:

```
hostname# show blocks all
Class 0, size 4
     Block    allocd_by      freed_by  data size     alloccnt      dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0            0            0 alloc not_specified
0x01798e80  0x00000000  0x00101603          0            0            0 alloc not_specified
0x017983c0  0x00000000  0x00101603          0            0            0 alloc not_specified

...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

Table 25-2 shows each field description.

Table 25-2   show blocks all Fields

Field	Description
Block	The block address.
allocd_by	The program address of the application that last used the block (0 if not used).
freed_by	The program address of the application that last released the block.
data size	The size of the application buffer/packet data that is inside the block.

Table 25-2   show blocks all Fields

Field	Description
alloccnt	The number of times this block has been used since the block came into existence.
dup_cnt	The current number of references to this block if used: 0 means 1 reference, 1 means 2 references.
oper	One of the four operations that was last performed on the block: alloc, get, put, or free.
location	The application that uses the block, or the program address of the application that last allocated the block (same as the allocd_by field).

The following is sample output from the **show blocks** command in a context:

```
hostname/contexta# show blocks
  SIZE    MAX     LOW    CNT  INUSE   HIGH
     4   1600    1599   1599      0      0
    80    400     400    400      0      0
   256   3600    3538   3540      0      1
  1550   4616    3077   3085      0      0
```

The following is sample output from the **show blocks queue history** command:

```
hostname# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type         User        Context
    186     1 put                                     contexta
     15     1 put                                     contexta
      1     1 put                                     contexta
      1     1 put                                     contextb
      1     1 put                                     contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type         User        Context
     21     1 put                                     contexta
      1     1 put                                     contexta
      1     1 put                                     contexta
      1     1 put                                     contextb
      1     1 put                                     contextc
Blk_cnt Q_cnt Last_Op Queue_Type         User        Context
    200     1 alloc   ip_rx              tcp         contexta
    108     1 get     ip_rx              udp         contexta
     85     1 free    fixup              h323_ras    contextb
     42     1 put     fixup              skinny      contextb

Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type         User        Context
    186     1 put                                     contexta
     15     1 put                                     contexta
      1     1 put                                     contexta
      1     1 put                                     contextb
      1     1 put                                     contextc
...
```

The following is sample output from the **show blocks queue history detail** command:

```
hostname# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
```

```
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type       User        Context
    186    1 put                                    contexta
     15    1 put                                    contexta
      1    1 put                                    contexta
      1    1 put                                    contextb
      1    1 put                                    contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type       User        Context
     21    1 put                                    contexta
      1    1 put                                    contexta
      1    1 put                                    contexta
      1    1 put                                    contextb
      1    1 put                                    contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

The following is sample output from the **show blocks pool summary** command:

```
hostname# show blocks pool 1550 summary
Class 3, size 1550

================================================
       total_count=1531    miss_count=0
Alloc_pc        valid_cnt        invalid_cnt
0x3b0a18        00000256        00000000
       0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000012
       0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
       total_count=9716    miss_count=0
Freed_pc        valid_cnt        invalid_cnt
0x9a81f3        00000104        00000007
       0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326        00000053        00000033
       0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2        00000005        00000000
       0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
```

```
          total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

==================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0   03a8b7c0   03a7fc40   03a6ff20   03a6f5c0   03a6ec60 kao-f1#
```

Table 25-3 shows each field description.

Table 25-3   show blocks pool summary Fields

Field	Description
total_count	The number of blocks for a given class.
miss_count	The number of blocks not reported in the specified category due to technical reasons.
Freed_pc	The program addresses of applications that released blocks in this class.
Alloc_pc	The program addresses of applications that allocated blocks in this class.
Queue	The queues to which valid blocks in this class belong.
valid_cnt	The number of blocks that are currently allocated.
invalid_cnt	The number of blocks that are not currently allocated.
Invalid Bad qtype	Either this queue has been freed and the contents are invalid or this queue was never initialized.
Valid tcp_usr_conn_inp	The queue is valid.

Related Commands

Command	Description
blocks	Increases the memory assigned to block diagnostics
clear blocks	Clears the system buffer statistics.
show conn	Shows active connections.

show bootvar

To show the boot file and configuration properties, use the **show boot** command in privileged configuration mode.

show bootvar

Syntax Description

show bootvar	The system boot properties.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines   The BOOT variable specifies a list of bootable images on various devices. The CONFIG_FILE variable specifies the configuration file used during system initialization. Set these variables with the **boot system** command, and **boot config** command, respectively.

Examples   The following example, the BOOT variable contains disk0:/f1_image, which is the image booted when the system reloads. The current value of BOOT is disk0:/f1_image; disk0:/f1_backupimage. This meansboot variable has been modified with the boot system command, but the running configuration has notbeen saved with the **write memory** command. When the running config is saved, the BOOT variable and current BOOT variable will both be disk0:/f1_image; disk0:/f1_backupimage. Assuming the running configuration is saved the boot loader will attempt to load the contents of the BOOT variable, starting with disk0:/f1image, but if that is not present or invalid, it will attempt to boot disk0:1/f1_backupimage.

The CONFIG_FILE variable points to the system startup configuration. In this example it is not set, so the startup configuration file is the default specified with the **boot config** command. The current CONFIG_FILE variable may be modified with the **boot config** command and saved with the **write memory** command.

```
hostname# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
CONFIG_FILE variable =
Current CONFIG_FILE variable =
hostname#
```

Related Commands	Command	Description
	boot	Specifies the configuration file or image file used at startup.

show capture

To display the capture configuration when no options are specified, use the **show capture** command.

> **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**]
> [**dump**] [**packet-number** *number*]

Syntax Description

capture_name	(Optional) Name of the packet capture.
access-list *access_list_name*	(Optional) Displays information for packets that are based on IP or higher fields for the specific access list identification.
count *number*	(Optional) Displays the number of packets specified data.
decode	This option is useful when a capture of type isakmp is applied to an interface. All isakmp data flowing through that interface will be captured after decryption and shown with more information after decoding the fields.
detail	(Optional) Displays additional protocol information for each packet.
dump	(Optional) Displays a hexadecimal dump of the packets that are transported over the data link transport.
packet-number *number*	Starts the display at the specified packet number.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If you specify the *capture_name*, then the capture buffer contents for that capture are displayed.

The **dump** keyword does not display MAC information in the hexadecimal dump.

The decoded output of the packets depend on the protocol of the packet. In Table 25-4, the bracketed output is displayed when you specify the **detail** keyword.

Table 25-4   Packet Capture Output Formats

Packet Type	Capture Output Format
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*

Table 25-4   Packet Capture Output Formats (continued)

Packet Type	Capture Output Format
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source > ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/Other	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
Other	*HH:MM:SS.ms ether-hdr*: *hex-dump*

Examples   This example shows how to display the capture configuration:

```
hostname(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

This example shows how to display the packets that are captured by an ARP capture:

```
hostname(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
clear capture	Clears the capture buffer.
copy capture	Copies a capture file to a server.

show chardrop

To display the count of characters dropped from the serial console, use the **show chardrop** command in privileged EXEC mode.

show chardrop

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples   The following is sample output from the **show chardrop** command:

```
hostname# show chardrop
Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

show checkheaps

To show the checkheaps statistics, use the **show checkheaps** command in privileged EXEC mode. Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

> **show checkheaps**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples   The following is sample output from the **show checkheaps** command:

```
hostname# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run    : 42 secs
Duration of last run           : 0 millisecs
Number of buffers created      : 8082
Number of buffers allocated    : 7808
Number of buffers free         : 274
Total memory in use            : 43570344 bytes
Total memory in free buffers   : 87000 bytes
Total number of runs           : 310
```

Related Commands

Command	Description
checkheaps	Sets the checkheap verification intervals.

show checksum

To display the configuration checksum, use the **show checksum** command in privileged EXEC mode.

show checksum

Syntax Description   This command has no arguments or keywords.

Defaults   This command has no default settings.

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

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

Command History

Release	Modification
7.0(1)	Support for this command was introduced on the security appliance.

Usage Guidelines   The **show checksum** command allows you to display four groups of hexadecimal numbers that act as a digital summary of the configuration contents. This checksum is calculated only when you store the configuration in Flash memory.

If a dot (".") appears before the checksum in the **show config** or **show checksum** command output, the output indicates a normal configuration load or write mode indicator (when loading from or writing to the security appliance Flash partition). The "." shows that the security appliance is preoccupied with the operation, but is not "hung up." This message is similar to a "system processing, please wait" message.

Examples   This example shows how to display the configuration or the checksum:

```
hostname(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

To display the chunk statistics, use the **show chunkstat** command in privileged EXEC mode.

> **show chunkstat**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples   This example shows how to display the chunk statistics:

```
hostname# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end
@ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.
show cpu	Displays the CPU utilization information.

show class

To show the contexts assigned to a class, use the **show class** command in privileged EXEC mode.

show class *name*

Syntax Description

name	Specifies the name as a string up to 20 characters long. To show the default class, enter **default** for the name.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following is sample output from the **show class default** command:

```
hostname# show class default

Class Name        Members    ID   Flags
default           All        1    0001
```

Related Commands

Command	Description
class	Configures a resource class.
clear configure class	Clears the class configuration.
context	Configures a security context.
limit-resource	Sets the resource limit for a class.
member	Assigns a context to a resource class.

show clock

To view the time on the security appliance, use the **show clock** command in user EXEC mode.

> **show clock** [**detail**]

Syntax Description

detail	(Optional) Indicates the clock source (NTP or user configuration) and the current summer-time setting (if any).

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples   The following is sample output from the **show clock** command:

```
hostname> show clock
12:35:45.205 EDT Tue Jul 27 2004
```

The following is sample output from the **show clock detail** command:

```
hostname> show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

Related Commands

Command	Description
clock set	Manually sets the clock on the security appliance.
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.
ntp server	Identifies an NTP server.
show ntp status	Shows the status of the NTP association.

show compression svc

To view compression statistics for SVC connections on the security appliance, use the **show compression svc** command from privileged EXEC mode:

> **show compression svc**

Defaults   There is no default behavior for this command.

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples   The following example shows the output of the **show compression svc** command:

```
hostname# show compression svc
Compression SVC Sessions                  1
Compressed Frames                    249756
Compressed Data In (bytes)          0048042
Compressed Data Out (bytes)         4859704
Expanded Frames                           1
Compression Errors                        0
Compression Resets                        0
Compression Output Buf Too Small          0
Compression Ratio                      2.06
Decompressed Frames                  876687
Decompressed Data In              279300233
```

Related Commands

Command	Description
compression	Enables compression for all SVC and WebVPN connections.
svc compression	Enables compression of http data over an SVC connection for a specific group or user.

show configuration

To display the adaptive security appliance configuration , use the **show configuration** command in global configuration mode.

> **show configuration**

Syntax Description   This command has no arguments or keywords.

Defaults   This command has no default settings.

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	Support for this command was introduced on the security appliance.

Usage Guidelines   The **show configuration** command allows you to display settings on the adaptive security appliance.

Examples   This example shows how to display the configuration:

```
hostname(config)# show configuration
: Saved
: Written by enable_15 at 23:04:47.770 UTC Thu Apr 14 2005
!
ASA Version 7.2(2)22
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
multicast-routing
names
dns-guard
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.11.2.5 255.255.255.0
 ospf network point-to-point non-broadcast
 ospf authentication-key hello
 ospf message-digest-key 1 md5 2234
!
interface GigabitEthernet0/0.1
 vlan 702
```

```
 nameif outside1
 security-level 0
 no ip address
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 195.130.12.3 255.255.255.0
 igmp version 1
!
interface GigabitEthernet0/1.1
 vlan 400
 nameif third
 security-level 0
 ip address 195.133.12.3 255.255.255.0
!
interface GigabitEthernet0/1.2
 vlan 401
 nameif fourth
 security-level 0
 ip address 195.133.13.3 255.255.255.0
!
interface GigabitEthernet0/1.3
 vlan 402
 nameif fifth
 security-level 0
 ip address 195.180.12.3 255.255.255.0
!
interface GigabitEthernet0/1.4
 vlan 140
 nameif sixth
 security-level 0
 ip address 195.180.13.3 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/cdisk.7.2.2.22
ftp mode passive
access-list permitIp extended permit ip any any
pager lines 24
logging console debugging
mtu inside 1500
mtu outside1 1500
mtu outside 1500
mtu third 1500
mtu fourth 1500
```

```
mtu fifth 1500
mtu sixth 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdmfile.50074.rls
no asdm history enable
arp timeout 14400
global (outside) 1 195.130.12.111-195.130.12.119
global (fifth) 1 195.180.12.30-195.180.12.33
global (sixth) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
access-group permitIp in interface inside
access-group permitIp in interface outside
!
route-map map1 permit 0
!
route-map map1 permit 10
!
route-map map1 permit 65535
 match metric 0
 set metric 0
!
route inside 10.129.0.30 255.255.255.255 10.11.2.2 1
route outside 0.0.0.0 0.0.0.0 195.130.12.25 1
route outside 11.1.0.0 255.255.0.0 195.130.12.55 1
route outside 20.1.0.0 255.255.0.0 195.130.12.23 1
route outside 50.0.0.0 255.0.0.0 195.130.12.120 1
route outside 88.0.0.0 255.0.0.0 195.130.12.120 1
route outside 158.1.1.0 255.255.255.0 195.130.12.120 1
route third 108.1.1.1 255.255.255.255 195.133.12.15 1
!
router ospf 1
 network 10.11.2.0 255.255.255.0 area 10.11.2.0
 area 10.11.2.0 virtual-link 192.168.5.2
 neighbor 10.11.2.2
 log-adj-changes
 redistribute static subnets
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd dns 1.3.3.3
!
!
class-map class_sip_tcp
 match port tcp eq sip
class-map class_sip_udp
 match port udp eq sip
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
```

```
          inspect h323 ras
          inspect rsh
          inspect rtsp
          inspect esmtp
          inspect sqlnet
          inspect skinny
          inspect sunrpc
          inspect xdmcp
          inspect netbios
          inspect tftp
          inspect sip
        class class_sip_tcp
          inspect sip
        class class_sip_udp
          inspect sip
        !
       service-policy global_policy global
       prompt hostname context
       Cryptochecksum:796d8c57a13e9ded7e77e34fcc7a6f78
       hostname(config)#
```

show conn

To display the connection state for the designated connection type, use the **show conn** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

> **show conn** [**count** | [**all**] [**detail**] [**long**] [**state** *state_type*] [**protocol** {**tcp** | **udp**}]
> [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]]
> [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*]]]

Syntax Description

address	(Optional) Displays connections with the specified source or destination IP address.
all	(Optional) Displays connections that are to the device or from the device, in addition to through-traffic connections.
count	(Optional) Displays the number of active connections.
dest_ip	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-), For example: `10.1.1.1-10.1.1.5`
dest_port	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-), For example: `1000-2000`
detail	(Optional) Displays connections in detail, including translation type and interface information.
long	(Optional) Displays connections in long format.
netmask *mask*	(Optional) Specifies a subnet mask for use with the given IP address.
port	(Optional) Displays connections with the specified source or destination port.
protocol {**tcp**	**udp**}	(Optional) Specifies the connection protocol, **tcp** or **udp**.
src_ip	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-), For example: `10.1.1.1-10.1.1.5`
src_port	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-), For example: `1000-2000`
state *state_type*	(Optional) Specifies the connection state type. See Table 25-5 for a list of the keywords available for connection state types.

Defaults   All through connections are shown by default. You need to use the **all** keyword to also view management connections to the device.

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

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

Command History

Release	Modification
7.0(8)/7.2(4)	The syntax was simplified to use source and destination concepts instead of "local" and "foreign." In the new syntax, the source address is the first address entered and the destination is the second address. The old syntax used keywords like **foreign** and **fport** to determine the destination address and port.
7.2(5)	The **tcp_embryonic** state type was added. This type shows all TCP connections with the i flag (incomplete connections); i flag connections for UDP are not shown.

Usage Guidelines   The **show conn** command displays the number of active TCP and UDP connections, and provides information about connections of various types. Use the **show conn all** command to see the entire table of connections.

✎
Note   When the security appliance creates a pinhole to allow secondary connections, this is shown as an incomplete conn by the **show conn** command. To clear this incomplete conn use the **clear conn** command.

The connection types that you can specify using the **show conn state** command are defined in Table 25-5. When specifying multiple connection types, use commas without spaces to separate the keywords.

Table 25-5   Connection State Types

Keyword	Connection Type Displayed
up	Connections in the up state.
conn_inbound	Inbound connections.
ctiqbe	CTIQBE connections
data_in	Inbound data connections.
data_out	Outbound data connections.
finin	FIN inbound connections.
finout	FIN outbound connections.
h225	H.225 connections
h323	H.323 connections
http_get	HTTP get connections.

Table 25-5   Connection State Types (continued)

Keyword	Connection Type Displayed
mgcp	MGCP connections.
nojava	Connections that deny access to Java applets.
rpc	RPC connections.
service_module	Connections being scanned by an SSM.
sip	SIP connections.
skinny	SCCP connections.
smtp_data	SMTP mail data connections.
tcp_embryonic	TCP embryonic connections.
sqlnet_fixup_data	SQL*Net data inspection engine connections.

When you use the **detail** option, the system displays information about the translation type and interface information using the connection flags defined in Table 25-6.

Table 25-6   Connection Flags

Flag	Description
a	awaiting outside ACK to SYN
A	awaiting inside ACK to SYN
B	initial SYN from outside
C	Computer Telephony Interface Quick Buffer Encoding (CTIQBE) media connection
d	dump
D	DNS
E	outside back connection
f	inside FIN
F	outside FIN
g	Media Gateway Control Protocol (MGCP) connection
G	connection is part of a group[1]
h	H.225
H	H.323
i	incomplete TCP or UDP connection
I	inbound data
k	Skinny Client Control Protocol (SCCP) media connection
K	GTP t3-response
m	SIP media connection
M	SMTP data
O	outbound data
p	replicated (unused)
P	inside back connection

Table 25-6   Connection Flags (continued)

Flag	Description
q	SQL*Net data
r	inside acknowledged FIN
R	outside acknowledged FIN for TCP connection
R	UDP RPC[2]
s	awaiting outside SYN
S	awaiting inside SYN
t	SIP transient connection[3]
T	SIP connection[4]
U	up
X	Inspected by the service module, such as a CSC SSM.

1. The G flag indicates the connection is part of a group. It is set by the GRE and FTP Strict fixups to designate the control connection and all its associated secondary connections. If the control connection terminates, then all associated secondary connections are also terminated.

2. Because each row of **show conn** command output represents one connection (TCP or UDP), there will be only one R flag per row.

3. For UDP connections, the value t indicates that it will timeout after one minute.

4. For UDP connections, the value T indicates that the connection will timeout according to the value specified using the **timeout sip** command.

Note For connections using a DNS server, the source port of the connection may be replaced by the *IP address of DNS server* in the **show conn** command output.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by *app_id*, and the idle timer for each app_id runs independently.

Because the app_id expires independently, a legitimate DNS response can only pass through the security appliance within a limited period of time and there is no resource build-up. However, when you enter the **show conn** command, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

Note When there is no TCP traffic for the period of inactivity defined by the **conn timeout** command (by default, 1:00:00), the connection is closed and the corresponding conn flag entries are no longer displayed.

When the following TCP connection directionality flags are applied to connections between same-security interfaces (see the **same-security permit** command), the direction in the flag is not relevant because for same-security interfaces, there is no "inside" or "outside." Because the security appliance has to use these flags for same-security connections, the security appliance may choose one flag over another (for example, f vs. F) based on other connection characteristics, but you should ignore the directionality chosen.

- B—Initial SYN from outside

- a—Awaiting outside ACK to SYN

- A—Awaiting inside ACK to SYN

- f—Inside FIN

- F—Outside FIN

- s—Awaiting outside SYN

- S—Awaiting inside SYN

Examples   When specifying multiple connection types, use commas without spaces to separate the keywords. The following example displays information about RPC, H.323, and SIP connections in the Up state:

```
hostname# show conn state up,rpc,h323,sip
```

The following example shows a TCP session connection from inside host 10.1.1.15 to the outside Telnet server at 192.168.49.10. Because there is no B flag, the connection is initiated from the inside. The "U", "I", and "O" flags denote that the connection is active and has received inbound and outbound data.

```
hostname# show conn
2 in use, 2 most used
TCP out 192.168.49.10:23 in 10.1.1.15:1026 idle 0:00:22
Bytes 1774 flags UIO
UDP out 192.168.49.10:31649 in 10.1.1.15:1028 idle 0:00:14
flags D-
```

The following example includes the "X" flag to indicate that the connection is being scanned by the SSM.

```
hostname(config)# show conn address 10.0.0.122 state service_module
TCP out 10.1.0.121:22 in 10.0.0.122:34446 idle 0:00:03 bytes 2733 flags UIOX
```

The following example shows a UDP connection from outside host 192.168.49.10 to inside host 10.1.1.15. The D flag denotes that this is a DNS connection. The number 1028 is the DNS ID over the connection.

```
hostname(config)# show conn detail
2 in use, 2 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIBQE media, D - DNS, d - dump,
       E - outside back connection, f - inside FIN, F - outside FIN,
       G - group, g - MGCP, H - H.323, h - H.255.0, I - inbound data, i - incomplete,
       k - Skinny media, M - SMTP data, m - SIP media
       O - outbound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
       X - inspected by service module
TCP outside:192.168.49.10/23 inside:10.1.1.15/1026 flags UIO
UDP outside:192.168.49.10/31649 inside:10.1.1.15/1028 flags dD
```

The following is sample output from the **show conn all** command:

```
hostname# show conn all
6 in use, 6 most used
  TCP out 209.165.201.1:80 in 10.3.3.4:1404 idle 0:00:00 Bytes 11391
  TCP out 209.165.201.1:80 in 10.3.3.4:1405 idle 0:00:00 Bytes 3709
  TCP out 209.165.201.1:80 in 10.3.3.4:1406 idle 0:00:01 Bytes 2685
  TCP out 209.165.201.1:80 in 10.3.3.4:1407 idle 0:00:01 Bytes 2683
  TCP out 209.165.201.1:80 in 10.3.3.4:1403 idle 0:00:00 Bytes 15199
  TCP out 209.165.201.1:80 in 10.3.3.4:1408 idle 0:00:00 Bytes 2688
```

```
UDP out 209.165.201.7:24 in 10.3.3.4:1402 idle 0:01:30
UDP out 209.165.201.7:23 in 10.3.3.4:1397 idle 0:01:30
UDP out 209.165.201.7:22 in 10.3.3.4:1395 idle 0:01:30
```

In this example, host 10.3.3.4 on the inside has accessed a website at 209.165.201.1. The global address on the outside interface is 209.165.201.7.

	Commands	Description
Related Commands	**clear conn**	Clears connections.
	inspect ctiqbe	Enables CTIQBE application inspection.
	inspect h323	Enables H.323 application inspection.
	inspect mgcp	Enables MGCP application inspection.
	inspect sip	Removes Java applets from HTTP traffic.
	inspect skinny	Enables SCCP application inspection.

show console-output

To display the currently captured console output, use the **show console-output** command in privileged EXEC mode.

> **show console-output**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples   The following example shows the message that displays when there is no console output:

```
hostname# show console-output
Sorry, there are no messages to display
```

Related Commands

Command	Description
clear configure console	Restores the default console connection settings.
clear configure timeout	Restores the default idle time durations in the configuration.
console timeout	Sets the idle timeout for a console connection to the security appliance.
show running-config console timeout	Displays the idle timeout for a console connection to the security appliance.

show context

To show context information including allocated interfaces and the configuration file URL, the number of contexts configured, or from the system execution space, a list of all contexts, use the **show context** command in privileged EXEC mode.

> **show context** [*name* | **detail** | **count**]

Syntax Description

count	(Optional) Shows the number of contexts configured.
detail	(Optional) Shows additional detail about the context(s) including the running state and information for internal use.
name	(Optional) Sets the context name. If you do not specify a name, the security appliance displays all contexts. Within a context, you can only enter the current context name.

Defaults

In the system execution space, the security appliance displays all contexts if you do not specify a name.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

See the "Examples" section for a description of the display output.

Examples

The following is sample output from the **show context** command. The following sample display shows three contexts:

```
hostname# show context

Context Name      Interfaces                URL
*admin            GigabitEthernet0/1.100    flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200    flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300    flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

Table 25-7 shows each field description.

Table 25-7   show context Fields

Field	Description
Context Name	Lists all context names. The context name with the asterisk (*) is the admin context.
Interfaces	The interfaces assigned to the context.
URL	The URL from which the security appliance loads the context configuration.

The following is sample output from the **show context detail** command:

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
    GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
    GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
    GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
    GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

Table 25-8 shows each field description.

Table 25-8   Context States

Field	Description
Context	The context name. The null context information is for internal use only. The system context represents the system execution space.
State Message:	The context state. See the possible messages below.

Table 25-8   Context States

Field	Description
Has been created, but initial ACL rules not complete	The security appliance parsed the configuration but has not yet downloaded the default ACLs to establish the default security policy. The default security policy applies to all contexts initially, and includes disallowing traffic from lower security levels to higher security levels, enabling application inspection, and other parameters. This security policy ensures that no traffic can pass through the security appliance after the configuration is parsed but before the configuration ACLs are compiled. You are unlikely to see this state because the configuration ACLs are compiled very quickly.
Has been created, but not initialized	You entered the **context** *name* command, but have not yet entered the **config-url** command.
Has been created, but the config hasn't been parsed	The default ACLs were downloaded, but the security appliance has not parsed the configuration. This state might exist because the configuration download might have failed because of network connectivity issues, or you have not yet entered the **config-url** command. To reload the configuration, from within the context, enter **copy startup-config running-config**. From the system, reenter the **config-url** command. Alternatively, you can start configuring the blank running configuration.
Is a system resource	This state applies only to the system execution space and to the null context. The null context is used by the system, and the information is for internal use only.
Is a zombie	You deleted the context using the **no context** or **clear context** command, but the context information persists in memory until the security appliance reuses the context ID for a new context, or you restart.
Is active	This context is currently running and can pass traffic according to the context configuration security policy.
Is ADMIN and active	This context is the admin context and is currently running.
Was a former ADMIN, but is now a zombie	You deleted the admin context using the **clear configure context** command, but the context information persists in memory until the security appliance reuses the context ID for a new context, or you restart.
Real Interfaces	The interfaces assigned to the context. If you mapped the interface IDs in the **allocate-interface** command, this display shows the real name of the interface. The system execution space includes all interfaces.
Mapped Interfaces	If you mapped the interface IDs in the **allocate-interface** command, this display shows the mapped names. If you did not map the interfaces, the display lists the real names again.
Flag	For internal use only.
ID	An internal ID for this context.

The following is sample output from the **show context count** command:

```
hostname# show context count
Total active contexts: 2
```

Related Commands	Command	Description
	admin-context	Sets the admin context.
	allocate-interface	Assigns interfaces to a context.
	changeto	Changes between contexts or the system execution space.
	config-url	Specifies the location of the context configuration.
	context	Creates a security context in the system configuration and enters context configuration mode.

■ show controller

show controller

To view controller-specific information of all interfaces present in the system of an ASA 5505 adaptive security appliance, use the **show controller** command in privileged EXEC mode.

show controller [*switch_port*]

Syntax Description

switch_port	(Optional) Identifies the interface ID: **ethernet0/0** through **ethernet0/7**.

Defaults

If you do not identify a switch port, this command shows information for all interfaces.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command helps Cisco TAC gather useful debug information about the controller when investigating internal and customer found defects.

Examples

The following is sample output from the **show controller** command:

```
hostname# show controller

Ethernet0/0:
   Marvell 88E6095 revision 2, switch port 7
     PHY Register:
        Control:       0x3000  Status:       0x786d
        Identifier1:   0x0141  Identifier2:  0x0c85
        Auto Neg:      0x01e1  LP Ability:   0x40a1
        Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
        PHY Status:    0x4c00  PHY Intr En:  0x0400
        Int Port Sum:  0x0000  Rcv Err Cnt:  0x0000
        Led select:    0x1a34
        Reg 29:        0x0003  Reg 30:       0x0000
     Port Registers:
        Status:        0x0907  PCS Ctrl:     0x0003
        Identifier:    0x0952  Port Ctrl:    0x0074
        Port Ctrl-1:   0x0000  Vlan Map:     0x077f
        VID and PRI:   0x0001  Port Ctrl-2:  0x0cc8
        Rate Ctrl:     0x0000  Rate Ctrl-2:  0x3000
```

```
          Port Asc Vt:    0x0080
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

     Global Registers:
          Control:        0x0482


-----------------------------------------------------------------------
Number of VLANs: 1
-----------------------------------------------------------------------
Vlan[db]\Port| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
-----------------------------------------------------------------------
  <0001[01]> | EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUM| NM | NM |
-----------------------------------------------------------------------

Ethernet0/1:
   Marvell 88E6095 revision 2, switch port 6
     PHY Register:
          Control:        0x3000  Status:        0x7849
          Identifier1:    0x0141  Identifier2:   0x0c85
          Auto Neg:       0x01e1  LP Ability:    0x0000
          Auto Neg Ex:    0x0004  PHY Spec Ctrl: 0x0130
          PHY Status:     0x0040  PHY Intr En:   0x0400
          Int Port Sum:   0x0000  Rcv Err Cnt:   0x0000
          Led select:     0x1a34
          Reg 29:         0x0003  Reg 30:        0x0000
     Port Registers:
          Status:         0x0007  PCS Ctrl:      0x0003
          Identifier:     0x0952  Port Ctrl:     0x0077
          Port Ctrl-1:    0x0000  Vlan Map:      0x07bf
          VID and PRI:    0x0001  Port Ctrl-2:   0x0cc8
          Rate Ctrl:      0x0000  Rate Ctrl-2:   0x3000
          Port Asc Vt:    0x0040
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/2:
   Marvell 88E6095 revision 2, switch port 5
     PHY Register:
          Control:        0x3000  Status:        0x786d
          Identifier1:    0x0141  Identifier2:   0x0c85
          Auto Neg:       0x01e1  LP Ability:    0x41e1
          Auto Neg Ex:    0x0005  PHY Spec Ctrl: 0x0130
          PHY Status:     0x6c00  PHY Intr En:   0x0400
          Int Port Sum:   0x0000  Rcv Err Cnt:   0x0000
          Led select:     0x1a34
          Reg 29:         0x0003  Reg 30:        0x0000
     Port Registers:
          Status:         0x0d07  PCS Ctrl:      0x0003
          Identifier:     0x0952  Port Ctrl:     0x0077
          Port Ctrl-1:    0x0000  Vlan Map:      0x07df
          VID and PRI:    0x0001  Port Ctrl-2:   0x0cc8
          Rate Ctrl:      0x0000  Rate Ctrl-2:   0x3000
          Port Asc Vt:    0x0020
          In Discard Lo: 0x0000  In Discard Hi: 0x0000
          In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/3:
   Marvell 88E6095 revision 2, switch port 4
     PHY Register:
          Control:        0x3000  Status:        0x786d
          Identifier1:    0x0141  Identifier2:   0x0c85
          Auto Neg:       0x01e1  LP Ability:    0x41e1
          Auto Neg Ex:    0x0005  PHY Spec Ctrl: 0x0130
```

```
                 PHY Status:    0x6c00  PHY Intr En:   0x0400
                 Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
                 Led select:    0x1a34
                 Reg 29:        0x0003  Reg 30:        0x0000
              Port Registers:
                 Status:        0x0d07  PCS Ctrl:      0x0003
                 Identifier:    0x0952  Port Ctrl:     0x0077
                 Port Ctrl-1:   0x0000  Vlan Map:      0x07ef
                 VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
                 Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
                 Port Asc Vt:   0x0010
                 In Discard Lo: 0x0000  In Discard Hi: 0x0000
                 In Filtered:   0x0000  Out Filtered:  0x0000


       Ethernet0/4:
          Marvell 88E6095 revision 2, switch port 3
             PHY Register:
                 Control:       0x3000  Status:        0x786d
                 Identifier1:   0x0141  Identifier2:   0x0c85
                 Auto Neg:      0x01e1  LP Ability:    0x41e1
                 Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
                 PHY Status:    0x6c00  PHY Intr En:   0x0400
                 Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
                 Led select:    0x1a34
                 Reg 29:        0x0003  Reg 30:        0x0000
             Port Registers:
                 Status:        0x0d07  PCS Ctrl:      0x0003
                 Identifier:    0x0952  Port Ctrl:     0x0077
                 Port Ctrl-1:   0x0000  Vlan Map:      0x07f7
                 VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
                 Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
                 Port Asc Vt:   0x0008
                 In Discard Lo: 0x0000  In Discard Hi: 0x0000
                 In Filtered:   0x0000  Out Filtered:  0x0000


       Ethernet0/5:
          Marvell 88E6095 revision 2, switch port 2
             PHY Register:
                 Control:       0x3000  Status:        0x786d
                 Identifier1:   0x0141  Identifier2:   0x0c85
                 Auto Neg:      0x01e1  LP Ability:    0x41e1
                 Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
                 PHY Status:    0x6c00  PHY Intr En:   0x0400
                 Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
                 Led select:    0x1a34
                 Reg 29:        0x0003  Reg 30:        0x0000
             Port Registers:
                 Status:        0x0d07  PCS Ctrl:      0x0003
                 Identifier:    0x0952  Port Ctrl:     0x0077
                 Port Ctrl-1:   0x0000  Vlan Map:      0x07fb
                 VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
                 Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
                 Port Asc Vt:   0x0004
                 In Discard Lo: 0x0000  In Discard Hi: 0x0000
                 In Filtered:   0x0000  Out Filtered:  0x0000


       Ethernet0/6:
          Marvell 88E6095 revision 2, switch port 1
             PHY Register:
                 Control:       0x3000  Status:        0x7849
                 Identifier1:   0x0141  Identifier2:   0x0c85
                 Auto Neg:      0x01e1  LP Ability:    0x0000
                 Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
                 PHY Status:    0x0040  PHY Intr En:   0x8400
```

```
              Int Port Sum:  0x0000  Rcv Err Cnt:    0x0000
              Led select:    0x1a34
              Reg 29:        0x0003  Reg 30:         0x0000
          Port Registers:
              Status:        0x0007  PCS Ctrl:       0x0003
              Identifier:    0x0952  Port Ctrl:      0x0077
              Port Ctrl-1:   0x0000  Vlan Map:       0x07fd
              VID and PRI:   0x0001  Port Ctrl-2:    0x0cc8
              Rate Ctrl:     0x0000  Rate Ctrl-2:    0x3000
              Port Asc Vt:   0x0002
              In Discard Lo: 0x0000  In Discard Hi: 0x0000
              In Filtered:   0x0000  Out Filtered:  0x0000
          ----Inline power related counters and registers----
          Power on fault: 0  Power off fault: 0
          Detect enable fault: 0  Detect disable fault: 0
          Faults: 0
          Driver counters:
          I2C Read Fail: 0    I2C Write Fail: 0
          Resets: 1  Initialized: 1
          PHY reset error: 0
          LTC4259 registers:
          INTRPT STATUS = 0x88  INTRPT MASK  = 0x00  POWER EVENT  = 0x00
          DETECT EVENT  = 0x03  FAULT EVENT  = 0x00  TSTART EVENT = 0x00
          SUPPLY EVENT  = 0x02  PORT1 STATUS = 0x06  PORT2 STATUS = 0x06
          PORT3 STATUS  = 0x00  PORT4 STATUS = 0x00  POWER STATUS = 0x00
          OPERATE MODE  = 0x0f  DISC. ENABLE = 0x30  DT/CLASS ENBL = 0x33
          TIMING CONFIG = 0x00  MISC. CONFIG = 0x00


      Ethernet0/7:
          Marvell 88E6095 revision 2, switch port 0
            PHY Register:
              Control:       0x3000  Status:         0x7849
              Identifier1:   0x0141  Identifier2:    0x0c85
              Auto Neg:      0x01e1  LP Ability:     0x0000
              Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
              PHY Status:    0x0040  PHY Intr En:    0x8400
              Int Port Sum:  0x0000  Rcv Err Cnt:    0x0000
              Led select:    0x1a34
              Reg 29:        0x0003  Reg 30:         0x0000
          Port Registers:
              Status:        0x0007  PCS Ctrl:       0x0003
              Identifier:    0x0952  Port Ctrl:      0x0077
              Port Ctrl-1:   0x0000  Vlan Map:       0x07fe
              VID and PRI:   0x0001  Port Ctrl-2:    0x0cc8
              Rate Ctrl:     0x0000  Rate Ctrl-2:    0x3000
              Port Asc Vt:   0x0001
              In Discard Lo: 0x0000  In Discard Hi: 0x0000
              In Filtered:   0x0000  Out Filtered:  0x0000
          ----Inline power related counters and registers----
          Power on fault: 0  Power off fault: 0
          Detect enable fault: 0  Detect disable fault: 0
          Faults: 0
          Driver counters:
          I2C Read Fail: 0   I2C Write Fail: 0
          Resets: 1  Initialized: 1
          PHY reset error: 0
          LTC4259 registers:
          INTRPT STATUS = 0x88  INTRPT MASK  = 0x00  POWER EVENT  = 0x00
          DETECT EVENT  = 0x03  FAULT EVENT  = 0x00  TSTART EVENT = 0x00
          SUPPLY EVENT  = 0x02  PORT1 STATUS = 0x06  PORT2 STATUS = 0x06
          PORT3 STATUS  = 0x00  PORT4 STATUS = 0x00  POWER STATUS = 0x00
          OPERATE MODE  = 0x0f  DISC. ENABLE = 0x30  DT/CLASS ENBL = 0x33
          TIMING CONFIG = 0x00  MISC. CONFIG = 0x00
```

```
Internal-Data0/0:
  Y88ACS06 Register settings:
   rap                         0xe0004000 = 0x00000000
   ctrl_status                 0xe0004004 = 0x5501064a
   irq_src                     0xe0004008 = 0x00000000
   irq_msk                     0xe000400c = 0x00000000
   irq_hw_err_src              0xe0004010 = 0x00000000
   irq_hw_err_msk              0xe0004014 = 0x00001000
   bmu_cs_rxq                  0xe0004060 = 0x002aaa80
   bmu_cs_stxq                 0xe0004068 = 0x01155540
   bmu_cs_atxq                 0xe000406c = 0x012aaa80

  Bank 2: MAC address registers:
   mac_addr1_lo                0xe0004100 = 0x00000000
   mac_addr1_hi                0xe0004104 = 0x00000000
   mac_addr2_lo                0xe0004108 = 0x00000000
   mac_addr2_hi                0xe000410c = 0x00000000
   mac_addr3_lo                0xe0004110 = 0x00000000
   mac_addr3_hi                0xe0004114 = 0x00000000
   chip_info                   0xe0004118 = 0xb0110000
   eprom                       0xe000411c = 0x00000000
   flash_addr_reg              0xe0004120 = 0x0001fffe
   flash_data_port             0xe0004124 = 0x000000ff
   loader                      0xe0004128 = 0x00000400
   timer_init_val              0xe0004130 = 0x00000000
   timer_val                   0xe0004134 = 0x00000000
   timer_ctrl                  0xe0004138 = 0x00000202
   irq_mod_timer_init_val      0xe0004140 = 0x00000000
   irq_mod_timer               0xe0004144 = 0x00000000
   irq_mod_timer_ctrl          0xe0004148 = 0x00000202
   irq_mod_msk                 0xe000414c = 0x00000000
   irq_hw_err_mod_mask         0xe0004150 = 0x00000000
   tst_ctrl                    0xe0004158 = 0x00000001
   gp_io                       0xe000415c = 0x0000000f
   i2c_ctrl                    0xe0004160 = 0x00000000
   i2c_data                    0xe0004164 = 0x00000000
   i2c_irq                     0xe0004168 = 0x00000000
   i2c_sw                      0xe000416c = 0x00000003

  RAM Random Registers:
   ram_addr                    0xe0004180 = 0x00000000
   ram_data_port_lo            0xe0004184 = 0x00000000
   ram_data_port_hi            0xe0004188 = 0x00000000

  Ram Interface Registers:
   ram_if_to_lo                0xe0004190 = 0x24242424
   ram_if_to_hi                0xe0004194 = 0x00002424
   ram_if_timeout_val          0xe000419c = 0x00000000
   ram_if_ctrl                 0xe00041a0 = 0x000a0002

  Transmit Arbiter MAC:
   tx_arb_iti_init             0xe0004200 = 0x00000000
   tx_arb_iti_val              0xe0004204 = 0x00000000
   tx_arb_lim_init             0xe0004208 = 0x00000000
   tx_arb_lim_val              0xe000420c = 0x00000000
   tx_arb_ctrl_tst_status      0xe0004210 = 0x00001256

  Bank 8: Receive queue registers:
   rx_qregs.buf_ctrl           0xe0004400 = 0xc8550800
   rx_qregs.next_desc_addr_lo  0xe0004404 = 0x016d4020
   rx_qregs.buf_addr_lo        0xe0004408 = 0x019acd00
   rx_qregs.buf_addr_hi        0xe000440c = 0x00000000
   rx_qregs.frame_sw           0xe0004410 = 0x00000000
   rx_qregs.time_stamp         0xe0004414 = 0x00000000
```

```
    rx_qregs.tcp_csum              0xe0004418 = 0x00000000
    rx_qregs.tcp_csum_start        0xe000441c = 0x00000000
    rx_qregs.desc_addr_lo          0xe0004420 = 0x016d4000
    rx_qregs.desc_addr_hi          0xe0004424 = 0x00000000
    rx_qregs.addr_cntr_lo          0xe0004428 = 0x016d4020
    rx_qregs.addr_cntr_hi          0xe000442c = 0x00000000
    rx_qregs.byte_cntr             0xe0004430 = 0x00000000
    rx_qregs.bmu_cs                0xe0004434 = 0x002aaa80
    rx_qregs.flag                  0xe0004438 = 0x00000600
    rx_qregs.tst1                  0xe000443c = 0xd2020202
    rx_qregs.tst2                  0xe0004440 = 0x00000050
    rx_qregs.tst3                  0xe0004444 = 0x00000000

Bank 12: Synchronous transmit queue registers:
    stx_qregs.buf_ctrl             0xe0004600 = 0x00000000
    stx_qregs.next_desc_addr_lo    0xe0004604 = 0x00000000
    stx_qregs.buf_addr_lo          0xe0004608 = 0x00000000
    stx_qregs.buf_addr_hi          0xe000460c = 0x00000000
    stx_qregs.frame_sw             0xe0004610 = 0x00000000
    stx_qregs.time_stamp           0xe0004614 = 0x00000000
    stx_qregs.tcp_csum             0xe0004618 = 0x00000000
    stx_qregs.tcp_csum_start       0xe000461c = 0x00000000
    stx_qregs.desc_addr_lo         0xe0004620 = 0x00000000
    stx_qregs.desc_addr_hi         0xe0004624 = 0x00000000
    stx_qregs.addr_cntr_lo         0xe0004628 = 0x00000000
    stx_qregs.addr_cntr_hi         0xe000462c = 0x00000000
    stx_qregs.byte_cntr            0xe0004630 = 0x00000000
    stx_qregs.bmu_cs               0xe0004634 = 0x01155540
    stx_qregs.flag                 0xe0004638 = 0x0a000600
    stx_qregs.tst1                 0xe000463c = 0x02020202
    stx_qregs.tst2                 0xe0004640 = 0x00000050
    stx_qregs.tst3                 0xe0004644 = 0x00000000

Bank 13: Asynchronous transmit queue registers:
    atx_qregs.buf_ctrl             0xe0004680 = 0x00000000
    atx_qregs.next_desc_addr_lo    0xe0004684 = 0x00000000
    atx_qregs.buf_addr_lo          0xe0004688 = 0x00000000
    atx_qregs.buf_addr_hi          0xe000468c = 0x00000000
    atx_qregs.frame_sw             0xe0004690 = 0x00000000
    atx_qregs.time_stamp           0xe0004694 = 0x00000000
    atx_qregs.tcp_csum             0xe0004698 = 0x00000000
    atx_qregs.tcp_csum_start       0xe000469c = 0x00000000
    atx_qregs.desc_addr_lo         0xe00046a0 = 0x016d9000
    atx_qregs.desc_addr_hi         0xe00046a4 = 0x00000000
    atx_qregs.addr_cntr_lo         0xe00046a8 = 0x016d901c
    atx_qregs.addr_cntr_hi         0xe00046ac = 0x00000000
    atx_qregs.byte_cntr            0xe00046b0 = 0x00000000
    atx_qregs.bmu_cs               0xe00046b4 = 0x012aaa80
    atx_qregs.flag                 0xe00046b8 = 0x0a000600
    atx_qregs.tst1                 0xe00046bc = 0x02020202
    atx_qregs.tst2                 0xe00046c0 = 0x00000050
    atx_qregs.tst3                 0xe00046c4 = 0x00000000

Bank 16: Receive RAM buffer registers:
    rx_ram_buf_regs.start_addr     0xe0004800 = 0x00000000
    rx_ram_buf_regs.end_addr       0xe0004804 = 0x000017ff
    rx_ram_buf_regs.wr_ptr         0xe0004808 = 0x00000000
    rx_ram_buf_regs.rd_ptr         0xe000480c = 0x00000000
    rx_ram_buf_regs.up_thres_pp    0xe0004810 = 0x00001400
    rx_ram_buf_regs.lo_thres_pp    0xe0004814 = 0x00001000
    rx_ram_buf_regs.up_thres_hp    0xe0004818 = 0x00000000
    rx_ram_buf_regs.lo_thres_hp    0xe000481c = 0x00000000
    rx_ram_buf_regs.pak_cnt        0xe0004820 = 0x00000000
    rx_ram_buf_regs.level          0xe0004824 = 0x00000000
```

```
                          rx_ram_buf_regs.ctrl         0xe0004828 = 0x0002222a


Bank 20: Synchronous transmit RAM buffer registers:
 stx_ram_buf_regs.start_addr   0xe0004a00 = 0x00000000
 stx_ram_buf_regs.end_addr     0xe0004a04 = 0x00000000
 stx_ram_buf_regs.wr_ptr       0xe0004a08 = 0x00000000
 stx_ram_buf_regs.rd_ptr       0xe0004a0c = 0x00000000
 stx_ram_buf_regs.pak_cnt      0xe0004a20 = 0x00000000
 stx_ram_buf_regs.level        0xe0004a24 = 0x00000000
 stx_ram_buf_regs.ctrl         0xe0004a28 = 0x00022215


Bank 21: Asynchronous transmit RAM buffer registers:
 atx_ram_buf_regs.start_addr   0xe0004a80 = 0x00001800
 atx_ram_buf_regs.end_addr     0xe0004a84 = 0x00002fff
 atx_ram_buf_regs.wr_ptr       0xe0004a88 = 0x00001800
 atx_ram_buf_regs.rd_ptr       0xe0004a8c = 0x00001800
 atx_ram_buf_regs.up_thres_pp  0xe0004a90 = 0x00000000
 atx_ram_buf_regs.lo_thres_pp  0xe0004a94 = 0x00000000
 atx_ram_buf_regs.up_thres_hp  0xe0004a98 = 0x00000000
 atx_ram_buf_regs.lo_thres_hp  0xe0004a9c = 0x00000000
 atx_ram_buf_regs.pak_cnt      0xe0004aa0 = 0x00000000
 atx_ram_buf_regs.level        0xe0004aa4 = 0x00000000
 atx_ram_buf_regs.ctrl         0xe0004aa8 = 0x0002222a


Bank 24: Receive GMAC FIFO registers:
 rx_gmfifo_regs.end_addr       0xe0004c40 = 0x0000007f
 rx_gmfifo_regs.thr            0xe0004c44 = 0x00000070
 rx_gmfifo_regs.ctrl           0xe0004c48 = 0x0000224a


Bank 26: Transmit GMAC FIFO registers:
 tx_gmfifo_regs.end_addr       0xe0004d40 = 0x0000007f
 tx_gmfifo_regs.thr            0xe0004d44 = 0x00000010
 tx_gmfifo_regs.ctrl           0xe0004d48 = 0x0002220a
 tx_gmfifo_regs.wr_ptr         0xe0004d60 = 0x00000000
 tx_gmfifo_regs.wr_shdw_ptr    0xe0004d64 = 0x00000000
 tx_gmfifo_regs.wr_level       0xe0004d68 = 0x00000000
 tx_gmfifo_regs.rd_ptr         0xe0004d70 = 0x00000000
 tx_gmfifo_regs.restart_ptr    0xe0004d74 = 0x00000000
 tx_gmfifo_regs.rd_level       0xe0004d78 = 0x00000000


Descriptor poll timer registers:
 dpt_init_val                  0xe0004e00 = 0x00000000
 dpt_val                       0xe0004e04 = 0x00000000
 dpt_ctrl                      0xe0004e08 = 0x00020001


Timestamp timer register:
 ts_timer_val                  0xe0004e14 = 0x00000000
 ts_timer_ctrl                 0xe0004e18 = 0x00000202


GMAC and GPHY control registers:
 gmac_ctrl                     0xe0004f00 = 0x00000056
 gphy_ctrl                     0xe0004f04 = 0x0b7de002
 gmac_irq_src                  0xe0004f08 = 0x00000000
 gmac_irq_msk                  0xe0004f0c = 0x0000003a
 gmac_link_ctrl                0xe0004f10 = 0x00000002


Wake on LAN control registers:
 wol_ctrl                      0xe0004f20 = 0x00000555
 wol_mac_addr_lo               0xe0004f24 = 0x00000000
 wol_mac_addr_hi               0xe0004f28 = 0x00000000
 wol_patt_rd_ptr               0xe0004f2c = 0x00000000
 wol_patt_len_lo               0xe0004f30 = 0x3b3b3b3b
 wol_patt_len_hi               0xe0004f34 = 0x003b3b3b
 wol_patt_cnt_lo               0xe0004f38 = 0x00000000
```

```
        wol_patt_cnt_hi              0xe0004f3c = 0x00000000

    Bank 80 (0x50): GMAC registers:
     gmac_gpsr                       0xe0006800 = 0x0000f014
     gmac_gpcr                       0xe0006804 = 0x000038ff
     gmac_tx_ctrl                    0xe0006808 = 0x00001c00
     gmac_rx_ctrl                    0xe000680c = 0x0000a000
     gmac_tx_fctrl                   0xe0006810 = 0x0000ffff
     gmac_tx_parm                    0xe0006814 = 0x0000c000
     gmac_smod                       0xe0006818 = 0x00002306
     gmac_sa1_lo                     0xe000681c = 0x0000d000
     gmac_sa1_md                     0xe0006820 = 0x0000ff2b
     gmac_sa1_hi                     0xe0006824 = 0x00009f44
     gmac_sa2_lo                     0xe0006828 = 0x0000d000
     gmac_sa2_md                     0xe000682c = 0x0000ff2b
     gmac_sa2_hi                     0xe0006830 = 0x00009f44
     gmac_mcast_addr_hash1           0xe0006834 = 0x00000000
     gmac_mcast_addr_hash2           0xe0006838 = 0x00000000
     gmac_mcast_addr_hash3           0xe000683c = 0x00000000
     gmac_mcast_addr_hash4           0xe0006840 = 0x00000000
     gmac_tx_irq_src                 0xe0006844 = 0x00000000
     gmac_rx_irq_src                 0xe0006848 = 0x00000000
     gmac_tr_irq_src                 0xe000684c = 0x00000000
     gmac_tx_irq_msk                 0xe0006850 = 0x00000000
     gmac_rx_irq_msk                 0xe0006854 = 0x00000000
     gmac_tr_irq_msk                 0xe0006858 = 0x00000000

Internal-Data0/1:
    Marvell 88E6095 revision 2, switch port 8
      Port Registers:
         Status:      0x0e84  PCS Ctrl:      0xc13e
         Identifier:  0x0952  Port Ctrl:     0x0177
         Port Ctrl-1: 0x0000  Vlan Map:      0x06ff
         VID and PRI: 0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:   0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt: 0x0100
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
```

Related Commands

Command	Description
show interface	Shows the interface statistics.
show tech-support	Shows information so Cisco TAC can diagnose problems.

show counters

To display the protocol stack counters, use the **show counters** command in privileged EXEC mode.

> **show counters [all** | **context** *context-name* | **summary** | **top** *N*] [**detail**] [**protocol** *protocol_name*
> [**:***counter_name*]] [**threshold** *N*]

Syntax Description

all	Displays the filter details.
context *context-name*	Specifies the context name.
:*counter_name*	Specifies a counter by name.
detail	Displays additional counters information.
protocol *protocol_name*	Displays the counters for the specified protocol.
summary	Displays a counter summary.
threshold *N*	Displays only those counters at or above the specified threshold. The range is 1 through 4294967295.
top *N*	Displays the counters at or above the specified threshold. The range is 1 through 4294967295.

Defaults   **show counters summary detail threshold 1**

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples   The following example shows how to display all counters:

```
hostname# show counters all
Protocol      Counter          Value   Context
IOS_IPC       IN_PKTS              2    single_vf
IOS_IPC       OUT_PKTS             2    single_vf

hostname# show counters
Protocol      Counter          Value   Context
NPCP          IN_PKTS           7195    Summary
NPCP          OUT_PKTS          7603    Summary
IOS_IPC       IN_PKTS            869    Summary
IOS_IPC       OUT_PKTS           865    Summary
IP            IN_PKTS            380    Summary
```

```
IP          OUT_PKTS        411   Summary
IP          TO_ARP          105   Summary
IP          TO_UDP            9   Summary
UDP         IN_PKTS           9   Summary
UDP         DROP_NO_APP       9   Summary
FIXUP       IN_PKTS         202   Summary
```

The following example shows how to display a summary of counters:

```
hostname# show counters summary
Protocol    Counter         Value   Context
IOS_IPC     IN_PKTS             2   Summary
IOS_IPC     OUT_PKTS            2   Summary
```

The following example shows how to display counters for a context:

```
hostname# show counters context single_vf
Protocol    Counter         Value   Context
IOS_IPC     IN_PKTS             4   single_vf
IOS_IPC     OUT_PKTS            4   single_vf
```

Related Commands	Command	Description
	clear counters	Clears the protocol stack counters.

show cpu

To display the CPU utilization information, use the **show cpu usage** command in privileged EXEC mode.

> **show cpu** [**usage** | **profile**]

From the system configuration in multiple context mode:

> **show cpu** [**usage**] [**context** {**all** | *context_name*}]

Syntax Description

all	Specifies that the display show all contexts.
context	Specifies that the display show a context.
context_name	Specifies the name of the context to display.
profile	Displays CPU profile usage. The information displayed can be used by TAC for troubleshooting purposes.
usage	(Optional) Displays the CPU usage.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines   The cpu usage is computed using an approximation of the load every five seconds, and by further feeding this approximation into two, following moving averages.

You can use the **show cpu** command to find process related loads (that is, activity on behalf of items listed by the output of the **show process** command in both single mode and from the system configuration in multiple context mode).

Further, you can request, when in multiple context mode, a breakdown of the process related load to CPU consumed by any configured contexts by changing to each context and entering the **show cpu** command or by entering the **show cpu context** variant of this command.

While process related load is rounded to the nearest whole number, context related loads include one additional decimal digit of precision. For example, entering **show cpu** from the system context produces a different number than from entering the **show cpu context system** command. The former is an approximate summary of everything in **show cpu context all**, and the latter is only a portion of that summary.

The **show cpu profile** command can be used in conjunction with the **cpu profile activate** command to display information that can be collected and used by the TAC to aid in troubleshooting CPU issues. The information displayed by the **show cpu profile** command is in hexadecimal.

Examples   The following example shows how to display the CPU utilization:

```
hostname# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

This example shows how to display the CPU utilization for the system context in multiple mode:

```
hostname# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

The following shows how to display the CPU utilization for all contexts:

```
hostname# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%   system
0.0%   0.0%   0.0%   admin
5.0%   5.0%   5.0%   one
4.2%   4.3%   4.2%   two
```

This example shows how to display the CPU utilization for a context named "one":

```
hostname/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

The following example activates the profiler and instructs it to store 5000 samples.

```
hostname# cpu profile activate 5000
Activated CPU profiling for 5000 samples.
```

Use the **show cpu profile** command to see the results.

Note   Executing the **show cpu profile** command while the **cpu profile activate** command is running will display the progress.

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 CPU profiling currently in
progress, 1640 out of 5000 samples collected.
```

Once it is complete, the **show cpu profile** command output will provide the results. Copy this information and provide to the TAC to be decoded.

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 Profiling finished, 5000 samples:
 00c483f5 00115283 002199d3 001151d1 002199e5 00116258 002199fc 00115230  0021984e
002198f6 00c48496 00219803 004a55b1 002198b1 00c484d9 00c48472
 00116258 00c48401 002199f3 00c48401 00c484b2 004a5580 0011520a 002198b4
```

```
 00116258 00219807 0011520a 00116258 002198a9 00116258 00219a2e 00112009  0021989c
00fff023 008be861 0011525e 002198be 0021984e 00115277 00219807  002199d0 00114a6d 002198af
0011520a 00115260 00115274 004a55a6 00c48472
 00c48472 00c48496 002199f9 002198ad 00c484c4 004a55a6 00115260 002198f4  0011528e
002198e0 00c484bb 00c48496 00c484a6 002199f3 00219810 001161d6 .
```

Related Commands	Command	Description
	show counters	Displays the protocol stack counters.
	cpu profile activate	Activates CPU profiling.

show crashinfo

To display the contents of the crash file stored in Flash memory, enter the **show crashinfo** command in privileged EXEC mode.

> **show crashinfo** [**save**]

Syntax Description

save	(Optional) Displays if the security appliance is configured to save crash information to Flash memory or not.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines   If the crash file is from a test crash (generated from the **crashinfo test** command), the first string of the crash file is "**: Saved_Test_Crash**" and the last string is "**: End_Test_Crash**". If the crash file is from a real crash, the first string of the crash file is "**: Saved_Crash**" and the last string is "**: End_Crash**". (This includes crashes from use of the **crashinfo force page-fault** or **crashinfo force watchdog** commands).

If there is no crash data saved in flash, or if the crash data has been cleared by entering the **clear crashinfo** command, the **show crashinfo** command displays an error message.

Examples   The following example shows how to display the current crash information configuration:

```
hostname# show crashinfo save
crashinfo save enable
```

The following example shows the output for a crash file test. (However, this test does not actually crash the security appliance. It provides a simulated example file.)

```
hostname(config)# crashinfo test
hostname(config)# exit
hostname# show crashinfo
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)
```

```
Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
        edi 0x004f20c4
        esi 0x00000000
        ebp 0x00e88c20
        esp 0x00e88bd8
        ebx 0x00000001
        edx 0x00000074
        ecx 0x00322f8b
        eax 0x00322f8b
error code n/a
        eip 0x0010318c
         cs 0x00000008
     eflags 0x00000000
        CR2 0x00000000
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
```

```
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
0x00e88cc8: 0x00f7f96c
```

```
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
```

```
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008


Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X


Compiled on Fri 15-Nov-04 14:35 by root


hostname up 10 days 0 hours


Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB


0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:          Disabled
VPN-DES:           Enabled
VPN-3DES-AES:      Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:            Enabled
URL-filtering:     Enabled
Inside Hosts:      Unlimited
Throughput:        Unlimited
IKE peers:         Unlimited


This XXX has a Restricted (R) license.


Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2004

------------------ show memory ------------------

Free memory:       50444824 bytes
Used memory:       16664040 bytes
```

```
            ------------     ----------------
            Total memory:       67108864 bytes

            ----------------- show conn count ------------------

            0 in use, 0 most used

            ----------------- show xlate count ------------------

            0 in use, 0 most used

            ----------------- show blocks ------------------

              SIZE    MAX    LOW    CNT
                 4   1600   1600   1600
                80    400    400    400
               256    500    499    500
              1550   1188    795    927

            ----------------- show interface ------------------

            interface ethernet0 "outside" is up, line protocol is up
              Hardware is i82559 ethernet, address is 0003.e300.73fd
              IP address 172.23.59.232, subnet mask 255.255.0.0
              MTU 1500 bytes, BW 10000 Kbit half duplex
                    6139 packets input, 830375 bytes, 0 no buffer
                    Received 5990 broadcasts, 0 runts, 0 giants
                    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
                    90 packets output, 6160 bytes, 0 underruns
                    0 output errors, 13 collisions, 0 interface resets
                    0 babbles, 0 late collisions, 47 deferred
                    0 lost carrier, 0 no carrier
                    input queue (curr/max blocks): hardware (5/128) software (0/2)
                    output queue (curr/max blocks): hardware (0/1) software (0/1)
            interface ethernet1 "inside" is up, line protocol is down
              Hardware is i82559 ethernet, address is 0003.e300.73fe
              IP address 10.1.1.1, subnet mask 255.255.255.0
              MTU 1500 bytes, BW 10000 Kbit half duplex
                    0 packets input, 0 bytes, 0 no buffer
                    Received 0 broadcasts, 0 runts, 0 giants
                    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
                    1 packets output, 60 bytes, 0 underruns
                    0 output errors, 0 collisions, 0 interface resets
                    0 babbles, 0 late collisions, 0 deferred
                    1 lost carrier, 0 no carrier
                    input queue (curr/max blocks): hardware (128/128) software (0/0)
                    output queue (curr/max blocks): hardware (0/1) software (0/1)
            interface ethernet2 "intf2" is administratively down, line protocol is down
              Hardware is i82559 ethernet, address is 00d0.b7c8.139e
              IP address 127.0.0.1, subnet mask 255.255.255.255
              MTU 1500 bytes, BW 10000 Kbit half duplex
                    0 packets input, 0 bytes, 0 no buffer
                    Received 0 broadcasts, 0 runts, 0 giants
                    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
                    0 packets output, 0 bytes, 0 underruns
                    0 output errors, 0 collisions, 0 interface resets
                    0 babbles, 0 late collisions, 0 deferred
                    0 lost carrier, 0 no carrier
                    input queue (curr/max blocks): hardware (128/128) software (0/0)
                    output queue (curr/max blocks): hardware (0/0) software (0/0)

            ----------------- show cpu usage ------------------

            CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%
```

```
                ----------------- show process ------------------


      PC      SP       STATE      Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8         0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8         0 008060fc 3792/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18         0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718         0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8         0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8         0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8         0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8         0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600         0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8         0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8         0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8         0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8         0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90         0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8         0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920         0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8         0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30         0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368         0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674         0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4         0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534      2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0      4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8         0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360         0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0         0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20         0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8         0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40 508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8         0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0         0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48       120 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc        10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198         0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174         0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150         0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850         0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c         0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108         0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4         0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0         0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534         0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c         0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078         0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054         0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8         0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8         0 00f786c4 7640/8192 Crypto CA

                ----------------- show failover ------------------


No license for Failover

                ----------------- show traffic ------------------


outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
```

```
                         90 packets      6160 bytes
                         0 pkts/sec      0 bytes/sec
           inside:
                  received (in 865565.090 secs):
                         0 packets       0 bytes
                         0 pkts/sec      0 bytes/sec
                  transmitted (in 865565.090 secs):
                         1 packets       60 bytes
                         0 pkts/sec      0 bytes/sec
           intf2:
                  received (in 865565.090 secs):
                         0 packets       0 bytes
                         0 pkts/sec      0 bytes/sec
                  transmitted (in 865565.090 secs):
                         0 packets       0 bytes
                         0 pkts/sec      0 bytes/sec


           ----------------- show perfmon ------------------


           PERFMON STATS:    Current      Average
           Xlates            0/s          0/s
           Connections       0/s          0/s
           TCP Conns         0/s          0/s
           UDP Conns         0/s          0/s
           URL Access        0/s          0/s
           URL Server Req    0/s          0/s
           TCP Fixup         0/s          0/s
           TCPIntercept      0/s          0/s
           HTTP Fixup        0/s          0/s
           FTP Fixup         0/s          0/s
           AAA Authen        0/s          0/s
           AAA Author        0/s          0/s
           AAA Account       0/s          0/s
           : End_Test_Crash
```

Related Commands	Command	Description
	clear crashinfo	Deletes the contents of the crash file.
	crashinfo force	Forces a crash of the security appliance.
	crashinfo save disable	Disables crash information from writing to Flash memory.
	crashinfo test	Tests the ability of the security appliance to save crash information to a file in Flash memory.

show crashinfo console

To display the configuration setting of the **crashinfo console** command, use the **show crashinfo console** command in privileged EXEC mode.

show crashinfo console

Syntax Description   This command has no arguments or keywords.

Defaults   This command has no default settings.

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

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

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines   Compliance with FIPS 140-2 prohibits the distribution of Critical Secu rity Parameters (keys, passwords, etc.) outside of the crypto boundary (chassis). When the device crashes, due to an assert or checkheaps failure, it is possible that the stack or memory regions dumped to the console contain sensitive data. This output must be suppressed in FIPS-mode.

Examples
```
sw8-5520(config)# show crashinfo console
crashinfo console enable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.

Command	Description
fips self-test poweron	Executes power-on self-tests.
show running-config fips	Displays the FIPS configuration that is running on the security appliance.

show crypto accelerator statistics

To display the global and accelerator-specific statistics from the hardware crypto accelerator MIB, use the **show crypto accelerator statistics** command in global configuration or privileged EXEC mode.

    show crypto accelerator statistics

Syntax Description   This command has no keywords or variables.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples   The following example entered in global configuration mode, displays global crypto accelerator statistics:

```
hostname # show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
```

```
               Total dropped packets: 0
               [Input statistics]
                  Input packets: 0
                  Input bytes: 0
                  Input hashed packets: 0
                  Input hashed bytes: 0
                  Decrypted packets: 0
                  Decrypted bytes: 0
               [Output statistics]
                  Output packets: 0
                  Output bad packets: 0
                  Output bytes: 0
                  Output hashed packets: 0
                  Output hashed bytes: 0
                  Encrypted packets: 0
                  Encrypted bytes: 0
               [Diffie-Hellman statistics]
                  Keys generated: 0
                  Secret keys derived: 0
               [RSA statistics]
                  Keys generated: 0
                  Signatures: 0
                  Verifications: 0
                  Encrypted packets: 0
                  Encrypted bytes: 0
                  Decrypted packets: 0
                  Decrypted bytes: 0
               [DSA statistics]
                  Keys generated: 0
                  Signatures: 0
                  Verifications: 0
               [SSL statistics]
                  Outbound records: 0
                  Inbound records: 0
               [RNG statistics]
                  Random number requests: 98
                  Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                              Boot microcode    : CNlite-MC-Boot-Cisco-1.2
                              SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                              IPSec microcode   : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
```

```
        Keys generated: 97
        Secret keys derived: 1
    [RSA statistics]
        Keys generated: 0
        Signatures: 0
        Verifications: 0
        Encrypted packets: 0
        Encrypted bytes: 0
        Decrypted packets: 0
        Decrypted bytes: 0
    [DSA statistics]
        Keys generated: 0
        Signatures: 0
        Verifications: 0
    [SSL statistics]
        Outbound records: 0
        Inbound records: 0
    [RNG statistics]
        Random number requests: 1
        Random number request failures: 0
hostname #
```

Related Commands	Command	Description
	clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
	clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
	show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

show crypto ca certificates

To display the certificates associated with a specific trustpoint or to display all the certificates installed on the system, use the **show crypto ca certificates** command in global configuration or privileged EXEC mode.

> **show crypto ca certificates** [*trustpointname*]

Syntax Description

trustpointname	(Optional) The name of a trustpoint. If you do not specify a name, this command displays all certificates installed on the system.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples   The following example entered in global configuration mode, displays a CA certificate for a trustpoint named tp1:

```
hostname(config)# show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = a@b.com
```

```
        CRL Distribution Point
            ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
        Validity Date:
            start date: 14:11:40 UTC Jun 26 2004
            end date: 14:01:30 UTC Jun 4 2022
        Associated Trustpoints: tp2 tp1
hostname(config)#
```

Related Commands	Command	Description
	crypto ca authenticate	Obtains a CA certificate for a specified trustpoint.
	crypto ca crl request	Requests a CRL based on the configuration parameters of a specified trustpoint.
	crypto ca enroll	Initiates the enrollment process with a CA.
	crypto ca import	Imports a certificate to a specified trustpoint.
	crypto ca trustpoint	Enters trustpoint mode for a specified trustpoint.

show crypto ca crls

To display all cached CRLs or to display all CRLs cached for a specified trustpoint, use the **show crypto ca crls** command in global configuration or privileged EXEC mode.

> **show crypto ca crls** [*trustpointname*]

Syntax Description

trustpointname	(Optional) The name of a trustpoint. If you do not specify a name, this command displays all CRLs cached on the system.

Defaults   No default behavior or values.

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

	Firewall Mode		Security Context	Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Global configuration	●	●	●	●	
Privileged EXEC	●	●	●	●	

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples   The following example entered in global configuration mode, displays a CRL for a trustpoint named tp1:

```
hostname(config)# show crypto ca crls tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@cisco.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
hostname(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains a CA certificate for a specified trustpoint.
crypto ca crl request	Requests a CRL based on the configuration parameters of a specified trustpoint.
crypto ca enroll	Initiates the enrollment process with a CA.
crypto ca import	Imports a certificate to a specified trustpoint.
crypto ca trustpoint	Enters trustpoint mode for a specified trustpoint.

show crypto ipsec df-bit

To display the IPSec DF-bit policy for IPSec packets for a specified interface, use the **show crypto ipsec df-bit** command in global configuration mode and privileged EXEC mode.

> **show crypto ipsec df-bit** *interface*

Syntax Description

interface	Specifies an interface name.
token	Indicate a token-based server for user authentication is used.

Defaults   No default behaviors or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples   The following example displays the IPSec DF-bit policy for interface named inside:

```
hostname(config)# show crypto ipsec df-bit inside
df-bit inside copy
hostname(config)#
```

Related Commands

Command	Description
crypto ipsec df-bit	Configures the IPSec DF-bit policy for IPSec packets.
crypto ipsec fragmentation	Configures the fragmentation policy for IPSec packets.
show crypto ipsec fragmentation	Displays the fragmentation policy for IPSec packets.

show crypto ipsec fragmentation

To display the fragmentation policy for IPSec packets, use the **show crypto ipsec fragmentation** command in global configuration or privileged EXEC modes.

show crypto ipsec fragmentation *interface*

Syntax Description

interface	Specifies an interface name.
token	Indicate a token-based server for user authentication is used.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples   The following example, entered in global configuration mode, displays the IPSec fragmentation policy for an interface named inside:

```
hostname(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
hostname(config)#
```

Related Commands

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPSec packets.
crypto ipsec df-bit	Configures the DF-bit policy for IPSec packets.
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.

show crypto ipsec sa

To display a list of IPSec SAs, use the **show crypto ipsec sa** command in global configuration mode or privileged EXEC mode. You can also use the alternate form of this command: **show ipsec sa**.

show crypto ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

Syntax Description

detail	(Optional) Displays detailed error information on what is displayed.
entry	(Optional) Displays IPSec SAs sorted by peer address
identity	(Optional) Displays IPSec SAs for sorted by identity, not including ESPs. This is a condensed form.
map *map-name*	(Optional) Displays IPSec SAs for the specified crypto map.
peer *peer-addr*	(Optional) Displays IPSec SAs for specified peer IP addresses.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples   The following example, entered in global configuration mode, displays IPSec SAs.

```
hostname(config)# show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

        local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
        remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
        current_peer: 172.20.0.21
        dynamic allocated peer ip: 10.135.1.5

        #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
        #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
        #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
        #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
        #send errors: 0, #recv errors: 0
```

```
                    local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

                    path mtu 1500, ipsec overhead 60, media mtu 1500
                    current outbound spi: DC15BF68

                inbound esp sas:
                  spi: 0x1E8246FC (511854332)
                      transform: esp-3des esp-md5-hmac
                      in use settings ={RA, Tunnel, }
                      slot: 0, conn_id: 3, crypto-map: def
                      sa timing: remaining key lifetime (sec): 548
                      IV size: 8 bytes
                      replay detection support: Y
                outbound esp sas:
                  spi: 0xDC15BF68 (3692412776)
                      transform: esp-3des esp-md5-hmac
                      in use settings ={RA, Tunnel, }
                      slot: 0, conn_id: 3, crypto-map: def
                      sa timing: remaining key lifetime (sec): 548
                      IV size: 8 bytes
                      replay detection support: Y

                Crypto map tag: def, local addr: 10.132.0.17

                    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```

Note Fragmentation statistics are pre-fragmentation statistics if the IPSec SA policy states that fragmentation occurs before IPSec processing. Post-fragmentation statistics appear if the SA policy states that fragmentation occurs after IPSec processing.

The following example, entered in global configuration mode, displays IPSec SAs for a crypto map named def.

```
hostname(config)# show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

        local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
        remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
        current_peer: 10.132.0.21
        dynamic allocated peer ip: 90.135.1.5

        #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
        #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
        #send errors: 0, #recv errors: 0

        local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

        path mtu 1500, ipsec overhead 60, media mtu 1500
        current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 3, crypto-map: def
          sa timing: remaining key lifetime (sec): 480
          IV size: 8 bytes
          replay detection support: Y
```

```
        outbound esp sas:
          spi: 0xDC15BF68 (3692412776)
             transform: esp-3des esp-md5-hmac
             in use settings ={RA, Tunnel, }
             slot: 0, conn_id: 3, crypto-map: def
             sa timing: remaining key lifetime (sec): 480
             IV size: 8 bytes
             replay detection support: Y

     Crypto map tag: def, local addr: 172.20.0.17

        local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
        remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
        current_peer: 10.135.1.8
        dynamic allocated peer ip: 0.0.0.0

        #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
        #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
        #send errors: 0, #recv errors: 0

        local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

        path mtu 1500, ipsec overhead 60, media mtu 1500
        current outbound spi: 3B6F6A35

     inbound esp sas:
        spi: 0xB32CF0BD (3006066877)
           transform: esp-3des esp-md5-hmac
           in use settings ={RA, Tunnel, }
           slot: 0, conn_id: 4, crypto-map: def
           sa timing: remaining key lifetime (sec): 263
           IV size: 8 bytes
           replay detection support: Y
     outbound esp sas:
        spi: 0x3B6F6A35 (997157429)
           transform: esp-3des esp-md5-hmac
           in use settings ={RA, Tunnel, }
           slot: 0, conn_id: 4, crypto-map: def
           sa timing: remaining key lifetime (sec): 263
           IV size: 8 bytes
           replay detection support: Y
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs for the keyword **entry**.

```
hostname(config)# show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

       local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
       remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
       current_peer: 10.132.0.21
       dynamic allocated peer ip: 90.135.1.5

       #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
       #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
       #send errors: 0, #recv errors: 0

       local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
```

```
            path mtu 1500, ipsec overhead 60, media mtu 1500
            current outbound spi: DC15BF68

        inbound esp sas:
          spi: 0x1E8246FC (511854332)
             transform: esp-3des esp-md5-hmac
             in use settings ={RA, Tunnel, }
             slot: 0, conn_id: 3, crypto-map: def
             sa timing: remaining key lifetime (sec): 429
             IV size: 8 bytes
             replay detection support: Y
        outbound esp sas:
          spi: 0xDC15BF68 (3692412776)
             transform: esp-3des esp-md5-hmac
             in use settings ={RA, Tunnel, }
             slot: 0, conn_id: 3, crypto-map: def
             sa timing: remaining key lifetime (sec): 429
             IV size: 8 bytes
             replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

       local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
       remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
       current_peer: 10.135.1.8
       dynamic allocated peer ip: 0.0.0.0

       #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
       #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
       #send errors: 0, #recv errors: 0

       local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

       path mtu 1500, ipsec overhead 60, media mtu 1500
       current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

The following example, entered in global configuration mode, shows IPSec SAs with the keywords **entry detail**.

```
hostname(config)# show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17
```

```
                    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
                    remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
                    current_peer: 10.132.0.21
                    dynamic allocated peer ip: 90.135.1.5

                    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
                    #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
                    #pkts compressed: 0, #pkts decompressed: 0
                    #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
                    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
                    #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
                    #pkts invalid prot (rcv): 0, #pkts verify failed: 0
                    #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
                    #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
                    #pkts replay failed (rcv): 0
                    #pkts internal err (send): 0, #pkts internal err (rcv): 0

                    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

                    path mtu 1500, ipsec overhead 60, media mtu 1500
                    current outbound spi: DC15BF68

                 inbound esp sas:
                    spi: 0x1E8246FC (511854332)
                       transform: esp-3des esp-md5-hmac
                       in use settings ={RA, Tunnel, }
                       slot: 0, conn_id: 3, crypto-map: def
                       sa timing: remaining key lifetime (sec): 322
                       IV size: 8 bytes
                       replay detection support: Y
                 outbound esp sas:
                    spi: 0xDC15BF68 (3692412776)
                       transform: esp-3des esp-md5-hmac
                       in use settings ={RA, Tunnel, }
                       slot: 0, conn_id: 3, crypto-map: def
                       sa timing: remaining key lifetime (sec): 322
                       IV size: 8 bytes
                       replay detection support: Y

          peer address: 10.135.1.8
             Crypto map tag: def, local addr: 172.20.0.17

                    local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
                    remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
                    current_peer: 10.135.1.8
                    dynamic allocated peer ip: 0.0.0.0

                    #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
                    #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
                    #pkts compressed: 0, #pkts decompressed: 0
                    #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
                    #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
                    #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
                    #pkts invalid prot (rcv): 0, #pkts verify failed: 0
                    #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
                    #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
                    #pkts replay failed (rcv): 0
                    #pkts internal err (send): 0, #pkts internal err (rcv): 0

                    local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

                    path mtu 1500, ipsec overhead 60, media mtu 1500
                    current outbound spi: 3B6F6A35
```

Cisco Security Appliance Command Reference 7.2(2) ■

```
            inbound esp sas:
              spi: 0xB32CF0BD (3006066877)
                  transform: esp-3des esp-md5-hmac
                  in use settings ={RA, Tunnel, }
                  slot: 0, conn_id: 4, crypto-map: def
                  sa timing: remaining key lifetime (sec): 104
                  IV size: 8 bytes
                  replay detection support: Y
            outbound esp sas:
              spi: 0x3B6F6A35 (997157429)
                  transform: esp-3des esp-md5-hmac
                  in use settings ={RA, Tunnel, }
                  slot: 0, conn_id: 4, crypto-map: def
                  sa timing: remaining key lifetime (sec): 104
                  IV size: 8 bytes
                  replay detection support: Y
hostname(config)#
```

The following example shows IPSec SAs with the keyword **identity**.

```
hostname(config)# show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

The following example shows IPSec SAs with the keywords **identity** and **detail**.

```
hostname(config)# show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17
```

```
            local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
            remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
            current_peer: 10.132.0.21
            dynamic allocated peer ip: 90.135.1.5

            #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
            #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
            #pkts compressed: 0, #pkts decompressed: 0
            #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
            #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
            #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
            #pkts invalid prot (rcv): 0, #pkts verify failed: 0
            #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
            #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
            #pkts replay failed (rcv): 0
            #pkts internal err (send): 0, #pkts internal err (rcv): 0

            local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

            path mtu 1500, ipsec overhead 60, media mtu 1500
            current outbound spi: DC15BF68

          Crypto map tag: def, local addr: 172.20.0.17

            local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
            remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
            current_peer: 10.135.1.8
            dynamic allocated peer ip: 0.0.0.0

            #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
            #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
            #pkts compressed: 0, #pkts decompressed: 0
            #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
            #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
            #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
            #pkts invalid prot (rcv): 0, #pkts verify failed: 0
            #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
            #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
            #pkts replay failed (rcv): 0
            #pkts internal err (send): 0, #pkts internal err (rcv): 0

            local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

            path mtu 1500, ipsec overhead 60, media mtu 1500
            current outbound spi: 3B6F6A35
```

Related Commands	Command	Description
	clear configure isakmp	Clears all the ISAKMP configuration.
	clear configure isakmp policy	Clears all ISAKMP policy configuration.
	clear isakmp sa	Clears the IKE runtime SA database.
	isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
	show running-config isakmp	Displays all the active ISAKMP configuration.

show crypto ipsec stats

To display a list of IPSec statistics, use the **show crypto ipsec stats** command in global configuration mode or privileged EXEC mode.

show crypto ipsec stats

Syntax Description   This command has no keywords or variables.

Defaults   No default behavior or values.

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	●	●	●	—	—
Privileged EXEC	●	●	●	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples   The following example, entered in global configuration mode, displays IPSec statistics:

```
hostname(config)# show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
```

```
 Encryption failures: 0
Fragmentation successes: 3
    Pre-fragmentation successes:2
    Post-fragmentation successes: 1
Fragmentation failures: 2
    Pre-fragmentation failures:1
    Post-fragmentation failures: 1
Fragments created: 10
PMTUs sent: 1
PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

Related Commands	Command	Description
	clear ipsec sa	Clears IPSec SAs or counters based on specified parameters.
	crypto ipsec transform-set	Defines a transform set.
	show ipsec sa	Displays IPSec SAs based on specified parameters.
	show ipsec sa summary	Displays a summary of IPSec SAs.

show crypto isakmp stats

To display runtime statistics, use the **show crypto isakmp stats** command in global configuration mode or privileged EXEC mode.

show crypto isakmp stats

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	●	—	●	—	—
Privileged EXEC	●	—	●	—	—

Command History

Release	Modification
7.0(1)	The **show isakmp stats** command was introduced.
7.2(1)	The **show isakmp stats** command was deprecated. The **show crypto isakmp stats** command replaces it.

Usage Guidelines   The output from this command includes the following fields:

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets

- Out Notifys

- Out P2 Exchanges

- Out P2 Exchange Invalids

- Out P2 Exchange Rejects

- Out P2 Sa Delete Requests

- Initiator Tunnels

- Initiator Fails

- Responder Fails

- System Capacity Fails

- Auth Fails

- Decrypt Fails

- Hash Valid Fails

- No Sa Fails

Examples   The following example, issued in global configuration mode, displays ISAKMP statistics:

```
hostname(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto isakmp sa

To display the IKE runtime SA database, use the **show crypto isakmp sa** command in global configuration mode or privileged EXEC mode.

>   **show crypto isakmp sa** [**detail**]

Syntax Description

detail	Displays detailed output about the SA database.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	The **show isakmp sa** command was introduced.
7.2(1)	This command was deprecated. The **show crypto isakmp sa** command replaces it.

Usage Guidelines   The output from this command includes the following fields:

Detail not specified.

Table 25-9

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

Table 25-10

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

Examples   The following example, entered in global configuration mode, displays detailed information about the SA database:

```
hostname(config)# show crypto isakmp sa detail

IKE Peer  Type  Dir  Rky  State     Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active 3des   SHA   preshrd 86400

IKE Peer  Type  Dir  Rky  State     Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE 3des   SHA   preshrd 86400

IKE Peer  Type  Dir  Rky  State     Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE 3des   SHA   preshrd 86400

IKE Peer  Type  Dir  Rky  State     Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE 3des   SHA   preshrd 86400

hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto isakmp stats

To display runtime statistics, use the **show crypto isakmp stats** command in global configuration mode or privileged EXEC mode.

> **show crypto isakmp stats**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	The **show isakmp stats** command was introduced.
7.2(1)	The **show isakmp stats** command was deprecated. The **show crypto isakmp stats** command replaces it.

Usage Guidelines   The output from this command includes the following fields:

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets

- Out Notifys

- Out P2 Exchanges

- Out P2 Exchange Invalids

- Out P2 Exchange Rejects

- Out P2 Sa Delete Requests

- Initiator Tunnels

- Initiator Fails

- Responder Fails

- System Capacity Fails

- Auth Fails

- Decrypt Fails

- Hash Valid Fails

- No Sa Fails

Examples   The following example, issued in global configuration mode, displays ISAKMP statistics:

```
hostname(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto protocol statistics

To display the protocol-specific statistics in the crypto accelerator MIB, use the **show crypto protocol statistics** command in global configuration or privileged EXEC mode.

show crypto protocol statistics *protocol*

Syntax Description

protocol	Specifies the name of the protocol for which to display statistics. Protocol choices are as follows:
	ikev1—Internet Key Exchange version 1.
	ipsec—IP Security Phase-2 protocols.
	ssl—Secure Socket Layer.
	other—Reserved for new protocols.
	all—All protocols currently supported.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples   The following examples entered in global configuration mode, display crypto accelerator statistics for specified protocols:

```
hostname # show crypto protocol statistics ikev1
[IKEv1 statistics]
  Encrypt packet requests: 39
  Encapsulate packet requests: 39
  Decrypt packet requests: 35
  Decapsulate packet requests: 35
  HMAC calculation requests: 84
  SA creation requests: 1
  SA rekey requests: 3
   SA deletion requests: 2
  Next phase key allocation requests: 2
  Random number generation requests: 0
   Failed requests: 0
```

```
hostname # show crypto protocol statistics ipsec
[IPsec statistics]
    Encrypt packet requests: 700
    Encapsulate packet requests: 700
    Decrypt packet requests: 700
    Decapsulate packet requests: 700
    HMAC calculation requests: 1400
    SA creation requests: 2
    SA rekey requests: 0
    SA deletion requests: 0
    Next phase key allocation requests: 0
    Random number generation requests: 0
    Failed requests: 0

hostname # show crypto protocol statistics ssl
[SSL statistics]
    Encrypt packet requests: 0
    Encapsulate packet requests: 0
    Decrypt packet requests: 0
    Decapsulate packet requests: 0
    HMAC calculation requests: 0
    SA creation requests: 0
    SA rekey requests: 0
    SA deletion requests: 0
    Next phase key allocation requests: 0
    Random number generation requests: 0
    Failed requests: 0

hostname # show crypto protocol statistics other
[Other statistics]
    Encrypt packet requests: 0
    Encapsulate packet requests: 0
    Decrypt packet requests: 0
    Decapsulate packet requests: 0
    HMAC calculation requests: 0
    SA creation requests: 0
    SA rekey requests: 0
    SA deletion requests: 0
    Next phase key allocation requests: 0
    Random number generation requests: 99
    Failed requests: 0

hostname # show crypto protocol statistics all
[IKEv1 statistics]
    Encrypt packet requests: 46
    Encapsulate packet requests: 46
    Decrypt packet requests: 40
    Decapsulate packet requests: 40
    HMAC calculation requests: 91
     SA creation requests: 1
    SA rekey requests: 3
    SA deletion requests: 3
    Next phase key allocation requests: 2
    Random number generation requests: 0
    Failed requests: 0
[IKEv2 statistics]
    Encrypt packet requests: 0
    Encapsulate packet requests: 0
     Decrypt packet requests: 0
    Decapsulate packet requests: 0
    HMAC calculation requests: 0
    SA creation requests: 0
    SA rekey requests: 0
    SA deletion requests: 0
```

```
            Next phase key allocation requests: 0
            Random number generation requests: 0
            Failed requests: 0
        [IPsec statistics]
            Encrypt packet requests: 700
            Encapsulate packet requests: 700
             Decrypt packet requests: 700
            Decapsulate packet requests: 700
            HMAC calculation requests: 1400
            SA creation requests: 2
            SA rekey requests: 0
            SA deletion requests: 0
            Next phase key allocation requests: 0
            Random number generation requests: 0
            Failed requests: 0
        [SSL statistics]
            Encrypt packet requests: 0
            Encapsulate packet requests: 0
            Decrypt packet requests: 0
            Decapsulate packet requests: 0
            HMAC calculation requests: 0
            SA creation requests: 0
            SA rekey requests: 0
            SA deletion requests: 0
            Next phase key allocation requests: 0
            Random number generation requests: 0
            Failed requests: 0
        [SSH statistics are not supported]
        [SRTP statistics are not supported]
        [Other statistics]
            Encrypt packet requests: 0
            Encapsulate packet requests: 0
            Decrypt packet requests: 0
            Decapsulate packet requests: 0
             HMAC calculation requests: 0
            SA creation requests: 0
            SA rekey requests: 0
            SA deletion requests: 0
            Next phase key allocation requests: 0
            Random number generation requests: 99
            Failed requests: 0
        hostname #
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics from the crypto accelerator MIB.

show csc node-count

A node is any distinct source IP address or the address of a device that is on a network protected by the security appliance. The security appliance keeps track of a daily node count and communicates this to the CSC SSM for user license enforcement. To display the number of nodes for which the CSC SSM scanned traffic, use the **show csc node-count** command in privileged EXEC mode:

show csc node-count [**yesterday**]

Syntax Description

yesterday	(Optional) Shows the number of nodes for which the CSC SSM scanned traffic in the preceding 24-hour period, from midnight to midnight.

Defaults

By default, the node count displayed is the number of nodes scanned since midnight.

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	•	•	•	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Examples

This example shows the use of the **show csc node-count** command to display the number of nodes for which the CSC SSM has scanned traffic since midnight:

```
hostname# show csc node-count
Current node count is 1
```

This example shows the use of the **show csc node-count** command to display the number of nodes for which the CSC SSM scanned traffic in the preceding 24-hour period, from midnight to midnight:

```
hostname(config)# show csc node-count yesterday
Yesterday's node count is 2
```

Related Commands

csc	Sends network traffic to the CSC SSM for scanning of FTP, HTTP, POP3, and SMTP, as configured on the CSC SSM.
show running-config class-map	Show current class map configuration.

show running-config policy-map	Show current policy map configuration.
show running-config service-policy	Show current service policy configuration.

show ctiqbe

To display information about CTIQBE sessions established across the security appliance, use the **show ctiqbe** command in privileged EXEC mode.

> **show ctiqbe**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines   The **show ctiqbe** command displays information of CTIQBE sessions established across the security appliance. Along with **debug ctiqbe** and **show local-host**, this command is used for troubleshooting CTIQBE inspection engine issues.

Note   We recommend that you have the **pager** command configured before using the **show ctiqbe** command. If there are a lot of CTIQBE sessions and the **pager** command is not configured, it can take a while for the **show ctiqbe** command output to reach the end.

Examples   The following is sample output from the **show ctiqbe** command under the following conditions. There is only one active CTIQBE session setup across the security appliance. It is established between an internal CTI device (for example, a Cisco IP SoftPhone) at local address 10.0.0.99 and an external Cisco Call Manager at 172.29.1.77, where TCP port 2748 is the Cisco CallManager. The heartbeat interval for the session is 120 seconds.

```
hostname# show ctiqbe

Total: 1
      LOCAL        FOREIGN       STATE   HEARTBEAT
---------------------------------------------------------------
1   10.0.0.99/1117  172.29.1.77/2748  1   120
      RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028  1029)
```

```
|MEDIA: Device ID 27|Call ID 0
|Foreign 172.29.1.99|(1028|1029)
|Local|172.29.1.88|(26822|26823)
|-------------------------------------------
```

The CTI device has already registered with the CallManager. The device internal address and RTP listening port is PATed to 172.29.1.99 UDP port 1028. Its RTCP listening port is PATed to UDP 1029.

The line beginning with `RTP/RTCP: PAT xlates:` appears only if an internal CTI device has registered with an external CallManager and the CTI device address and ports are PATed to that external interface. This line does not appear if the CallManager is located on an internal interface, or if the internal CTI device address and ports are NATed to the same external interface that is used by the CallManager.

The output indicates a call has been established between this CTI device and another phone at 172.29.1.88. The RTP and RTCP listening ports of the other phone are UDP 26822 and 26823. The other phone locates on the same interface as the CallManager because the security appliance does not maintain a CTIQBE session record associated with the second phone and CallManager. The active call leg on the CTI device side can be identified with Device ID 27 and Call ID 0.

The following is the xlate information for these CTIBQE connections:

```
hostname# show xlate debug
3 in use, 3 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
 |o|outside, r|portmap, s|static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
hostname#
```

Related Commands	Commands	Description
	class-map	Defines the traffic class to which to apply security actions.
	inspect ctiqbe	Enables CTIQBE application inspection.
	service-policy	Applies a policy map to one or more interfaces.
	show conn	Displays the connection state for different connection types.
	timeout	Sets the maximum idle time duration for different protocols and session types.

show curpriv

To display the current user privileges, use the **show curpriv** command:

> **show curpriv**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behaviors or values.

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

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

Command History

Release	Modification
7.0(1)	Modified to conform to CLI guidelines.

Usage Guidelines   **The show curpriv command displays the current privilege level.** Lower privilege level numbers indicate lower privilege levels.

Examples   These examples show output from the **show curpriv** command when a user named enable_15 is at different privilege levels. The username indicates the name that the user entered when the user logged in, P_PRIV indicates that the user has entered the **enable** command, and P_CONF indicates that the user has entered the **config terminal** command.

```
hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_1
Current privilege level : 1
```

```
Current Mode/s : P_UNPR
hostname(config)#
```

The following is a known issue. When you are in enable mode then enters disable mode the initial logged in username is replaced with enable_1 as shown in the example below:

```
hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
asa2(config)# disable
asa2> show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
```

	Command	Description
Related Commands	**clear configure privilege**	Remove privilege command statements from the configuration.
	show running-config privilege	Display privilege levels for commands.