

## Chapter 26

# Intrusion Detection Services Interfaces Operational Mode Commands

Table 50 summarizes the command-line interface (CLI) commands you can use to monitor and troubleshoot Intrusion Detection Services (IDS) interfaces. In the table, the commands are grouped by functionality. In the remainder of this chapter, they are explained alphabetically.

**Table 50: Commands for Monitoring IDS Interfaces**

Task or Information to Monitor	CLI Command
Display IDS event information.	show services ids on page 362
Clear (zero) IDS events and event information.	clear services ids on page 359 clear services ids destination-table on page 360 clear services ids pair-table on page 360 clear services ids source-table on page 361

## clear services ids

<b>Syntax</b>	clear services ids <interface <i>interface-name</i> > <service-set <i>service-set-name</i> >
<b>Description</b>	Clear Intrusion Detection Service (IDS) events.
<b>Options</b>	none—Clear all IDS events for all service sets and reset IDS.  interface <i>interface-name</i> —(Optional) Clear all IDS events for a particular adaptive services interface and reset IDS.  service-set <i>service-set-name</i> —(Optional) Clear all IDS events for a particular service set.
<b>Required Privilege Level</b>	view

## clear services ids destination-table

---

<b>Syntax</b>	clear services ids destination-table <destination-prefix <i>destination-prefix-name</i> > <interface <i>interface-name</i> > <service-set <i>service-set-name</i> >
<b>Description</b>	Clear the Intrusion Detection Service (IDS) events for a particular address that might be under attack.
<b>Options</b>	<p>none—Clear the attack destination address table.</p> <p>destination-prefix <i>destination-prefix-name</i>—(Optional) Clear the attack destination table for a particular destination prefix.</p> <p>interface <i>interface-name</i>—(Optional) Clear the attack destination table for a particular adaptive services interface and reset IDS.</p> <p>service-set <i>service-set-name</i>—(Optional) Clear the attack destination table for a particular service set.</p>
<b>Required Privilege Level</b>	view

## clear services ids pair-table

---

<b>Syntax</b>	clear services ids pair-table <destination-prefix <i>destination-prefix-name</i> > <source-prefix <i>source-prefix-name</i> > <interface <i>interface-name</i> > <service-set <i>service-set-name</i> >
<b>Description</b>	Clear the Intrusion Detection Service (IDS) attack source and destination address pair table.
<b>Options</b>	<p>none—Clear the attack source and destination address pair table.</p> <p>destination-prefix <i>destination-prefix-name</i>—(Optional) Clear the attack source and destination address pair table for a particular destination prefix.</p> <p>source-prefix <i>source-prefix-name</i>—(Optional) Clear the attack source and destination address pair table for a particular source prefix.</p> <p>interface <i>interface-name</i>—(Optional) Clear the attack source and destination address pair table for a particular adaptive services interface and reset IDS.</p> <p>service-set <i>service-set-name</i>—(Optional) Clear the attack source and destination address pair table for a particular service set.</p>
<b>Required Privilege Level</b>	view

## clear services ids source-table

---

<b>Syntax</b>	clear services ids source-table <source-prefix <i>source-prefix-name</i> > <interface <i>interface-name</i> > <service-set <i>service-set-name</i> >
<b>Description</b>	Clear Intrusion Detection Service (IDS) events for addresses that are suspected attackers.
<b>Options</b>	<p>none—Clear the attack source address table.</p> <p>interface <i>interface-name</i>—(Optional) Clear the attack source address table for a particular adaptive services interface and reset IDS.</p> <p>source-prefix <i>source-prefix-name</i>—(Optional) Clear the attack source address table for a particular source prefix.</p> <p>service-set <i>service-set-name</i>—(Optional) Clear the attack source address table for a particular service set.</p>
<b>Required Privilege Level</b>	view

## show services ids

---

**Syntax** show services ids (destination-table | pair-table | source-table)  
 <brief | extensive | terse>  
 <destination-prefix *destination-prefix-name*>  
 <interface *interface-name*>  
 <source-prefix *source-prefix-name*>  
 <limit *number*>  
 <order (anomalies | bytes | flows | packets)>  
 <service-set *service-set-name*>  
 <threshold *number*>

**Description** Display information about Intrusion Detection Service (IDS) events.

**Options**

- destination-table—Display information for an address under possible attack.
- source-table—Display information for an address that is a suspected attacker.
- pair-table—Display information for a particular suspected attack source and destination address pair.
- brief—(Optional) Display a brief version of information.
- extensive—(Optional) Display a detailed version of information.
- terse—(Optional) Display a summary version of information.
- destination-prefix *destination-prefix-name*—(Optional) Display information for a particular destination prefix.
- interface *interface-name*—(Optional) Display information for a particular adaptive services interface.
- source-prefix *source-prefix-name*—(Optional) Display information about a particular source prefix.
- limit *number*—(Optional) Display a maximum of this number of entries.
- order—(Optional) Display events according to one of the following table-ordering criteria. The default is anomalies.
  - anomalies—Display information for particular anomalies.
  - bytes—Order output by number of bytes received.
  - flows—Order output by number of flows.
  - packets—Order output by number of packets received.
- service-set *service-set-name*—(Optional) Display information about a particular service set.

*threshold number*—(Optional) Limit the display to events with this number of anomalies, bytes, flows, or packets, whichever criterion you specify for order. For example, to display all events with more than 100 flows, specify `order flows` and `threshold 100`.

**Required Privilege Level** view

**Output Fields** Interface—Name of an adaptive services interface.

Service set—Name of a service set.

Sorting order—Primary mode to display information: Anomalies, Bytes, Flows, or Packets.

Source address—Name of the source address.

Dest address—Name of the destination address.

Time—Total time the information has been in the table.

Flags—Flags can be Forced, F (terse mode), SYNcookie, S (terse mode), Forced+SYNcookie, and F+S (terse mode).

Application—Configured application, such as FTP or Telnet.

Bytes—Total number of bytes sent from source to destination address, in thousands (k) or millions (m).

Packets—Total number of packets sent from source to destination address, in thousands (k) or millions (m).

Flows—Total number of flows of packets sent from source to destination address, in thousands (k) or millions (m).

Anomalies—Total number of packets in the anomaly table, in thousands (k) or millions (m).

Anomaly description—Type of anomaly:

TCP source or destination port zero

TCP header length check failed

TCP seq number zero and no flags set

TCP seq number zero and FIN/PSH/RST flags set

TCP FIN/RST or SYN/(URG|FIN|RST) flags set

UDP source or destination port zero

UDP header length check failed

ICMP header length check failed

IP packet too short

IP packet with version other than 4

IP packet with TTL equal to 0

IP packet with incorrect length

IP packet with broadcast destination address

Land attack (IP src address = dest address)

IP packet with checksum error

ICMP packet length greater than 64K

IP packet length greater than 64K

IP fragment length error

IP fragment overlap

IP fragment assembly timeout

TCP SYN flood attack

TCP port scan (port not in LISTEN state)

First packet of TCP session not SYN

UDP port scan (port not in LISTEN state)

Smurf attack (ping to IP broadcast address)

SFW discard flow requires packet to be dropped

SFW rules request packet to be discarded; attempting to create discard flow

No matching SFW rule; attempting to create discard flow

SFW [stateful firewall] discard packet contains non-configured IP option types

SFW rules request packet to be rejected; attempting to create reject flow

SFW rules request packet to be accepted; attempting to create forward or watch flow

SFW drop packet because of discard flow

SFW SYN defense

SFW application message too long

ICMP echo request dropped, because sequence number duplicated

ICMP echo request dropped. Too many echo requests without echo reply

ICMP echo reply dropped. No matching sequence number

SFW dropped TCP watch packet

SFW rules request FTP passive mode data packets to be accepted; attempting to create forward flow

SFW rules requests FTP active mode data packets to be accepted; attempting to create forward flow

Count—Total amount of times that a particular anomaly occurred, in thousands (k) or millions (m).

Rate—Anomaly events per second (eps).

Elapsed—Time since the same type of event last occurred.

Total IDS table entries— Number of entries in the IDS table. This is number not necessarily the sum of all entries displayed.

Total failed IDS table entry insertions—Number of IDS entries not allowed into the table because the table was full.

Total number of events (closed flows and anomalies detected)—Total number of events since the system was started or since show ids services was executed.

**Sample Output: show services ids destination-table**

```
user@host> show services ids destination-table
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address  Dest address  Time  Flags  Application
any            -> 10.58.255.146 36m12s SYN cookie
Bytes: 35.0 m, Packets: 822.0 k, Flows: 274.0 k, Anomalies: 2251.0 k
```

```
Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2606018
```

**Sample Output: show services ids destination-table terse**

```
user@host> show services ids destination-table terse
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address  Dest address  Time  Flags  Packets  Application
any            -> 10.58.255.146 36m47s S 842.0 k
```

```
Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2612864
```

**Sample Output: show services ids destination-table extensive**

```

user@host> show services ids destination-table extensive
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address  Dest address  Time  Flags  Application
any            -> 10.58.255.146 35m52s SYN cookie
Bytes: 34.0 m, Packets: 798.0 k, Flows: 266.0 k, Anomalies: 2251.0 k
Anomalies
Count Rate(eps) Elapsed
First packet of TCP session not SYN 160.0 k 0 14s
TCP source or destination port zero 634.0 k 154.6 3m37s
UDP source or destination port zero 633.0 k 170.0 3m37s
ICMP header length check failed 2875 0.9 3m37s
IP fragment assembly timeout 820.0 k 12.8 3m18s
UDP header length check failed 385 0.5 3m53s
TCP header length check failed 383 0.5 3m53s

Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2598063
    
```

**Sample Output: show services ids pair-table terse**

```

user@host> show services ids pair-table terse
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address  Dest address  Time  Flags  Packets  Application
10.58.255.18 -> 10.58.255.146 37m25s S 2538.0 k
10.58.255.29 -> 10.58.255.146 17m32s S 126.0 k
10.58.255.24 -> 10.58.255.146 17m32s S 125.0 k
10.58.255.16 -> 10.58.255.146 17m32s S 124.0 k
10.58.255.21 -> 10.58.255.146 17m32s S 126.0 k
10.58.255.30 -> 10.58.255.146 17m32s S 126.0 k
10.58.255.27 -> 10.58.255.146 17m32s S 125.0 k
10.58.255.25 -> 10.58.255.146 17m32s S 124.0 k
10.58.255.31 -> 10.58.255.146 17m32s S 125.0 k
10.58.255.28 -> 10.58.255.146 17m32s S 126.0 k
10.58.255.22 -> 10.58.255.146 17m32s S 126.0 k
10.58.255.19 -> 10.58.255.146 17m32s S 124.0 k
10.58.255.23 -> 10.58.255.146 17m32s S 125.0 k
10.58.255.17 -> 10.58.255.146 17m32s S 125.0 k
10.58.255.26 -> 10.58.255.146 17m32s S 125.0 k
10.58.255.20 -> 10.58.255.146 17m32s S 125.0 k

Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2627388
    
```

**Sample Output: show  
services ids pair-table  
brief**

```

user@host> show services ids pair-table brief limit 8
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address  Dest address  Time  Flags      Application
10.58.255.27   -> 10.58.255.146  18m 6s SYN cookie
Bytes: 100.0 m, Packets: 409.0 k, Flows: 144, Anomalies: 124.0 k

10.58.255.23   -> 10.58.255.146  18m 6s SYN cookie
Bytes: 101.0 m, Packets: 409.0 k, Flows: 148, Anomalies: 124.0 k

10.58.255.28   -> 10.58.255.146  18m 6s SYN cookie
Bytes: 101.0 m, Packets: 409.0 k, Flows: 150, Anomalies: 124.0 k

10.58.255.20   -> 10.58.255.146  18m 6s SYN cookie
Bytes: 101.0 m, Packets: 407.0 k, Flows: 141, Anomalies: 124.0 k

10.58.255.26   -> 10.58.255.146  18m 6s SYN cookie
Bytes: 100.0 m, Packets: 407.0 k, Flows: 144, Anomalies: 123.0 k

10.58.255.16   -> 10.58.255.146  18m 6s SYN cookie
Bytes: 100.0 m, Packets: 406.0 k, Flows: 138, Anomalies: 123.0 k

10.58.255.19   -> 10.58.255.146  18m 6s SYN cookie
Bytes: 100.0 m, Packets: 406.0 k, Flows: 140, Anomalies: 123.0 k

10.58.255.31   -> 10.58.255.146  18m 6s SYN cookie
Bytes: 101.0 m, Packets: 407.0 k, Flows: 142, Anomalies: 124.0 k
Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2641212

```

**Sample Output: show services ids pair-table extensive**

```

user@host> show services ids pair-table extensive limit 3
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address  Dest address  Time  Flags  Application

10.58.255.18  ->  10.58.255.146  38m41s SYN cookie
Bytes: 286.0 m, Packets: 2823.0 k, Flows: 324.0 k, Anomalies: 387.0 k
Anomalies
Count Rate(eps) Elapsed
First packet of TCP session not SYN 160.0 k 0.1 25s
TCP source or destination port zero 69.0 k 14.1 6m26s
UDP source or destination port zero 68.0 k 12.7 6m26s
ICMP header length check failed 318 0.1 7m6s
IP fragment assembly timeout 88.0 k 1.3 6m7s
UDP header length check failed 39 0.0 6m58s
TCP header length check failed 46 0.0 6m45s

10.58.255.23  ->  10.58.255.146  18m48s SYN cookie
Bytes: 104.0 m, Packets: 421.0 k, Flows: 230, Anomalies: 124.0 k
Anomalies
Count Rate(eps) Elapsed
TCP source or destination port zero 37.0 k 9.8 6m26s
UDP source or destination port zero 37.0 k 8.4 6m26s
IP fragment assembly timeout 48.0 k 1.0 6m7s
ICMP header length check failed 190 0.2 6m47s
UDP header length check failed 29 0.0 6m51s
TCP header length check failed 23 0.0 6m59s

10.58.255.25  ->  10.58.255.146  18m48s SYN cookie
Bytes: 104.0 m, Packets: 420.0 k, Flows: 232, Anomalies: 123.0 k
Anomalies
Count Rate(eps) Elapsed
TCP source or destination port zero 37.0 k 9.8 6m26s
UDP source or destination port zero 37.0 k 8.6 6m26s
IP fragment assembly timeout 48.0 k 1.5 6m7s
ICMP header length check failed 173 0.1 6m43s
UDP header length check failed 24 0.0 6m43s
TCP header length check failed 19 0.0 6m56s

Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2659291
    
```

**Sample Output: show services ids source-table terse**

```

user@host> show services ids source-table terse limit 3
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address  Dest address  Time  Flags  Packets  Application

10.58.255.18  ->  any 40m50s S 2060.0 k
10.58.255.20  ->  any 20m57s S 426.0 k
10.58.255.23  ->  any 20m57s S 426.0 k

Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2711898
    
```

**Sample Output: show services ids source-table brief**

```

user@host> show services ids source-table brief limit 3
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address  Dest address  Time  Flags      Application
10.58.255.18   ->         any  40m18s SYN cookie
Bytes: 251.0 m, Packets: 2011.0 k, Flows: 364.0 k, Anomalies: 387.0 k
10.58.255.30   ->         any  20m25s SYN cookie
Bytes: 107.0 m, Packets: 427.0 k, Flows: 264, Anomalies: 125.0 k
10.58.255.16   ->         any  20m25s SYN cookie
Bytes: 106.0 m, Packets: 426.0 k, Flows: 264, Anomalies: 124.0 k
Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2699588

```

**Sample Output: show services ids source-table extensive**

```

user@host> show services ids source-table extensive limit 3
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address  Dest address  Time  Flags      Application
10.58.255.18   ->         any  40m 0s SYN cookie
Bytes: 250.0 m, Packets: 1978.0 k, Flows: 356.0 k, Anomalies: 387.0 k
Anomalies                Count Rate(eps) Elapsed
TCP source or destination port zero      37.0 k  9.8  6m26s
First packet of TCP session not SYN      160.0 k  0.0  40s
TCP source or destination port zero      69.0 k  62.5  7m45s
UDP source or destination port zero      68.0 k  56.2  7m45s
ICMP header length check failed          319  0.1  7m49s
IP fragment assembly timeout             89.0 k  4.4  7m26s
UDP header length check failed            39  0.0  8m17s
TCP header length check failed            46  0.0  8m4s

10.58.255.30   ->         any  20m 7s SYN cookie
Bytes: 107.0 m, Packets: 427.0 k, Flows: 264, Anomalies: 125.0 k
Anomalies                Count Rate(eps) Elapsed
UDP source or destination port zero      38.0 k  65.5  7m45s
TCP source or destination port zero      37.0 k  38.1  7m45s
IP fragment assembly timeout             49.0 k  4.1  7m26s
TCP header length check failed            24  0.0  9m23s
ICMP header length check failed           165  0.1  8m6s
UDP header length check failed            26  0.0  8m13s

10.58.255.17   ->         any  20m10s SYN cookie
Bytes: 107.0 m, Packets: 426.0 k, Flows: 262, Anomalies: 125.0 k
Anomalies                Count Rate(eps) Elapsed
TCP source or destination port zero      38.0 k  55.  7m45s
UDP source or destination port zero      38.0 k  55.1  7m45s
ICMP header length check failed           147  0.1  7m50s
IP fragment assembly timeout             49.0 k  2.8  7m26s
TCP header length check failed            22  0.0  9m33s
UDP header length check failed            22  0.0  8m1s
Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2691423
Interface: sp-1/3/0, Service set: blue
NAT pool      Address          Port  Ports in use
d2-pool       10.59.16.100-10.59.16.100  4000-4002  1

```

