

Chapter 24

Stateful Firewall Services Operational Mode Commands

Table 48 summarizes the command-line interface (CLI) commands you can use to monitor and troubleshoot stateful firewall services interfaces. In the table, the commands are grouped by functionality. In the remainder of this chapter, they are explained alphabetically.

Table 48: Commands for Monitoring Stateful Firewall Services Interfaces

Task or Information to Monitor	CLI Command
Display stateful firewall flow information.	show services stateful-firewall on page 352
Clear stateful firewall flows.	clear services stateful-firewall flows on page 351

clear services stateful-firewall flows

Syntax	clear services stateful-firewall flows <service-set-name>
Description	Clear stateful firewall flows.
Options	none—Clear all stateful firewall flows for all service sets. <i>service-set-name</i> —(Optional) Clear all stateful firewall flows for a particular service set.
Output Fields	Interface—Name of an adaptive services interface. Service set—Name of the service set flows being cleared. Flow removed—Number of service set flows removed.
Required Privilege Level	view
Sample Output	<pre>user@host> clear services stateful-firewall flows Interface Service set Flow removed sp-0/3/0 svc_set_trust 0 sp-0/3/0 svc_set_untrust 0</pre>

show services stateful-firewall

Syntax show services stateful-firewall (conversations | flows <count>)
 <brief | extensive | terse>
 <destination-port *destination-port*>
 <destination-prefix *destination-prefix*>
 <source-port *source-port*>
 <source-prefix *source-prefix*>
 <interface *interface*>
 <protocol (ah | egp | esp | gre | icmp | igmp | ipip | ipv6 | ospf | pim | rsvp | sctp | tcp |
 udp)>
 <service-set *service-set*>
 <limit *number*>

Description Display information about a group of flows.

Options conversations—Display stateful firewall conversation information.

flows—Display flow table entries.

count—Display a count of the matching entries.

brief—(Optional) Display brief flow information.

extensive—(Optional) Display detailed flow information.

terse—(Optional) Display summary flow information.

destination-port *destination-port*—(Optional) Display information for a particular destination port.

destination-prefix *destination-prefix*—(Optional) Display information for a particular destination prefix.

source-port *source-port*—(Optional) Display information for a particular source port.

source-prefix *source-prefix*—(Optional) Display information for a particular source prefix.

interface *interface*—(Optional) Display information about a particular adaptive services interface.

protocol—(Optional) Display information about one of the following IP protocol types:

ah—IPSec Authentication Header protocol

egp—An exterior gateway protocol

esp—IPSec Encapsulating Security Payload protocol

gre—A generic routing encapsulation protocol

icmp—Internet Control Message Protocol

igmp—Internet Group Management Protocol

ipip—IP-within-IP Encapsulation Protocol

ipv6—IPv6 within IP

ospf—Open Shortest Path First protocol

pim—Protocol Independent Multicast protocol

rsvp—Resource Reservation Protocol

sctp—Stream Control Protocol

tcp—Transmission Control Protocol

udp—User Datagram Protocol

service-set *service-set*—(Optional) Display information for a particular service set.

limit *number*—(Optional) Display this maximum number of entries.

Required Privilege Level view

Output Fields Interface—Name of an adaptive services interface.

Service set—Name of a service set.

Flow Count—Number of flows in a session.

Flow—Information about the flow.

Protocol—Protocol used for this flow.

Source—Source prefix of the flow in the format *source-prefix:port*.

Destination—Destination prefix of the flow.

State—Status of the flow:

Drop—Drop all packets in the flow without response.

Forward—Forward the packet in the flow without looking at it.

Reject—Drop all packets in the flow with response.

Watch—Inspect packets in the flow.

Dir—Direction of the flow. It can be input (I) or output (O).

Frmcnt—Number of frames in the flow.

Source NAT—Original and translated source addresses are displayed if Network Address Translation (NAT) is configured on this particular flow or conversation.

Destin NAT—Original and translated destination IP addresses are displayed if NAT is configured on this particular flow or conversation.

Conversation—Information about a group of related flows.

AGL Protocol—Application Level Gateway Protocol.

Number of initiators—Number of flows that initiated a session.

Number of responders—Number of flows that responded in a session.

Byte count—Number of bytes forwarded in the flow.

TCP established—Whether a TCP connection was established: Yes or No.

TCP window size—Negotiated TCP connection window size, in bytes.

TCP acknowledge—TCP acknowledgment sequence number.

TCP tickle—Whether TCP inquiry mode is on (enabled or disabled) and the time remaining to send the next inquiry, in seconds.

Master flow—Flow that initiated the conversation.

Timeout—Lifetime of the flow, in seconds.

```

Sample Output: show services stateful-firewall flows count
user@host> show services stateful-firewall flows count
Interface      Service set      Flow Count
sp-1/3/0       green            2
    
```

```

Sample Output: show services stateful-firewall flows
user@host> show services stateful-firewall flows
Interface: sp-1/3/0, Service set: green
Flow
Prot  Source          Dest          State  Dir  Frm count
TCP   10.58.255.178:23 -> 10.59.16.100:4000 Forward O
TCP   10.58.255.50:33005-> 10.58.255.178:23 Forward I      1
     Source NAT 10.58.255.50:33005-> 10.59.16.100:4000
     Destin NAT 10.58.255.178:23 -> 0.0.0.0:4000
    
```

Sample Output: show services stateful-firewall conversations

```

user@host> show services stateful-firewall conversations
Interface: sp-1/3/0, Service set: green

Conversation: ALG Protocol: any, Number of initiators: 1,
Number of responders: 1

Flow
Prot  Source          Dest          State  Dir  Frmnt
TCP   10.58.255.50:33005-> 10.58.255.178:23 Forward I    13
     Source NAT 10.58.255.50:33005-> 10.59.16.100:4000
     Destin NAT 10.58.255.178:23 -> 0.0.0.0:4000
Byte count: 918
TCP established, TCP window size: 65535, TCP acknowledge: 2502627025
TCP tickle enabled, 0 seconds,
Master flow, Timeout: 30 seconds
TCP   10.58.255.178:23 -> 10.59.16.100:4000 Forward O    8

```

Sample Output: show services stateful-firewall flows destination-port 21

```

user@router> show services stateful-firewall flows destination-port 21
Interface: sp-0/3/0, Service set: svc_set_trust
Flow
State  Dir  Frm count
TCP   10.50.10.2:2143 -> 10.50.20.2:21 Watch O    0

```

Sample Output: show services stateful-firewall flows source-port 2143

```

user@router> show services stateful-firewall flows source-port 2143
Interface: sp-0/3/0, Service set: svc_set_trust
Flow
State  Dir  Frm count
TCP   10.50.10.2:2143 -> 10.50.20.2:21 Watch O    0

```

Sample Output: show services stateful-firewall conversations destination-port 21

```

user@host> show services stateful-firewall conversations destination-port 21
Interface: sp-0/3/0, Service set: svc_set_trust

Interface: sp-0/3/0, Service set: svc_set_untrust
Conversation: ALG protocol: ftp
Number of initiators: 1, Number of responders: 1
Flow
State  Dir  Frm count
TCP   10.50.10.2:2143 -> 10.50.20.2:21 Watch O    0
TCP   10.50.20.2:21 -> 10.50.10.2:2143 Watch I    0

```

Sample Output: show services stateful-firewall conversations source-port 2143

```

user@router> show services stateful-firewall conversations source-port 2143
Interface: sp-0/3/0, Service set: svc_set_trust

Interface: sp-0/3/0, Service set: svc_set_untrust
Conversation: ALG protocol: ftp
Number of initiators: 1, Number of responders: 1
Flow
State  Dir  Frm count
TCP   10.50.10.2:2143 -> 10.50.20.2:21 Watch O    0
TCP   10.50.20.2:21 -> 10.50.10.2:2143 Watch I    0

```

