CHAPTER 25

show asp drop コマンド～ show curpriv コマンド

show asp drop

高速セキュリティ パスでドロップされたパケットまたは接続をデバッグするには、特権 EXEC モードで **show asp drop** コマンドを使用します。

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

構文の説明

flow [*flow_drop_reason*]	（任意）ドロップされたフロー（接続）を表示します。*flow_drop_reason* 引数を使用して、特定の理由を指定できます。*flow_drop_reason* 引数の有効な値は、下記の「使用上のガイドライン」に示されています。
frame [*frame_drop_reason*]	（任意）ドロップされたパケットを表示します。*frame_drop_reason* 引数を使用して、特定の理由を指定できます。*frame_drop_reason* 引数の有効な値は、下記の「使用上のガイドライン」に示されています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.0(8)/7.2(4)/8.0(4)	カウンタが最後にクリアされた時間を示すタイムスタンプが出力に含まれるようになりました（**clear asp drop** コマンドを参照）。また、説明の横にドロップ理由のキーワードが表示されるため、そのキーワードを使用して簡単に **capture asp-drop** コマンドを使用できます。

使用上のガイドライン

show asp drop コマンドは、高速セキュリティ パスによってドロップされたパケットまたは接続を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。この情報はデバッグの目的でのみ使用されます。また、情報の出力は変更される可能性があります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

次の項では、各ドロップ理由の名前、説明、および推奨事項を示します。

- 「フレームのドロップ理由」（P.25-2）
- 「フローのドロップ理由」（P.25-38）

フレームのドロップ理由

```
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

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

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

Syslogs:
    337001.


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

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

Syslogs:
    337002.
```

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

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

Syslogs:
    337003.


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

Recommendation:
    No action is required.

Syslogs:
    337004.


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

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

Syslogs:
    None.


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

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

Syslogs:
    None.


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

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

```
Syslogs:
    None.


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

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

Syslogs:
    None.


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

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

Syslogs:
    None.


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

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

Syslogs:
    None.


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

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

Syslogs:
    None.


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

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

Syslogs:
    None.

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

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

Syslogs:
    421003
    421004

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

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

Syslogs:
    None.

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

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

Syslog:
    None.


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

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

Syslogs:
    None.


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

Recommendation:
    Verify that a route exists for Cache Engine.

Syslogs:
   None.


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

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

 Syslogs:
    402117


----------------------------------------------------------------
Name: 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


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

フローのドロップ理由

```
----------------------------------------------------------------
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.


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

Recommendation:
    No action required.

Syslogs:
    302014, 302016


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

Recommendation:
    This is an information counter.

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

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

Recommendation:
    This is an information counter.

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


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

Recommendation:
    No action required.

Syslogs:
    302014, 302016, 302018, 302021


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

Recommendation:
    None.

Syslogs:
    201011


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

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

Syslogs:
    302014


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

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

Syslogs:
    302014
```

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

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

Syslogs:
    302014


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

Recommendation:
    None.

Syslogs:
    302014


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

Recommendation:
    None.

Syslogs:
    302014


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

Recommendation:
    None.

Syslogs:
    302014


----------------------------------------------------------------
Name: recurse
Close recursive flow:
    A flow was recursively freed.  This reason applies to pair flows 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 retranmission with different data from the original
packet.

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

Syslogs:
    302014


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

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

Syslogs:
    302014


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

Recommendations:
```

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

Syslogs:
    302014


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

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

Syslogs:
    None


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

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

Syslogs:
    None


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

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

Syslogs:
    None


----------------------------------------------------------------
Name: audit-failure
Audit failure:
```

```
    A flow was freed after matching an "ip audit" signature that had reset as the
associated action.

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

Syslogs:
    None


----------------------------------------------------------------
Name: 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 unable to create a VPN handle
because the VPN handle already exists.

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

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

Syslogs:
    None


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

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

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

```
    show asp table vpn-context detail

Syslogs:
    None


------------------------------------------------------------------
Name: 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
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


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

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

 Syslogs:
    402116


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

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

Syslog:
    None.
```

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

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

Syslog:
    722032


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

例

次に、**show asp drop** コマンドの出力例を示します。タイムスタンプが、カウンタが最後にクリアされた時間を示しています。

```
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
```

関連コマンド

コマンド	説明
capture	パケットをキャプチャします。asp drop コードに基づいてパケットをキャプチャするオプションも含まれています。
clear asp drop	高速セキュリティ パスのドロップ統計情報をクリアします。
show conn	接続に関する情報を表示します。

show asp table arp

高速セキュリティ パスの ARP テーブルをデバッグするには、特権 EXEC モードで **show asp table arp** コマンドを使用します。

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

構文の説明

address *ip_address*	（任意）ARP テーブル エントリを表示する IP アドレスを指定します。
interface *interface_name*	（任意）ARP テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	（任意）IP アドレスのサブネット マスクを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show arp コマンドがコントロール プレーンの内容を表示するのに対して、**show asp table arp** コマンドは高速セキュリティ パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table arp** コマンドの出力例を示します。

```
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
```

関連コマンド

コマンド	説明
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。

show asp table classify

高速セキュリティ パスの分類子テーブルをデバッグするには、特権 EXEC モードで **show asp table classify** コマンドを使用します。分類子は、着信パケットのプロパティ（プロトコル、送信元アドレス、宛先アドレスなど）を検査して、各パケットを適切な分類ルールと対応付けます。それぞれのルールには、パケットのドロップや通過の許可など、どのタイプのアクションを実行するかを規定した分類ドメインのラベルが付けられます。

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

構文の説明

domain *domain_name*	（任意）特定の分類子ドメインのエントリを表示します。ドメインのリストについては、「使用上のガイドライン」を参照してください。
hits	（任意）0 以外のヒット値を持つ分類子エントリを表示します。
interface *interface_name*	（任意）分類子テーブルを表示する特定のインターフェイスを指定します。
crypto	（任意）暗号、暗号解除、および IPSec トンネル フロー ドメインのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(4)	**hits** オプション、および asp テーブルのカウンタが最後にクリアされたのがいつかを示すタイムスタンプが追加されました。
8.0(2)	tmatch コンパイルが中止された回数を示すために、新しいカウンタが追加されました。このカウンタは、値が 0 より大きい場合のみ表示されます。

使用上のガイドライン

show asp table classifier コマンドは、高速セキュリティ パスの分類子の内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

分類子ドメインには、次のものがあります。

```
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
```

例

次に、**show asp table classify** コマンドの出力例を示します。

```
hostname# show asp table classify

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

次に、**show asp table classify hits** コマンドの出力例を示します。ヒット カウンタの最後のクリアのレコードが示されています。

```
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
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。

show asp table interfaces

高速セキュリティ パスのインターフェイス テーブルをデバッグするには、特権 EXEC モードで **show asp table interfaces** コマンドを使用します。

show asp table interfaces

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show asp table interfaces コマンドは、高速セキュリティ パスのインターフェイス テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table interfaces** コマンドの出力例を示します。

```
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
...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

show asp table routing

高速セキュリティ パスのルーティング テーブルをデバッグするには、特権 EXEC モードで **show asp table routing** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

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

構文の説明

address *ip_address*	ルーティング エントリを表示する IP アドレスを設定します。IPv6 アドレスの場合は、スラッシュ（/）に続けてプレフィックス（0 ～ 128）を入力し、サブネット マスクを含めることができます。たとえば、次のように入力します。 `fe80::2e0:b6ff:fe01:3b7a/128`
input	入力ルート テーブルにあるエントリを表示します。
interface *interface_name*	（任意）ルーティング テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	IPv4 アドレスの場合は、サブネット マスクを指定します。
output	出力ルート テーブルにあるエントリを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show asp table routing コマンドは、高速セキュリティ パスのルーティング テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table routing** コマンドの出力例を示します。

```
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
```

関連コマンド

コマンド	説明
show route	コントロール プレーン内のルーティング テーブルを表示します。

show asp table socket

アクセラレーション セキュリティ パスのソケット情報をデバッグするには、特権 EXEC モードで **show asp table socket** コマンドを使用します。

show asp table socket

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
8.0(1)	このコマンドが導入されました。

使用上のガイドライン

show asp table socket コマンドを実行すると、アクセラレーション セキュリティ パスのソケット情報をデバッグできます。

例

次に、**show asp table socket** コマンドの例を示します。

```
Protocol  Socket    Local Address              Foreign Address         State
TCP       00012bac  10.86.194.224:23           0.0.0.0:*               LISTEN
TCP       0001c124  10.86.194.224:22           0.0.0.0:*               LISTEN
SSL       00023b84  10.86.194.224:443          0.0.0.0:*               LISTEN
SSL       0002d01c  192.168.1.1:443            0.0.0.0:*               LISTEN
DTLS      00032b1c  10.86.194.224:443          0.0.0.0:*               LISTEN
SSL       0003a3d4  0.0.0.0:443                0.0.0.0:*               LISTEN
DTLS      00046074  0.0.0.0:443                0.0.0.0:*               LISTEN
TCP       02c08aec  10.86.194.224:22           171.69.137.139:4190     ESTAB
```

関連コマンド

コマンド	説明
show asp table vpn-context	アクセラレーション セキュリティ パスの VPN コンテキスト テーブルをデバッグします。

show asp table vpn-context

高速セキュリティ パスの VPN コンテキスト テーブルをデバッグするには、特権 EXEC モードで **show asp table vpn-context** コマンドを使用します。

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

構文の説明

detail	（任意）VPN コンテキスト テーブルに関する追加の詳細情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(4)	トンネルのドロップ後にステートフル フローを保持する各コンテキストに +PRESERVE フラグが追加されました。

使用上のガイドライン

show asp table vpn-context コマンドは、高速セキュリティ パスの VPN コンテキストの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。高速セキュリティ パスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。これらの表はデバッグ目的でのみ使用され、情報出力は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合わせください。

例

次に、**show asp table vpn-context** コマンドの出力例を示します。

```
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
...
```

次に、PRESERVE フラグで示されているように固定の IPsec トンネル フロー機能がイネーブルになっている場合の **show asp table vpn-context** コマンドの出力例を示します。

```
hostname(config)# show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

次に、**show asp table vpn-context detail** コマンドの出力例を示します。

```
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
...
```

次に、PRESERVE フラグで示されているように固定の IPsec トンネル フロー機能がイネーブルになっている場合の **show asp table vpn-context detail** コマンドの出力例を示します。

```
hostname(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54

Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
```

```
VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
hostname(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。

show blocks

パケット バッファの使用状況を表示するには、特権 EXEC モードで **show blocks** コマンドを使用します。

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

構文の説明

address *hex*	（任意）このアドレスに対応するブロックを 16 進数形式で表示します。
all	（任意）すべてのブロックを表示します。
assigned	（任意）割り当て済みでアプリケーションによって使用されているブロックを表示します。
detail	（任意）一意のキュー タイプごとに最初のブロックの一部（128 バイト）を表示します。
dump	（任意）ヘッダーとパケットの情報を含め、ブロックの内容全体を表示します。dump と packet の相違点は、dump の場合、ヘッダーとパケットに関する追加情報が含まれることです。
diagnostics	（任意）ブロックの診断を表示します。
free	（任意）使用可能なブロックを表示します。
header	（任意）ブロックのヘッダーを表示します。
old	（任意）1 分よりも前に割り当てられたブロックを表示します。
packet	（任意）ブロックのヘッダーおよびパケットの内容を表示します。
pool *size*	（任意）特定のサイズのブロックを表示します。
queue history	（任意）セキュリティ アプライアンスがブロックを使い果たしたときに、ブロックが割り当てられる位置を表示します。プール内のブロックが割り当てられることはありますが、ブロックがキューに割り当てられることはありません。この場合は、ブロックを割り当てたコードのアドレスが割り当て場所になります。
summary	（任意）ブロックの使用状況に関する詳細情報を表示します。この情報は、このクラスにブロックを割り当てたアプリケーションのプログラム アドレス、このクラスのブロックを解放したアプリケーションのプログラム アドレス、およびこのクラスの有効なブロックが属しているキューを基準としてソートされています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**pool summary** オプションが追加されました。
8.0(2)	dupb ブロックは、4 バイト ブロックではなく長さが 0 のブロックを使用するようになりました。0 バイト ブロック用の 1 行が追加されました。

使用上のガイドライン

show blocks コマンドは、セキュリティ アプライアンスが過負荷になっているかどうかを判断する場合に役立ちます。このコマンドは、事前割り当て済みのシステム バッファの使用状況を表示します。トラフィックがセキュリティ アプライアンス経由で伝送されている限り、メモリがいっぱいになっている状態は問題にはなりません。**show conn** コマンドを使用すると、トラフィックが伝送されているかどうかを確認できます。トラフィックが伝送されておらず、かつメモリがいっぱいになっている場合は、問題がある可能性があります。

この情報は、SNMP を使用して表示することもできます。

セキュリティ コンテキスト内で表示される情報には、使用中のブロック、およびブロック使用状況の高基準値に関する、システム全体の情報およびコンテキスト固有の情報が含まれます。

出力表示の詳細については、「例」を参照してください。

例

次に、シングル モードでの **show blocks** コマンドの出力例を示します。

```
hostname# show blocks
  SIZE    MAX    LOW    CNT
     0    100     99    100
     4   1600   1598   1599
    80    400    398    399
   256   3600   3540   3542
  1550   4716   3177   3184
 16384     10     10     10
  2048   1000   1000   1000
```

表 25-1 に、各フィールドの説明を示します。

表 25-1　show blocks のフィールド

フィールド	説明
SIZE	ブロック プールのサイズ（バイト単位）。それぞれのサイズは、特定のタイプを表しています。次に例を示します。
0	dupb ブロックで使用されます。
4	DNS、ISAKMP、URL フィルタリング、uauth、TFTP、TCP モジュールなどのアプリケーションの既存ブロックを複製します。またこのサイズのブロックは、通常、パケットをドライバに送信するコードなどで使用されます。
80	TCP 代行受信で確認応答パケットを生成するために、およびフェールオーバー hello メッセージに使用されます。

表 25-1　show blocks のフィールド （続き）

フィールド	説明
256	ステートフル フェールオーバーの更新、syslog 処理、およびその他の TCP 機能に使用されます。 これらのブロックは、主にステートフル フェールオーバーのメッセージに使用されます。アクティブなセキュリティ アプライアンスは、パケットを生成してスタンバイセキュリティ アプライアンスに送信し、変換と接続のテーブルを更新します。接続が頻繁に作成または切断されるバースト トラフィックが発生すると、使用可能なブロックの数が 0 まで低下することがあります。この状況は、1 つまたはそれ以上の接続がスタンバイセキュリティ アプライアンスに対して更新されなかったことを示しています。ステートフル フェールオーバー プロトコルは、不明な変換または接続を次回に捕捉します。256 バイト ブロックの CNT カラムが長時間にわたって 0 またはその付近で停滞している場合は、セキュリティ アプライアンスの処理している 1 秒あたりの接続数が非常に多いために、変換テーブルと接続テーブルの同期が取れている状態をセキュリティ アプライアンスが維持できない問題が発生します。 セキュリティ アプライアンスから送信される syslog メッセージも 256 バイト ブロックを使用しますが、256 バイト ブロック プールが枯渇するような量が発行されることは通常ありません。CNT カラムの示す 256 バイト ブロックの数が 0 に近い場合は、Debugging（レベル 7）のログを syslog サーバに記録していないことを確認してください。この情報は、セキュリティ アプライアンス コンフィギュレーションの logging trap 行に示されています。ロギングは、デバッグのために詳細な情報が必要となる場合を除いて、Notification（レベル 5）以下に設定することを推奨します。
1550	セキュリティ アプライアンスで処理するイーサネット パケットを格納するために使用されます。 パケットは、セキュリティ アプライアンス インターフェイスに入ると入力インターフェイス キューに配置され、次にオペレーティング システムに渡されてブロックに配置されます。セキュリティ アプライアンスは、パケットを許可するか拒否するかをセキュリティ ポリシーに基づいて決定し、パケットを発信インターフェイス上の出力キューに配置します。セキュリティ アプライアンスがトラフィックの負荷に対応できていない場合は、使用可能なブロックの数が 0 付近で停滞します（このコマンドの出力の CNT カラムに示されます）。CNT カラムが 0 になると、セキュリティ アプライアンスはさらにブロックを確保しようとします（最大で 8192 個まで）。使用可能なブロックがなくなった場合、セキュリティ アプライアンスはパケットをドロップします。
16384	64 ビット 66 MHz のギガビット イーサネット カード（i82543）にのみ使用されます。 イーサネット パケットの詳細については、1550 の説明を参照してください。
2048	制御の更新に使用される制御フレームまたはガイド付きフレーム。
MAX	指定したバイト ブロックのプールで使用可能なブロックの最大数。起動時に、最大限のブロック数がメモリから切り分けられます。通常、ブロックの最大数は変化しません。例外は 256 バイト ブロックと 1550 バイト ブロックで、セキュリティ アプライアンスはこれらのブロックを必要に応じてダイナミックに作成できます（最大で 8192 個）。
LOW	低基準値。この数は、セキュリティ アプライアンスの電源がオンになった時点、またはブロックが（**clear blocks** コマンドで）最後にクリアされた時点から、このサイズの使用可能なブロックが最も少なくなったときの数を示しています。LOW カラムが 0 である場合は、先行のイベントでメモリがいっぱいになったことを示します。
CNT	特定のサイズのブロック プールで現在使用可能なブロックの数。CNT カラムが 0 である場合は、メモリが現在いっぱいであることを意味します。

次に、**show blocks all** コマンドの出力例を示します。

```
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
```

表 25-2 に、各フィールドの説明を示します。

表 25-2　show blocks all のフィールド

フィールド	説明
Block	ブロックのアドレス。
allocd_by	ブロックを最後に使用したアプリケーションのプログラム アドレス（使用されていない場合は 0）。
freed_by	ブロックを最後に解放したアプリケーションのプログラム アドレス。
data size	ブロック内部のアプリケーション バッファまたはパケット データのサイズ。
alloccnt	このブロックが作成されてから使用された回数。
dup_cnt	このブロックに対する現時点での参照回数（このブロックが使用されている場合）。0 は 1 回の参照、1 は 2 回の参照を意味します。
oper	ブロックに対して最後に実行された操作。alloc、get、put、free の 4 つのいずれかです。
location	ブロックを使用しているアプリケーション。または、ブロックを最後に割り当てたアプリケーションのプログラム アドレス（allocd_by フィールドと同じ）。

次に、コンテキスト内での **show blocks** コマンドの出力例を示します。

```
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
```

次に、**show blocks queue history** コマンドの出力例を示します。

```
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
...
```

次に、**show blocks queue history detail** コマンドの出力例を示します。

```
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
```

次に、**show blocks pool summary** コマンドの出力例を示します。

```
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#
```

表 25-3 に、各フィールドの説明を示します。

表 25-3　show blocks pool summary のフィールド

フィールド	説明
total_count	指定したクラスのブロックの数。
miss_count	技術的な理由により、指定したカテゴリでレポートされなかったブロックの数。
Freed_pc	このクラスのブロックを解放したアプリケーションのプログラム アドレス。
Alloc_pc	このクラスにブロックを割り当てたアプリケーションのプログラム アドレス。
Queue	このクラスの有効なブロックが属しているキュー。
valid_cnt	現時点で割り当てられているブロックの数。
invalid_cnt	現時点では割り当てられていないブロックの数。
Invalid Bad qtype	このキューが解放されて内容が無効になっているか、このキューは初期化されていませんでした。
Valid tcp_usr_conn_inp	キューは有効です。

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てられるメモリを増やします。

コマンド	説明
clear blocks	システム バッファの統計情報をクリアします。
show conn	アクティブな接続を表示します。

show bootvar

ブート ファイルとコンフィギュレーションのプロパティを表示するには、特権 EXEC モードで **show boot** コマンドを使用します。

show bootvar

構文の説明

show bootvar	システムのブート プロパティ。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

BOOT 変数は、さまざまなデバイス上の起動イメージのリストを指定します。CONFIG_FILE 変数は、システム初期化中に使用されるコンフィギュレーション ファイルを指定します。これらの変数は、それぞれ **boot system** コマンドと **boot config** コマンドで設定します。

例

次に、BOOT 変数が disk0:/f1_image を保持している例を示します。これは、システムのリロード時にブートされるイメージです。BOOT の現在の値は、disk0:/f1_image; disk0:/f1_backupimage です。これは、BOOT 変数が boot system コマンドで変更されているものの、実行コンフィギュレーションがまだ **write memory** コマンドで保存されていないことを意味しています。実行コンフィギュレーションを保存すると、BOOT 変数と現在の BOOT 変数が両方とも disk0:/f1_image; disk0:/f1_backupimage になります。実行コンフィギュレーションが保存済みである場合、ブートローダは BOOT 変数の内容をロードしようとします。つまり、disk0:/f1image を起動します。このイメージが存在しないか無効である場合は、disk0:1/f1_backupimage をブートしようとします。

CONFIG_FILE 変数は、システムのスタートアップ コンフィギュレーションを指します。この例ではこの変数が設定されていないため、スタートアップ コンフィギュレーション ファイルは、**boot config** コマンドで指定したデフォルトです。現在の CONFIG_FILE 変数は、**boot config** コマンドで変更して、**write memory** コマンドで保存できます。

```
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#
```

関連コマンド

コマンド	説明
boot	起動時に使用されるコンフィギュレーション ファイルまたはイメージ ファイルを指定します。

show capture

オプションを何も指定しない場合にキャプチャのコンフィギュレーションを表示するには、**show capture** コマンドを使用します。

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

構文の説明

capture_name	（任意）パケット キャプチャの名前。
access-list *access_list_name*	（任意）特定のアクセス リスト ID の IP フィールドまたはより高位のフィールドに基づいて、パケットに関する情報を表示します。
count *number*	（任意）指定されたデータのパケット数を表示します。
decode	このオプションは、isakmp タイプのキャプチャがインターフェイスに適用されている場合に役立ちます。当該のインターフェイスを通過する isakmp データは、復号化の後にすべてキャプチャされ、フィールドをデコードした後にその他の情報とともに表示されます。
detail	（任意）各パケットについて、プロトコル情報を追加表示します。
dump	（任意）データ リンク トランスポート経由で転送されたパケットの 16 進ダンプを表示します。
packet-number *number*	指定したパケット番号から表示を開始します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

capture_name を指定した場合は、そのキャプチャのキャプチャ バッファの内容が表示されます。

dump キーワードを指定しても、MAC 情報は 16 進ダンプに表示されません。

パケットのデコード出力は、パケットのプロトコルによって異なります。表 25-4 で角カッコに囲まれている出力は、**detail** キーワードを指定した場合に表示されます。

表 25-4　パケット キャプチャの出力形式

パケット タイプ	キャプチャの出力形式
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*
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*

例

次に、キャプチャのコンフィギュレーションを表示する例を示します。

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

次に、ARP キャプチャによってキャプチャされたパケットを表示する例を示します。

```
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
```

関連コマンド

コマンド	説明
capture	パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。
clear capture	キャプチャ バッファをクリアします。
copy capture	キャプチャ ファイルをサーバにコピーします。

show chardrop

シリアル コンソールからドロップされた文字の数を表示するには、特権 EXEC モードで **show chardrop** コマンドを使用します。

show chardrop

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show chardrop** コマンドの出力例を示します。

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

関連コマンド

コマンド	説明
show running-config	現在の動作設定を表示します。

show checkheaps

checkheaps に関する統計情報を表示するには、特権 EXEC モードで **show checkheaps** コマンドを使用します。チェックヒープは、ヒープ メモリ バッファの正常性およびコード領域の完全性を検証する定期的なプロセスです（ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられます）。

show checkheaps

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show checkheaps** コマンドの出力例を示します。

```
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
```

関連コマンド

コマンド	説明
checkheaps	checkheap の確認間隔を設定します。

show checksum

コンフィギュレーションのチェックサムを表示するには、特権 EXEC モードで **show checksum** コマンドを使用します。

show checksum

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

show checksum コマンドを使用すると、コンフィギュレーションの内容のデジタル サマリーとして機能する 4 つのグループの 16 進数を表示できます。このチェックサムが計算されるのは、コンフィギュレーションをフラッシュ メモリに格納するときのみです。

show config コマンドまたは **show checksum** コマンドの出力でチェックサムの前にドット「.」が表示された場合、この出力は、通常のコンフィギュレーション読み込みまたは書き込みモードのインジケータを示しています（セキュリティ アプライアンス のフラッシュ パーティションからの読み込み、または フラッシュ パーティションへの書き込み時)。「.」は、セキュリティ アプライアンスが処理に占有されているが「ハングアップ」していないことを示しています。このメッセージは、「system processing, please wait」メッセージと同様です。

例

次に、コンフィギュレーションまたはチェックサムを表示する例を示します。

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

show chunkstat

チャンクに関する統計情報を表示するには、特権 EXEC モードで **show chunkstat** コマンドを使用します。

show chunkstat

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、チャンクに関する統計情報を表示する例を示します。

```
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
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
show cpu	CPU の使用状況に関する情報を表示します。

show class

クラスに割り当てられたコンテキストを表示するには、特権 EXEC モードで **show class** コマンドを使用します。

show class *name*

構文の説明

name	20 文字までの文字列で名前を指定します。デフォルト クラスを表示するには、名前として **default** と入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show class default** コマンドの出力例を示します。

```
hostname# show class default

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

関連コマンド

コマンド	説明
class	リソース クラスを設定します。
clear configure class	クラス コンフィギュレーションをクリアします。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスのリソース制限を設定します。
member	コンテキストをリソース クラスに割り当てます。

show clock

セキュリティ アプライアンスに時刻を表示するには、ユーザ EXEC モードで **show clock** コマンドを使用します。

show clock [**detail**]

構文の説明

detail	（任意）クロック ソース（NTP またはユーザ コンフィギュレーション）と現在の夏時間設定（存在する場合）を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show clock** コマンドの出力例を示します。

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

次に、**show clock detail** コマンドの出力例を示します。

```
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
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付の範囲を設定します。
clock timezone	時間帯を設定します。
ntp server	NTP サーバを指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show compression svc

セキュリティ アプライアンスで SVC 接続の圧縮統計情報を表示するには、特権 EXEC モードで **show compression svc** コマンドを使用します。

show compression svc

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、**show compression svc** コマンドの出力例を示します。

```
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
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続および WebVPN 接続の圧縮をイネーブルにします。
svc compression	特定のグループまたはユーザに対して SVC 接続を介する HTTP データの圧縮をイネーブルにします。

show configuration

セキュリティ アプライアンスでフラッシュ メモリに保存されているコンフィギュレーションを表示するには、特権 EXEC モードで **show configuration** コマンドを使用します。

show configuration

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドが変更されました。

使用上のガイドライン

show configuration コマンドは、セキュリティ アプライアンスのフラッシュ メモリに保存されているコンフィギュレーションを表示します。**show running-config** コマンドとは異なり、**show configuration** コマンドの実行ではそれほど多くの CPU リソースが使用されません。

セキュリティ アプライアンスのメモリ内のアクティブなコンフィギュレーション（保存されているコンフィギュレーションの変更など）を表示するには、**show running-config** コマンドを使用します。

例

次の例では、セキュリティ アプライアンスのフラッシュ メモリに保存されている設定を表示する方法を示します。

```
hostname# show configuration
: enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.2.5 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.132.12.6 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
```

```
 security-level 50
 ip address 40.0.0.5 255.0.0.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/newImage
ftp mode passive
access-list acl1 extended permit ip any any
access-list mgcpacl extended permit udp any any eq 2727
access-list mgcpacl extended permit udp any any eq 2427
access-list mgcpacl extended permit udp any any eq tftp
access-list mgcpacl extended permit udp any any eq 1719
access-list permitIp extended permit ip any any
pager lines 25
logging enable
logging console debugging
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
icmp permit any dmz
asdm image disk0:/pdm
no asdm history enable
arp timeout 14400
global (outside) 1 10.132.12.50-10.132.12.52
global (outside) 1 interface
global (dmz) 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
access-group mgcpacl in interface dmz
!
router ospf 1
 network 40.0.0.0 255.0.0.0 area 192.168.2.0
 network 192.168.2.0 255.255.255.0 area 192.168.2.0
 log-adj-changes
 redistribute static subnets
 default-information originate
!
route outside 0.0.0.0 0.0.0.0 10.132.12.1 1
route outside 10.129.0.0 255.255.0.0 10.132.12.1 1
route outside 88.0.0.0 255.0.0.0 10.132.12.1 1
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
dynamic-access-policy-record DfltAccessPolicy
```

```
aaa authentication ssh console LOCAL
http server enable
http 10.132.12.0 255.255.255.0 outside
http 192.168.2.0 255.255.255.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 192.168.2.0 255.255.255.0 inside
telnet 10.132.12.0 255.255.255.0 outside
telnet timeout 5
ssh 192.168.2.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect mgcp
policy-map type inspect mgcp mgcpapp
 parameters
  call-agent 150.0.0.210 101
  gateway 50.0.0.201 101
  gateway 100.0.0.201 101
  command-queue 150
!
service-policy global_policy global
webvpn
 memory-size percent 25
 enable inside
 internal-password enable
 onscreen-keyboard logon
username snoopy password /JcYsjvxHfBHc4ZK encrypted
prompt hostname context
Cryptochecksum:62bf8f5de9466cdb64fe758079594635:
end
```

関連コマンド

コマンド	説明
configure	ターミナルからセキュリティ アプライアンスを設定します。

show conn

指定した接続タイプの接続状態を表示するには、特権 EXEC モードで **show conn** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

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*]]]

構文の説明

address	（任意）指定した送信元 IP アドレスまたは宛先 IP アドレスとの接続を表示します。
all	（任意）通過トラフィックの接続に加えて、デバイスへの接続とデバイスからの接続を表示します。
count	（任意）アクティブな接続の数を表示します。
dest_ip	（任意）宛先 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、次のように、IP アドレスをダッシュ（-）で区切ります。 `10.1.1.1-10.1.1.5`
dest_port	（任意）宛先ポート番号を指定します。範囲を指定するには、次のように、ポート番号をダッシュ（-）で区切ります。 `1000-2000`
detail	（任意）変換タイプとインターフェイスの情報を含め、接続の詳細を表示します。
long	（任意）接続をロング フォーマットで表示します。
netmask *mask*	（任意）指定された IP アドレスで使用するサブネット マスクを指定します。
port	（任意）指定した送信元ポートまたは宛先ポートとの接続を表示します。
protocol {tcp | udp}	（任意）接続プロトコル **tcp** または **udp** を指定します。
src_ip	（任意）送信元 IP アドレス（IPv4 または IPv6）を指定します。範囲を指定するには、次のように、IP アドレスをダッシュ（-）で区切ります。 `10.1.1.1-10.1.1.5`
src_port	（任意）送信元ポートの番号を指定します。範囲を指定するには、次のように、ポート番号をダッシュ（-）で区切ります。 `1000-2000`
state *state_type*	（任意）接続状態タイプを指定します。接続状態タイプに使用できるキーワードのリストについては、表 25-5 を参照してください。

デフォルト

デフォルトでは、すべての通過接続が表示されます。デバイスへの管理接続も表示するには、**all** キーワードを使用する必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(8)/7.2(4)/8.0(4)	構文が簡略化され、「ローカル」と「外部」の概念の代わりに送信元と宛先の概念を使用するようになりました。新しい構文では、送信元アドレスを最初のアドレスとして入力し、宛先アドレスを 2 番めのアドレスとして入力します。以前の構文では、**foreign** や **fport** などのキーワードを使用して宛先アドレスおよびポートを設定していました。

使用上のガイドライン

show conn コマンドは、アクティブな TCP 接続および UDP 接続の数を表示し、さまざまなタイプの接続に関する情報を提供します。接続のテーブル全体を参照するには、**show conn all** コマンドを使用します。

（注） セキュリティ アプライアンスで第 2 の接続を許すピンホールが作成された場合、このピンホールは、**show conn** コマンドでは不完全な接続として表示されます。この不完全な接続をクリアするには、**clear conn** コマンドを使用します。

表 25-5 に、**show conn state** コマンドを使用するときに指定できる接続タイプを示します。複数の接続タイプを指定する場合、キーワードの区切りにはカンマを使用します。ただし、スペースは必要ありません。

表 25-5　接続状態のタイプ

キーワード	表示される接続タイプ
up	アップ状態の接続
conn_inbound	着信接続
ctiqbe	CTIQBE 接続
data_in	着信データ接続
data_out	発信データ接続
finin	FIN 着信接続
finout	FIN 発信接続
h225	H.225 接続
h323	H.323 接続
http_get	HTTP get 接続
mgcp	MGCP 接続
nojava	Java アプレットへのアクセスを拒否する接続
rpc	RPC 接続

表 25-5　接続状態のタイプ （続き）

キーワード	表示される接続タイプ
service_module	SSM によってスキャンされる接続
sip	SIP 接続
skinny	SCCP 接続
smtp_data	SMTP メール データ接続
sqlnet_fixup_data	SQL*Net データ インスペクション エンジン接続
vpn_orphan	孤立した VPN トンネル フロー

detail オプションを使用すると、表 25-6 に示した接続フラグを使用して、変換タイプとインターフェイスに関する情報が表示されます。

表 25-6　接続フラグ

フラグ	説明
a	SYN に対する外部 ACK を待機
A	SYN に対する内部 ACK を待機
B	外部からの初期 SYN
C	Computer Telephony Interface Quick Buffer Encoding（CTIQBE; コンピュータ テレフォニー インターフェイス クイック バッファ エンコーディング）メディア接続。
d	dump
D	DNS
E	外部バック接続
f	内部 FIN
F	外部 FIN
g	メディア ゲートウェイ コントロール プロトコル（MGCP）接続
G	接続がグループの一部。G フラグは、接続がグループの一部であることを示します。GRE および FTP の Strict フィックスアップによって設定され、制御接続と関連するすべてのセカンダリ接続を指定します。制御接続が切断されると、関連するすべてのセカンダリ接続も切断されます。
h	H.225
H	H.323
i	不完全な TCP 接続または UDP 接続
I	着信データ
k	Skinny Client Control Protocol（SCCP）メディア接続
K	GTP t3 応答
m	SIP メディア接続
M	SMTP データ
O	発信データ
p	複製（未使用）
P	内部バック接続
q	SQL*Net データ

表 25-6　接続フラグ （続き）

フラグ	説明
r	確認応答された内部 FIN
R	TCP 接続に対する、確認応答された外部 FIN
R	UDP RPC.show conn コマンド出力の各行は 1 つの接続（TCP または UDP）を表すため、1 行に 1 つの R フラグだけが存在します。
	外部 SYN を待機
S	内部 SYN を待機
t	SIP 一時接続。UDP 接続の場合、値 t は接続が 1 分後にタイムアウトすることを示しています。
T	SIP 接続。UDP 接続の場合、値 T は、timeout sip コマンドを使用して指定した値に従って接続がタイムアウトすることを示しています。
U	up
V	VPN の孤立
W	WAAS
X	CSC SSM などのサービス モジュールによって検査

（注）　DNS サーバを使用する接続の場合、**show conn** コマンドの出力で、接続の送信元ポートが *DNS サーバの IP アドレス*に置き換えられることがあります。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元/宛先 IP アドレス、送信元/宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つだけ作成されます。DNS ID は *app_id* で追跡され、各 app_id のアイドル タイマーは独立して実行されます。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内だけであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力すると、DNS 接続のアイドル タイマーが新しい DNS セッションによってリセットされているように見えます。これは共有 DNS 接続の性質によるものであり、仕様です。

（注）　**timeout conn** コマンドで定義した非アクティブ期間（デフォルトは 1:00:00）中に TCP トラフィックがまったく発生しなかった場合は、接続が終了し、対応する接続フラグ エントリも表示されなくなります。

LAN-to-LAN トンネルまたはネットワーク拡張モード トンネルがドロップし、回復しない場合は、孤立したトンネル フローが数多く発生します。このようなフローはトンネルのダウンによって切断されませんが、これらのフローを介して通過を試みるすべてのデータがドロップされます。**show conn** コマンドの出力では、このような孤立したフローを **V** フラグで示します。

例

複数の接続タイプを指定する場合、キーワードの区切りにはカンマを使用します。ただし、スペースは必要ありません。次に、アップ状態の RPC 接続、H.323 接続、および SIP 接続に関する情報を表示する例を示します。

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

次に、**show conn count** コマンドの出力例を示します。

```
hostname# show conn count
54 in use, 123 most used
```

次に、**show conn** コマンドの出力例を示します。次に、内部ホスト 10.1.1.15 から 10.10.49.10 の外部 Telnet サーバへの TCP セッション接続の例を示します。B フラグが存在しないため、接続は内部から開始されています。「U」、「I」および「O」フラグは、接続がアクティブであり、着信データと発信データを受信したことを示します。

```
hostname# show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags
UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags
UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0,
flags Ti
```

次に、**show conn** コマンドの出力例を示します。接続が SSM によってスキャンされていることを示す「X」フラグが含まれています。

```
hostname# 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
```

次に、**show conn detail** コマンドの出力例を示します。次に、外部ホスト 10.10.49.10 から内部ホスト 10.1.1.15 への UDP 接続の例を示します。D フラグは、DNS 接続であることを示しています。1028 は、接続上の DNS ID です。

```
hostname# show conn detail
54 in use, 123 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
TCP outside:10.10.49.10/23 inside:10.1.1.15/1026,
    flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028,
    flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060,
```

```
    flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060,
    flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346
TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000,
    flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464
TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000,
    flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156
TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000,
    flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405
TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060,
    flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
    flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529
TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000,
    flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718
TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000,
    flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694
TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000,
    flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000,
    flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
    flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

次に、**show conn** コマンドの出力例を示します。**V** フラグで示されているとおり、孤立したフローが存在します。

```
hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

孤立したフローがあるこのような接続へのレポートを制限するには、次の例で示すように、**show conn state** コマンドに **vpn_orphan** オプションを追加します。

```
hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
UOVB
```

関連コマンド

コマンド	説明
clear conn	接続をクリアします。
inspect ctiqbe	CTIQBE アプリケーション インスペクションをイネーブルにします。
inspect h323	H.323 アプリケーション インスペクションをイネーブルにします。
inspect mgcp	MGCP アプリケーション インスペクションをイネーブルにします。
inspect sip	Java アプレットを HTTP トラフィックから削除します。
inspect skinny	SCCP アプリケーション インスペクションをイネーブルにします。

show console-output

現在キャプチャされているコンソール出力を表示するには、特権 EXEC モードで **show console-output** コマンドを使用します。

show console-output

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次の例は、コンソール出力がない場合に表示されるメッセージを示しています。

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

関連コマンド

コマンド	説明
clear configure console	デフォルトのコンソール接続設定に戻します。
clear configure timeout	コンフィギュレーションのアイドル時間継続時間をデフォルトに戻します。
console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを設定します。
show running-config console timeout	セキュリティ アプライアンスに対するコンソール接続のアイドル タイムアウトを表示します。

show context

割り当てられているインターフェイス、コンフィギュレーション ファイルの URL、および設定済みコンテキストの数を含めてコンテキスト情報を表示するには（または、システム実行スペースからすべてのコンテキストのリストを表示するには）、特権 EXEC モードで **show context** コマンドを使用します。

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

構文の説明

count	（任意）設定済みコンテキストの数を表示します。
detail	（任意）実行状態および内部使用のための情報を含めて、コンテキストに関する詳細な情報を表示します。
name	（任意）コンテキスト名を設定します。名前を指定しない場合、セキュリティ アプライアンスはすべてのコンテキストを表示します。コンテキスト内で入力できるのは、現在のコンテキスト名のみです。

デフォルト

システム実行スペースでは、名前を指定しない場合、セキュリティ アプライアンスはすべてのコンテキストを表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
8.0(2)	割り当てられた IPS 仮想センサーについての情報が追加されました。

使用上のガイドライン

出力表示の詳細については、「例」を参照してください。

例

次に、**show context** コマンドの出力例を示します。この例では、3 つのコンテキストが表示されています。

```
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
```

表 25-7 に、各フィールドの説明を示します。

表 25-7　show context のフィールド

フィールド	説明
Context Name	すべてのコンテキスト名が表示されます。アスタリスク（*）の付いているコンテキスト名は、管理コンテキストです。
Interfaces	このコンテキストに割り当てられたインターフェイス。
URL	セキュリティ アプライアンスがコンテキストのコンフィギュレーションをロードする URL。

次に、システム実行スペースでの **show context detail** コマンドの出力例を示します。

```
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
  Real IPS Sensors: ips1, ips2
  Mapped IPS Sensors: highsec, lowsec
  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
  Real IPS Sensors: ips1, ips3
  Mapped IPS Sensors: highsec, lowsec
  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
```

表 25-8 に、各フィールドの説明を示します。

表 25-8　コンテキストの状態

フィールド	説明
Context	コンテキストの名前。ヌル コンテキストの情報は内部でのみ使用されます。system というコンテキストは、システム実行スペースを表しています。
状態メッセージ：	コンテキストの状態。次に、表示される可能性のあるメッセージを示します。
Has been created, but initial ACL rules not complete	セキュリティ アプライアンスはコンフィギュレーションを解析しましたが、デフォルト セキュリティ ポリシーを確立するためのデフォルト ACL をまだダウンロードしていません。デフォルト セキュリティ ポリシーは、すべてのコンテキストに対して最初に適用されるもので、下位セキュリティ レベルから上位セキュリティ レベルへのトラフィック送信を禁止したり、アプリケーション インスペクションおよびその他のパラメータをイネーブルにします。このセキュリティ ポリシーによって、コンフィギュレーションが解析されてからコンフィギュレーションの ACL がコンパイルされるまでの間に、トラフィックがセキュリティ アプライアンスをいっさい通過しないことが保証されます。コンフィギュレーションの ACL は非常に高速でコンパイルされるため、この状態が表示されることはほとんどありません。
Has been created, but not initialized	**context** *name* コマンドを入力しましたが、まだ **config-url** コマンドを入力していません。
Has been created, but the config hasn't been parsed	デフォルトの ACL がダウンロードされましたが、まだセキュリティ アプライアンスがコンフィギュレーションを解析していません。この状態が表示される場合は、ネットワーク接続に問題があるために、コンフィギュレーションのダウンロードが失敗した可能性があります。または、**config-url** コマンドをまだ入力していません。コンフィギュレーションをリロードするには、コンテキスト内から **copy startup-config running-config** を入力します。システムから、**config-url** コマンドを再度入力します。または、ブランクの実行コンフィギュレーションの設定を開始します。
Is a system resource	この状態に該当するのは、システム実行スペースとヌル コンテキストのみです。ヌル コンテキストはシステムによって使用され、この情報は内部でのみ使用されます。
Is a zombie	**no context** コマンドまたは **clear context** コマンドを使用してコンテキストを削除しましたが、コンテキストの情報は、セキュリティ アプライアンスがコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。
Is active	このコンテキストは現在実行中であり、コンテキスト コンフィギュレーションのセキュリティ ポリシーに従ってトラフィックを通過させることができます。
Is ADMIN and active	このコンテキストは管理コンテキストであり、現在実行中です。

表 25-8　コンテキストの状態 （続き）

フィールド	説明
Was a former ADMIN, but is now a zombie	**clear configure context** コマンドを使用して管理コンテキストを削除しましたが、コンテキストの情報は、セキュリティ アプライアンスがコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。
Real Interfaces	このコンテキストに割り当てられたインターフェイス。インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、表示されるのはインターフェイスの実際の名前です。
Mapped Interfaces	インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、表示されるのはマッピングされた名前です。インターフェイスをマッピングしなかった場合は、実際の名前がもう一度表示されます。
Real IPS Sensors	AIP SSM をインストールしている場合に、コンテキストに割り当てられる IPS 仮想センサー。センサー名を **allocate-ips** コマンドでマッピングした場合、表示されるのはセンサーの実際の名前です。
Mapped IPS Sensors	センサー名を **allocate-ips** コマンドでマッピングした場合、表示されるのはマッピングされた名前です。センサー名をマッピングしなかった場合は、実際の名前がもう一度表示されます。
Flag	内部でのみ使用されます。
ID	このコンテキストの内部 ID。

次に、**show context count** コマンドの出力例を示します。

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

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。

show controller

存在するすべてのインターフェイスについて、コントローラ固有の情報を表示するには、特権 EXEC モードで **show controller** コマンドを使用します。

show controller [*physical_interface*] [**detail**]

構文の説明

detail	（任意）コントローラの詳細を表示します。
physical_interface	（任意）インターフェイス ID を指定します。

デフォルト

スイッチ ポートを指定しない場合、このコマンドはすべてのインターフェイスの情報を表示します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	このコマンドは ASA 5505 のみではなく、すべてのプラットフォームに適用されるようになりました。**detail** キーワードが追加されました。

使用上のガイドライン

このコマンドは、内部的不具合やカスタマーにより発見された不具合を調査するときに、Cisco TAC がコントローラについての有用なデバッグ情報を収集するために役立ちます。実際の出力は、モデルとイーサネット コントローラによって異なります。

例

次に、**show controller** コマンドの出力例を示します。

```
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
```

次に、**show controller detail** コマンドの出力例を示します。

```
hostname# show controller gigabitethernet0/0 detail

GigabitEthernet0/0:
   Intel i82546GB revision 03

     Main Registers:
         Device Control:             0xf8260000 = 0x003c0249
         Device Status:              0xf8260008 = 0x00003347
         Extended Control:           0xf8260018 = 0x000000c0
         RX Config:                  0xf8260180 = 0x0c000000
         TX Config:                  0xf8260178 = 0x000001a0
         RX Control:                 0xf8260100 = 0x04408002
         TX Control:                 0xf8260400 = 0x000400fa
         TX Inter Packet Gap:        0xf8260410 = 0x00602008
         RX Filter Cntlr:            0xf8260150 = 0x00000000
         RX Chksum:                  0xf8265000 = 0x00000300

     RX Descriptor Registers:
         RX Descriptor 0 Cntlr:      0xf8262828 = 0x00010000
         RX Descriptor 0 AddrLo:     0xf8262800 = 0x01985000
```

```
    RX Desccriptor 0 AddrHi:    0xf8262804 = 0x00000000
    RX Descriptor 0 Length:     0xf8262808 = 0x00001000
    RX Descriptor 0 Head:       0xf8262810 = 0x00000000
    RX Descriptor 0 Tail:       0xf8262818 = 0x000000ff
    RX Descriptor 1 Cntlr:      0xf8262828 = 0x00010000
    RX Descriptor 1 AddrLo:     0xf8260138 = 0x00000000
    RX Descriptor 1 AddrHi:     0xf826013c = 0x00000000
    RX Descriptor 1 Length:     0xf8260140 = 0x00000000
    RX Descriptor 1 Head:       0xf8260148 = 0x00000000
    RX Descriptor 1 Tail:       0xf8260150 = 0x00000000

TX Descriptor Registers:
    TX Descriptor 0 Cntlr:      0xf8263828 = 0x00000000
    TX Descriptor 0 AddrLo:     0xf8263800 = 0x01987000
    TX Descriptor 0 AddrHi:     0xf8263804 = 0x00000000
    TX Descriptor 0 Length:     0xf8263808 = 0x00001000
    TX Descriptor 0 Head:       0xf8263810 = 0x00000000
    TX Descriptor 0 Tail:       0xf8263818 = 0x00000000

RX Address Array:
    Ethernet Address 0:         0012.d948.ef58
    Ethernet Address 1:         Not Valid!
    Ethernet Address 2:         Not Valid!
    Ethernet Address 3:         Not Valid!
    Ethernet Address 4:         Not Valid!
    Ethernet Address 5:         Not Valid!
    Ethernet Address 6:         Not Valid!
    Ethernet Address 7:         Not Valid!
    Ethernet Address 8:         Not Valid!
    Ethernet Address 9:         Not Valid!
    Ethernet Address a:         Not Valid!
    Ethernet Address b:         Not Valid!
    Ethernet Address c:         Not Valid!
    Ethernet Address d:         Not Valid!
    Ethernet Address e:         Not Valid!
    Ethernet Address f:         Not Valid!

PHY Registers:
    Phy Control:                0x1140
    Phy Status:                 0x7969
    Phy ID 1:                   0x0141
    Phy ID 2:                   0x0c25
    Phy Autoneg Advertise:      0x01e1
    Phy Link Partner Ability:   0x41e1
    Phy Autoneg Expansion:      0x0007
    Phy Next Page TX:           0x2801
    Phy Link Partnr Next Page:  0x0000
    Phy 1000T Control:          0x0200
    Phy 1000T Status:           0x4000
    Phy Extended Status:        0x3000

Detailed Output - RX Descriptor Ring:

rx_bd[000]: baddr      = 0x019823A2, length = 0x0000, status  = 0x00
            pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000
rx_bd[001]: baddr      = 0x01981A62, length = 0x0000, status  = 0x00
            pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000

.........
```

関連コマンド

コマンド	説明
show interface	インターフェイス統計情報を表示します。
show tech-support	Cisco TAC による問題の診断を可能にするような情報を表示します。

show counters

プロトコル スタック カウンタを表示するには、特権 EXEC モードで **show counters** コマンドを使用します。

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

構文の説明

all	フィルタの詳細を表示します。
context *context-name*	コンテキスト名を指定します。
:*counter_name*	カウンタを名前で指定します。
detail	詳細なカウンタ情報を表示します。
protocol *protocol_name*	指定したプロトコルのカウンタを表示します。
summary	カウンタの要約を表示します。
threshold *N*	指定したしきい値以上のカウンタのみを表示します。指定できる範囲は 1 ～ 4294967295 です。
top *N*	指定したしきい値以上のカウンタを表示します。指定できる範囲は 1 ～ 4294967295 です。

デフォルト

show counters summary detail threshold 1

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、すべてのカウンタを表示する例を示します。

```
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
```

次に、カウンタの要約を表示する例を示します。

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

次に、コンテキストのカウンタを表示する例を示します。

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

関連コマンド

コマンド	説明
clear counters	プロトコル スタック カウンタをクリアします。

show cpu

CPU の使用状況に関する情報を表示するには、特権 EXEC モードで **show cpu** コマンドを使用します。

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

マルチ コンテキスト モードでは、システム コンフィギュレーションから次のように入力します。

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

構文の説明

all	すべてのコンテキストを表示することを指定します。
context	1 つのコンテキストを表示することを指定します。
context_name	表示するコンテキストの名前を指定します。
detailed	（任意）CPU の内部使用に関する詳細な情報を表示します。
profile	（任意）CPU のプロファイリング データを表示します。
usage	（任意）CPU 使用状況を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

CPU の使用状況は、5 秒ごとの負荷の近似値を使用し、この概算値をさらに以降の 2 つの移動平均に適用することによって算出されます。

show cpu コマンドを使用すると、プロセス関連の負荷を検出できます（つまり、**show process** コマンドを、シングルモードとマルチ コンテキスト モードのシステム コンフィギュレーションの両方で実行した場合に表示される項目の代わりに、アクティビティを表示できます）。

さらに、マルチ コンテキスト モードでは、プロセス関連負荷を分散するよう、設定されたすべてのコンテキストで消費される CPU に要求できます。このためには、各コンテキストに変更して **show cpu** コマンドを入力するか、このコマンドのバリアントである **show cpu context** を入力します。

プロセス関連の負荷は、最も近い整数に丸められますが、コンテキスト関連の負荷の場合は精度を表す 10 進数が 1 つ追加されます。たとえば、**show cpu** をシステム コンテキストから入力すると、**show cpu context system** コマンドを入力したときとは別の数値が示されます。前者は **show cpu context all** の要約とほぼ同じですが、後者はその要約の一部にすぎません。

show cpu profile コマンドと、cpu profile activate コマンドを併用することで、CPU の問題の修復を支援するために TAC が収集および使用できる情報を表示できます。show cpu profile コマンドによって表示される情報は 16 進数です。

例

次に、CPU 使用状況を表示する例を示します。

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

次に、マルチ モードでシステム コンテキストの CPU 使用状況を表示する例を示します。

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

次に、すべてのコンテキストの CPU 使用状況を表示する例を示します。

```
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
```

次に、「one」というコンテキストの CPU 使用状況を表示する例を示します。

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

次の例では、プロファイラが稼働し、5000 個のサンプルの格納が命令されます。

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

結果を確認するには、**show cpu profile** コマンドを使用します。

（注） **cpu profile activate** コマンドの実行中に **show cpu profile** を実行すると、進捗が表示されます。

```
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.
```

完了すると、**show cpu profile** コマンドの出力に結果が表示されます。この情報をコピーし、デコードする TAC に提供します。

```
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 .
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
cpu profile activate	CPU プロファイリングをアクティブにします。

show crashinfo

フラッシュ メモリに格納されているクラッシュ ファイルの内容を表示するには、特権 EXEC モードで **show crashinfo** コマンドを使用します。

show crashinfo [**save**]

構文の説明

save	（任意）クラッシュ情報をフラッシュ メモリに保存するようにセキュリティ アプライアンスが設定されているかどうかを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

クラッシュ ファイルがテスト クラッシュ（**crashinfo test** コマンドで生成）である場合、クラッシュ ファイルの最初のストリングは「**: Saved_Test_Crash**」であり、最後のストリングは「**: End_Test_Crash**」です。クラッシュ ファイルが実際のクラッシュである場合、クラッシュ ファイルの最初の行の文字列は「**: Saved_Crash**」で、最後の文字列は「**: End_Crash**」です。（**crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドを使用して発生させたクラッシュを含む）。

クラッシュ データがフラッシュにまったく保存されていない場合や、**clear crashinfo** コマンドを入力してクラッシュ データをクリアしていた場合は、**show crashinfo** コマンドを実行するとエラー メッセージが表示されます。

例

次に、現在のクラッシュ情報コンフィギュレーションを表示する例を示します。

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

次に、クラッシュ ファイル テストの出力例を示します （このテストによって、セキュリティ アプライアンスが実際にクラッシュすることはありません。このテストで提供されるのは、シミュレートされたサンプル ファイルです)。

```
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
```

関連コマンド

コマンド	説明
clear crashinfo	クラッシュ ファイルの内容を削除します。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリにクラッシュ情報を書き込めないようにします。
crashinfo test	セキュリティ アプライアンスでフラッシュ メモリ内のファイルにクラッシュ情報を保存できるかどうかをテストします。

show crashinfo console

crashinfo console コマンドのコンフィギュレーション設定を表示するには、**show crashinfo console** コマンドを入力します。

show crashinfo console

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

FIPS 140-2 に準拠していることにより、キーやパスワードなどのクリティカル セキュリティ パラメータをクリプト境界（シャーシ）の外側に配布することが禁止されています。アサートまたはチェックヒープのエラーによってデバイスがクラッシュしたとき、コンソールにダンプされるスタック領域やメモリ領域には、機密データが含まれていることがあります。この出力は、FIPS モードでは表示されないようにする必要があります。

例

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

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	電源投入時自己診断テストを実行します。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

show crypto accelerator statistics

ハードウェア クリプト アクセラレータ MIB 内のグローバルな統計情報またはアクセラレータ固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto accelerator statistics** コマンドを使用します。

show crypto accelerator statistics

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

出力統計情報は、次のように定義されます。

アクセラレータ 0 はソフトウェアベースのクリプト エンジンです。

アクセラレータ 1 はハードウェアベースのクリプト エンジンです。

RSA 統計情報には、ソフトウェアでのみ実行される、2048 ビット キーの RSA 処理が表示されます。つまり、2048 ビット キーがある場合、IKE/SSL VPN は、IPSec/SSL ネゴシエーション フェーズ中にソフトウェアで RSA 処理を実行します。実際の IPSec/SSL トラフィックは、引き続きハードウェアを使用して処理されます。これにより、同時に開始された同時セッションが数多くある場合、CPU の高使用となります。このため、RSA キー処理が複数発生し、CPU の高使用となる可能性があります。このようにして CPU の高使用状態となった場合は、1024 ビット キーを使用して、ハードウェアで RSA キー処理を実行する必要があります。このためには、アイデンティティ証明書を再度登録する必要があります。

2048 ビットの RSA キーを使用しており、ソフトウェアで RSA 処理が実行されている場合は、CPU プロファイリングを使用して、CPU の高使用状況の原因となっている関数を特定できます。通常、bn_* 関数と BN_* 関数は RSA に使用される大規模なデータ セットでの数学的処理であり、ソフトウェアでの RSA 処理中に CPU の使用状況を確認する場合に最も役立ちます。次に例を示します。

```
@@@@@@@@@@@@@@@@@@@@..............................  36.50% : _bn_mul_add_words
@@@@@@@@@@.....................................  19.75% : _bn_sqr_comba8
```

Diffie-Hellman 統計情報には、ソフトウェアで 1024 より大きいモジュラス サイズの暗号処理が実行されたことが表示されます（DH5（Diffie-Hellman グループ 5 が 1536 を使用しています）など）。この場合、2048 ビット キー証明書はソフトウェアで処理されます。このため、数多くのセッションが実行されるときに CPU の高使用状況となります。

（注）　ASA 5580（Cavium クリプト チップ搭載）のみが、ハードウェアにより高速化される 2048 ビットの RSA キー生成をサポートしています。ASA 5510、5520、5540、および 5550 は、ハードウェアにより高速化される 2048 ビットのキー生成をサポートしていません。ASA 5505（Cavium CN505 プロセッサ搭載）のみが、ハードウェアにより高速化される 768 ビットおよび 1024 ビットのキー生成の Diffie-Hellman グループ 1 および 2 をサポートしています。Diffie-Hellman グループ 5（1536 ビットのキー生成）は、ソフトウェアで実行されます。

適応型セキュリティ アプライアンスでは 1 つのクリプト エンジンが IPSec 処理および SSL 処理を実行します。起動時にハードウェア クリプト アクセラレータにロードされたクリプト（Cavium）マイクロコードのバージョンを表示するには、**show version** コマンドを入力します。次に例を示します。

```
hostname(config) show version

Cisco Adaptive Security Appliance Software Version 8.0(4)8
Device Manager Version 6.1(5)
Compiled on Wed 15-Oct-09 17:27 by builders
System image file is "disk0:/interim/asa804-8-k8.bin"
Config file at boot was "startup-config"
asa up 5 days 17 hours
Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 512MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB
Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.05
```

DSA 統計情報には、2 つのフェーズでのキー生成が表示されます。最初のフェーズは、アルゴリズム パラメータの選択です。このパラメータは、システムの他のユーザと共有することがあります。2 番めのフェーズは、1 人のユーザ用の秘密キーと公開キーの算出です。

SSL 統計情報には、ハードウェア クリプト アクセラレータへの SSL トランザクションで使用される、プロセッサ集約的な公開キーの暗号化アルゴリズムに関するレコードが表示されます。

RNG 統計情報には、キーとして使用する同じ乱数のセットを自動的に生成できる送信元とレシーバに関するレコードが表示されます。

例

次に、グローバル コンフィギュレーション モードでグローバルなクリプト アクセラレータ統計情報を表示する例を示します。

```
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
```

次に、出力エントリが示す内容について説明した表を示します。

出力	説明
Capacity	このセクションは、セキュリティ アプライアンスがサポートできるクリプト アクセラレーションに関連しています。
Supports hardware crypto	(True/False) セキュリティ アプライアンスはハードウェア クリプト アクセラレーションをサポートできます。
Supports modular hardware crypto	(True/False) サポートされている任意のハードウェア クリプト アクセラレータを個別のプラグイン カードまたはモジュールとして挿入できます。
Max accelerators	セキュリティ アプライアンスでサポートされるハードウェア クリプト アクセラレータの最大数。
Mac crypto throughput	セキュリティ アプライアンスの最大定格 VPN スループット。
Max crypto connections	セキュリティ アプライアンスのサポート対象 VPN トンネルの最大数。
Global Statistics	このセクションは、セキュリティ アプライアンスの複合ハードウェア クリプト アクセラレータに関連しています。
Number of active accelerators	アクティブなハードウェア アクセラレータの数。アクティブなハードウェア アクセラレータが初期化されており、crypto コマンドの処理に使用可能です。

出力 （続き）	説明 （続き）
Number of non-operational accelerators	非アクティブなハードウェア アクセラレータの数。非アクティブなハードウェア アクセラレータが検出されました。初期化が完了していないか、障害が発生して使用できなくなっています。
Input packets	すべてのハードウェア クリプト アクセラレータで処理される着信パケットの数。
Input bytes	処理される着信パケット内のデータのバイト数。
Output packets	すべてのハードウェア クリプト アクセラレータで処理される発信パケットの数。
Output error packets	エラーが検出された、すべてのハードウェア クリプト アクセラレータで処理される発信パケットの数。
Output bytes	処理される発信パケット内のデータのバイト数。
Accelerator 0	各セクションは、クリプト アクセラレータに関連しています。最初のセクション（Accelerator 0）は、常に、ソフトウェア クリプト エンジンです。ハードウェア アクセラレータではありませんが、セキュリティ アプライアンスはこのソフトウェア クリプト エンジンを使用して、特定のクリプト タスクを実行します。ここには、その統計情報が表示されます。Accelerators 1 以上は、常に、ハードウェア クリプト アクセラレータです。
Status	アクセラレータのステータス。アクセラレータが初期化されているか、アクティブか、あるいは失敗したかを示します。
Software crypto engine	アクセラレータのタイプとファームウェア バージョン（該当する場合）。
Slot	アクセラレータのスロット番号（該当する場合）。
Active time	アクセラレータがアクティブ状態であった時間の長さ。
Total crypto transforms	アクセラレータによって実行された crypto コマンドの合計数。
Total dropped packets	エラーのためアクセラレータによってドロップされたパケットの合計数。
Input statistics	このセクションは、アクセラレータで処理された入力トラフィックに関連しています。入力トラフィックは、複合か認証、またはその両方を行う必要がある暗号文と見なされます。
Input packets	アクセラレータによって処理された入力パケットの数。
Input bytes	アクセラレータによって処理された入力バイト数。
Input hashed packets	アクセラレータがハッシュを実行したパケットの数。
Input hashed bytes	アクセラレータがハッシュを実行したバイト数。
Decrypted packets	アクセラレータが対称復号化を実行したパケットの数。
Decrypted bytes	アクセラレータが対称復号化を実行したバイト数。
Output statistics	このセクションは、アクセラレータで処理された出力トラフィックに関連しています。入力トラフィックは、暗号化かハッシュ、またはその両方を実行する必要があるクリア テキストと見なされます。
Output packets	アクセラレータによって処理された出力パケットの数。

出力 （続き）	説明 （続き）
Output bad packets	エラーが検出された、アクセラレータで処理された出力パケットの数。
Output bytes	アクセラレータによって処理された出力バイト数。
Output hashed packets	アクセラレータが出力ハッシュを実行したパケットの数。
Output hashed bytes	アクセラレータが出力ハッシュを実行したバイト数。
Encyrpted packets	アクセラレータが対称暗号化を実行したパケットの数。
Encyrpted bytes	アクセラレータが対称暗号化を実行したバイト数。
Diffie-Hellman statistics	このセクションは、Diffie-Hellman のキー交換処理に関連しています。
Keys generated	アクセラレータによって生成された Diffie-Hellman キー セットの数。
Secret keys derived	アクセラレータによって生成された Diffie-Hellman 共有秘密の数。
RSA statistics	このセクションは、RSA 暗号処理に関連しています。
Keys generated	アクセラレータによって生成された RSA キー セットの数。
Signatures	アクセラレータによって実行された RSA シグニチャ処理の数。
Verifications	アクセラレータによって実行された RSA シグニチャ確認の数。
Encrypted packets	アクセラレータが RSA 暗号化を実行したパケットの数。
Decrypted packets	アクセラレータが RSA 復号化を実行したパケットの数。
Decrypted bytes	アクセラレータが RSA 復号化を実行したデータのバイト数。
DSA statistics	このセクションは、DSA 処理に関連しています。DSA はバージョン 8.2 以上ではサポートされないため、この統計情報は表示されません。
Keys generated	アクセラレータによって生成された DSA キー セットの数。
Signatures	アクセラレータによって実行された DSA シグニチャ処理の数。
Verifications	アクセラレータによって実行された DSA シグニチャ確認の数。
SSL statistics	このセクションは、SSL レコード処理に関連しています。
Outbound records	アクセラレータによって暗号化され、認証された SSL レコードの数。
Inbound records	アクセラレータによって復号化され、認証された SSL レコードの数。
RNG statistics	このセクションは、乱数生成に関連しています。
Random number requests	アクセラレータに対する乱数の要求の数。
Random number request failures	アクセラレータに対する乱数要求のうち、失敗した要求の数。

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto protocol statistics	暗号アクセラレータ MIB からプロトコル固有の統計情報を表示します。

show crypto ca certificates

特定のトラストポイントに関連付けられている証明書、またはシステムにインストールされているすべての証明書を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ca certificates** コマンドを使用します。

show crypto ca certificates [*trustpointname*]

構文の説明

trustpointname	（任意）トラストポイントの名前。名前を指定しない場合は、システムにインストールされているすべての証明書が表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、tp1 というトラストポイントの CA 証明書を表示する例を示します。

```
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)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定されたトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定されたトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求します。
crypto ca enroll	CA を使用して、登録プロセスを開始します。
crypto ca import	指定されたトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定されたトラストポイントでトラストポイント モードを開始します。

show crypto ca crls

キャッシュされているすべての CRL、または指定したトラストポイントでキャッシュされているすべての CRL を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ca crls** コマンドを使用します。

show crypto ca crls [*trustpointname*]

構文の説明

trustpointname	（任意）トラストポイントの名前。名前を指定しない場合は、システムにキャッシュされているすべての CRL が表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、tp1 というトラストポイントの CRL を表示する例を示します。

```
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)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定されたトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定されたトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求します。
crypto ca enroll	CA を使用して、登録プロセスを開始します。

コマンド	説明
crypto ca import	指定されたトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定されたトラストポイントでトラストポイント モードを開始します。

show crypto ca server

セキュリティ アプライアンスにあるローカル Certificate Authority（CA; 認証局）コンフィギュレーションのステータスを表示するには、**show crypto ca server** コマンドを使用します。

show crypto ca server

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、ローカル CA サーバのすべてのコンフィギュレーション データのステータスを表示する例を示します。

```
hostname# show crypto ca server
#Certificate Server LOCAL-CA-SERVER:
    Status: disabled
    State: disabled
    Server's configuration is unlocked (enter "no shutdown" to lock it)
    Issuer name: CN=asa1.cisco.com
    CA cert fingerprint: -Not found-
    Last certificate issued serial number: 0x0
    CA certificate expiration timer: 00:00:00 UTC Jan 1 1970
    CRL not present.
    Current primary storage dir: nvram:
hostname#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
debug crypto ca server	ローカル CA サーバを設定するときに、デバッグ メッセージを表示します。
show crypto ca server certificate	ローカル CA の証明書を Base-64 形式で表示します。
show crypto ca server crl	ローカル CA CRL のライフタイムを表示します。

show crypto ca server cert-db

特定のユーザに対して発行される証明書を含め、ローカル Certificate Authority（CA; 認証局）サーバのすべての証明書、またはそのサブセットを表示するには、**show crypto ca server cert-db** コマンドを使用します。

show crypto ca server cert-db [user *username* **| allowed | enrolled | expired | on-hold]**

[serial *certificate-serial-number*]

構文の説明

allowed	証明書のステータスに関係なく、登録を許可されているユーザを表示するように指定します。
enrolled	有効な証明書を持つユーザを表示するように指定します。
expired	期限切れの証明書を保持しているユーザを表示するように指定します。
on-hold	まだ登録されていないユーザを表示するように指定します。
serial *certificate-serial-number*	表示する特定の証明書のシリアル番号を指定します。シリアル番号は 16 進形式で入力します。
user **username**	証明書の所有者を指定します。ユーザ名は、単純なユーザ名または電子メール アドレスです。

デフォルト

デフォルトでは、ユーザ名や証明書のシリアル番号が指定されていない場合は、発行された証明書のデータベース全体が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

show crypto ca server cert-db コマンドは、ローカル CA サーバによって発行されたユーザ証明書のリストを表示します。1 つ以上の証明書タイプ キーワードをオプションとして付けて、またはオプションの証明書シリアル番号を付けて、特定のユーザ名を指定し、証明書データベースのサブセットを表示できます。

キーワードまたはシリアル番号なしでユーザ名を指定すると、そのユーザに対して発行された証明書がすべて表示されます。ユーザごとに、ユーザ名、*renewal allowed till* フィールド、*number of times the user is notified* カウント、および *PKCS12 file stored till* 値が、そのユーザに対して発行された証明書の前に表示されます。

それぞれの証明書には、証明書のシリアル番号、発行日付と有効期限日付、および証明書のステータス（Revoked/Not Revoked）が表示されます。

例

次に、CA サーバが Janedoe に対して発行した証明書をすべて表示するよう要求する例を示します。

```
hostname# show crypto ca server cert-db user janedoe
```

次に、ローカル CA サーバによって発行された、シリアル番号が 0x100 以上の証明書をすべて表示するよう要求する例を示します。

```
hostname# show crypto ca server cert-db serial 1oo
```

次に、ローカル CA サーバによって発行された証明書をすべて表示するよう要求する例を示します。

```
hostname# show crypto ca server cert-db
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
crypto ca server revoke	証明書データベースと Certificate Revocation List（CRL; 証明書失効リスト）の両方で、ローカル CA サーバによって発行された証明書を失効としてマークします。
lifetime crl	証明書失効リストのライフタイムを指定します。

show crypto ca server certificate

ローカル Certificate Authority（CA; 認証局）サーバの証明書を Base-64 形式で表示するには、**show crypto ca server certificate** コマンドを使用します。

show crypto ca server certificate

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

show crypto ca server certificate コマンドにより、ローカル CA サーバの証明書が Base-64 形式で表示されます。これで、ローカル CA サーバを信頼する必要がある他のデバイスに証明書をエクスポートするときに、その証明書をカット アンド ペーストできます。

例

次に、ローカル CA サーバのサーバ証明書を表示する例を示します。

```
hostname# show crypto ca server certificate

The base64 encoded local CA certificate follows:

MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHAYJKo
ZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3SDOiDwZG9
n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZTS1E4L0fSaC3
uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZPrzoG1J8BFqdPa1j
BGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYYbP86tvbZ2yOVZR6aKFVI
0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3
qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

hostname#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
keysize	ユーザ証明書登録で生成される公開キーと秘密キーのサイズを指定します。
lifetime	CA 証明書と発行済みの証明書のライフタイムを指定します。
show crypto ca server	ローカル CA コンフィギュレーションを ASCII テキスト形式で表示します。

show crypto ca server crl

ローカル Certificate Authority（CA; 認証局）の現在の Certificate Revocation List（CRL; 証明書失効リスト）を表示するには、**show crypto ca server crl** コマンドを表示します。

show crypto ca server crl

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、組み込み CA サーバの現在の CRL を表示する例を示します。

```
hostname# show crypto ca server crl
asa5540(config)# sh cry ca ser crl
Certificate Revocation List:
    Issuer: cn=asa5540.frqa.cisco.com
    This Update: 07:32:27 UTC Oct 16 2006
    Next Update: 13:32:27 UTC Oct 16 2006
    Number of CRL entries: 0
    CRL size: 232 bytes
asa5540(config)#
hostname#
```

関連コマンド

コマンド	説明
cdp-url	CA が発行する証明書に含める、Certificate Revocation List（CRL; 証明書失効リスト）の Distribution Point（CDP; 配布ポイント）を指定します。
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。

コマンド	説明
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。
lifetime crl	Certificate Revocation List（CRL; 証明書失効リスト）のライフタイムを指定します。
show crypto ca server	CA コンフィギュレーションのステータスを表示します。

show crypto ca server user-db

ローカル Certificate Authority（CA; 認証局）サーバのユーザ データベースに存在するユーザを表示するには、**show crypto ca server user-db** コマンドを使用します。

show crypto ca server user-db [**expired** | **allowed** | **on-hold** | **enrolled**]

構文の説明

allowed	（任意）証明書のステータスに関係なく、登録を許可されたユーザを表示するように指定します。
enrolled	（任意）有効な証明書を持つユーザを表示するように指定します。
expired	（任意）期限切れの証明書を保持しているユーザを表示するように指定します。
on-hold	（任意）まだ登録されていないユーザを表示するように指定します。

デフォルト

デフォルトでは、キーワードが入力されない場合にはデータベース内のすべてのユーザが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CA サーバ コンフィギュレーション	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、現在登録されているユーザを表示する例を示します。

```
hostname# crypto ca server user-db enrolled
Username    DN                Certificate issued    Certificate expiration
jandoe      cn=Jan Doe,o=...  5/31/2006             5/31/2007

hostname#
```

関連コマンド

コマンド	説明
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
crypto ca server user-db allow	CA サーバ データベース内の特定のユーザまたはユーザのサブセットに、ローカル CA への登録を許可します。
crypto ca server user-db remove	CA サーバのユーザ データベースからユーザを削除します。
crypto ca server user-db write	ローカル CA データベースで設定されているユーザ情報をストレージに書き込みます。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。

show crypto debug-condition

IPSec および ISAKMP のデバッグ メッセージに対して現在設定されているフィルタ、一致しない状態、およびエラー ステートを表示するには、グローバル コンフィギュレーション モードで **show crypto debug-condition** コマンドを使用します。

show crypto debug-condition

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

例

次に、フィルタリング条件を表示する例を示します。

```
hostname(config)# show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag:  OFF
IPSec debug context unmatched flag:  ON

IKE peer IP address filters:
1.1.1.0/24   2.2.2.2

IKE user name filters:
my_user
```

関連コマンド

コマンド	説明
debug crypto condition	IPSec および ISAKMP デバッグ メッセージのフィルタリング条件を設定します。
debug crypto condition error	フィルタリング条件が指定されているかどうかのデバッグ メッセージを表示します。
debug crypto condition unmatched	フィルタリングに十分なコンテキスト情報が含まれていない IPSec および ISAKMP のデバッグ メッセージを表示します。

show crypto ipsec df-bit

指定したインターフェイスの IPSec パケットの IPSec DF-bit ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec df-bit** コマンドを使用します。

show crypto ipsec df-bit *interface*

構文の説明

interface	インターフェイス名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、inside というインターフェイスの IPSec DF-bit ポリシーを表示する例を示します。

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

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPSec パケットの IPSec DF-bit ポリシーを設定します。
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを表示します。

show crypto ipsec fragmentation

IPSec パケットのフラグメンテーション ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec fragmentation** コマンドを使用します。

show crypto ipsec fragmentation *interface*

構文の説明

interface	インターフェイス名を指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、inside というインターフェイスの IPSec フラグメンテーション ポリシーを表示する例を示します。

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

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
crypto ipsec df-bit	IPSec パケットの DF ビット ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show crypto ipsec sa

IPSec SA のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec sa** コマンドを使用します。このコマンドの別の形式である **show ipsec sa** を使用することもできます。

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

構文の説明

detail	（任意）表示されているものに対する詳細なエラー情報を表示します。
entry	（任意）IPSec SA をピア アドレスの順に表示します。
identity	（任意）IPSec SA を ID の順に表示します。ESP は含まれません。これは簡略化された形式です。
map *map-name*	（任意）指定されたクリプト マップの IPSec SA を表示します。
peer *peer-addr*	（任意）指定されたピア IP アドレスの IPSec SA を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec SA が表示されます。

```
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)#
```

（注） IPSec SA ポリシーに、フラグメンテーションは IPSec 処理の前に発生すると明記されている場合、フラグメンテーション統計情報は、フラグメンテーション前の統計情報です。SA ポリシーで、フラグメンテーションは IPSec 処理の後に発生すると明記されている場合、フラグメンテーション後の統計情報が表示されます。

次の例をグローバル コンフィギュレーション モードで入力すると、def という名前のクリプト マップの IPSec SA が表示されます。

```
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)#
```

次の例をグローバル コンフィギュレーション モードで入力すると、キーワード **entry** に対する IPSec SA が表示されます。

```
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)#
```

次の例をグローバル コンフィギュレーション モードで入力すると、キーワード **entry detail** を使って、IPSec SA が表示されます。

```
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

    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)#
```

次に、キーワード **identity** を使った IPSec SA の例を示します。

```
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
```

次に、キーワード **identity** および **detail** を使った IPSec SA の例を示します。

```
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
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto ipsec stats

IPSec 統計情報のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec stats** コマンドを使用します。

show crypto ipsec stats

構文の説明

このコマンドには、キーワードや変数はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次の例をグローバル コンフィギュレーション モードで入力すると、IPSec 統計情報が表示されます。

```
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)#
```

関連コマンド

コマンド	説明
clear ipsec sa	指定されたパラメータに基づいて、IPSec SA またはカウンタをクリアします。
crypto ipsec transform-set	トランスフォーム セットを定義します。
show ipsec sa	指定されたパラメータに基づいて IPSec SA を表示します。
show ipsec sa summary	IPSec SA の要約を表示します。

show crypto isakmp stats

実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp stats** コマンドを使用します。

show crypto isakmp stats

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが追加されました。
7.2(1)	**show isakmp stats** コマンドが非推奨コマンドになりました。**show crypto isakmp stats** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- 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

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
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)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp sa

IKE ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp sa** コマンドを使用します。

show crypto isakmp sa [**detail**]

構文の説明

detail	SA データベースに関する詳細出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp sa** コマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**show crypto isakmp sa** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合

IKE ピア	タイプ	Dir	Rky	ステート
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合

IKE ピア	タイプ	Dir	Rky	ステート	暗号	ハッシュ	認証	ライフタイム
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

次の例をグローバル コンフィギュレーション モードで入力すると、SA データベースに関する詳細情報が表示されます。

```
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)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp stats

実行時統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp stats** コマンドを使用します。

show crypto isakmp stats

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが追加されました。
7.2(1)	**show isakmp stats** コマンドが非推奨コマンドになりました。**show crypto isakmp stats** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- 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

例

次の例をグローバル コンフィギュレーション モードで入力すると、ISAKMP 統計情報が表示されます。

```
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)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto protocol statistics

クリプト アクセラレータ MIB 内のプロトコル固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto protocol statistics** コマンドを使用します。

show crypto protocol statistics *protocol*

構文の説明

protocol	統計情報を表示するプロトコルの名前を指定します。プロトコルの選択肢は次のとおりです。 **ikev1**：インターネット キー交換バージョン 1。 **ipsec**：IP セキュリティ フェーズ 2 プロトコル。 **ssl**：Secure Socket Layer。 **other**：新規プロトコル用に予約済み。 **all**：現在サポートされているすべてのプロトコル。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードで、指定したプロトコルに関するクリプト アクセラレータ統計情報を表示する例を示します。

```
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 #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB にあるグローバルおよびアクセラレータ固有の統計情報をクリアします。
clear crypto protocol statistics	暗号アクセラレータ MIB にあるプロトコル固有の統計情報をクリアします。
show crypto accelerator statistics	暗号アクセラレータ MIB からグローバルおよびアクセラレータ固有の統計情報を表示します。

show csc node-count

ノードとは、固有の送信元 IP アドレス、またはセキュリティ アプライアンスにより保護されているネットワーク上のデバイスのアドレスです。セキュリティ アプライアンスは、毎日のノード カウントを追跡し、ユーザ ライセンスの強制のために CSC SSM に伝えます。CSC SSM がスキャンしたトラフィックのノード数を表示するには、特権 EXEC モードで **show csc node-count** コマンドを使用します。

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

構文の説明

yesterday	（任意）CSC SSM が前日の 24 時間（午前 0 時から翌日の午前 0 時まで）スキャンしたトラフィックのノード数を表示します。

デフォルト

デフォルトで表示されるノード カウントは、午前 0 時からスキャンされたノード数です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、**show csc node-count** コマンドを使用して、CSC SSM が午前 0 時からスキャンしたトラフィックのノード数を表示する例を示します。

```
hostname# show csc node-count
Current node count is 1
```

次に、**show csc node-count** コマンドを使用して、CSC SSM が前日の 24 時間（午前 0 時から翌日の午前 0 時まで）スキャンしたトラフィックのノード数を表示する例を示します。

```
hostname(config)# show csc node-count yesterday
Yesterday's node count is 2
```

関連コマンド

csc	ネットワーク トラフィックを CSC SSM に送信して、CSC SSM で設定されているとおりに FTP、HTTP、POP3、および SMTP をスキャンします。
show running-config class-map	現在のクラス マップ コンフィギュレーションを表示します。

show running-config policy-map	現在のポリシー マップ コンフィギュレーションを表示します。
show running-config service-policy	現在のサービス ポリシー コンフィギュレーションを表示します。

show ctiqbe

セキュリティ アプライアンスを越えて確立された CTIQBE セッションの情報を表示するには、特権 EXEC モードで **show ctiqbe** コマンドを使用します。

show ctiqbe

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

show ctiqbe コマンドは、セキュリティ アプライアンスを越えて確立された CTIQBE セッションの情報を表示します。**debug ctiqbe** や **show local-host** とともに、このコマンドは、CTIQBE インスペクション エンジンの問題のトラブルシューティングに使用されます。

（注）　**show ctiqbe** コマンドを使用する前に **pager** コマンドを設定することを推奨します。多くの CTIQBE セッションが存在し、**pager** コマンドが設定されていない場合、**show ctiqbe** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。

例

次の条件における **show ctiqbe** コマンドの出力例を示します。セキュリティ アプライアンスを越えてセットアップされているアクティブ CTIQBE セッションは 1 つだけです。そのセッションは、ローカル アドレス 10.0.0.99 の内部 CTI デバイス（たとえば、Cisco IP SoftPhone）と 172.29.1.77 の外部 Cisco CallManager の間で確立されています。ここで、TCP ポート 2748 は、Cisco CallManager です。このセッションのハートビート間隔は 120 秒です。

```
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)
|-----------------------------------------------
```

CTI デバイスは、すでに CallManager に登録されています。デバイスの内部アドレスおよび RTP 受信ポートは 172.29.1.99 の UDP ポート 1028 に PAT 変換されています。Real-Time Control Protocol（RTCP; リアルタイム制御プロトコル）受信ポートは UDP 1029 に PAT 変換されています。

`RTP/RTCP: PAT xlates:` で始まる行は、内部 CTI デバイスが外部 CallManager に登録され、CTI デバイスのアドレスとポートがその外部インターフェイスに PAT 変換されている場合に限り表示されます。この行は、CallManager が内部インターフェイス上に位置する場合、または内部 CTI デバイスのアドレスとポートが、CallManager が使用しているのと同じ外部インターフェイスに NAT 変換されている場合は、表示されません。

この出力は、コールがこの CTI デバイスと 172.29.1.88 にある別の電話機の間に確立されていることを示します。他の電話機の RTP および RTCP 受信ポートは、UDP 26822 および 26823 です。セキュリティ アプライアンスは 2 番目の電話機と CallManager に関連する CTIQBE セッション レコードを維持できないので、他の電話機は、CallManager と同じインターフェイス上にあります。CTI デバイス側のアクティブ コール レッグは、Device ID 27 および Call ID 0 で確認できます。

次に、これらの CTIBQE 接続に対する xlate 情報を示します。

```
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#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect ctiqbe	CTIQBE アプリケーション インスペクションをイネーブルにします。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show curpriv

現在のユーザ特権を表示するには、**show curpriv** コマンドを使用します。

show curpriv

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•
特権 EXEC	•	•	—	—	•
ユーザ EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに準拠するように変更されました。

使用上のガイドライン

show curpriv コマンドは、現在の特権レベルを表示します。特権レベルの数値が小さいほど、特権レベルが低いことを示しています。

例

次に、enable_15 という名前のユーザが異なる特権レベルにある場合の **show curpriv** コマンドの出力例を示します。ユーザ名はログイン時にユーザが入力した名前を示し、P_PRIV はユーザが **enable** コマンドを入力したことを示し、P_CONF はユーザが **config terminal** コマンドを入力したことを示します。

```
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)#
```

次に、既知の動作を示します。次の例に示すように、イネーブル モードの場合は、ディセーブル モードを開始し、初期のログイン ユーザ名を enable_1 で置き換えます。

```
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
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド ステートメントを削除します。
show running-config privilege	コマンドの特権レベルを表示します。