show s - sz

show cluster zero-trust

To view the summary of zero trust statistics across nodes in a cluster, use the **show cluster zero-trust** command.

show cluster zero-trust statistics

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

None

Examples

The following is sample output for the zero trust statistics across nodes in a cluster. The summary section shows a cumulative sum of statistics across nodes in the cluster. The subsequent sections display the statistics in the respective nodes.

```
> show cluster zero-trust statistics
Usage Summary In Cluster:**********************************************
Active zero-trust sessions                    5
Active users                                  0*
Total zero-trust sessions                     5
Total users authorised                        0*
Total zero-trust sessions failed              0*
Total active applications                     2
Total SAML AuthN Requests                     5
Total SAML AuthN Responses                    5
Total SAML Auth Failures                      0*
SAML Assertions Passed                        5
SAML Assertions Failed                        0*
Total bytes in                                1000 Bytes
Total bytes out                               27570 Bytes
Pre-auth latency in millisec (min/max/avg)    7/11/9
Post-auth latency in millisec (min/max/avg)   6/9/7

unit-1-1(LOCAL):******************************************************
Active zero-trust sessions                    5
Active users                                  0*
Total zero-trust sessions                     5
Total users authorised                        0*
Total zero-trust sessions failed              0*
Total active applications                     2
Total SAML AuthN Requests                     5
Total SAML AuthN Responses                    5
Total SAML Auth Failures                      0*
SAML Assertions Passed                         5
SAML Assertions Failed                         0*
Total bytes in                                1000 Bytes
Total bytes out                               27570 Bytes
Pre-auth latency in millisec (min/max/avg)     7/11/9
Post-auth latency in millisec (min/max/avg)    6/9/7
```

Related Commands

Command	Description
show zero-trust	Displays the run-time zero trust statistics and session information
show running-config zero-trust	Displays the zero trust running configuration
clear zero-trust	Clears zero trust sessions and statistics
show counters protocol zero_trust	Displays the counters that are hit for zero trust flow

show counters protocol zero_trust

To view the counters that are hit for zero trust flow, use the **show counters protocol zero_trust** command.

show counters protocol zero_trust

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

None

Examples

The following is sample output of the counters that are hit during a zero trust flow.

```
> show counters protocol zero_trust
Protocol  Counter                          Value     Context
ZERO_TRUST MAX_USERS_LIMIT                   1        Summary
ZERO_TRUST MAX_SESSIONS_PER_USER_LIMIT       3        Summary
ZERO_TRUST LONG_URL_LIMIT                    4        Summary
ZERO_TRUST DUPLICATE_ASSERTION               2        Summary
ZERO_TRUST DUPLICATE_SESSION                 1        Summary
ZERO_TRUST COOKIE_DISABLED_BROWSER           3        Summary
ZERO_TRUST RELAY_STATE_FAILURE               1        Summary
ZERO_TRUST REDIRECTED_FOR_AUTHN              11       Summary
ZERO_TRUST TRAFFIC_ON_WRONG_INTERFACE        2        Summary
ZERO_TRUST NON_ZTNA_REQUEST                  6        Summary
ZERO_TRUST MISSING_URL_DATA                  3        Summary
ZERO_TRUST INVALID_GROUP_URL_PARAMS          3        Summary
ZERO_TRUST RANDOM_GEN_FAILURE                1        Summary
ZERO_TRUST INVALID_COOKIE                    3        Summary
ZERO_TRUST FORM_SUBMISSION_ERRORS            1        Summary
ZERO_TRUST HUGE_PAYLOAD                      1        Summary
```

Counter	Description
MAX_USERS_LIMIT	Number of times the maximum number of users per application limit was reached for a client IP
MAX_SESSIONS_PER_USER_LIMIT	Number of times the maximum number of sessions per user per application limit was reached
LONG_URL_LIMIT	Number of times the URL reached the maximum URL length limit
DUPLICATE_ASSERTION	Number of times duplicate assertion was received
DUPLICATE_SESSION	Number of times duplicate session was received
COOKIE_DISABLED_BROWSER	Number of times cookies were disabled by the browser

Counter	Description
RELAY_STATE_FAILURE	Number of times relay state verification failed
REDIRECTED_FOR_AUTHN	Number of times connections were redirected for authentication
TRAFFIC_ON_WRONG_INTERFACE	Number of times traffic was on the wrong interface
NON_ZTNA_REQUEST	Number of non-zero trust requests
MISSING_URL_DATA	Number of times required data was missing in the URL
INVALID_GROUP_URL_PARAMS	Number of times group URL parameters were invalid
RANDOM_GEN_FAILURE	Number of times random number generation failed
INVALID_COOKIE	Number of times invalid cookie was seen
FORM_SUBMISSION_ERRORS	Number of times form submission error was seen
HUGE_PAYLOAD	Number of times huge payload was seen

The following is a sample output of all HA specific counters prefixed with HA.

```
>show counters protocol zero_trust
Protocol       Counter              Value     Context
ZERO_TRUST HA_COOKIE_TX_SUCCESS      2         Summary
ZERO_TRUST HA_COOKIE_BULK_TX_SUCCESS 2         Summary
ZERO_TRUST HA_GRP_COOKIE_TX_SUCCESS  2         Summary
ZERO_TRUST HA_SALT_TX_SUCCESS        2         Summary
ZERO_TRUST HA_COOKIE_RX_SUCCESS      2         Summary
ZERO_TRUST HA_COOKIE_BULK_RX_SUCESS  2         Summary
ZERO_TRUST HA_GRP_COOKIE_RX_SUCCESS  2         Summary
ZERO_TRUST HA_SALT_RX_SUCCESS        2         Summary
```

Counter	Description
HA_COOKIE_TX_SUCCESS	Cookie messages were successfully sent from the active node
HA_COOKIE_TX_FAILURE	Cookie messages failed to be sent from the active node
HA_COOKIE_RX_SUCCESS	Cookie messages were successfully replicated on the standby node
HA_COOKIE_RX_FAILURE	Cookie messages failed to replicate on the standby node
HA_COOKIE_BULK_TX_SUCCESS	Cookie bulk sync messages were successfully sent from the active node
HA_COOKIE_BULK_TX_FAILURE	Cookie bulk sync messages failed to sent from the active node

Counter	Description
HA_COOKIE_BULK_RX_SUCCESS	Cookie bulk sync replication was successful on the standby node
HA_COOKIE_BULK_RX_FAILURE	Cookie bulk sync replication failed on the standby node
HA_GRP_COOKIE_TX_SUCCESS	Group cookie messages were successfully sent from the active node
HA_GRP_COOKIE_TX_FAILURE	Group cookie messages failed to be sent from the active node
HA_GRP_COOKIE_RX_SUCCESS	Group cookie messages were successfully replicated on the standby node
HA_GRP_COOKIE_RX_FAILURE	Group cookie messages failed to replicate on the standby node
HA_SALT_TX_SUCCESS	Salt messages were successfully sent from the active node
HA_SALT_TX_FAILURE	Salt messages failed to be sent from the active node
HA_SALT_RX_SUCCESS	Salt replication was successful on the standby node
HA_SALT_RX_FAILURE	Salt replication failed on the standby node

The following is a sample output of all cluster specific counters prefixed with CLUSTER.

```
> show counters protocol zero_trust
Protocol    Counter                      Value Context
ZERO_TRUST CLUSTER_COOKIE_TX_SUCCESS      2  Summary
ZERO_TRUST CLUSTER_COOKIE_TX_FAILURE      1  Summary
ZERO_TRUST CLUSTER_COOKIE_RX_SUCCESS      2  Summary
ZERO_TRUST CLUSTER_COOKIE_RX_FAILURE      3  Summary
ZERO_TRUST CLUSTER_COOKIE_BULK_TX_SUCCESS 2  Summary
ZERO_TRUST CLUSTER_COOKIE_BULK_TX_FAILURE 2  Summary
ZERO_TRUST CLUSTER_COOKIE_BULK_RX_SUCCESS 2  Summary
ZERO_TRUST CLUSTER_COOKIE_BULK_RX_FAILURE 2  Summary
ZERO_TRUST CLUSTER_GRP_COOKIE_TX_SUCCESS  3  Summary
ZERO_TRUST CLUSTER_GRP_COOKIE_TX_FAILURE  5  Summary
ZERO_TRUST CLUSTER_GRP_COOKIE_RX_SUCCESS  3  Summary
ZERO_TRUST CLUSTER_GRP_COOKIE_RX_FAILURE  3  Summary
ZERO_TRUST CLUSTER_SALT_TX_SUCCESS        4  Summary
ZERO_TRUST CLUSTER_SALT_TX_FAILURE        4  Summary
ZERO_TRUST CLUSTER_SALT_TX_SUCCESS        9  Summary
ZERO_TRUST CLUSTER_SALT_RX_FAILURE        4  Summary
```

Counter	Description
CLUSTER_COOKIE_TX_SUCCESS	Cookie messages were successfully sent from the control node
CLUSTER_COOKIE_TX_FAILURE	Cookie messages failed to be sent from the control node

Counter	Description
CLUSTER_COOKIE_RX_SUCCESS	Cookie messages were successfully replicated to the data nodes
CLUSTER_COOKIE_RX_FAILURE	Cookie messages failed to replicate on the data nodes
CLUSTER_COOKIE_BULK_TX_SUCCESS	Bulk sync messages were successfully sent from the control node
CLUSTER_COOKIE_BULK_TX_FAILURE	Bulk sync messages failed to be sent from the control node
CLUSTER_COOKIE_BULK_RX_SUCCESS	Successful bulk syncs on the data nodes
CLUSTER_COOKIE_BULK_RX_FAILURE	Bulk sync failed on the data nodes
CLUSTER_GRP_COOKIE_TX_SUCCESS	Group cookie messages were successfully sent from the control node
CLUSTER_GRP_COOKIE_TX_FAILURE	Group cookie messages failed to be sent from the control node
CLUSTER_GRP_COOKIE_RX_SUCCESS	Group cookie messages were successfully replicated on the data nodes
CLUSTER_GRP_COOKIE_RX_FAILURE	Group cookie messages failed to replicate on the data nodes
CLUSTER_SALT_TX_SUCCESS	Salt messages were successfully sent from the control node
CLUSTER_SALT_TX_FAILURE	Salt message failed to be sent from the control node
CLUSTER_SALT_RX_SUCCESS	Successful salt replications on the data nodes
CLUSTER_SALT_RX_FAILURE	Salt replication failed on the data nodes

Related Commands

Command	Description
show zero-trust	Displays the run-time zero trust statistics and session information
show cluster zero-trust	Displays cluster statistics
clear zero-trust	Clears zero trust sessions and statistics
show running-config zero-trust	Displays the zero trust running configuration

show running-config zero-trust

To view the zero trust running configuration, use the **show running-config zero-trust** command.

show running-config zero-trust [**application** | **application-group**]

Syntax Description

application	Displays application configuration information
application-group	Displays application group configuration information

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

None

Examples

The following is sample output for the global zero trust configuration.

```
> show running-config zero-trust
  base url https://acme.com
  port-range 20000-22000
  log enable
  enable
```

The following is a sample output for a standalone application configuration.

```
> show running-config zero-trust application
 application app1
  application-id 268434437
  application-interface Outside
  internal-url https://internal-bitbucket.acme.com
  external-url https://bitbucket.acme.com
  mapped-port 20000
  idp-entity-id http://www.okta.com/exk5tqpgl9VXLOeaQ5d7
  idp-sign-in
https://dv-10198439.okta.com/app/dev-10198439_bitbucketwebvpn_1/exk5tqpgl9VXLOeaQ5d7/sso/saml

  trustpoint idp bitbucket_okta
  trustpoint sp asa_saml_sp
  signature rsa-sha256
  sp-entity-id https://bitbucket.pcorp.com/saml/sp/metadata/bitbucket.pranavcorp.com
  sp-acs-url https://bitbucket.pcorp.com/+CSCOE+/saml/sp/acs0x3Ftgname=DefaultZeroTrustGroup

  authentication-timeout 1440
  log enable
  enable
```

The following is a sample output for an application group configuration.

```
> show running-config zero-trust application-group
application-group finance
 application-group-id 268434438
 idp-entity-id http://www.okta.com/exk4e25lkbtsEN07E5d7
 idp-sign-in
https://dv-10198439.okta.com/app/dev-10198439_sfcnzasapp1_1/exk4e25lkbtsEN07E5d7/sso/saml
 trustpoint idp finance_okta
 trustpoint sp asa_saml_sp
 signature rsa-sha256
 sp-entity-id https://acme.com/finance/saml/sp/metadata
 sp-acs-url https://acme.com/finance/+CSCOE+/saml/sp/acs0x3Ftgname=DefaultZeroTrustGroup
 authentication-timeout 1440
 enable
application app-fin1
 application-id 268434439
 application-interface Outside
 internal-url https://internal-workday.acme.com
 external-url https://workday.acme.com
 mapped-port 20001
 application-group-name finance
 authentication-timeout 1440
 enable
```

Related Commands

Command	Description
show zero-trust	Displays the run-time zero trust statistics and session information
show cluster zero-trust	Displays cluster statistics
clear zero-trust	Clears zero trust sessions and statistics
show counters protocol zero_trust	Displays the counters that are hit for zero trust flow

show sctp

To display current Stream Control Transmission Protocol (SCTP) cookies and associations, use the **show sctp** command.

show sctp [**detail**]

Syntax Description

detail	Displays detailed information about SCTP associations.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show sctp** command displays information about SCTP cookies and associations.

If you enable SCTP inspection using a FlexConfig from management center, this command can show the SCTP information.

Examples

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

```
> show sctp

AssocID: 2279da7a
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40174 (ESTABLISHED)

AssocID: 4924f520
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40200 (ESTABLISHED)
```

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

```
> show sctp detail

AssocID: 8b7e3ffb
Local:  192.168.100.56/3868 (ESTABLISHED)
    Receiver Window: 48000
    Cumulative TSN: 5cb6cd9b
    Next TSN: 5cb6cd9c
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
Remote: 192.168.200.78/3868 (ESTABLISHED)
    Receiver Window: 114688
    Cumulative TSN: 5cb6cd98
    Next TSN: 0
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
```

Related Commands

Command	Description
show local-host	Shows information on hosts making connections through the device, per interface.
show service-policy inspect sctp	Shows SCTP inspection statistics.
show traffic	Shows connection and inspection statistics per interface

show serial-number

To display the printed circuit board (PCB) serial number, use the **show serial-number** command. This command is not available on virtual devices.

show serial-number

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use the **show serial-number** command to view the printed circuit board's serial number. This information is also shown in **show version system** and **show running-config** output.

Use the **show inventory** command to view the chassis serial number

Examples

The following example shows how to display the serial number. The number in this example has been changed to be invalid.

```
> show serial-number
XXX175078X5
```

show service-policy

To display the service policy statistics, use the **show service-policy** command.

show service-policy [**global** | **interface** *intf*] [**cluster flow-mobility** | **inspect** *inspection* [*arguments*] | **police** | **priority** | **set connection** [**details**] | **sfr** | **shape** | **user-statistics**]
show service-policy [**global** | **interface** *intf*] [**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} [**eq** *src_port*] {**host** *dest_host* | *dest_ip dest_mask*} [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

Syntax Description

cluster flow-mobility	(Optional.) Shows status information on flow mobility in threat defense clusters.
dest_ip dest_mask	For the **flow** keyword, the destination IP address and netmask of the traffic flow.
details	(Optional) For the **set connection** keyword, displays per-client connection information, if a per-client connection limit is enabled.
eq *dest_port*	(Optional) For the **flow** keyword, equals the destination port for the flow.
eq *src_port*	(Optional) For the **flow** keyword, equals the source port for the flow.
flow *protocol*	(Optional) Shows policies that match a particular flow identified by the 5-tuple (protocol, source IP address, source port, destination IP address, destination port). You can use this command to check that your service policy configuration will provide the services you want for specific connections.
global	(Optional) Limits output to the global policy.
host *dest_host*	For the **flow** keyword, the host destination IP address of the traffic flow.
host *src_host*	For the **flow** keyword, the host source IP address of the traffic flow.
icmp_control_message	(Optional) For the **flow** keyword when you specify ICMP as the protocol, specifies an ICMP control message of the traffic flow.
icmp_number	(Optional) For the **flow** keyword when you specify ICMP as the protocol, specifies the ICMP protocol number of the traffic flow.
inspect *inspection* [*arguments*]	(Optional) Shows detailed information about policies that include an **inspect** command. Not all **inspect** commands are supported for detailed output. To see all inspections, use the **show service-policy inspect ?** command. The arguments available for each inspection vary; see the CLI help for more information.
interface *intf*	(Optional) Displays policies applied to the interface specified by the *intf* argument, where *intf* is the interface name.
police	(Optional) Shows detailed information about policies that include the **police** command.
priority	(Optional) Shows detailed information about policies that include the **priority** command.

set connection	(Optional) Shows detailed information about policies that include the **set connection** command.
sfr	(Optional) Shows detailed information about policies for ASA FirePOWER modules. This keyword is not meaningful for threat defense.
shape	(Optional) Shows detailed information about policies that include the **shape** command.
src_ip src_mask	For the **flow** keyword, the source IP address and netmask used in the traffic flow.
user-statistics	(Optional) Shows detailed information about policies that include the **user-statistics** command. This keyword is not meaningful for threat defense.

Command Default

If you do not specify any arguments, this command shows all global and interface policies.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The number of embryonic connections displayed in the **show service-policy** command output indicates the current number of embryonic connections to an interface for traffic matching that defined for a traffic class. The "embryonic-conn-max" field shows the maximum embryonic limit configured for the traffic class. If the current embryonic connections displayed equals or exceeds the maximum, TCP intercept is applied to new TCP connections that match the traffic.

When you make service policy changes to the configuration, all new connections use the new service policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. **show** command output will not include data about the old connections. To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy. See the **clear conn** or **clear local-host** commands.

You cannot directly configure service policies using management center or device manager. Some changes are made indirectly when you edit various connection settings or configure QoS policies. You can also adjust which default inspections are enabled using the **configure inspection** command. If you use FlexConfig in management center to configure service policies, this command shows statistics related to your configuration.

Note For an **inspect icmp** and **inspect icmp error** policies, the packet counts only include the echo request and reply packets.

Examples

The following is sample output for the **show service-policy** command.

```
> show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
```

```
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: esmtp _default_esmtp_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: skinny , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: xdmcp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: netbios, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ip-options UM_STATIC_IP_OPTIONS_MAP, packet 0, lock fail 0, drop 0,
reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
    Class-map: class-default
      Default Queueing      Set connection policy:         drop 0
      Set connection advanced-options: UM_STATIC_TCP_MAP
        Retransmission drops: 0                   TCP checksum drops : 0
        Exceeded MSS drops  : 0                   SYN with data drops: 0
        Invalid ACK drops   : 0                   SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0            OoO no buffer drops: 0
        OoO buffer timeout drops : 0              SEQ past window drops: 0
        Reserved bit cleared: 0                   Reserved bit drops : 0
        IP TTL modified     : 0                   Urgent flag cleared: 0
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0                Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

For devices that have multiple CPU cores, there is a counter for lock failure. The locking mechanism is used to protect shared data structures and variables, because they can be used by multiple cores.When the core fails to acquire a lock, it tries to get the lock again. The lock fail counter increments for each failed attempt.

```
> show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      ...
      Inspect: esmtp _default_esmtp_map, packet 96716502, lock fail 7, drop 25,
reset-drop 0
      Inspect: sqlnet, packet 2526511491, lock fail 21, drop 2362, reset-drop 0
```

The following command shows the statistics for GTP inspection. The output is explained in the table that follows the example.

```
> show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                  67     total_dropped             1
  signalling_msg_dropped            1     data_msg_dropped          0
  signalling_msg_forwarded         67     data_msg_forwarded        0
  total created_pdp                33     total deleted_pdp        32
  total created_pdpmcb             31     total deleted_pdpmcb     30
  total dup_sig_mcbinfo             0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo            0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                  1
```

Table 1: GPRS GTP Statistics

Column Heading	Description
version_not_support	Displays packets with an unsupported GTP version field.
msg_too_short	Displays packets less than 8 bytes in length.
unknown_msg	Displays unknown type messages.
unexpected_sig_msg	Displays unexpected signaling messages.
unexpected_data_msg	Displays unexpected data messages.
mandatory_ie_missing	Displays messages missing a mandatory Information Element (IE).
mandatory_ie_incorrect	Displays messages with an incorrectly formatted mandatory Information Element (IE).
optional_ie_incorrect	Displays messages with an invalid optional Information Element (IE).
ie_unknown	Displays messages with an unknown Information Element (IE).
ie_out_of_order	Displays messages with out-of-sequence Information Elements (IEs).
ie_unexpected	Displays messages with an unexpected Information Element (IE).
ie_duplicated	Displays messages with a duplicated Information Element (IE).
optional_ie_incorrect	Displays messages with an incorrectly formatted optional Information Element (IE).
total_dropped	Displays the total messages dropped.
signalling_msg_dropped	Displays the signaling messages dropped.
data_msg_dropped	Displays the data messages dropped.

Column Heading	Description
total_forwarded	Displays the total messages forwarded.
signalling_msg_forwarded	Displays the signaling messages forwarded.
data_msg_forwarded	Displays the data messages forwarded.
total created_pdp	Displays the total Packet Data Protocol (PDP) or bearer contexts created.
total deleted_pdp	Displays the total Packet Data Protocol (PDP) or bearer contexts deleted.
total created_pdpmcb total deleted_pdpmcb total dup_sig_mcbinfo total dup_data_mcbinfo no_new_sgw_sig_mcbinfo no_new_sgw_data_mcbinfo	These fields relate to the use of PDP master control blocks, which is an implementation feature. These counters are used by Cisco Technical Support for troubleshooting and are not of direct interest to end users.
pdp_non_existent	Displays the messages received for a non-existent PDP context.

The following command displays information about the PDP contexts:

```
> show service-policy inspect gtp pdp-context
4 in use, 5 most used
Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146
```

The following table describes the output from the **show service-policy inspect gtp pdp-context** command.

Table 2: PDP Contexts

Column Heading	Description
Version	Displays the version of GTP.
TID	Displays the tunnel identifier.
MS Addr	Displays the mobile station address.
SGSN Addr SGW Addr	Displays the serving gateway service node (SGSN) or serving gateway (SGW).
Idle	Displays the time for which the PDP or bearer context has not been in use.

Column Heading	Description
APN	Displays the access point name.

Related Commands

Command	Description
clear service-policy	Clears all service policy statistics.
configure inspection	Enables or disables the default inspections.
show running-config service-policy	Displays the service policies configured in the running configuration.

show shun

To display shun information, use the **show shun** command.

show shun [*src_ip* | **statistics**]

Syntax Description

src_ip	(Optional) Displays the information for that address.
statistics	(Optional) Displays the interface shun statistics.

Command History

Release	Modification
6.1	This command was introduced.

Examples

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

```
> show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

Related Commands

Command	Description
clear shun	Disables all the shuns that are currently enabled and clears the shun statistics.
shun	Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection.

show sip

To display SIP sessions, use the **show sip** command.

show sip

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show sip** command displays information for SIP sessions established across the threat defense device.

Examples

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

```
> show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 | state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 | state Active, idle 0:00:06
```

This sample shows two active SIP sessions on the threat defense device (as shown in the Total field). Each call-id represents a call.

The first session, with the call-id c3943000-960ca-2e43-228f@10.130.56.44, is in the state Call Init, which means the session is still in call setup. Call setup is complete only when the ACK is seen. This session has been idle for 1 second.

The second session is in the state Active, in which call setup is complete and the endpoints are exchanging media. This session has been idle for 6 seconds.

Related Commands

Commands	Description
show conn	Displays the connection state for different connection types.

show skinny

To displays information for SCCP (Skinny) sessions, use the **show skinny** command.

show skinny [**audio** | **video**]

Syntax Description

audio	Show SCCP audio sessions
video	Show SCCP video sessions

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show skinny** command under the following conditions. There are two active Skinny sessions set up across the device. The first one is established between an internal Cisco IP Phone at local address 10.0.0.11 and an external Cisco Unified Communications Manager at 172.18.1.33. TCP port 2000 is the Cisco Unified Communications Manager. The second one is established between another internal Cisco IP Phone at local address 10.0.0.22 and the same Cisco Unified Communications Manager.

```
> show skinny
MEDIA 10.0.0.22/20798         172.18.1.11/22948
LOCAL                   FOREIGN                 STATE
-----------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

The output indicates a call has been established between both internal Cisco IP Phones. The RTP listening ports of the first and second phones are UDP 22948 and 20798 respectively.

Related Commands

Commands	Description
show conn	Displays the connection state for different connection types.

show sla monitor

To display information on the Internet Protocol Service Level Agreement (IP SLA), use the **show sla monitor** command.

show sla monitor {**configuration** | **operational-state**} [*sla_id*]

Syntax Description

configuration	Displays the SLA configuration values, including the defaults.
operational-state	Displays the operational state of SLA operations.
sla_id	(Optional) The ID number of the SLA operation. Valid values are from 1 to 2147483647.

Command Default

If the SLA ID is not specified, the configuration values for all SLA operations are shown.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use the **show running-config sla monitor** command to see the SLA operation commands in the running configuration.

Examples

The following is sample output from the **show sla monitor configuration** command. It displays the configuration values for SLA operation 124. Following the output of the **show sla monitor configuration** command is the output of the **show running-config sla monitor** command for the same SLA operation.

```
> show sla monitor configuration 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

```
> show running-config sla monitor 124

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

The following is sample output from the **show sla monitor operational-state** command:

```
> show sla monitor operational-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

Related Commands

Command	Description
show running-config sla monitor	Displays the SLA operation configuration commands in the running configuration.

show snmp-server

To display information about the SNMP servers configured on the device, use the **show snmp-server** command.

show snmp-server {**engineID** | **group** | **host** | **statistics** | **user** [*username*]}

Syntax Description

engineID	Displays the identification of the SNMP engine.
group	Displays the names of configured SNMP groups, the security model being used, the status of different views, and the storage type of each group.
host	Displays the names of configured SNMP hosts that belong to a host group, the interface being used, and the version of SNMP being used.
statistics	Displays SNMP server statistics.
user [*username*]	Displays information about the characteristics of SNMP users. You can optionally specify a username to limit the information to that user.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

An SNMP engine is a copy of SNMP that can reside on a local device. The engine ID is a unique value that is assigned for each SNMP agent. The engine ID is not configurable. The engine ID is 25 bytes long, and is used to generate encrypted passwords. In a failover pair, the engine ID is synchronized with the peer.

SNMP users and groups are used according to the View-based Access Control Model (VACM) for SNMP. The SNMP group determines the security model to be used. The SNMP user should match the security model of the SNMP group. Each SNMP group name and security level pair must be unique.

Note The statistics show information on input and output packets to the SNMP module. The fact that packets are output does not mean they reached the destination. Route problems, intervening firewalls, unplugged interfaces, and so forth can prevent the transmission of an output packet. If packets are not reaching the SNMP server, check for other issues using commands such as **show asp drop** and **show logging**.

Examples

The following is sample output from the **show snmp-server engineid** command:

```
> show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

The following is sample output from the **show snmp-server group** command:

```
> show snmp-server group
groupname: public                              security model:v1
```

```
readview : <no readview specified>          writeview: <no writeview specified>
notifyview: <no readview specified>
row status: active

groupname: public                           security model:v2c
readview : <no readview specified>          writeview: <no writeview specified>
notifyview: *<no readview specified>
row status: active

groupname: privgroup                    security model:v3 priv
readview : def_read_view                writeview: <no writeview specified>
notifyview: def_notify_view
row status: active
```

The following is sample output from the **show snmp-server host** command, which shows only the active hosts polling the device:

```
> show snmp-server host
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
```

The following is sample output from the **show snmp-server user** command:

```
> show snmp-server user authuser
User name: authuser
Engine ID: 000000090200000000C025808
storage-type: nonvolatile       active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

The output provides the following information:

- The username, which is a string that identifies the name of the SNMP user.
- The engine ID, which is a string that identifies the copy of SNMP on the device.
- The storage-type, which indicates whether or not the settings have been set in volatile or temporary memory on the device, or in nonvolatile or persistent memory, in which settings remain after the device has been turned off and on again.
- The active access list, which is the standard IP access list associated with the SNMP user.
- The Rowstatus, which indicates whether or not it is active or inactive.
- The authentication protocol, which identifies which authentication protocol is being used. Options are MD5, SHA, or none. If authentication is not supported in your software image, this field does not appear.
- The privacy protocol, which indicates whether or not DES packet encryption is enabled. If privacy is not supported in your software image, this field does not appear.
- The group name, which indicates to which SNMP group the user belongs. SNMP groups are defined according to the View-based Access Control Model (VACM).

Related Commands

Command	Description
clear snmp-server statistics	Clears the SNMP packet input and output counters.
show running-config snmp-server	Displays the SNMP server configuration.

show snort counters

To display the statistics for the Snort preprocessor connections, use the **show snort counters** command.

show snort counters {**action** | **stream** | **sip** | **ssl** | **smtp** | **vrf**} {**all** | **instance** *x*}

Syntax Description

action	Shows instance level statistics of Snort for actions, limits, and verdicts.
stream	Shows statistics for the stream preprocessor.
sip	Shows statistics for the SIP preprocessor.
ssl	Shows statistics for the SSL preprocessor.
smtp	Shows statistics for the SMTP preprocessor.
vrf	Shows the number of live sessions going through each virtual router.
all	Shows statistics for all the Snort instances in the system. For example, **show snort counters action all**, **show snort counters smtp all**, and so on.
instance *x*	Shows statistics for the selected Snort instance in the system. For example, **show snort counters smtp instance 11**. Use the **show snort instances** command to determine the available instance numbers.

Command History

Release	Modification
6.3	This command was introduced.
6.6	The **vrf** keyword was added.

Usage Guidelines

Use this command to display statistics for Snort instances in your system. You can use these statistics for informational and debugging purposes. Consult Cisco TAC to help you debug your system with this command. Use the **show snort counters action all** command to view instance level statistics of Snort for actions, limits, and verdicts for all the Snort instances in your system. Use the **show snort instances** command to determine the available instance numbers.

The following example displays instance level statistics of Snort for actions, limits, and verdicts for all the Snort instances in your system.

```
> show snort counters action all
Instance : 1
------------

Action Stats are not available
 Total Action Processed:          0

...

================================================================================
```

```
Instance : 16
------------

Action Stats:
     Alerts:            0 (  0.000%)
     Logged:            0 (  0.000%)
     Passed:            0 (  0.000%)
Limits:
      Match:            0
      Queue:            0
        Log:            0
      Event:            0
      Alert:            0
Verdicts:
      Allow:       220009 (100.000%)
      Block:         5076 (  2.307%)
    Replace:            0 (  0.000%)
  Whitelist:            0 (  0.000%)
  Blacklist:            0 (  0.000%)
     Ignore:            0 (  0.000%)
      Retry:            0 (  0.000%)

================================================================================
```

The following example shows steam statistics.

```
> show snort counters stream all
Instance : 1
------------

Stream statistics not available
 Total sessions: 0
================================================================================

...

Instance : 16
------------

Stream statistics:
            Total sessions: 665
              TCP sessions: 665
              UDP sessions: 0
             ICMP sessions: 0
               IP sessions: 0
                TCP Prunes: 0
                UDP Prunes: 0
               ICMP Prunes: 0
                 IP Prunes: 0
TCP StreamTrackers Created: 0
TCP StreamTrackers Deleted: 0
              TCP Timeouts: 661
              TCP Overlaps: 0
       TCP Segments Queued: 0
     TCP Segments Released: 0
       TCP Rebuilt Packets: 0
         TCP Segments Used: 0
              TCP Discards: 0
                  TCP Gaps: 0
      UDP Sessions Created: 0
```

```
      UDP Sessions Deleted: 0
              UDP Timeouts: 0
              UDP Discards: 0
                    Events: 0
           Internal Events: 0
           TCP Port Filter
                  Filtered: 0
                Inspected: 0
                  Tracked: 910736
           UDP Port Filter
                  Filtered: 0
                Inspected: 0
                  Tracked: 0

===============================================================================
```

The following example shows SMTP statistics for Snort instance 1.

```
> show snort counters smtp instance 1
Instance : 1
------------

SMTP Preprocessor Statistics
  Total sessions                                  : 80
  Max concurrent sessions                         : 1
  Base64 attachments decoded                      : 0
  Total Base64 decoded bytes                      : 0
  Quoted-Printable attachments decoded            : 0
  Total Quoted decoded bytes                      : 0
  UU attachments decoded                          : 0
  Total UU decoded bytes                          : 0
  Non-Encoded MIME attachments extracted          : 0
  Total Non-Encoded MIME bytes extracted          : 0

===============================================================================
```

Related Commands

Command	Description
clear snort statistics	Clears Snort inspection statistics.
show snort statistics	Displays the number of packets that are matched for various Snort verdicts when traffic is inspected by Snort.
show snort tls-offload	Displays statistics related to packets encrypted and decrypted by the inspection engine (Snort) in the hardware.

show snort instances

To display a list of the Snort instance numbers, which you can use in other **show snort** commands, use the **show snort instances** command.

show snort instances

Command History

Release	Modification
6.3	This command was introduced.

Example

The following example displays the list of Snort instances.

```
> show snort instances
Total number of instances available - 2

+----------+---------+
| INSTANCE |   PID   |
+----------+---------+
|    1     |   2787  |
|    2     |   2788  |
+----------+---------+
```

show snort preprocessor-memory-usage

To display memory usage statics for Snort preprocessors per Snort instance, use the **show snort preprocessor-memory-usage** command.

show snort preprocessor-memory-usage *instance_ID* {**all** | **imap** | **pop** | **smtp**}

Syntax Description

instance_ID	The ID number of the Snort instance. Use the **show snort instances** command to obtain a list of the instance ID numbers that are active on your system.
all	Displays the statistics for all preprocessors.
imap	Displays the statistics for the IMAP preprocessor only.
pop	Displays the statistics for the POP preprocessor only.
smtp	Displays the statistics for the SMTP preprocessor only.

Command History

Release	Modification
6.3	This command was introduced.

Example

The following example displays statistics for the SMTP preprocessor for Snort instance 1. You are prompted for the admin password.

```
> show snort preprocessor-memory-usage 1 smtp

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

Password:

Snort Memory Usage for: Instance-1
----------------------------------


Memory Statistics of SMTP on: Fri Jul 12 09:13:02 2019

SMTP Session Statistics:
       Total Sessions seen: 0
   Max concurrent sessions: 0
   Current Active sessions: 0

   Memory Pool:
        Free Memory:
            SMTP Mime Pool:       17968000 bytes
                 SMTP Pool:              0 bytes
        Used Memory:
```

```
            SMTP Mime Pool:              0 bytes
                 SMTP Pool:              0 bytes
          ------------------       ---------------
          Total Memory:            17968000 bytes

   Heap Memory:
                       Session:              0 bytes
                 Configuration:          16784 bytes
                 --------------         ------------
                  Total Memory:          16784 bytes
                  No of allocs:             38 times
                   IP sessions:             30 times
-----------------------------------------------------
```

show snort statistics

To display the number of packets that are matched for various Snort verdicts when traffic is inspected by Snort, use the **show snort statistics** command.

show snort statistics

Command History

Release	Modification
6.0.1	This command was introduced.

Usage Guidelines

Use this command to show Snort inspection results of your access policy and intrusion rule configurations. This command is typically used when debugging unexpected Snort inspection behavior. The statistics include the following:

- Passed Packets—The number of packets sent to Snort from Lina.
- Blocked Packets—The number of packets blocked in Lina and not sent to Snort.
- Injected Packets—The number of packets Snort created and added to the traffic stream. For example, if you configure a block with reset action, Snort generates packets to reset the connection.
- Packets bypassed (Snort Down or Snort Busy)—If you configure the system to allow packets that require Snort inspection and Snort cannot perform the inspection, these counters are the number of packets that bypassed inspection when Snort was either down or too busy to handle the packets.

Caution When flows are bypassed (passed without inspection) these busy and down counters increment until the bypassed session ends, which can occur even when Snort is no longer busy or down. For example, counters could increment for days if a persistent TCP connection that lasts for days sends a packet while Snort is busy or down and then continues after Snort resumes.

- Fast-forwarded flows—The number of flows that were fast forwarded by policy, and thus not inspected.
- Blacklisted flows—The number of flows from policy configuration that were dropped by Snort.
- Start-of-flow events—The Lina process sends start-of-flow events to Snort when it fast paths a flow without sending it to Snort. These events help Snort keep track of the connections and report the connection events.
- End-of-flow events—The Lina process sends end-of-flow events to Snort when a fast path flow ends.
- Denied flow events—The Lina process sends denied flow events to Snort when it decides to drop a flow before sending it to Snort.
- Frames forwarded to Snort before drop—Valid for NGIPS interfaces only. This is the number of to-be-dropped packets forwarded to Snort. When the Lina process decides to drop the frame for some reason such as (Invalid TCP header length, Invalid UDP length or Invalid IP length), the frames are also sent to Snort for visibility.
- Inject packets dropped—The number of packets that Snort added to the traffic stream that were dropped.

Examples

The following sample transcript shows the information displayed by the **show snort statistics** command:

```
show snort statistics
Packet Counters:
  Passed Packets                                         6
  Blocked Packets                                        321
  Injected Packets                                       284
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   0
  Blacklisted Flows                                      0

Miscellaneous Counters:
  Start-of-Flow events                                   0
  End-of-Flow events                                     0
  Denied flow events                                     0
  Frames forwarded to Snort before drop                  0
  Inject packets dropped                                 0
```

In the following example, consider a case where the access control policy is configured to block and reset on all traffic. Lina cannot handle the reset, so it promotes the packets to Snort to block and inject the reset to both client and server.

- Passed packets—shows eight packets passed from Lina to Snort.
- Injected packets—shows the two packets sent to client and server.
- Blacklisted flows—shows the flows Snort has told Lina to block.

Note There are no *blocked* packets in this example.

```
> show snort statistics
Packet Counters:
  Passed Packets                                         8
  Blocked Packets                                        0
  Injected Packets                                       2
  Packets bypassed (Snort Down)                          0
  Packets bypassed (Snort Busy)                          0

Flow Counters:
  Fast-Forwarded Flows                                   0
  Blacklisted Flows                                      3

Miscellaneous Counters:
  Start-of-Flow events                                   0
  End-of-Flow events                                     0
  Denied flow events                                     0
  Frames forwarded to Snort before drop                  0
  Inject packets dropped                                 0
```

In the following example, consider a case where the access control policy has one rule that matches an FTP port and has a block action, and another rule that matches an HTTP application and has an allow action.

- Passed packets—shows 60 HTTP packets because Lina sends packets for allow rules to Snort.
- Denied flow events—shows two data and control channel packets that Lina handled with an FTP port match.

Note There are no *blocked* packets in this example.

```
> show snort statistics
Packet Counters:
  Passed Packets                                        60
  Blocked Packets                                       0
  Injected Packets                                      0
  Packets bypassed (Snort Down)                         0
  Packets bypassed (Snort Busy)                         0

Flow Counters:
  Fast-Forwarded Flows                                  0
  Blacklisted Flows                                     0

Miscellaneous Counters:
  Start-of-Flow events                                  0
  End-of-Flow events                                    0
  Denied flow events                                    2
  Frames forwarded to Snort before drop                 0
  Inject packets dropped                                0
```

Related Commands

Command	Description
clear snort statistics	Clears Snort inspection statistics.
configure snort preserve-connection	Determine whether to preserve existing TCP/UDP connections on routed and transparent interfaces in case the Snort process goes down.

show snort tls-offload

To display statistics related to packets encrypted and decrypted by the inspection engine (Snort) in hardware, use the **show snort tls-offload** command. This command is available only on the following managed devices, which support SSL hardware acceleration:

- Firepower 2100 with threat defense
- Firepower 4100/9300 with threat defense

  For information about TLS crypto acceleration support on Firepower 4100/9300 threat defense container instances, see the *FXOS Configuration Guide*.

TLS crypto acceleration is *not* supported on any virtual appliances or on any hardware except for the preceding.

show snort tls-offload [proxy | tracker | description]

Syntax Description

proxy	(Optional.) Shows statistics for the proxy only.
tracker	(Optional.) Shows statistics for the tracker only.
description	(Optional.) Shows descriptions of the counters for both the proxy and the tracker.

Command History

Release	Modification
6.2.3	This command was introduced.

Usage Guidelines

Use this command to display detailed statistics for Snort's proxy and tracker components. You can use these statistics for informational and debugging purposes. Use the **show snort tls-offload description** command to view a description of the counters. Consult Cisco TAC to help you debug your system with this command.

Following is an example **show snort tls-offload** command:

```
====== Tracker Statistics ======
TOTAL_CONNECTION                2774
TOTAL_RSA_KEY_EXCHANGE_4K       2774
TOTAL_CIPHER_SUITE_ENCR_AES     2774
TOTAL_CIPHER_SUITE_HASH_SHA1    2774
TOTAL_CKE_PMS_DECRYPTED         2774
TOTAL_RECORD_DECRYPTED          363001
TOTAL_RECORD_ENCRYPTED          363001
TOTAL_CONNECTION_W_DUR (<0.5s)  2771
AVG_CONNECTION_DURATION  (ms)   184
AVG_HANDSHAKE_TIME       (ms)   37
AVG_CKE_PMS_DECRYPT_TIME (us)   21402
AVG_RECORD_DECRYPT_TIME  (us)   619
AVG_RECORD_ENCRYPT_TIME  (us)   477
PEAK_CONNECTION_DURATION (ms)   400
PEAK_HANDSHAKE_TIME      (ms)   62
CONCURRENT_CONNECTION/Peak      3/3
CPS_ATTEMPTED/Peak              7/8
CPS_COMPLETED/Peak              8/8
CKE_PMS_DECRYPTING_Q/Peak       0/2
SKE_DH_PARAM_SIGNING_Q/Peak     0/0
```

```
RECORD_ENCRYPTING_Q/Peak         1/25
RECORD_DECRYPTING_Q/Peak         1/2
======= Proxy Statistics =======
TOTAL_CONNECTION(LW+FP)          15855
TOTAL_CONNECTION_FP              15853
CONNECTION_FP_RECV_FIN           31697
CONNECTION_FP_RECV_RST           27
CONNECTION_LW_RECV_FIN           2
CONCURRENT_CONNECTION_LW/Peak    0/2
CONCURRENT_CONNECTION_FP/Peak    3/7
BYPASS_NOT_ENOUGH_MEM            0
```

Related Commands

Command	Description
clear snort tls-offload	Clear statistics counters.
debug snort tls-offload	Displays error debug messages of all types for all Snort processes.

show software authenticity

To show software authenticity information, use the **show software authenticity** command.

show software authenticity {**development** | **file** *filename* | **keys** | **running**}

Syntax Description

development	Displays whether the loading of development key signed images is enabled or disabled.
file *filename*	Displays digital signature information related to software authentication for a specific image file.
keys	Displays information about development keys and release keys that are stored in SPI flash.
running	Displays digital signature information related to software authentication for the currently running image file.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The output for files and the running image provides the following information.

- The filename, which is the name of the filename in memory.
- The image type, which is the type of image being shown.
- The signer information specifies the signature information, which includes the following:
  - The common name, which is the name of the software manufacturer.
  - The organization unit, which indicates the hardware that the software image is deployed on.
  - The organization name, which is the owner of the software image.
- The certificate serial number, which is the certificate serial number for the digital signature.
- The hash algorithm, which indicates the type of hash algorithm used in digital signature verification.
- The signature algorithm, which identifies the type of signature algorithm used in digital signature verification.
- The key version, which indicates the key version used for verification.

Examples

The following is sample output from the **show software authenticity development** command:

```
> show software authenticity development
Loading of development images is disabled
```

The following is sample output from the **show software authenticity file** command. In this example, the file is a development image. You would see the same output for **show software authenticity running** about the image file that is currently running on the device.

```
> show software authenticity file os.img
File Name                     : disk0:/os.img
Image type                    : Development
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 57F4610F
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

The following is sample output from the show software authenticity keys command.

```
> show software authenticity keys
Public Key #1 Information
-------------------------
Key Type              : Release (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #2 Information
-------------------------
Key Type              : Development (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
```

```
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
Public Key #3 Information
-------------------------
Key Type              : Release (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #4 Information
-------------------------
Key Type              : Development (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
```

Related Commands

Command	Description
show version	Displays the software version, hardware configuration, license key, and related uptime data.

show ssd

To view the status of the SSDs, use the **show ssd** command.

Note This command is only supported on the Secure Firewall 3100.

show ssd

Command History

Release	Modification
7.1	This command was introduced.

Examples

The following sample display shows information about the SSDs:

```
> show ssd
Local Disk: 1
Name: nvme0n1
Size(MB): 858306
Operability:
operable
Presence:
equipped
Model: Micron_7300_MTFDHBE960TDF
Serial: MSA244302N0
Drive State: online
SED Support:
yes
SED State:
unlocked
SED Auth Status: ok
RAID action: none
```

Related Commands

Command	Description
configure raid	Adds or removes an SSD from the RAID.
show raid	Shows the RAID status.

show ssh-access-list

To show the SSH access list settings for the management interface, use the **show ssh-access-list** command.

show ssh-access-list

Command History

Release	Modification
6.0.1	This command was introduced.

Usage Guidelines

Use this command to show SSH access list settings for the management interface. The access list determines from which IP addresses users can attempt SSH connections to the management IP address. This list does not control SSH access to any data interface.

Examples

The following sample is default output from the **show ssh-access-list** command. This access list allows SSH connections to the management IP address from any IP address. Any user must supply a valid username/password to actually complete the SSH connection.

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:ssh
```

Related Commands

Command	Description
configure ssh-access-list	Configure the SSH access list for the management interface.

show ssl

To display information about the active SSL sessions and available ciphers, use the **show ssl** command.

show ssl [**cache** | **ciphers** [*level*] | **errors** [**trace**] | **mib** [**64**] | **objects**]

Syntax Description

cache	(Optional) Displays SSL session cache statistics.
ciphers	(Optional) Displays SSL ciphers available for use. Include the level keyword to view only those ciphers available for the given level, which indicates cipher strength. The following are the possible levels in increasing order of strength. • **all** • **low** • **medium** (This is the default if you do not specify a level) • **fips** • **high** (applies to TLSv1.2 only)
errors [**trace**]	(Optional) Displays SSL errors. Include the trace keyword to include trace information for each error.
mib [**64**]	(Optional) Displays SSL MIB statistics. Include the 64 keyword to see 64-bit counter statistics.
objects	(Optional) Displays SSL object statistics.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

This command shows information about the current SSLv3 or greater sessions, including the enabled cipher order, which ciphers are disabled, SSL trustpoints being used, and whether certificate authentication is enabled. These settings are for SSL connections on the data interfaces, not on the management interface.

Examples

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

```
> show ssl
Accept connections using SSLv3 or greater and negotiate to TLSv1 or greater
Start connections using TLSv1 and negotiate to TLSv1 or greater
SSL DH Group: group2 (1024-bit modulus)
SSL ECDH Group: group19 (256-bit EC)

SSL trust-points:
  Self-signed (RSA 2048 bits RSA-SHA256) certificate available
  Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
```

```
Certificate authentication is not enabled
```

The following is sample output from the **show ssl ciphers** command.

```
> show ssl ciphers
Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
dtlsv1 (medium):
```

```
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
>
```

show ssl-policy-config

To display information about the currently applied SSL policy configuration, including policy description, default logging settings, all enabled SSL rules and rule configurations, trusted CA certificates, and undecryptable traffic actions, use the **show ssl-policy-config** command.

show ssl-policy-config

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

You configure the SSL policy in management center and attach it to the access control policy assigned to a device. You can use this command to view information on the actions configured for SSL decryption on traffic that passes through the device.

Examples

The following example shows what appears if you have not configured an SSL policy for the device.

```
> show ssl-policy-config
SSL policy not yet applied.
```

The following example shows a configured SSL policy.

```
> show ssl-policy-config
===============[ General SSL Policy ]===============

=================[ Default Action ]=================
Default Action            : Do Not Decrypt

======[ Category: admin_category (Built-in) ]=======

=====[ Category: standard_category (Built-in) ]=====

----------[ Block unwanted applications ]-----------
State                     : Enabled
Action                    : Block
Source Zones              : outside_zone
Destination Zones         : dmz_zone
Applications              : HTTP/SSL Tunnel (3860)

=======[ Category: root_category (Built-in) ]=======

============[ Trusted CA Certificates ]=============

Cisco-Trusted-Authorities (group)
                              thawte-Primary-Root-CA
                              UTN-DATACorp-SGC
                              Chambers-of-Commerce-Root-2008
                              Izenpe.com-1
                              A-Trust-Qual-02
                              A-Trust-nQual-03
                              Common-Policy
```

```
                                Starfield-Root-Certificate-Authority-G2
                                GeoTrust-Primary-Certification-Authority
                                Certum-Trusted-Network-CA
                                UTN-USERFirst-Object

C_US-O_VeriSign-Inc.-OU_Class-3-Public-Primary-Certification-Authority-G2-OU_
c-1998-VeriSign-Inc.-For-authorized-use-only-OU_VeriSign-Trust-Network
                                CA-Disig-Root-R1
                                C_US-O_Equifax-OU_Equifax-Secure-Certificate-Authority
                                Thawte-Server-CA-1
                                VeriSign-Class-3-Public-Primary-Certification-Authority-G3
                                COMODO-Certification-Authority
                                VeriSign-Class-3-Public-Primary-Certification-Authority-G5
                                UTN-USERFirst-Client-Authentication-and-Email
                                TC-TrustCenter-Universal-CA-III
                                Cisco-Root-CA-2048
                                Staat-der-Nederlanden-Root-CA-G2

(...Remaining trusted CA certificates removed...)

=============[ Undecryptable Actions ]==============
Unsupported Cipher Suite  : Inherit Default Action
Unknown Cipher Suite      : Inherit Default Action
Compressed Session        : Inherit Default Action
Uncached Session ID       : Inherit Default Action
SSLv2 Session             : Inherit Default Action
Handshake Error           : Inherit Default Action
Decryption Error          : Block
```

Related Commands

Command	Description
show access-policy-config	Shows information about the currently configure access control policy.

show ssl-protocol

To show the SSL protocols currently configured for HTTPS access to the local device manager (device manager), use the **show ssl-protocol** command.

show ssl-protocol

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to view the SSL protocols configured for the management interface. These are the allowed protocols for HTTPS connections, which are used to open the local manager, device manager. These protocols are not used for remote managers.

Use the **configure ssl-protocol** command to configure these protocols.

Examples

The following example shows how to view the SSL protocols currently defined when using the local manager.

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
```

Related Commands

Command	Description
configure ssl-protocol	Configures the SSL protocols for HTTPS access to the management interface.

show startup-config

To show the startup configuration or to show any errors when the startup configuration loaded, use the **show startup-config** command.

show startup-config [**errors**]

Syntax Description

errors	(Optional) Shows any errors that were generated when the startup configuration loaded.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show startup-config** command displays the startup system configuration. You cannot directly configure these commands. Instead, they are configured by the manager controlling the device, for example, management center or device manager.

However, this is a partial configuration. It shows what can be configured using ASA Software configuration commands only, although some commands might be specific to threat defense. These commands are ported to threat defense. Thus, you should use the information in the startup configuration as a troubleshooting aid only. Use the device manager as the main means to analyze the device configuration.

Examples

The following is sample output from the **show startup-config** command:

```
> show startup-config
: Saved

:
: Serial Number: JAD192100RG
: Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
: Written by enable_1 at 20:39:10.749 UTC Tue Jun 28 2016
!
NGFW Version 6.1.0
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names

(...Output Truncated...)
```

Related Commands

Command	Description
show running-config	Shows the running configuration.

show summary

To display a summary of the most commonly used information (version, type, UUID, and so on) about the device, use the **show summary** command.

show summary

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Summary information includes basic **show version** output, plus a list of applied policies and Snort version information.

Examples

The following is an example of showing summary information.

```
> show summary
--------[ ftd1.example.com ]---------
Model                     : Cisco ASA5512-X Threat Defense (75) Version 6.1.0 (Build 2007)
UUID                      : 703006f4-8ff6-11e6-bb6e-8f2d5febf243
Rules update version      : 2016-03-28-001-vrt
VDB version               : 271
----------------------------------------------------

------------------[ policy info ]-------------------
Access Control Policy     : Initial AC Policy
Intrusion Policy          : Balanced Security and Connectivity

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

---------------[ snort version info ]---------------
Snort Version             : 2.9.10 GRE (Build 20)
libpcap Version           : 1.1.1
PCRE Version              : 7.6 2008-01-28
ZLIB Version              : 1.2.8
----------------------------------------------------
```

show sunrpc-server active

To display the pinholes open for Sun RPC services, such as NFS and NIS, use the **show sunrpc-server active** command.

show sunrpc-server active

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following is sample output from the **show sunrpc-server active** command:

```
> show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

The entry in the LOCAL column shows the IP address of the client or server on the inside interface, while the value in the FOREIGN column shows the IP address of the client or server on the outside interface.

Related Commands

Command	Description
clear sunrpc-server active	Clears the pinholes opened for Sun RPC services, such as NFS or NIS.
show running-config sunrpc-server	Displays information about the SunRPC services configuration.

show switch mac-address-table

To view the switch MAC address table, use the **show switch mac-address-table** command.

Note Supported for the Firepower 1010 only.

show switch mac-address-table

Command History

Release	Modification
6.5	This command was introduced.

Usage Guidelines

The switch MAC address table maintains the MAC address-to-switch port mapping for traffic within each VLAN in the switch hardware. The bridge MAC address table maintains the MAC address-to-VLAN interface mapping for traffic that passes between VLANs.

MAC address entries age out in 5 minutes.

Examples

The following is sample output from the **show switch mac-address-table** command.

```
> show switch mac-address-table
Legend: Age - entry expiration time in seconds
 Mac Address | VLAN | Type | Age | Port
-----------------------------------------------------
 000e.0c4e.2aa4 | 0001 | dynamic | 287 | Et1/1
 0012.d927.fb03 | 0001 | dynamic | 287 | Et1/1
 0013.c4ca.8a8c | 0001 | dynamic | 287 | Et1/1
 00b0.6486.0c14 | 0001 | dynamic | 287 | Et1/1
 00d0.2bff.449f | 0001 | static | - | In0/1
 0100.5e00.000d | 0001 | static multicast | - | In0/1,Et1/1-8
Total Entries: 6
```

The following table shows each field description:

Table 3: show switch mac-address-table Fields

Field	Description
Mac Address	Shows the MAC address.
VLAN	Shows the VLAN associated with the MAC address.
Type	Shows if the MAC address was learned dynamically, as a static multicast address, or statically. The only static entry is for the internal backplane interface.
Age	Shows the age of a dynamic entry in the MAC address table.
Port	Shows the switch port through which the host with the MAC address can be reached.

Related Commands

Command	Description
show switch vlan	Shows the VLAN and physical MAC address association.

show switch vlan

To view the VLANs and the associated switch ports, use the **show switch vlan** command.

Note Supported for the Firepower 1010 only.

show switch vlan

Command History

Release	Modification
6.5	This command was introduced.

Usage Guidelines

This command is for models with built-in switches only. For other models, use the **show vlan** command.

Examples

The following is sample output from the **show switch vlan** command.

```
> show switch vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                          up        Et1/1, Et1/2
200  outside                         up        Et1/8
300  -                               down      Et1/2, Et1/3
400  backup                          down      Et1/4
```

The following table shows each field description:

Table 4: show switch vlan Fields

Field	Description
VLAN	Shows the VLAN number.
Name	Shows the name of the VLAN interface. If no name is set, or if there is no VLAN interface, the display shows a dash (-).
Status	Shows the status, up or down, to receive and send traffic to and from the VLAN in the switch. At least one switch port in the VLAN needs to be in an up state for the VLAN state to be up.
Ports	Shows the switch ports assigned to each VLAN. If a switch port is listed for multiple VLANs, it is a trunk port. The above sample output shows Ethernet 1/2 is a trunk port that carries VLAN 100 and 300.

Related Commands

Command	Description
show switch mac-address-table	Shows the switch MAC address table.

show tcpstat

To display the status of the TCP stack and the TCP connections that are terminated on the device (for debugging), use the **show tcpstat** command.

show tcpstat

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show tcpstat** command allows you to display the status of the TCP stack and TCP connections that are terminated on the device. The TCP statistics displayed are described in the following table.

Table 5: TCP Statistics in the show tcpstat Command

Statistic	Description
tcb_cnt	Number of TCP users.
proxy_cnt	Number of TCP proxies. TCP proxies are used by user authorization.
tcp_xmt pkts	Number of packets that were transmitted by the TCP stack.
tcp_rcv good pkts	Number of good packets that were received by the TCP stack.
tcp_rcv drop pkts	Number of received packets that the TCP stack dropped.
tcp bad chksum	Number of received packets that had a bad checksum.
tcp user hash add	Number of TCP users that were added to the hash table.
tcp user hash add dup	Number of times a TCP user was already in the hash table when trying to add a new user.
tcp user srch hash hit	Number of times a TCP user was found in the hash table when searching.
tcp user srch hash miss	Number of times a TCP user was not found in the hash table when searching.
tcp user hash delete	Number of times that a TCP user was deleted from the hash table.
tcp user hash delete miss	Number of times that a TCP user was not found in the hash table when trying to delete the user.
lip	Local IP address of the TCP user.
fip	Foreign IP address of the TCP user.
lp	Local port of the TCP user.
fp	Foreign port of the TCP user.

Statistic	Description
st	State (see RFC 793) of the TCP user. The possible values are as follows: 1 CLOSED 2 LISTEN 3 SYN_SENT 4 SYN_RCVD 5 ESTABLISHED 6 FIN_WAIT_1 7 FIN_WAIT_2 8 CLOSE_WAIT 9 CLOSING 10 LAST_ACK 11 TIME_WAIT
rexqlen	Length of the retransmit queue of the TCP user.
inqlen	Length of the input queue of the TCP user.
tw_timer	Value of the time_wait timer (in milliseconds) of the TCP user.
to_timer	Value of the inactivity timeout timer (in milliseconds) of the TCP user.
cl_timer	Value of the close request timer (in milliseconds) of the TCP user.
per_timer	Value of the persist timer (in milliseconds) of the TCP user.
rt_timer	Value of the retransmit timer (in milliseconds) of the TCP user.
tries	Retransmit count of the TCP user.

Examples

This example shows how to display the status of the TCP stack.

```
> show tcpstat
                CURRENT MAX     TOTAL
tcb_cnt         2       12      320
proxy_cnt       0       0       160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 203.0.113.45 fip = 192.0.2.12 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
  rt_timer = 0 tries 0
```

Command	Description
show conn	Displays the connections used and those that are available.

show tech-support

To display the information that is used for diagnosis by technical support analysts, use the **show tech-support** command.

show tech-support

Command History

Release	Modification
6.1	This command was introduced.
7.1	The output from **show access-list element-count** and **show asp rule-engine** were added.

Usage Guidelines

The **show tech-support** command lets you list information that technical support analysts need to help you diagnose problems.

Examples

The following example shows how to display information that is used for technical support analysis. The output is shortened to show only its beginning. The output is extremely long and it will take a lot of time to page through the results.

```
> show tech-support

-------------[ ftd1.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (B
uild 226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(1)72

Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 3 days 16 hours

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB
Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
(...Remaining output truncated...)
```

show threat-detection memory

To show the memory used by advanced threat detection statistics, which are enabled by the **threat-detection statistics** command in the running configuration, use the **show threat-detection memory** command.

show threat-detection memory

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

Some statistics can use a lot of memory and can affect system performance. This command lets you monitor memory usage so you can adjust your configuration if necessary.

Use FlexConfig to configure the **threat-detection statistics** command.

Examples

The following is sample output from the **show threat-detection memory** command:

```
> show threat-detection memory
Cached chunks:
       CACHE TYPE             BYTES USED
TD Host                         70245888
TD Port                             2724
TD Protocol                         1476
TD ACE                               728
TD Shared counters                 14256
============================
Subtotal TD Chunks              70265072


Regular memory                BYTES USED
TD Port                             33824
TD Control block                   162064
============================
Subtotal Regular Memory            195888


Total TD memory:                70460960
```

Command	Description
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics port	Shows the port statistics.

Command	Description
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.

show threat-detection rate

When you enable basic threat detection using the **threat-detection basic-threat** command (using FlexConfig), you can view statistics using the **show threat-detection rate** command.

show threat-detection rate [**min-display-rate** *events_per_second*] [**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**]

Syntax Description

acl-drop	(Optional) Shows the rate for dropped packets caused by denial by access lists.
bad-packet-drop	(Optional) Shows the rate for dropped packets caused by denial by a bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length).
conn-limit-drop	(Optional) Shows the rate for dropped packets caused by the connection limits being exceeded (both system-wide resource limits, and limits set in the configuration).
dos-drop	(Optional) Shows the rate for dropped packets caused by a detected DoS attack (such as an invalid SPI, Stateful Firewall check failure).
fw-drop	(Optional) Shows the rate for dropped packets caused by basic firewall check failure. This option is a combined rate that includes all firewall-related packet drops in this command. It does not include non-firewall-related drops such as interface-drop, inspect-drop, and scanning-threat.
icmp-drop	(Optional) Shows the rate for dropped packets caused by denial by suspicious ICMP packets detected.
inspect-drop	(Optional) Shows the rate limit for dropped packets caused by packets failing application inspection.
interface-drop	(Optional) Shows the rate limit for dropped packets caused by an interface overload.
min-display-rate *events_per_second*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second, from 0 to 2147483647.
scanning-threat	(Optional) Shows the rate for dropped packets caused by a scanning attack detected. This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.
syn-attack	(Optional) Shows the rate for dropped packets caused by an incomplete session, such as TCP SYN attack or UDP session with no return data attack.

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger.
- The number of times the rates were exceeded.
- The total number of events over the fixed time periods.

The system computes the event counts 30 times over the average rate interval; in other words, the system checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 10 minutes, then the burst interval is 10 seconds. If the last burst interval was from 3:00:00 to 3:00:10, and you use the **show** command at 3:00:15, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the system calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the **show threat-detection rate** command:

```
> show threat-detection rate

                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0              0       0                   16
  1-hour ACL  drop:                0              0       0                  112
  1-hour SYN attck:                5              0       2                21438
  10-min  Scanning:                0              0      29                  193
  1-hour  Scanning:              106              0      10               384776
  1-hour Bad  pkts:               76              0       2               274690
  10-min  Firewall:                0              0       3                   22
  1-hour  Firewall:               76              0       2               274844
  10-min DoS attck:                0              0       0                    6
  1-hour DoS attck:                0              0       0                   42
  10-min Interface:                0              0       0                  204
  1-hour Interface:               88              0       0               318225
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection statistics	Shows statistics for threat detection.

show threat-detection scanning-threat

If you enable scanning threat detection with the **threat-detection scanning-threat** command (using FlexConfig), then view the hosts that are categorized as attackers and targets using the **show threat-detection scanning-threat** command.

show threat-detection scanning-threat [**attacker** | **target**]

Syntax Description

attacker	(Optional) Shows attacking host IP addresses.
target	(Optional) Shows targeted host IP addresses.

Command History

Release	Modification
6.3	This command was introduced.

Examples

The following is sample output from the **show threat-detection scanning-threat** command:

```
> show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l2l)
    192.168.1.249 (l2l)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
    192.168.10.0 (outside)
    192.168.10.2 (outside)
    192.168.10.3 (outside)
    192.168.10.4 (outside)
    192.168.10.5 (outside)
    192.168.10.6 (outside)
    192.168.10.7 (outside)
    192.168.10.8 (outside)
    192.168.10.9 (outside)
```

Related Commands

Command	Description
clear threat-detection scanning-threat	Clears the list of scanning threat attackers and targets.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection statistics	Shows statistics for threat detection.
shun	Blocks connections from specified hosts, such as scanning threat attackers.

show threat-detection shun

If you enable scanning threat detection with the **threat-detection scanning-threat** command (using FlexConfig), and you automatically shun attacking hosts, then view the currently shunned hosts using the **show threat-detection shun** command.

show threat-detection scanning-host

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

To release a host from being shunned, use the **clear threat-detection shun** command.

Examples

The following is sample output from the **show threat-detection shun** command:

```
> show threat-detection shun
Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

Related Commands

Command	Description
clear threat-detection shun	Clears the list of automatically shunned hosts.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
show threat-detection scanning-threat	Shows the scanning threat attackers and targets.
show threat-detection statistics	Shows statistics for threat detection.
shun	Blocks connections from specified hosts, such as scanning threat attackers.

show threat-detection statistics

If you enable threat statistics with the **threat-detection statistics** command (using FlexConfig), view the statistics using the **show threat-detection statistics** command. For clarity, the major keywords and options are shown separately in the following diagram.

show threat-detection statistics [**min-display-rate** *eps*] **host** [*ip_address* [*mask*]]

show threat-detection statistics [**min-display-rate** *eps*] **port** [*start_port*[*-end_port*]]

show threat-detection statistics [**min-display-rate** *eps*] **protocol** [*number* | *name*]

show threat-detection statistics [**min-display-rate** *eps*] **top** [**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**] | **tcp-intercept** [**all**] [**detail**] [**long**]]

Syntax Description

host [*ip_address* [*mask*]]	Shows host statistics. You can optionally specify an IP address to show statistics for a particular host. You can include the subnet mask for the host. Enable host statistics by configuring the **threat-detection statistics host** command using FlexConfig.
min-display-rate *eps*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second, between 0 and 2147483647.
port [*start_port*[*-end_port*]]	Shows TCP/UDP port statistics. You can optionally specify a single port or a range of ports, between 0 and 65535. Enable port statistics by configuring the **threat-detection statistics port** command using FlexConfig.
protocol [*number* | *name*]	Shows protocol statistics. You can optionally specify the protocol by number or name. The number can be 0 - 255. The name can be one of the following: ah, eigrp, esp, gre, icmp, igmp, igrp, ip ipinip, ipsec, nos, ospf, pcp, pim, pptp, snp, tcp, udp. Enable protocol statistics by configuring the **threat-detection statistics protocol** command using FlexConfig.

top [**access-list** | **host** | **port-protocol**] [**rate-1** | **rate-2** | **rate-3**]	Shows the top 10 access rules, hosts, and ports/protocols, depending on options for which you enabled statistics. You can narrow the view using the following keywords: • **access-list** shows the top 10 ACEs that that match packets, including both permit and deny ACEs. If you enable basic threat detection using the **threat-detection basic-threat** command, you can track access list denies using the **show threat-detection rate access-list** command. • **host** shows the top 10 host statistics for each fixed time period. Due to the threat detection algorithm, an interface used for a failover link or state link could appear as one of the top 10 hosts. This occurrence is more likely when you use one interface for both the failover and state link. This is expected behavior, and you can ignore this IP address in the display. • **port-protocol** shows the top 10 combined statistics of TCP/UDP port and IP protocol types. TCP (protocol 6) and UDP (protocol 17) are not included in the display for IP protocols. • **rate-1**, **rate-2**, **rate-3** shows the statistics for the specified fixed rate period only, with 1 being the smallest, 3 the largest intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then rate 1 is 1 hour, rate 2 is 8 hours, and rate 3 is 24 hours.
top tcp-intercept [**all**] [**detail**] [**long**]	Shows TCP Intercept statistics. The display includes the top 10 protected servers under attack. You can include the following keywords: • **all** shows the history data of all the traced servers. • **detail** shows history sampling data. • **long** shows the statistical history in a long format, with the real and the translated IP addresses of the server.

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

Threat detection statistics show both allowed and dropped traffic rates.

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger.
- The number of times the rates were exceeded (for dropped traffic statistics only).
- The total number of events over the fixed time periods.

The system computes the event counts 30 times over the average rate interval; in other words, the system checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20

minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the system calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

The following table explains the output for all commands with the exception of TCP Intercept views. See the TCP Intercept example for an explanation of that output.

Field	Description
Top Name, ID	For Top reports, the column shows the name or number of the access control entry, the IP address of the host, or the name/ID number of the port or protocol. Entries are grouped by the fixed rate intervals and they are ranked within the time period, from [0] (highest count) to [9] (lowest count). You might not have enough statistics for all 10 positions, so fewer than 10 items might be shown for a given interval. For host and port-protocol, the groupings are by sent and received bytes and packets per fixed interval.
Average(eps)	Shows the average rate in events/sec over each time period. The system stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the show command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the system calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.

Field	Description
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the system calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Entry heading	The statistics are grouped by fixed interval under a heading. The heading can include the information explained in the following rows. In general, the entry heading starts with the following: • Host, with the host IP address. • The port number/name. For example, 80/HTTP. • The protocol number or name. For example, ICMP. • For top reports, the fixed interval and statistics type. For access-list, the heading indicates this is for ACL hits.
tot-ses	Shows the total number of sessions for this host, port, or protocol since it was added to the database.
act-ses	Shows the total number of active sessions that the host, port, or protocol is currently involved in.
fw-drop (Host only.)	Shows the number of firewall drops. Firewall drops is a combined rate that includes all firewall-related packet drops tracked in basic threat detection, including access list denials, bad packets, exceeded connection limits, DoS attack packets, suspicious ICMP packets, TCP SYN attack packets, and UDP session with no return data attack packets. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.
insp-drop (Host only.)	Shows the number of packets dropped because they failed application inspection.
null-ses (Host only.)	Shows the number of null sessions, which are TCP SYN sessions that did not complete within the 30-second timeout, and UDP sessions that did not have any data sent by its server 3 seconds after the session starts.
bad-acc (Host only.)	Shows the number of bad access attempts to host ports that are in a closed state. When a port is determined to be in a null session (see above), the port state of the host is set to HOST_PORT_CLOSE. Any client accessing the port of the host is immediately classified as a bad access without the need to wait for a timeout.

Field	Description
20-min, 1-hour, 8-hour, and 24-hour	Shows statistics for these fixed rate intervals. • Sent byte, sent pkts—Shows the number of successful bytes or packets sent from the host, port, or protocol. • Sent drop—Shows the number of packets sent from the host, port, or protocol that were dropped because they were part of a scanning attack. • Recv byte, pkts—Shows the number of successful bytes or packets received by the host, port, or protocol. • Recv drop—Shows the number of packets received by the host, port, or protocol that were dropped because they were part of a scanning attack.

Examples

The following is sample output from the **show threat-detection statistics host** command:

```
> show threat-detection statistics host

                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:               2938               0       0             10580308
  8-hour Sent byte:                367               0       0             10580308
 24-hour Sent byte:                122               0       0             10580308
  1-hour Sent pkts:                 28               0       0               104043
  8-hour Sent pkts:                  3               0       0               104043
 24-hour Sent pkts:                  1               0       0               104043
  20-min Sent drop:                  9               0       1                10851
  1-hour Sent drop:                  3               0       1                10851
  1-hour Recv byte:               2697               0       0              9712670
  8-hour Recv byte:                337               0       0              9712670
 24-hour Recv byte:                112               0       0              9712670
  1-hour Recv pkts:                 29               0       0               104846
  8-hour Recv pkts:                  3               0       0               104846
 24-hour Recv pkts:                  1               0       0               104846
  20-min Recv drop:                 42               0       3                50567
  1-hour Recv drop:                 14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                  614
  8-hour Sent byte:                  0               0       0                  614
 24-hour Sent byte:                  0               0       0                  614
  1-hour Sent pkts:                  0               0       0                    6
  8-hour Sent pkts:                  0               0       0                    6
 24-hour Sent pkts:                  0               0       0                    6
  20-min Sent drop:                  0               0       0                    4
  1-hour Sent drop:                  0               0       0                    4
  1-hour Recv byte:                  0               0       0                  706
  8-hour Recv byte:                  0               0       0                  706
 24-hour Recv byte:                  0               0       0                  706
  1-hour Recv pkts:                  0               0       0                    7
```

The following is sample output from the **show threat-detection statistics port** command:

```
> show threat-detection statistics port
```

```
                          Average(eps)    Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:               2939              0       0             10580922
  8-hour Sent byte:                367          22043       0             10580922
 24-hour Sent byte:                122           7347       0             10580922
  1-hour Sent pkts:                 28              0       0               104049
  8-hour Sent pkts:                  3            216       0               104049
 24-hour Sent pkts:                  1             72       0               104049
  20-min Sent drop:                  9              0       2                10855
  1-hour Sent drop:                  3              0       2                10855
  1-hour Recv byte:               2698              0       0              9713376
  8-hour Recv byte:                337          20236       0              9713376
 24-hour Recv byte:                112           6745       0              9713376
  1-hour Recv pkts:                 29              0       0               104853
  8-hour Recv pkts:                  3            218       0               104853
 24-hour Recv pkts:                  1             72       0               104853
  20-min Recv drop:                 24              0       2                29134
  1-hour Recv drop:                  8              0       2                29134
```

The following is sample output from the **show threat-detection statistics protocol** command:

```
> show threat-detection statistics protocol

                          Average(eps)    Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                 0              0       0                 1000
  8-hour Sent byte:                 0              2       0                 1000
 24-hour Sent byte:                 0              0       0                 1000
  1-hour Sent pkts:                 0              0       0                   10
  8-hour Sent pkts:                 0              0       0                   10
 24-hour Sent pkts:                 0              0       0                   10
```

The following is sample output from the **show threat-detection statistics top access-list** command:

```
> show threat-detection statistics top access-list

                   Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]             173              0       0               623488
              200/2[1]              43              0       0               156786
              100/1[2]              43              0       0               156786
  8-hour ACL hits:
              100/3[0]              21           1298       0               623488
              200/2[1]               5            326       0               156786
              100/1[2]               5            326       0               156786
```

The following is sample output from the **show threat-detection statistics top port-protocol** command:

```
> show threat-detection statistics top port-protocol

Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv byte:
 1         gopher   70              71              0       0          32345678
 2  btp-clnt/dhcp   68              68              0       0          27345678
 3         gopher   69              65              0       0          24345678
 4    Protocol-96 * 96              63              0       0          22345678
 5      Port-7314 7314              62              0       0          12845678
 6 BitTorrent/trc 6969              61              0       0          12645678
 7     Port-8191-65535              55              0       0          12345678
 8           SMTP  366              34              0       0           3345678
```

```
 9          IPinIP *  4              30               0       0           2345678
10           EIGRP * 88              23               0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...

Note: Id preceded by * denotes the Id is an IP protocol type
```

The following is sample output from the **show threat-detection statistics top host** command:

```
> show threat-detection statistics top host

                   Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour Sent byte:
          10.0.0.1[0]            2938               0       0             10580308
  1-hour Sent pkts:
          10.0.0.1[0]              28               0       0               104043
  20-min Sent drop:
          10.0.0.1[0]               9               0       1                10851
  1-hour Recv byte:
          10.0.0.1[0]            2697               0       0              9712670
  1-hour Recv pkts:
          10.0.0.1[0]              29               0       0               104846
  20-min Recv drop:
          10.0.0.1[0]              42               0       3                50567
  8-hour Sent byte:
          10.0.0.1[0]             367               0       0             10580308
  8-hour Sent pkts:
          10.0.0.1[0]               3               0       0               104043
  1-hour Sent drop:
          10.0.0.1[0]               3               0       1                10851
  8-hour Recv byte:
          10.0.0.1[0]             337               0       0              9712670
  8-hour Recv pkts:
          10.0.0.1[0]               3               0       0               104846
  1-hour Recv drop:
          10.0.0.1[0]              14               0       1                50567
 24-hour Sent byte:
          10.0.0.1[0]             122               0       0             10580308
 24-hour Sent pkts:
          10.0.0.1[0]               1               0       0               104043
 24-hour Recv byte:
          10.0.0.1[0]             112               0       0              9712670
 24-hour Recv pkts:
          10.0.0.1[0]               1               0       0               104846
```

The following is sample output from the **show threat-detection statistics top tcp-intercept** command:

```
> show threat-detection statistics top tcp-intercept

Top 10 protected servers under attack (sorted by average rate)
```

```
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

The following table explains the TCP Intercept output.

Field	Description
Monitoring window size	Shows the period of time over which the system samples data for statistics. The default is 30 minutes. You can change this setting using the **threat-detection statistics tcp-intercept rate-interval** command using FlexConfig. The system samples data 30 times during this interval.
Sampling interval	Shows the interval between samples. This value is always the rate interval divided by 30.
Rank	Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.
Server IP:Port	Shows the server IP address and the port on which it is being attacked.
Interface	Shows the interface through which the server is being attacked.
Ave Rate	Shows the average rate of attack, in attacks per second over the sampling period.
Cur Rate	Shows the current attack rate, in attacks per second.
Total	Shows the total number of attacks.
Source IP	Shows the attacker IP address.
Last Attack Time	Shows when the last attack occurred.

The following is sample output from the **show threat-detection statistics top tcp-intercept long** command with the real server IP address in parentheses:

```
> show threat-detection statistics top tcp-intercept long

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port (Real IP:Real Port)> <Interface> <Ave Rate> <Cur Rate> <Total> <Source
 IP (Last Attack Time)>
--------------------------------------------------------------------------------
1    10.1.0.2:6025 (209.165.200.227:6025) inside 18 709 33911 10.0.0.201 (0 secs ago)
2    10.1.0.2:6026 (209.165.200.227:6026) inside 18 709 33911 10.0.0.201 (0 secs ago)
3    10.1.0.2:6027 (209.165.200.227:6027) inside 18 709 33911 10.0.0.201 (0 secs ago)
4    10.1.0.2:6028 (209.165.200.227:6028) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

```
5    10.1.0.2:6029 (209.165.200.227:6029) inside 18 709 33911 10.0.0.201 (0 secs ago)
6    10.1.0.2:6030 (209.165.200.227:6030) inside 18 709 33911 10.0.0.201 (0 secs ago)
7    10.1.0.2:6031 (209.165.200.227:6031) inside 18 709 33911 10.0.0.201 (0 secs ago)
8    10.1.0.2:6032 (209.165.200.227:6032) inside 18 709 33911 10.0.0.201 (0 secs ago)
9    10.1.0.2:6033 (209.165.200.227:6033) inside 18 709 33911 10.0.0.201 (0 secs ago)
10   10.1.0.2:6034 (209.165.200.227:6034) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

The following is sample output from the **show threat-detection statistics top tcp-intercept detail** command, which shows the sampling data. The sampling data is the number of attacks for each of the 30 sampling periods.

```
> show threat-detection statistics top tcp-intercept detail

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
     Sampling History (30 Samplings):
             95348      95337      95341      95339      95338      95342
             95337      95348      95342      95338      95339      95340
             95339      95337      95342      95348      95338      95342
             95337      95339      95340      95339      95347      95343
             95337      95338      95342      95338      95337      95342
             95348      95338      95342      95338      95337      95343
             95337      95349      95341      95338      95337      95342
             95338      95339      95338      95350      95339      95570
             96351      96351      96119      95337      95349      95341
             95338      95337      95342      95338      95338      95342
......
```

Related Commands

Command	Description
clear threat-detection statistics	Clears threat detection statistics.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.

show time

To display UTC and local time and date for the device, use the **show time** command.

show time

Command History

Release	Modification
6.0.1	This command was introduced.

Examples

The following is sample output from the **show time** command.

```
> show time
UTC -       Wed Aug  3 17:04:06 UTC 2016
Localtime - Wed Aug 03 13:04:06 EDT 2016
```

show time-range

To display the configuration of all time range objects, use the **show time-range** command.

Note This command does not display the device time. To view the device time, use `show time`.

show time-range timezone [*name*]

Syntax Description

name	(Optional) Shows information for this time range object only.
timezone	To view the configured timezone for the time-range policies, use timezone.

Command History

Release	Modification
6.3	This command was introduced.
6.6	The timezone keyword was added.

Examples

This example shows how to display the configuration of the time range objects. In this example, there is one object, which is named work-hours. Inactive means that the object is not being used.

```
> show time-range

time-range entry: work-hours (inactive)
   periodic weekdays 9:00 to 17:00
```

The following is sample output from the **show time-range timezone** command:

```
> show time-range timezone
Time-range Clock:
----------------------------
13:20:22.852 tzname Tue Aug 18 2020
```

show tls-proxy

To display TLS proxy and session information for encrypted inspections, use the **show tls-proxy** command.

show tls-proxy [*tls_name* | **session** [**host** *host_address* | **detail** [**cert-dump**] | **count** | **statistics**]]

Syntax Description

count	Shows only the session counters.
detail [**cert-dump**]	Shows detailed TLS proxy information including the cipher for each SSL leg and the LDC. Add the **cert-dump** keyword to get a hexadecimal dump of the local dynamic certificate (LDC). You can also use these keywords with the **host** option.
host *host_address*	Specifies the IPv4 or IPv6 address of a particular host to show the associated sessions associated.
session	Shows active TLS proxy sessions.
statistics	Shows statistics for monitoring and managing TLS sessions.
tls_name	The name of the TLS proxy to show.

Command History

Release	Modification
6.3	This command was introduced.

Usage Guidelines

The TLS proxies you can view with this command are those configured for encrypted application inspections only. They apply to the SIP, SCCP (Skinny), or Diameter inspections. These TLS proxies are not related to the SSL Decryption or VPN policies.

Examples

The following is sample output from the **show tls-proxy** command:

```
> show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
      Server proxy:
             Trust-point: local_ccm
      Client proxy:
             Local dynamic certificate issuer: ldc_signer
             Local dynamic certificate key-pair: phone_common
             Cipher-suite <unconfigured>
      Run-time proxies:
             Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
                   Active sess 1, most sess 4, byte 3244
```

The following is sample output from the **show tls-proxy session** command:

```
> show tls-proxy session
```

```
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
S:0x482e790 byte 3388
```

The following is sample output from the **show tls-proxy session detail** command:

```
> show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte
1831704
      Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1

      Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
      Status: Available
      Certificate Serial Number: 29
      Certificate Usage: General Purpose
      Public Key Type: RSA (1024 bits)
      Issuer Name:
             cn=TLS-Proxy-Signer
      Subject Name:
             cn=SEP0002B9EB0AAD
             o=Cisco Systems Inc
             c=US
      Validity Date:
            start date: 00:47:12 PDT Feb 27 2007
            end   date: 00:47:12 PDT Feb 27 2008
      Associated Trustpoints:
```

The following is sample output from the **show tls-proxy session statistics** command:

```
> show tls-proxy session stastics
TLS Proxy Sessions (Established: 600)
    Mobility:                                          0
Per-Session Licensed TLS Proxy Sessions
(Established: 222, License Limit: 3000)
    SIP:                                               2
    SCCP:                                             20
    DIAMETER:                                        200
Total TLS Proxy Sessions
    Established:                                     822
    Platform Limit:                                 1000
```

show track

To display information about object tracked by the security-level agreement (SLA) tracking process, use the **show track** command.

show track [*track-id*]

Syntax Description

track-id	A tracking entry object ID number, from 1 to 500.

Command History

Release	Modification
6.3	This command was introduced.

Examples

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

```
> show track

Track 5
      Response Time Reporter 124 reachability
      Reachability is UP
      2 changes, last change 03:41:16
      Latest operation return code: OK
      Tracked by:
                  STATIC-IP-ROUTING 0
```

show traffic

To display interface transmit and receive activity, use the **show traffic** command.

show traffic

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show traffic** command lists the number of packets and bytes moving through each interface since the last **show traffic** command was entered or since the device came online. The number of seconds is the duration the device has been online since the last reboot, unless the **clear traffic** command was entered since the last reboot. If this is the case, then the number of seconds is the duration since that command was entered.

The statistics are first shown based on interface name. After the named interfaces, statistics are shown based on the physical interface. The interfaces can include hidden virtual interfaces that are used by the system for internal communications.

Examples

The following is an abbreviated sample output from the **show traffic** command, showing the statistics for a single interface. Each interface shows the same statistics.

```
> show traffic
...
diagnostic:
        received (in 102.080 secs):
                2048 packets     204295 bytes
                20 pkts/sec      2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets       204056 bytes
                20 pkts/sec      1998 bytes/sec
      1 minute input rate 122880 pkts/sec,  5775360 bytes/sec
      1 minute output rate 122887 pkts/sec,  5775389 bytes/sec
      1 minute drop rate, 3 pkts/sec
      5 minute input rate 118347 pkts/sec,  5562309 bytes/sec
      5 minute output rate 119221 pkts/sec,  5603387 bytes/sec
      5 minute drop rate, 11 pkts/sec
...
```

Related Commands

Command	Description
clear traffic	Resets the counters for transmit and receive activity.

show upgrade

To show information about a system software upgrade, use the **show upgrade** command.

show upgrade { **revert-info** | **status** [**detail**] [**continuous**] }

Syntax Description

revert-info	Show which version you can revert the system to use, if any version is available for reversion. If no revert version is available, you cannot use the **upgrade revert** command.
status	Show the status of the upgrade. You can include the following optional keywords: • **detail** Show the upgrade log in addition to the summary status information. • **continuous** Show upgrade messages as they are generated. You can use this keyword alone or in conjunction with the detail keyword.

Command History

Release	Modification
6.7	This command was introduced.

Usage Guidelines

Possible statuses include the following:

- There is no upgrade in progress.
- Major upgrade in progress.
- Patch upgrade in progress.
- Hotfix upgrade in progress.
- Major upgrade failed. Run “cancel” to recover.

  Reboot might or might not happen depending on the upgrade failure stage.
- Major upgrade failed. Reboot the device to recover.

Examples

The following example shows the status of an upgrade that is currently in progress. To see the status of a completed upgrade, use the **show last-upgrade status** command.

```
> show upgrade status
Upgrade from 6.3.0 to 6.7.0 in progress (11% progress, time remaining 8 mins)
Time started: Tue Dec  3 23:50:31 UTC 2020
Current state: Tue Dec  3 23:51:01 UTC 2020 Running script 200_pre/001_check_reg.pl...
```

The following example shows revert information. In this example, a version does exist that you can revert to. If no version is available, the message is "No version is available for revert."

```
> show upgrade revert-info
You can revert to version 6.4.0-102
at 2020-03-20T22:49:43+0000

It uses 4946MB of disk space.

Version 6.4.0-102 is available for revert.
```

Related Commands

Command	Description
show last-upgrade status	Shows information on the last system software upgrade.
upgrade	Cancel, revert, or retry a system software upgrade.

show user

To show the user accounts for accessing the command line interface (CLI) on the device, use the **show user** command.

show user [*username1* [*usernam2*] [...]]

Syntax Description

username1 [*usernam2*] [...]	(Optional.) One or more space-separated user names. If you do not specify any names, all users are shown.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The following information is shown for each user. Create user accounts with the **configure user add** command.

- Login—The login name.
- UID—The numeric user ID.
- Auth—How the user is authenticated, either Local or Remote (through a directory server).
- Access—The user's privilege level, Basic or Config. Use the **configure user access** command to change this setting.
- Enabled—Whether the user is active, Enabled or Disabled. Use the **configure user enable**/**disable** commands to change this setting.
- Reset—Whether the user must change the account password at the next login, Yes or No. Use the **configure user forcereset** command to change this setting.
- Exp—The number of days until the user's password must be changed. Never indicates that the password does not expire. Use the **configure user aging** command to change this setting.
- Warn—The number of days a user is given a warning to change their password before it expires. N/A indicates that warnings are not applicable. Use the **configure user aging** command to change this setting.
- Grace—The grace period, which is the number of days a user can change the password after it expires. Disabled means there is no grace period. Grace periods apply to devices running FXOS only. Use the **configure user aging** command to change this setting.
- Str—Whether the user's password must meet strength checking criteria, Dis (disabled) or Ena (enabled). Configure this option with the **configure user strengthcheck** command.
- Lock—Whether the user's account has been locked due to too many login failures, Yes or No. Use the **configure user unlock** command to unlock a user account.
- Max—The maximum number of failed logins before the user's account is locked. N/A indicates the account can never be locked. Use the configure user maxfailedlogins command to change this setting.

Examples

The following example shows how to display the users defined for CLI access.

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
admin2            1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

The following example includes as external user and the grace period.

```
> show user
Login          UID   Auth Access  Enabled Reset   Exp   Warn    Grace  MinL Str Lock Max
admin          100  Local Config  Enabled    No  10000     7  Disabled    8 Ena   No N/A
extuser        501 Remote Config Disabled   N/A  99999     7  Disabled    1 Dis   No N/A
joeuser       1000  Local Config  Enabled   Yes    180     7         7    8 Dis   No   5
```

Related Commands

Command	Description
configure user add	Add a user account for CLI access.

show version

To display the hardware model, software version, UUID, intrusion rule update version, and VDB version, use the **show version** command.

show version [**detail** | **system**]

Syntax Description

detail	**show version** and **show version detail** display the same information.
system	This keyword appends additional system information to the information displayed by **show version**.

Command History

Release	Modification
6.1	This command was introduced.
7.1	Information on how long it took to start (boot) up the system was added to the output.

Usage Guidelines

The **show version** command and the **show version detail** command display the same basic system information. The **show version system** command displays this information plus additional system information such as operating time since the last reboot and more specific hardware information.

Examples

The following example shows the basic **show version** output.

```
> show version
-------------------[ firepower ]--------------------
Model : Secure Firewall Management Center for VMware (66) Version 7.2.0 (Build 1405)
UUID : 78ddf634-3754-11ec-87dd-ace5f9ec4cdc
Rules update version : 2022-01-11-001-vrt
LSP version : lsp-rel-20220111-1030
VDB version : 348
----------------------------------------------------
```

The following sample output from the **show version system** command appends the same output as the **show version** command with additional information.

```
> show version system
-------------[ example-sfr.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build 226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(1)72

Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"
```

```
firepower up 36 days 21 hours

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
                             Number of accelerators: 1

 1: Ext: GigabitEthernet1/1  : address is e865.49b8.97f2, irq 255
 2: Ext: GigabitEthernet1/2  : address is e865.49b8.97f3, irq 255
 3: Ext: GigabitEthernet1/3  : address is e865.49b8.97f4, irq 255
 4: Ext: GigabitEthernet1/4  : address is e865.49b8.97f5, irq 255
 5: Ext: GigabitEthernet1/5  : address is e865.49b8.97f6, irq 255
 6: Ext: GigabitEthernet1/6  : address is e865.49b8.97f7, irq 255
 7: Ext: GigabitEthernet1/7  : address is e865.49b8.97f8, irq 255
 8: Ext: GigabitEthernet1/8  : address is e865.49b8.97f9, irq 255
 9: Int: Internal-Data1/1    : address is e865.49b8.97f1, irq 255
10: Int: Internal-Data1/2    : address is 0000.0001.0002, irq 0
11: Int: Internal-Control1/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Data1/3    : address is 0000.0001.0003, irq 0
13: Ext: Management1/1       : address is e865.49b8.97f1, irq 0
14: Int: Internal-Data1/4    : address is 0000.0100.0001, irq 0

Serial Number: JAD192100RG
Configuration register is 0x1
Image type              : Release
Key Version             : A
Configuration last modified by enable_1 at 12:44:37.849 UTC Mon Jul 25 2016
```

Starting with version 7.1, you can see how long it took to boot up the system. The information is after status of how long the system has been running.

```
> show version system
--------------------[ ftdv1 ]----------------------
Model                     : Cisco Firepower Threat Defense for VMware (75) Version 7.1.0
(Build 1519)
UUID                      : b964ed5e-92c0-11eb-aaa2-cfab359c2436
LSP version               : lsp-rel-20210310-2255
VDB version               : 338
----------------------------------------------------

Cisco Adaptive Security Appliance Software Version 99.17(1)135
SSP Operating System Version 82.11(1.277i)

Compiled on Thu 25-Mar-21 00:49 GMT by builders
System image file is "boot:/asa99171-135-smp-k8.bin"
Config file at boot was "startup-config"

ftdv1 up 6 days 22 hours
Start-up time 5 secs

(remaining output redacted)
```

show vlan

To display all VLANs configured on the threat defense device, use the **show vlan** command.

show vlan [**mapping** [*primary_id*]]

Syntax Description

mapping	(Optional) Shows the secondary VLANs mapped to the primary VLAN.
primary_id	(Optional) Shows secondary VLANs for a specific primary VLAN.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example displays the configured VLANs:

```
> show vlan
10-11,30,40,300
```

The following example displays the secondary VLANs that are mapped to each primary VLAN:

```
> show vlan mapping
Interface                       Secondary VLAN ID                       Mapped VLAN ID
0/1.100                         200                                               300
0/1.100                         201                                               300
0/2.500                         400                                               200
```

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
show interface	Displays the runtime status and statistics of interfaces.

show vm

To display virtual platform information on the threat defense virtual device, use the **show vm** command.

show vm

Command History

Release	Modification
6.1	This command was introduced.

Example

The following example shows how to display information on VMware:

```
> show vm

Virtual Platform Resource Status
--------------------------------
Number of vCPUs           :  4
Processor Memory          :  8192 MB
Hypervisor                :  VMware
```

show vpdn

To show the status of virtual private dial-up network (VPDN) connections such as PPPoE or L2TP, use the **show vpdn** command.

show vpdn {**group** *name* | **pppinterface id** *number* | **session** {**l2tp** | **pppoe**} **id** *number* {**packets** | **state** | **window**} | **tunnel** {**l2tp** | **pppoe**} **id** *number* {**packets** | **state** | **summary** | **transport**} | **username** *name*}

Syntax Description

group *name*	Shows the VPDN group configuration.
id *number*	(Optional) Shows information about the VPDN session with the specified ID.
l2tp	(Optional) Shows session or tunnel information about L2TP.
packets	Shows session or tunnel packet information.
pppinterface	Shows PPP interface information.
pppoe	(Optional) Show session or tunnel information about PPPoE.
session	Shows session information.
state	Shows session or tunnel state information.
summary	Shows the tunnel summary.
transport	Shows tunnel transport information.
tunnel	Shows tunnel information.
username *name*	Shows user information.
window	Shows session window information.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Use this command to troubleshoot the VPDN PPPoE or L2TP connections.

Examples

The following is sample output from the **show vpdn session** command:

```
> show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
```

```
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
```

The following is sample output from the **show vpdn tunnel** command:

```
> show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
```

show vpn load-balancing

Do not use this command. It relates to a feature not supported by threat defense.

show vpn-sessiondb

To display information about VPN sessions, use one of the **show vpn-sessiondb** commands.

show vpn-sessiondb [**detail**] [**full**] {**anyconnect** | **l2l** | **ra-ikev1-ipsec** | **ra-ikev2-ipsec**} [**filter** *criteria*] [**sort** *criteria*]
show vpn-sessiondb [**detail**] [**full**] **index** *indexnumber*
show vpn-sessiondb failover
show vpn-sessiondb ospfv3 [**filter ipaddress** *IP_address*] [**sort ipaddress**]

Syntax Description

anyconnect	Displays AnyConnect VPN client sessions.
detail	(Optional) Displays extended details about a session. For example, using the detail option for an IPsec session displays additional details such as the IKE hashing algorithm, authentication mode, and rekey interval. If you choose detail, and the full option, the threat defense device displays the detailed output in a machine-readable format.
failover	Displays the session information for the failover IPsec tunnels.
filter *filter_criteria*	(Optional) Filters the output to according to the filter option you specify. For a list of options, see the "Usage Guidelines" section.
full	(Optional) Displays streamed, untruncated output. Output is delineated by | characters and a || string between records.
index *indexnumber*	Displays a single session by index number. Specify the index number for the session, which ranges from 1 - 65535.
l2l	Displays VPN LAN-to-LAN session information.
ospfv3	Displays OSPFv3 session information.
ra-ikev1-ipsec	Displays IPsec IKEv1 sessions.
ra-ikev2-ipsec	Displays details for IKEv2 remote access client connections.
sort *sort_criteria*	(Optional) Sorts the output according to the sort option you specify. For a list of options, see the "Usage Guidelines" section.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

You can use the following options to filter and to sort the session display. The values you can filter and sort on differ based on the session types you are listing.

Filter/Sort Option	Description
filter a-ipaddress *IP_address*	Filters the output to display information for the specified assigned IP address or addresses only. Use with: **anyconnect**, **ra-ikev2-ipsec**
sort a-ipaddress	Sorts the display by assigned IP addresses. Use with: **anyconnect**, **ra-ikev2-ipsec**
filter a-ipversion {**v4** | **v6**}	Filters the output to show only sessions assigned IPv4 or IPv6 addresses. Use with: **anyconnect**, **ra-ikev2-ipsec**
filter encryption *encryption_algorithm*	Filters the output to display information for sessions using the specified encryption algorithm only. Use ? to see the available methods. Use with: **anyconnect**, **l2l**, **ra-ikev2-ipsec**
sort encryption	Sorts the output by the encryption algorithm used in the session. Use with: **anyconnect**, **l2l**, **ra-ikev2-ipsec**
filter inactive	Filters by inactive sessions, which are sessions that have gone idle and have possibly lost connectivity (due to hibernation, mobile device disconnection, and so on). The number of inactive sessions increases when TCP keepalives are sent from the threat defense device without a response from the AnyConnect client. Each session is time stamped with the SSL tunnel drop time. If the session is actively passing traffic over the SSL tunnel, 00:00m:00s is displayed. Use with: **anyconnect** **Note** The threat defense device does not send TCP keepalives to some devices (such as the iPhone, iPad, and iPod) to save battery life, so the failure detection cannot distinguish between a disconnect and a sleep. For this reason, the inactivity counter remains as 00:00:00 by design.
sort inactivity	Sorts by inactive sessions. Use with: **anyconnect**
filter ipaddress *IP_address*	Filters the output to display information for the specified inside IP address or addresses only. Use with: **l2l**, **ospfv3**
sort ipaddress	Sorts the display by inside IP addresses. Use with: **l2l**, **ospfv3**
filter ipversion {**v4** | **v6**}	Filters the output to show only sessions originating from endpoints with IPv4 or IPv6 addresses. Use with: **l2l**

Filter/Sort Option	Description
filter name *username*	Filters the output to display sessions for the specified username. Use with: **anyconnect**, **l2l**,**ra-ikev2-ipsec**
sort name	Sorts the display by usernames in alphabetical order. Use with: **anyconnect**, **l2l**,**ra-ikev2-ipsec**
filter p-ipaddress *IP_address*	Filters the output to display information for the specified public outside IP address or addresses only. Use with: **anyconnect**, **ra-ikev2-ipsec**
sort p-ipaddress	Sorts the display by public outside IP addresses. Use with: **anyconnect**, **ra-ikev2-ipsec**
filter p-ipversion {**v4** | **v6**}	Filters the output to show only sessions originating from endpoints with public IPv4 or IPv6 addresses. Use with: **anyconnect**, **ra-ikev2-ipsec**
filter protocol *name*	Filters the output to display information for sessions using the specified protocol only. Use ? to see the available protocols. Use with: **anyconnect**, **l2l**, **ra-ikev2-ipsec**
sort protocol	Sorts the display by protocol. Use with: **anyconnect**, **l2l**, **ra-ikev2-ipsec**

The following table explains the fields you might see in the output.

Field	Description
Auth Mode	Protocol or mode used to authenticate this session.
Bytes Rx	Total number of bytes received from the remote peer or client by the system.
Bytes Tx	Number of bytes transmitted to the remote peer or client by the system.
Client Type	Client software running on the remote peer, if available.
Client Ver	Version of the client software running on the remote peer.
Connection	Name of the connection or the private IP address.
D/H Group	Diffie-Hellman Group. The algorithm and key size used to generate IPsec SA encryption keys.
Duration	Elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
EAPoUDP Session Age	Number of seconds since the last successful posture validation.

Field	Description
Encapsulation	Mode used to apply IPsec ESP (Encapsulation Security Payload protocol) encryption and authentication (that is, the part of the original IP packet that has ESP applied).
Encryption	Data encryption algorithm this session is using, if any.
EoU Age (T)	EAPoUDP Session Age. Number of seconds since the last successful posture validation.
Filter Name	Username specified to restrict the display of session information.
Hashing	Algorithm used to create a hash of the packet, which is used for IPsec data authentication.
Hold Left (T)	Hold-Off Time Remaining. 0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.
Hold-Off Time Remaining	0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.
IKE Neg Mode	IKE (IPsec Phase 1) mode for exchanging key information and setting up SAs: Aggressive or Main.
IKE Sessions	Number of IKE (IPsec Phase 1) sessions; usually 1. These sessions establish the tunnel for IPsec traffic.
Index	Unique identifier for this record.
IP Addr	Private IP address assigned to the remote client for this session. This is also known as the “inner” or “virtual” IP address. It lets the client appear to be a host on the private network.
IPsec Sessions	Number of IPsec (Phase 2) sessions, which are data traffic sessions through the tunnel. Each IPsec remote-access session can have two IPsec sessions: one consisting of the tunnel endpoints, and one consisting of the private networks reachable through the tunnel.
License Information	Shows information about the shared SSL VPN license.
Local IP Addr	IP address assigned to the local endpoint of the tunnel (that is the interface on the system).
Login Time	Date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.

Field	Description
NAC Result	State of Network Admission Control Posture Validation. It can be one of the following: • Accepted—The ACS successfully validated the posture of the remote host. • Rejected—The ACS could not successfully validate the posture of the remote host. • Exempted—The remote host is exempt from posture validation according to the Posture Validation Exception list configured on the threat defense device. • Non-Responsive—The remote host did not respond to the EAPoUDP Hello message. • Hold-off—The threat defense device lost EAPoUDP communication with the remote host after successful posture validation. • N/A—NAC is disabled for the remote host according to the VPN NAC group policy. • Unknown—Posture validation is in progress.
NAC Sessions	Number of Network Admission Control (EAPoUDP) sessions.
Packets Rx	Number of packets received from the remote peer by the system.
Packets Tx	Number of packets transmitted to the remote peer by the system.
PFS Group	Perfect Forward Secrecy group number.
Posture Token	Informational text string configurable on the Access Control Server. The ACS downloads the posture token to the system for informational purposes to aid in system monitoring, reporting, debugging, and logging. A typical posture token is Healthy, Checkup, Quarantine, Infected, or Unknown.
Protocol	Protocol the session is using.
Public IP	Publicly routable IP address assigned to the client.
Redirect URL	Following posture validation or clientless authentication, the ACS downloads the access policy for the session to the system. The Redirect URL is an optional part of the access policy payload. The system redirects all HTTP (port 80) and HTTPS (port 443) requests for the remote host to the Redirect URL if it is present. If the access policy does not contain a Redirect URL, the threat defense device does not redirect HTTP and HTTPS requests from the remote host. Redirect URLs remain in force until either the IPsec session ends or until posture revalidation, for which the ACS downloads a new access policy that can contain a different redirect URL or no redirect URL.
Rekey Int (T or D)	Lifetime of the IPsec (IKE) SA encryption keys. The T value is the lifetime in duration, the D value is in data transmitted. Only the T value is shown for remote access VPN.

Field	Description
Rekey Left (T or D)	Lifetime remaining of the IPsec (IKE) SA encryption keys. The T value is the lifetime in duration, the D value is in data transmitted. Only the T value is shown for remote access VPN.
Rekey Time Interval	Lifetime of the IPsec (IKE) SA encryption keys.
Remote IP Addr	IP address assigned to the remote endpoint of the tunnel (that is the interface on the remote peer).
Reval Int (T)	Revalidation Time Interval. Interval in seconds required between each successful posture validation.
Reval Left (T)	Time Until Next Revalidation. 0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
Revalidation Time Interval	Interval in seconds required between each successful posture validation.
Session ID	Identifier for the session component (subsession). Each SA has its own identifier.
Session Type	Type of session: LAN-to-LAN or Remote
SQ Int (T)	Status Query Time Interval. Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the system to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
Status Query Time Interval	Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the system to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
Time Until Next Revalidation	0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
Tunnel Group	Name of the tunnel group referenced by this tunnel for attribute values.
UDP Dst Port or UDP Destination Port	Port number used by the remote peer for UDP.
UDP Src Port or UDP Source Port	Port number used for UDP.
Username	User login name with which the session is established.

Field	Description
VLAN	Egress VLAN interface assigned to this session. The system forwards all traffic to that VLAN. One of the following elements specifies the value: Group policy or Inherited group policy

Examples

The following is sample output from the **show vpn-sessiondb** command:

```
> show vpn-sessiondb
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ------------------------------------------------
AnyConnect Client           :      1 :         12 :           3 :        0
  SSL/TLS/DTLS              :      1 :         12 :           3 :        0
Clientless VPN              :      0 :          6 :           2
  Browser                   :      0 :          6 :           2
--------------------------------------------------------------------------------
Total Active and Inactive   :      1             Total Cumulative :     18
Device Total VPN Capacity   :    250
Device Load                 :     0%
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ------------------------------------------------
Clientless                  :      0 :          7 :               2
AnyConnect-Parent           :      1 :         11 :               3
SSL-Tunnel                  :      1 :         12 :               3
DTLS-Tunnel                 :      1 :         12 :               3
--------------------------------------------------------------------------------
Totals                      :      3 :         42
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
IPv6 Usage Summary
--------------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
-------------------------------------------
AnyConnect SSL/TLS/DTLS : : :
IPv6 Peer : 1 : 41 : 2
Tunneled IPv6 : 1 : 70 : 2
AnyConnect IKEv2 : : :
IPv6 Peer : 0 : 4 : 1
Clientless : : :
IPv6 Peer : 0 : 1 : 1
--------------------------------------------------------------------------------
```

The following is sample output from the **show vpn-sessiondb detail** command:

```
> show vpn-sessiondb detail
--------------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
```

```
                            ---------------------------------------------
AnyConnect Client           :      1 :         12 :           3 :        0
  SSL/TLS/DTLS              :      1 :         12 :           3 :        0
Clientless VPN              :      0 :          6 :           2
  Browser                   :      0 :          6 :           2
-------------------------------------------------------------------------
Total Active and Inactive   :      1            Total Cumulative :     18
Device Total VPN Capacity   :    250
Device Load                 :     0%
-------------------------------------------------------------------------

-------------------------------------------------------------------------
Tunnels Summary
-------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ---------------------------------------------
Clientless                  :      0 :          7 :               2
AnyConnect-Parent           :      1 :         11 :               3
SSL-Tunnel                  :      1 :         12 :               3
DTLS-Tunnel                 :      1 :         12 :               3
-------------------------------------------------------------------------
Totals                      :      3 :         42
-------------------------------------------------------------------------
```

The following is sample output from the **show vpn-sessiondb detail l2l** command:

```
> show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed

Connection : 172.16.0.0
Index : 1
IP Addr : 172.16.0.0
Protocol : IKEv2 IPsec
Encryption : IKEv2: (1)AES256 IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 240 Bytes Rx : 160
Login Time : 14:50:35 UTC Tue May 1 2017
Duration : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
Tunnel ID : 1.1
UDP Src Port : 500 UDP Dst Port : 500
Rem Auth Mode: preSharedKeys
Loc Auth Mode: preSharedKeys
Encryption : AES256 Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86389 Seconds
PRF : SHA1 D/H Group : 5
Filter Name :
IPv6 Filter :

IPsec:
Tunnel ID : 1.2
Local Addr : 10.0.0.0/255.255.255.0
Remote Addr : 209.165.201.30/255.255.255.0
Encryption : AES256 Hashing : SHA1
Encapsulation: Tunnel PFS Group : 5
Rekey Int (T): 120 Seconds Rekey Left(T): 107 Seconds
Rekey Int (D): 4608000 K-Bytes Rekey Left(D): 4608000 K-Bytes
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Bytes Tx : 240 Bytes Rx : 160
Pkts Tx : 3 Pkts Rx : 2
```

```
NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 13 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

The following is sample output from the **show vpn-sessiondb detail index 1** command:

```
> show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username : user1
Index : 1
Assigned IP : 192.168.2.70 Public IP : 10.86.5.114
Protocol : IPsec Encryption : AES128
Hashing : SHA1
Bytes Tx : 0 Bytes Rx : 604533
Client Type : WinNT Client Ver : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time : 15:22:46 EDT Tue May 10 2005
Duration : 7h:02m:03s
Filter Name :
NAC Result : Accepted
Posture Token: Healthy
VM Result : Static
VLAN : 10

IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1

IKE:
Session ID : 1
UDP Src Port : 500 UDP Dst Port : 500
IKE Neg Mode : Aggressive Auth Mode : preSharedKeysXauth
Encryption : 3DES Hashing : MD5
Rekey Int (T): 86400 Seconds Rekey Left(T): 61078 Seconds
D/H Group : 2

IPsec:
Session ID : 2
Local Addr : 0.0.0.0
Remote Addr : 192.168.2.70
Encryption : AES128 Hashing : SHA1
Encapsulation: Tunnel
Rekey Int (T): 28800 Seconds Rekey Left(T): 26531 Seconds
Bytes Tx : 0 Bytes Rx : 604533
Pkts Tx : 0 Pkts Rx : 8126

NAC:
Reval Int (T): 3000 Seconds Reval Left(T): 286 Seconds
SQ Int (T) : 600 Seconds EoU Age (T) : 2714 Seconds
Hold Left (T): 0 Seconds Posture Token: Healthy
Redirect URL : www.cisco.com
```

The following is sample output from the **show vpn-sessiondb ospfv3** command:

```
> show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec
```

```
Connection :
Index : 1 IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none Hashing : IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:13m:11s
```

The following is sample output from the **show vpn-sessiondb detail ospfv3** command:

```
> show vpn-sessiondb detail ospfv3

Session Type: OSPFv3 IPsec Detailed

Connection :
Index : 1 IP Addr : 0.0.0.0
Protocol : IPsec
Encryption : IPsec: (1)none Hashing : IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 0
Login Time : 15:06:41 EST Wed Feb 1 2017
Duration : 1d 5h:14m:28s
IPsec Tunnels: 1

IPsec:
Tunnel ID : 1.1
Local Addr : ::/0/89/0
Remote Addr : ::/0/89/0
Encryption : none Hashing : SHA1
Encapsulation: Transport
Idle Time Out: 0 Minutes Idle TO Left : 0 Minutes
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 105268 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

The following is sample output from the **show vpn-sessiondb detail anyconnect** command:

```
> show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : userab Index : 2
Assigned IP : 65.2.1.100 Public IP : 75.2.1.60
Assigned IPv6: 2001:1000::10
Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent
License : AnyConnect Premium
Encryption : IKEv2: (1)3DES IPsecOverNatT: (1)3DES AnyConnect-Parent: (1)none
Hashing : IKEv2: (1)SHA1 IPsecOverNatT: (1)SHA1 AnyConnect-Parent: (1)none
Bytes Tx : 0 Bytes Rx : 21248
Pkts Tx : 0 Pkts Rx : 238
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy Tunnel Group : test1
Login Time : 22:44:59 EST Tue Aug 13 2017
Duration : 0h:02m:42s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

```
IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 2.1
Public IP : 75.2.1.60
Encryption : none Hashing : none
Auth Mode : userPassword
Idle Time Out: 400 Minutes Idle TO Left : 397 Minutes
Conn Time Out: 500 Minutes Conn TO Left : 497 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver : 3.1.05050

IKEv2:
Tunnel ID : 2.2
UDP Src Port : 64251 UDP Dst Port : 4500
Rem Auth Mode: userPassword
Loc Auth Mode: rsaCertificate
Encryption : 3DES Hashing : SHA1
Rekey Int (T): 86400 Seconds Rekey Left(T): 86241 Seconds
PRF : SHA1 D/H Group : 2
Filter Name : mixed1
Client OS : Windows

IPsecOverNatT:
Tunnel ID : 2.3
Local Addr : 75.2.1.23/255.255.255.255/47/0
Remote Addr : 75.2.1.60/255.255.255.255/47/0
Encryption : 3DES Hashing : SHA1
Encapsulation: Transport, GRE
Rekey Int (T): 28400 Seconds Rekey Left(T): 28241 Seconds
Idle Time Out: 400 Minutes Idle TO Left : 400 Minutes
Conn Time Out: 500 Minutes Conn TO Left : 497 Minutes
Bytes Tx : 0 Bytes Rx : 21326
Pkts Tx : 0 Pkts Rx : 239

NAC:
Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds
SQ Int (T) : 0 Seconds EoU Age(T) : 165 Seconds
Hold Left (T): 0 Seconds Posture Token:
Redirect URL :
```

The following is sample output from the **show vpn-sessiondb ra-ikev2-ipsec** command:

```
> show vpn-sessiondb detail ra-ikev2-ipsec

Session Type: Generic Remote-Access IKEv2 IPsec Detailed

Username : IKEV2TG Index : 1
Assigned IP : 95.0.225.200 Public IP : 85.0.224.12
Protocol : IKEv2 IPsec
License : AnyConnect Essentials
Encryption : IKEv2: (1)3DES IPsec: (1)AES256
Hashing : IKEv2: (1)SHA1 IPsec: (1)SHA1
Bytes Tx : 0 Bytes Rx : 17844
Pkts Tx : 0 Pkts Rx : 230
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEV2TG Tunnel Group : IKEV2TG
Login Time : 11:39:54 UTC Tue May 6 2017
Duration : 0h:03m:17s
Inactivity : 0h:00m:00s
```

```
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 5f00e105000010005368ca0a
Security Grp : none

IKEv2 Tunnels: 1
IPsec Tunnels: 1
```

The following is sample output from the **show vpn-sessiondb anyconnect** command:

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : user1                  Index        : 19576
Assigned IP  : 192.168.3.243          Public IP    : 192.168.10.61
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 15060                  Bytes Rx     : 20631
Group Policy : DfltGrpPolicy          Tunnel Group : Ad_group
Login Time   : 09:24:53 UTC Fri Apr 7 2017
Duration     : 0h:03m:20s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8013804c7800058e75ae5
Security Grp : none                   Tunnel Zone  : 0
```

Related Commands

Commands	Description
clear vpn-sessiondb statistics	Clears VPN session statistics.
show vpn-sessiondb ratio	Displays VPN session encryption or protocol ratios.
show vpn-sessiondb summary	Displays a session summary, including total current session, current sessions of each type, peak and total cumulative, maximum concurrent sessions.

show vpn-sessiondb ratio

To display the ratio of current sessions as a percentage by protocol or encryption algorithm, use the **show vpn-sessiondb ratio** command.

show vpn-sessiondb ratio {**encryption** | **protocol**} [**filter** *groupname*]

Syntax Description

encryption	Displays the number of sessions and the percentage of sessions using each encryption method.
protocol	Displays the number of sessions and the percentage of sessions using each VPN protocol.
filter *groupname*	(Optional.) Filters the output to include session ratios only for the tunnel group you specify.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example shows how to display the ratio of sessions based on encryption.

```
> show vpn-sessiondb ratio encryption

Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9
Encryption               Tunnels        Percent
none                     0                0%
DES                      0                0%
3DES                     0                0%
RC4                      0                0%
AES128                   4               80%
AES192                   1               20%
AES256                   0                0%
AES-GCM-128              0                0%
AES-GCM-192              0                0%
AES-GCM-256              0                0%
AES-GMAC-128             0                0%
AES-GMAC-192             0                0%
AES-GMAC-256             0                0%
```

The following example shows how to display the ratio of sessions based on protocol.

```
> show vpn-sessiondb ratio protocol

Filter Group         : All
Total Active Tunnels : 3
Cumulative Tunnels   : 42

Protocol                 Tunnels        Percent
```

```
IKEv1                    0               0%
IKEv2                    0               0%
IPsec                    0               0%
IPsecLAN2LAN             0               0%
IPsecLAN2LANOverNatT     0               0%
IPsecOverNatT            0               0%
IPsecOverTCP             0               0%
IPsecOverUDP             0               0%
L2TPOverIPsec            0               0%
L2TPOverIPsecOverNatT    0               0%
Clientless               0               0%
Port-Forwarding          0               0%
IMAP4S                   0               0%
POP3S                    0               0%
SMTPS                    0               0%
AnyConnect-Parent        1              33%
SSL-Tunnel               1              33%
DTLS-Tunnel              1              33%
```

Related Commands

Commands	Description
show vpn-sessiondb	Displays information about VPN sessions.
show vpn-sessiondb summary	Displays a session summary, including total current session, current sessions of each type, peak and total cumulative, maximum concurrent sessions.

show vpn-sessiondb summary

To display a summary of the number of active sessions, use the **show vpn-sessiondb summary** command.

show vpn-sessiondb summary

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The following table explains the fields in the Active Sessions and Session Information summaries:

Field	Description
Concurrent Limit	The maximum number of concurrently active sessions permitted on this system.
Cumulative Sessions	The number of sessions of all types since the system was last booted or reset.
LAN-to-LAN	The number of IPsec LAN-to-LAN sessions that are currently active.
Peak Concurrent	The highest number of sessions of all types that were concurrently active since the system was last booted or reset.
Percent Session Load	The percentage of the VPN session allocation in use. This value equals the Total Active Sessions divided by the maximum number of sessions available, displayed as a percentage.
Remote Access	ra-ikev1-ipsec—The number of IKEv1 IPsec remote-access user, L2TP over IPsec, and IPsec through NAT sessions that are currently active.
Total Active Sessions	The number of sessions of all types that are currently active.

Examples

The following is sample output from the **show vpn-sessiondb summary** command:

```
> show vpn-sessiondb summary
-------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
-----------------------------------------------
OSPFv3 IPsec : 1 : 1 : 1
-------------------------------------------------------------------------
Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 10000
Device Load : 0%
-------------------------------------------------------------------------
```

The following is sample output from the **show vpn-sessiondb summary** command for generic IKEv2 IPsec remote access sessions:

```
> show vpn-sessiondb summary
-------------------------------------------------------------------------------
VPN Session Summary
-------------------------------------------------------------------------------
Active : Cumulative : Peak Concur : Inactive
----------------------------------------------
Generic IKEv2 Remote Access : 1 : 1 : 1
-------------------------------------------------------------------------------
Total Active and Inactive : 1 Total Cumulative : 1
Device Total VPN Capacity : 250
Device Load : 0%
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Tunnels Summary
-------------------------------------------------------------------------------
Active : Cumulative : Peak Concurrent
----------------------------------------------
IKEv2 : 1 : 1 : 1
IPsec : 1 : 1 : 1
-------------------------------------------------------------------------------
Totals : 2 : 2
-------------------------------------------------------------------------------
```

Related Commands

Commands	Description
show vpn-sessiondb	Displays information about VPN sessions.
show vpn-sessiondb ratio	Displays VPN session encryption or protocol ratios.

show vrf

To show information about the virtual routers defined on a system, use the **show vrf** command.

show vrf [**counters** | **lock**]

Syntax Description

counters	(Optional) Displays the maximum number of user-defined virtual routers allowed on this system, and the number of actual virtual routers configured. The maximum count doc not include the global virtual router: for example, if the maximum count is 4, the total limit is 5.
lock	(Optional) Displays VRF lock information.

Command Default

Without keywords, the command shows the current virtual routers and the interfaces assigned to each virtual router.

Command History

Release	Modification
6.6	This command was introduced.

Usage Guidelines

Use the **show vrf** command to view basic information about the virtual routers defined on the system if you enabled virtual routing and forwarding (VRF). To view the routing tables for each virtual router, use the **show route vrf** *name* command for the IPv4 routing table, and **show ipv6 route vrf** *name* for the IPv6 routing table.

Examples

The following example displays the virtual routers and the interfaces assigned to each router:

```
> show vrf

Name            VRF ID          Description             Interfaces
vrf1            1                                   inside
                                                    inside_2
vrf2            2                                   inside_3
                                                    inside_4
```

The following example shows the maximum number of virtual routers allowed on this system, and the current number of virtual routers. Whether a virtual router is IPv4, IPv6, or both, depends on the IP addresses you assign to the interfaces within each virtual router. Note that the maximum number refers to user-defined virtual routers; in this example, for a VMware system, the total allowed limit is 15, one for the global virtual router, and 14 user defined routers.

```
> show vrf counters
Maximum number of VRFs supported: 14
Maximum number of IPv4 VRFs supported: 14
Maximum number of IPv6 VRFs supported: 14
Current number of VRFs: 2
Current number of VRFs in delete state: 0
```

The following example shows VRF lock information.

```
> show vrf lock

VRF Name: single_vf; VRF id = 0 (0x0)
VRF lock count: 1
VRF Name: vrf1; VRF id = 1 (0x1)
VRF lock count: 2
VRF Name: vrf2; VRF id = 2 (0x2)
VRF lock count: 2
```

Related Commands

Command	Description
show ipv6 route	Shows the IPv6 routing table.
show route	Shows the IPv4 routing table.

show wccp

To display global statistics related to Web Cache Communication Protocol (WCCP), use the **show wccp** command.

show wccp {**web-cache** | *service_number*} [**buckets** | **detail** | **service** | **view** | **hash** *dest_addr source_addr dest_port source_port*]
show wccp [**interfaces** [**detail**]]

Syntax Description

buckets	(Optional) Displays service group bucket assignments.
detail	(Optional) Displays information about the router and all web caches.
hash *dest_addr source_addr dest_port source_port*	(Optional) Displays the WCCP hash for the specified connection: • *dest_addr* is the IP address of the destination host. • *source_addr* is the IP address of the source host. • *dest_port* is the port of the destination host. • *source_port* is the port of the source host.
interfaces [**detail**]	(Optional) Displays the WCCP redirect interfaces. Include the detail keyword for the interface configuration.
service	(Optional) Displays service group definition information.
service-number	Identification number of the web-cache service group being controlled by the cache. The number can be from 0 to 254. For web caches using Cisco Cache Engines, the reverse proxy service is indicated by a value of 99.
view	(Optional) Displays whether other members of a particular service group have or have not been detected.
web-cache	Specifies statistics for the web-cache service.

Command History

Release	Modification
6.2	This command was introduced.

Examples

The following example shows how to display WCCP information:

```
> show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0
    Service Identifier: web-cache
```

```
Number of Cache Engines:             0
Number of routers:                   0
Total Packets Redirected:            0
Redirect access-list:                foo
Total Connections Denied Redirect:   0
Total Packets Unassigned:            0
Group access-list:                   foobar
Total Messages Denied to Group:      0
Total Authentication failures:       0
Total Bypassed Packets Received:     0
```

Related Commands

Commands	Description
clear wccp	Clears WCCP statistics.

show webvpn

To view information about remote access VPN, use the **show webvpn** command.

show webvpn {**anyconnect** | **debug-condition** | **group-alias** [*tunnel_group*] | **group-url** [*tunnel_group*] | **statistics**}

Syntax Description

anyconnect	Displays information about the AnyConnect images that are available for download to client endpoints.
debug-condition	Displays the current debug conditions as set by the **debug webvpn condition** command.
group-alias [*tunnel_group*]	Displays the aliases for tunnel groups (connection profiles). You can optionally specify the name of a tunnel group to view information about that group only. Each group can have multiple aliases or even no aliases.
group-url [*tunnel_group*]	Displays the URLs for tunnel groups (connection profiles). You can optionally specify the name of a tunnel group to view information about that group only. Each group can have multiple URLs or even no URLs.
statistics	Displays data about WebVPN events.

Command History

Release	Modification
6.2.1	This command was introduced.
7.1	Information about the external browser package was added to the AnyConnect output.

Examples

The following example shows output from the **show webvpn anyconnect** command:

```
> show webvpn anyconnect
1. disk0:/csm/anyconnect-win-4.2.06014-k9.pkg 1 cfg-regex=/Windows/
  CISCO STC win2k+
  4,2,06014
  Hostscan Version 4.2.06014
  Thu 10/06/2016 14:40:31.34

1 AnyConnect Client(s) installed
```

The following example of **show webvpn anyconnect** includes the external browser package, if one is being used with SAML authentication.

```
> show webvpn anyconnect
1. disk0:/anyconnpkgs/anyconnect-win-4.10.01075-webdeploy-k9.pkg 2 dyn-regex=/Windows NT/
  CISCO STC win2k+
  4,10,01075
  Hostscan Version 4.10.01075
```

```
  Wed 04/28/2021 12:36:03.98

1 AnyConnect Client(s) installed

2. disk0:/externalbrowserpkgs/external-sso-98.161.00015-webdeploy-k9.pkg
  Cisco AnyConnect External Browser Headend Package
  98.161.00015
  Wed 05/05/21 15:49:27.817381
```

The following example shows output from the **show webvpn debug-condition** command:

```
> show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: IP address filters:
INFO: 10.100.10.10/32
```

The following example shows output from the **show webvpn group-alias** command:

```
> show webvpn group-alias
Tunnel Group: Ad_group   Group Alias: ad_group enabled
Tunnel Group: Radius_group   Group Alias: Radius_group enabled
Tunnel Group: Cert_auth   Group Alias: cert_auth enabled
```

The following example shows output from the **show webvpn group-url** command:

```
> show webvpn group-url
http://www.cisco.com
https://ger1.example.com
https://ger2.example.com
```

The following example shows output from the **show webvpn statistics** command:

```
> show webvpn statistics
Total number of objects served  0
 html                           0
 js                             0
 css                            0
 vb                             0
 java archive                   0
 java class                     0
 image                          0
 undetermined                   0
Server compression statistics
 Decompression success from server                  0
 Unsolicited compression from server                0
 Unsupported compression algorithm used by server   0
 Decompression failure for server responses         0
IOBuf failure statistics
 uib_create_with_channel                            0
 uib_create_with_string                             0
 uib_create_with_string_and_channel                 0
 uib_transfer                                       0
 uib_add_filter                                     0
 uib_yyread                                         0
 uib_read                                           0
 uib_set_buffer_max                                 0
 uib_set_eof_symbol                                 0
 uib_get_capture_handle                             0
 uib_set_capture_handle                             0
```

```
uib_buflen                                0
uib_bufptr                                0
uib_buf_endptr                            0
uib_get_buf_offset                        0
uib_get_buf_offset_addr                   0
uib_get_nth_char                          0
uib_consume                               0
uib_advance_bufptr                        0
uib_eof                                   0
```

show xlate

To display information about NAT sessions (xlates or translations), use the **show xlate** command.

show xlate [**global** *ip1*[*-ip2*] [**netmask** *mask*]] [**local** *ip1*[*-ip2*] [**netmask** *mask*]] [**gport** *port1*[*-port2*]] [**lport** *port1*[*-port2*]] [**interface** *if_name*] [**type** *type*]
show xlate count

Syntax Description

count	Displays the translation count.
global *ip1*[*-ip2*]	(Optional) Displays the active translations by mapped IP address or range of addresses.
gport *port1*[*-port2*]	Displays the active translations by the mapped port or range of ports.
interface *if_name*	(Optional) Displays the active translations by interface.
local *ip1*[*-ip2*]	(Optional) Displays the active translations by real IP address or range of addresses.
lport *port1*[*-port2*]	Displays the active translations by real port or range of ports.
netmask *mask*	(Optional) Specifies the network mask to qualify the mapped or real IP addresses.
type *type*	(Optional) Displays the active translations by type. You can enter one or more of the following types: • **static** • **portmap** • **dynamic** • **twice-nat** (otherwise known as manual NAT) When specifying more than one type, separate the types with a space.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **show xlate** command displays the contents of the translation slots. The xlates can include those generated for internal interfaces, which do not appear in the NAT rules table in the device manager. These are required for internal processing.

When the VPN client configuration is enabled and the inside host is sending out DNS requests, the **show xlate** command may list multiple xlates for a static translation.

In a clustering environment, up to three xlates might be duplicated to different nodes in the cluster to handle a PAT session. One xlate is created on the unit that owns the connection. One xlate is created on a different unit to back up the PAT address. Finally, one xlate exists on the director that replicates the flow. In the case where the backup and director is the same unit, two instead of three xlates might be created.

Examples

The following is sample output from the **show xlate** command. The initial PAT xlates for nlp_int_tap relate to HTTPS access rules that allow device manager access to 192.168.1.1 rather than the management interface address. These are internal NAT xlates whose rules do not show up in the NAT table in the device manager.

```
> show xlate
13 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_2:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_3:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_4:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_5:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_6:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_7:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_8:0.0.0.0/0
    flags sIT idle 0:30:10 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_7:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_6:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_5:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_4:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_3:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_2:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
```

The following is sample output from the **show xlate** command showing a translation from IPv4 to IPv6.

```
> show xlate
14 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
(...other entries removed...)
NAT from outside:0.0.0.0/0 to inside1_8:2001:db8::/96
    flags s idle 0:01:36 timeout 0:00:00
```

Related Commands

Command	Description
clear xlate	Clears current translation and connection information.
show conn	Displays all active connections.
show local-host	Displays the local host network information.

show zero-trust

To view the run-time zero trust statistics and session information on a single threat defense or HA node, use the **show zero-trust** command.

show zero-trust sessions [**application** | **application-group** | **count** | **user** | **detail**]

show zero-trust statistics

Syntax Description

application	Displays zero-trust sessions for an application.
application-group	Displays zero-trust sessions for an application group.
count	Displays zero-trust sessions count
user	Displays zero-trust sessions for an user.
detail	Displays detailed information for a session.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

None

Examples

The following is sample output for all the zero trust sessions.

```
> show zero-trust sessions
Sessions display order: User, Application, Application-Group, Src Ip, Sessions
test@cisco.com, wiki.ztna.com, parent, 172.16.77.1, 1
test@cisco.com, wiki.bitbucket.com, bitbucket_grp, 172.16.77.1, 1
test@cisco.com, wiki.outlook.com, None, 172.16.77.1, 1
test@cisco.com, wiki.confluence.com, parent, 172.16.77.1, 1
```

The following is a sample detailed output for all the zero trust sessions.

```
>show zero-trust sessions detail
Sessions display order: User, Application, Application-Group, Src Ip, Cookie, Expiry Time
test@cisco.com, wiki.ztna.com, None, 172.16.77.1, E194C7F0..., 23:54:53
test@cisco.com, wiki.confluence.com, None, 172.16.77.1, F9E330A4..., 23:55:05
```

The following is a sample output for the number of zero trust sessions.

```
> show zero-trust sessions count
5 in use, 20 most used
```

The following is a sample output of statistics for usage data such as active data, sessions, and SAML related information.

```
> show zero-trust statistics
Active zero-trust sessions                  2
Active users                                0*
Total zero-trust sessions                   2
Total users authorised                      0*
Total zero-trust sessions failed            0*
Total active applications                   1
Total SAML AuthN Requests                   2
Total SAML AuthN Responses                  2
Total SAML Auth Failures                    0*
SAML Assertions Passed                      2
SAML Assertions Failed                      0*
Total bytes in                              5852
Bytes
Total bytes out                             27570
Bytes
Pre-auth latency in millisec (min/max/avg)  7/11/9
Post-auth latency in millisec (min/max/avg) 6/9/7
```

Parameter	Description
Active zero-trust sessions	Number of active session that applications are accessing.
Active users	Number of active users who have at least one application session active.
Total zero-trust sessions	Total number of sessions for application access on the threat defense
Total users authorised	Total number of users authorized on the threat defense
Total zero-trust sessions failed	Total number of failed zero trust sessions on the threat defense
Total active applications	Total number of applications with at least one active session
Total SAML AuthN Requests	Total number of SAML authentication requests sent from the threat defense
Total SAML AuthN Responses	Total number of SAML authentication responses received by the threat defense
Total SAML Auth Failures	Total number of SAML authentication failures occurred on the threat defense
SAML Assertions Passed	Total number of SAML assertion validation successes on the threat defense
SAML Assertions Failed	Total number of SAML assertion validation failures on the threat defense
Total bytes in	Total number of bytes received on the threat defense
Total bytes out	Total number of bytes sent from the threat defense

Parameter	Description
Pre-auth latency in millisec (min/max/avg)	Latency recorded on the threat defense for an application access request before authentication • Min—minimum latency on the threat defense • Max—maximum latency on the threat defense • Avg—Average latency on the threat defense
Post-auth latency in millisec (min/max/avg)	Latency recorded on the FTD device for an application access request after authentication • Min—minimum latency on the threat defense • Max—maximum latency on the threat defense • Avg—Average latency on the threat defense

Related Commands

Command	Description
show running-config zero-trust	Displays the zero trust running configuration
show cluster zero-trust	Displays cluster statistics
clear zero-trust	Clears zero trust sessions and statistics
show counters protocol zero_trust	Displays the counters that are hit for zero trust flow

show zone

To display traffic zone information, use the **show zone** command.

show zone [*name*]

Syntax Description

name	(Optional) The name of a traffic zone.

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

Traffic zones are not exactly the same as security zones. Although passive security zones are also automatically generated as traffic zones, routed and switched security zones are not. Traffic zones are used for traffic load balancing (using Equal Cost Multi-Path (ECMP) routing), route redundancy, and asymmetric routing across multiple interfaces.

To view the rest of the zone configuration, use the **show running-config zone** and **show running-config interface** commands.

Examples

The following example displays the configured traffic zones. In this example, the traffic zone is for passive interfaces. If the zone was for Equal Cost Multi-Path routing, the zone type would be ecmp. The interface configuration follows. The **zone-member** command configures the interface as a member of the zone.

```
> show zone passive-security-zone
Zone: passive-security-zone passive
    Security-level: 0
    Zone member(s): 1
      passive                       GigabitEthernet0/0

> show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 mode passive
 nameif passive
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 zone-member krjones-passive-security-zone
```

Related Commands

Command	Description
clear conn zone	Clears zone connections.
clear local-host zone	Clears zone hosts.
show interface	Displays the runtime status and statistics of interfaces.

Command	Description
show local-host zone	Shows the network states of local hosts within a zone.
show nameif zone	Shows the zone or inline set membership for interfaces.

shun

To block connections from an attacking host, use the **shun** command. To disable a shun, use the **no** form of this command.

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]
no shun *source_ip* [**vlan** *vlan_id*]

Syntax Description

dest_port	(Optional) Specifies the destination port of a current connection that you want to drop when you place the shun on the source IP address.
dest_ip	(Optional) Specifies the destination address of a current connection that you want to drop when you place the shun on the source IP address.
protocol	(Optional) Specifies the IP protocol of a current connection that you want to drop when you place the shun on the source IP address, such as UDP or TCP. By default, the protocol is 0 (any protocol).
source_ip	Specifies the address of the attacking host. If you only specify the source IP address, all future connections from this address are dropped; current connections remain in place. To drop a current connection and also place the shun, specify the additional parameters of the connection. Note that the shun remains in place for all future connections from the source IP address, regardless of destination parameters.
source_port	(Optional) Specifies the source port of a current connection that you want to drop when you place the shun on the source IP address.
vlan *vlan_id*	(Optional) Specifies the VLAN ID where the source host resides.

Command Default

The default protocol is 0 (any protocol).

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **shun** command lets you block connections from an attacking host. All future connections from the source IP address are dropped and logged until the blocking function is removed manually. The blocking function of the **shun** command is applied whether or not a connection with the specified host address is currently active.

If you specify the destination address, source and destination ports, and the protocol, then you drop the matching connection as well as placing a shun on all future connections from the source IP address; all future connections are shunned, not just those that match these specific connection parameters.

You can only have one **shun** command per source IP address.

Because the **shun** command is used to block attacks dynamically, it is not displayed in the threat defense device configuration.

Whenever an interface configuration is removed, all shuns that are attached to that interface are also removed.

Examples

The following example shows that the offending host (10.1.1.27) makes a connection with the victim (10.2.2.89) with TCP. The connection in the threat defense device connection table reads as follows:

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

Apply the **shun** command using the following options:

```
> shun 10.1.1.27 10.2.2.89 555 666 tcp
Shun 10.1.1.27 added in context: single_vf
Shun 10.1.1.27 successful
```

The command deletes the specific current connection from the threat defense device connection table and also prevents all future packets from 10.1.1.27 from going through the threat defense device.

Related Commands

Command	Description
clear shun	Disables all the shuns that are currently enabled and clears the shun statistics.
show conn	Shows all active connections.
show shun	Displays the shun information.

shutdown

To shut down the device, use the **shutdown** command.

shutdown

Command History

Release	Modification
6.0.1	This command was introduced.

Examples

The following example is sample output from the **shutdown** command when you shut down the device:

```
> shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': YES
```

Related Commands

Command	Description
reboot	Reboots the device.

system access-control clear-rule-counts

To reset the access control rule hit count to 0, use the **system access-control clear-rule-counts** command.

system access-control clear-rule-counts

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example shows output from the **system access-control clear-rule-counts** command:

```
> system access-control clear-rule-counts
Are you sure that you want to clear the rule hit counters? (y/n): y
Clearing the rule hit counters.
Success.
```

Related Commands

Command	Description
show access-control-config	Shows the access control policy summary and hit counts.

system generate-troubleshoot

To generate troubleshooting data for analysis by Cisco Technical Support when requested to do so, use the **system generate troubleshoot** command.

system generate-troubleshoot *options*

Syntax Description

options	The type of troubleshooting data you want to generate display. You can enter one or more option. Use spaces to separate multiple options. • **ALL**—Run all of the following options. • **SNT**—Snort performance and configuration. • **PER**—Hardware performance and logs. • **SYS**—System configuration, policy, and logs. • **DES**—Detection configuration, policy, and logs. • **NET**—Interface and network related data. • **VDB**—Discovery, awareness, VDB data, and logs. • **UPG**—Upgrade data and logs. • **DBO**—All database data. • **LOG**—All log data. • **NMP**—Network map information.

Command History

Release	Modification
6.1	This command was introduced.

Examples

The following example shows how to generate troubleshooting data for Snort and hardware performance.

```
> system generate-troubleshoot SNT PER
Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient.  This may take several minutes.
the troubleshoot options codes specified are SNT,PER.
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/index]
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/base-6.2.0]
Troubleshooting information successfully created at /ngfw/var/common/results-10-14-201
6--181112.tar.gz
```

Related Commands

Command	Description
copy	Copies files from or to the system.
delete	Deletes files from the system.

system lockdown-sensor

To remove access to expert mode and the Bash shell, use the **system lockdown-sensor** command.

system lockdown-sensor

Command History

Release	Modification
6.2.1	This command was introduced.

Usage Guidelines

Caution You cannot reverse this command. If you need to restore access to expert mode, you must contact the Cisco Technical Assistance Center and get a hotfix.

The **expert** command provides access to the Bash shell, which provides administrative users extensive access to the system's operating environment. Security certification regimes (such as Common Criteria (CC) or the Unified Capabilities Approved Products List (UC APL)) impose requirements that limit the access and information available to users of a system. Use the **system lockdown-sensor** command to remove access to the **expert** command to help meet these certification requirements.

Note After using this command, the **expert** command remains available in the current SSH session. You must log out and log back in to verify that the command has been removed and no longer works. Anyone else who logs in after you use the command will not be able to use expert mode either.

Example

The following example removes access to expert mode to comply with security requirements.

```
> system lockdown-sensor
This action will remove the 'expert' command from your system for all
future CLI sessions, rendering the bash shell inaccessible.

This cannot be reversed without a support call.
Continue and remove the 'expert' command?

Please enter 'YES' or 'NO': YES
>
```

system support commands

Most system support commands are used for debugging and troubleshooting at the assistance of the Cisco Technical Assistance Center. You should use the commands under the direction of Cisco support, with the exception of the following commands, which are of general use.

- system support diagnostic-cli, on page 132
- system support view-files, on page 138
- system support ssl-hw- commands, on page 135

system support ssl-client-hello- commands

These commands allow you to determine the behavior of Transport Layer Security (TLS) 1.3 downgrade to TLS 1.2. Because managed devices do not support TLS 1.3 encryption or decryption, TLS 1.3 sessions between a client and server can break, resulting in errors like the following in the client web browser:

ERR_SSL_PROTOCOL_ERROR

SEC_ERROR_BAD_SIGNATURE

ERR_SSL_VERSION_INTERFERENCE

Errors can occur when a client connects to a server and TLS inspection determines that the connection, which has been modified to downgrade, matches a **Do Not Decrypt** SSL rule action.

We recommend you use these commands after consulting with Cisco TAC.

system support ssl-client-hello-enabled aggressive_tls13_downgrade { **true** | **false** }

Syntax Description

true	Default. TLS 1.3 connections are downgraded whenever necessary to perform decryption. However, if data received after the ClientHello message causes the session to match a **Do Not Decrypt** rule, the session might fail.
false	TLS 1.3 connections are downgraded only when there is a reasonable certainty the session will not match a **Do Not Decrypt** rule. In some cases, TLS connections that need to be decrypted might not be downgraded. In those cases, traffic is not decrypted. The action specified in the SSL policy for **Session not cached** setting for its **Undecryptable Action** is taken instead.

Command History

Release	Modification
6.2.3.7	This command was introduced.

system support diagnostic-cli

To enter the diagnsotic CLI, which includes additional show and other troubleshooting commands, use the **system support diagnostic-cli** command.

system support diagnostic-cli

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The Diagnostic CLI contains additional show and other commands you can use to troubleshoot the system. The commands in the Diagnostic CLI are from ASA Software. The regular threat defense CLI contains many of the same commands, so you might not need the extra commands of the Diagnostic CLI.

When you enter the Diagnostic CLI, you are in a separate session from the regular threat defense CLI.

The prompt changes to include the system hostname. There are two modes, and the prompt indicates the mode you are in. For User EXEC mode, the prompt is:

```
hostname>
```

For Privileged EXEC mode, also known as Enable mode, the prompt is the following. You enter this mode using the enable command. Although you are prompted for a password, simply press Enter, by default there is no password required to enter this mode.

```
hostname#
```

Keep the following tips in mind when using the Diagnostic CLI:

- To exit the Diagnostic CLI and return to the regular CLI, press Ctrl+a, then d.
- Use the **exit** command to leave Privileged EXEC mode.

  The commands available in each mode differ. Privileged EXEC mode includes significantly more commands than User EXEC mode. Use **?** to see the available commands. You can find usage information in the ASA Software command references:

  - Cisco ASA Series Command Reference, A - H Commands, http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1.html
  - Cisco ASA Series Command Reference, I - R Commands, http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/I-R/cmdref2.html
  - Cisco ASA Series Command Reference, S Commands, http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/S/cmdref3.html
  - Cisco ASA Series Command Reference, T - Z Commands and IOS Commands for the ASASM, http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/T-Z/cmdref4.html

- The Diagnostic CLI can include commands that are not meaningful for threat defense. If you try a command that does not provide meaningful (or any) information, the related feature might not be configured or supported by threat defense.
- The Diagnostic CLI does not allow you to enter configuration mode. You cannot use the CLI to configure the device.
- When you detach from the Diagnostic CLI, the next time you enter it you are placed in the same mode you were in when you last detached.
- On the ASA 5506W-X, you can use the **session wlan** command to open a connection to the wireless module, and use its CLI to configure the access point. You must be in Privileged EXEC mode.

Examples

The following example shows how to enter the Diagnostic CLI and Privileged EXEC mode. When you get the password prompt after entering the **enable** command, simply press Enter. By default, there is no password to enter Privileged EXEC mode.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

system support elephant-flow-detection

To configure the elephant flow detection parameters, use the **system support elephant-flow-detection** command.

Attention This command is supported for the management center and threat defense Version 7.1 only.

system support elephant-flow-detection { **enable** | **disable** | **time-threshold** *time-in-seconds* | **bytes-threshold** *bytes-in-MB* }

Syntax Description

enable	Enables elephant flow detection.
disable	Disables elephant flow detection.
time-threshold *time-in-seconds*	Configures the time threshold (in seconds) to detect elephant flow.
bytes-threshold *bytes-in-MB*	Configures the size threshold (in bytes) to detect elephant flow.

Command Default

This command is enabled by default.

Command History

Release	Modification
7.1	This command was introduced.

Usage Guidelines

To enable, disable, or configure the size and time thresholds for elephant flow detection, use the **system support elephant-flow-detection** command.

Examples

The following example configures the time threshold to detect an elephant flow to 15 seconds.

```
> system support elephant-flow-detection time-threshold 15
command executed successfully.
```

Related Commands

Command	Description
show elephant-flow detection-config	Displays the configured parameters for elephant flow detection.
show elephant-flow status	Displays the elephant flow detection status (enabled or disabled).

system support ssl-hw- commands

These commands allow you to perform various operations on a feature referred to as *TLS/SSL hardware acceleration* in versions 6.2.3 and 6.3 and as *TLS crypto acceleration* in version 6.4. The available keywords depend on the threat defense software version.

Supported devices and whether or not the feature is enabled or disabled by default also depend on software version. For this information, refer to the *management center Configuration Guide*.

Syntax for versions 6.2.3 and 6.3:

system support {**ssl-hw-status** | **ssl-hw-supported-ciphers** | **ssl-hw-offload enable** | **ssl-hw-offload disable**}

Syntax for version 6.4:

system support ssl-hw-supported-ciphers

Syntax Description

ssl-hw-status	Displays the current status of SSL hardware acceleration. The default state is: • 6.2.3: disabled • 6.3 and 6.4: enabled
ssl-hw-supported-ciphers	Displays the list of ciphers supported by SSL hardware acceleration. This command is useful because SSL hardware acceleration doesn't support all of the ciphers supported by SSL software acceleration (in particular, decryption of SEED and Camellia ciphers is not supported).
ssl-hw-offload enable	Enables SSL hardware acceleration; you are prompted to reboot the device.
ssl-hw-offload disable	Disables SSL hardware acceleration; you are prompted to reboot the device.

Command History

Release	Modification
6.4	The feature name changed from TLS/SSL hardware acceleration to TLS crypto acceleration. The following keywords have been removed: **ssl-hw-offload enable** **ssl-hw-offload disable** **ssl-hw-status**
6.3	The feature is enabled by default.
6.2.3	This command was introduced. The feature is disabled by default.

Usage Guidelines

Note Of the commands discussed in this section, only **system support ssl-hw-offload-supported ciphers** applies to version 6.4.

Use these commands to display information about SSL hardware acceleration or to enable or disable the feature.

Enable SSL hardware acceleration to improve encryption and decryption performance.

Disable SSL hardware acceleration to use any of the features it does not support or if you encounter unexpected traffic interruptions with an enabled SSL policy.

Features *not* supported by SSL hardware acceleration include the following:

- Managed devices where threat defense container instance is enabled.
- If the inspection engine is configured to preserve connections and the inspection engine fails unexpectedly, TLS/SSL traffic is dropped until the engine restarts.

  This behavior is controlled by the **configure snort preserve-connection {enable | disable}** command.

Use the **system support ssl-hw-status** command to display the current status.

Use the **system support ssl-hw-supported-ciphers** command to display the list of ciphers supported by SSL hardware acceleration.

Examples

Following is an example of viewing the current status of SSL hardware acceleration:

```
> system support ssl-hw-status
Hardware Offload configuration set to Disabled
```

Following is an example of enabling SSL hardware acceleration with prompting to reboot the device:

```
If you enable SSL hardware acceleration, you cannot:
    1.    Decrypt passive or inline tap traffic.
    2.    Preserve Do Not Decrypt connections when the inspection engine restarts.
Continue? (y/n) [n]: y


Enabling or disabling SSL hardware acceleration reboots the system. Continue? (y/n) [n]: y

SSL hardware acceleration will be enabled on system boot.
```

You are required to confirm all of the preceding before the device is rebooted.

Following is a partial list of the ciphers supported by SSL hardware acceleration:

```
> system support ssl-hw-supported-ciphers
CID     Cipher Suite Name                                CH_mod Keep     Support Inline
Support Passive
-----------------------------------------------------------------------------------------------
0x0004  TLS_RSA_WITH_RC4_128_MD5                         Yes             Yes             Yes
```

```
0x0005  TLS_RSA_WITH_RC4_128_SHA                 Yes             Yes             Yes
0x0009  TLS_RSA_WITH_DES_CBC_SHA                 Yes             Yes             Yes
0x000a  TLS_RSA_WITH_3DES_EDE_CBC_SHA            Yes             Yes             Yes
0x000c  TLS_DH_DSS_WITH_DES_CBC_SHA               No              No              No
0x000d  TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA          No              No              No
0x000f  TLS_DH_RSA_WITH_DES_CBC_SHA               No              No              No
0x0010  TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA          No              No              No
0x0012  TLS_DHE_DSS_WITH_DES_CBC_SHA              No              No              No
0x0013  TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA         No              No              No
0x0015  TLS_DHE_RSA_WITH_DES_CBC_SHA              Yes             Yes             No
0x0016  TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA         Yes             Yes             No
0x0018  TLS_DH_Anon_WITH_RC4_128_MD5              No              Yes             No
0x001a  TLS_DH_Anon_WITH_DES_CBC_SHA              No              Yes             No
0x001b  TLS_DH_Anon_WITH_3DES_EDE_CBC_SHA         No              Yes             No
0x001e  TLS_KRB5_WITH_DES_CBC_SHA                 No              No              No
0x001f  TLS_KRB5_WITH_3DES_EDE_CBC_SHA            No              No              No
0x0020  TLS_KRB5_WITH_RC4_128_SHA                 No              No              No
0x0024  TLS_KRB5_WITH_RC4_128_MD5                 No              No              No
0x002f  TLS_RSA_WITH_AES_128_CBC_SHA              Yes             Yes             Yes
0x0030  TLS_DH_DSS_WITH_AES_128_CBC_SHA           No              No              No
0x0031  TLS_DH_RSA_WITH_AES_128_CBC_SHA           No              No              No
… more
```

system support view-files

To view system log contents when working with the Cisco Technical Assistance Center (TAC) to resolve a problem, use the **system support view-files** command.

system support view-files

Command History

Release	Modification
6.1	This command was introduced.

Usage Guidelines

The **system support view-files** command opens a system log. Use this command while working with the Cisco Technical Assistance Center (TAC) so that they can help you interpret the output and to select the appropriate log to view.

The command presents a menu for selecting a log. Use the following commands to navigate the wizard:

- To change to a sub-directory, type in the name of the directory and press Enter.
- To select a file to view, enter **s** at the prompt. You are then prompted for a file name. You must type the complete name, and capitalization matters. The file list shows you the size of the log, which you might consider before opening very large logs.
- Press the space bar when you see --More-- to see the next page of log entries; press Enter to see just the next log entry. When you reach the end of the log, you are taken to the main menu. The --More-- line shows you the size of the log and how much of it you have viewed. **Use Ctrl+C to close the log and exit the command if you do not want to page through the entire log.**
- Type **b** to go up one level in the structure to the menu.

If you want to leave the log open so you can see new messages as they are added, use the **tail-logs** command.

Examples

The following example shows how view the ngfw.log file. The file listing starts with directories at the top, then a list of files in the current directory.

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
```

```
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>

2016-10-06 15:38:22.630001 | 9194       | ngfw.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> ngfw.log
2016-10-06 15:38:03 Starting Cisco Firepower Threat Defense ...
2016-10-06 15:38:03 Found USB flash drive /dev/sdb
2016-10-06 15:38:03 Found hard drive(s):  /dev/sda

<remaining log truncated>
```

Related Commands

Command	Description
tail-logs	Opens a log and keeps it open.