Configuring Firewall Load Balancing

This chapter describes how to configure the CSS Firewall Load Balancing (FWLB) feature. Information in this chapter applies to all CSS models, except where noted.

This chapter contains the following major sections:

Overview of FWLB

FWLB enables you to configure a maximum of 15 firewalls per CSS. Configuring multiple firewalls can overcome performance limitations and remove the single point of failure when all traffic is forced through a single firewall. The FWLB feature ensures that the CSS will forward all packets with the same source and destination IP addresses through the same firewall. The CSS accomplishes this task by performing an XOR on the source and destination IP address.

Because the CSS can exist on either side of a firewall, it can balance traffic over multiple firewalls simultaneously. Each firewall is active and available in the load balancing firewall algorithm. The CSS uses the source and destination IP addresses in the algorithm to calculate which firewall to use for each flow.

A CSS monitors the health of a firewall by sending a custom ICMP keepalive request every second to the remote CSS on the other side of the firewall. If the CSS does not receive a keepalive request from the remote CSS for 3 to 16 seconds (configurable timeout), the CSS declares the firewall path unusable. Each CSS does not reply to the sending CSS, but transmits its own keepalive requests every second totally independent of the other CSS. For details about configuring the keepalive timeout, see the "Configuring a Keepalive Timeout for a Firewall" section.

FWLB acts as a Layer 3 device. Each connection to the firewall is a separate IP subnet. All flows between a pair of IP addresses, in either direction, traverse the same firewall. FWLB performs routing functions; it does not apply content rules to FWLB decisions.

Note Firewalls cannot perform Network Address Translation (NAT). If your configuration requires NATing, you must configure a content rule or source group on the CSS to provide this function.

To configure FWLB, you must define the following parameters for each path through the firewalls on both local and remote CSSs:

- Firewall index (identifies the physical firewall), local firewall IP address, remote firewall IP address, and CSS VLAN IP address
- Static route that the CSS will use for each firewall

See the sections that follow for information on configuring FWLB.

Firewall Synchronization

Firewall solutions providing Stateful Inspection, such as Check Point™ FireWall-1®, create and maintain virtual state for all connections through their devices, even for stateless protocols such as UDP and RPC. This state information, including details on Network Address Translation (NAT), is updated according to the data transferred. Different firewall modules running on different machines, such as those in a FWLB environment, can then share this information by mutually updating each other on the different state information of their connections.

Firewall synchronization (as shown in Figure 5-1) provides a significant benefit whereby each firewall device is aware of all connections in a firewall load balanced environment, making recovery of a failed firewall immediate and transparent to its users.

Note For details on configuring firewall synchronization, refer to your specific firewall documentation. In the case of a FireWall-1 device, you can find detailed configuration information in the *Check Point Software FireWall-1 Architecture and Administration* guide, in the chapter Active Network Management.

Configuring FWLB

A CSS must exist on each side of the firewall to control which firewall is selected for each flow. Within the firewall configuration, you must configure both the local and remote CSSs with the same firewall index number.

To avoid dropping packets, the CSS directs all packets between a pair of IP addresses across the same firewall. This applies to packets flowing in either direction. If a failure occurs on one path, all traffic will use the remaining path or balance traffic on the remaining paths.

Note You must define the firewall index before you define the firewall route or the CSS will return an error message. To configure the route, see the **ip route... firewall** command.

You must define firewall parameters for each path through the firewalls on both local and remote CSSs. Use the **ip firewall** command to define firewall parameters.

The syntax for this global configuration mode command is:

ip firewall *index local_firewall_address remote_firewall_address remote_switch_address*

The variables are:

Note Enter all IP addresses in dotted-decimal notation (for example, 192.168.11.1).

- *index* - The index number to identify the firewall. Enter a number from 1 to 254.
- *local_firewall_IP address* - The IP address of the firewall on a subnet connected to the CSS.
- *remote_firewall_IP address* - The IP address of the firewall on the remote subnet that connects to the remote CSS.
- *remote_switch_IP address* - The IP address of the remote CSS.

For example:

```
(config)# ip firewall 1 192.168.27.1 192.168.28.1 192.168.28.3
```

To delete a firewall index, enter:

```
(config)# no ip firewall 1
```

Caution When you delete a firewall index, all routes associated with that index are also deleted.

Configuring a Keepalive Timeout for a Firewall

A CSS sends a custom ICMP keepalive request to the remote CSS on the other side of the firewall every second. The two CSS switches at the endpoints of the firewall configuration must use the same firewall keepalive timeout value. Otherwise, routes on one CSS may not failover simultaneously with those on the other CSS, which could result in asymmetric routing across the firewalls.

Use the **ip firewall timeout** *number* command to specify the number of seconds the CSS will wait to receive a keepalive message from the remote CSS before declaring the firewall unreachable.The timeout range is 3 to 16 seconds. The default is 3 seconds.

Note The amount of time required for a firewall path to become available is unaffected by this command; it remains at three seconds.

For example, to set a timeout of 16 enter:

```
(config)# ip firewall timeout 16
```

To reset the firewall timeout to the default value of three seconds, enter:

```
(config)# no ip firewall timeout
```

Configuring an IP Static Route for a Firewall

To configure a static route for firewalls, use the **ip route... firewall** command. You can optionally set the administrative distance for the IP route.

Note You must define the firewall index before you define the firewall static route or the CSS will return an error message. To configure the firewall index, see the **ip firewall** command.

The syntax for this command is:

ip route *ip_address subnet_mask* **firewall** *index distance*

The variables are:

- *ip_address* - The destination network address. Enter the IP address in dotted-decimal notation (for example, 192.168.11.1).
- *subnet_mask* - The IP subnet mask. Enter the mask in either:
  - CIDR bitcount notation (for example, /24). Do not enter a space to separate the IP address from the prefix length.
  - Dotted-decimal notation (for example, 255.255.255.0).

- *index* - An existing index number for the firewall route. For information on configuring a firewall index, see the **ip firewall** command.
- *distance* - The optional administrative distance. Enter an integer from 1 to 254. A smaller number is preferable. The default value is 1.

Note The CLI prevents you from configuring IP static routes that are firewall routes and IP static routes that are not firewall routes with the same destination addresses and administrative costs. Make either the costs or the addresses unique between firewall and non-firewall routes.

For example:

```
(config)# ip route 192.168.2.0/24 firewall 1 2
```

To remove a firewall route, enter:

```
(config)# no ip route 192.168.2.0/24 firewall 1
```

Configuring OSPF to Advertise Firewall Routes

To advertise firewall routes from other protocols through OSPF, use the **ospf redistribute firewall** command. Redistribution of these routes makes them OSPF external routes.

You can optionally:

- Define the network cost for the route by including the **metric** option. Enter a number from 1 to 16,777,215. The default is 1.
- Define a 32-bit tag value to advertise each external route by including the **tag** option. You can use it to communicate information between autonomous system boundary routers (ASBRs).
- Advertise the routes as ASE type1 by including the **type1** option. The default is ASE type2. The difference between type1 and type2 is how the cost is calculated. For a type2 ASE, only the external cost (metric) is considered when comparing multiple paths to the same destination. For type1 ASE, the combination of the external cost and the cost to reach the ASBR is used.

For example:

```
(config)# ospf redistribute firewall metric 3 type1
```

To stop advertising firewall routes, enter:

```
(config)# no ospf redistribute firewall
```

Configuring RIP to Advertise Firewall Routes

To advertise firewall routes from other protocols through RIP, use the **rip redistribute firewall** command. You may also include an optional metric that the CSS uses when advertising this route. Enter a number from 1 to 15. The default is 1.

For example, to advertise a firewall route through RIP, enter:

```
(config)# rip redistribute firewall 3
```

Note By default, RIP advertises RIP routes and local routes for interfaces running RIP. This command also advertises other routes.

To stop advertising firewall routes, enter:

```
(config)# no rip redistribute firewall
```

Example of FWLB Static Route Configuration

This section describes how to configure FWLB for two firewalls between two CSSs. To configure a static route for FWLB, you must define the following parameters for each path through the firewalls on both the local (client) and a remote (server) CSSs:

- Firewall index (identifies the physical firewall), local firewall IP address, remote firewall IP address, and CSS VLAN IP address. You must configure the **ip firewall** command before you configure the static route or the CSS will report an error.
- Static route each CSS will use for each firewall.

To configure CSS-A (the client side of the network configuration) as shown in Figure 5-1:

1. Use the **ip firewall** command to define firewall 1. For example:

```
(config)# ip firewall 1 192.168.28.1 192.168.27.1 192.168.27.3
```

2. Use the **ip route** command to define the static route for firewall 1. For example:

```
(config)# ip route 192.168.2.0/24 firewall 1
```

3. Use the **ip firewall** command to define firewall 2. For example:

```
(config)# ip firewall 2 192.168.28.2 192.168.27.2 192.168.27.3
```

4. Use the **ip route** command to define the static route for firewall 2. For example:

```
(config)# ip route 192.168.2.0/24 firewall 2
```

To configure CSS-B (the server side of the network configuration) as shown in Figure 5-1:

1. Use the **ip firewall** command to define firewall 1. For example:

```
(config)# ip firewall 1 192.168.27.1 192.168.28.1 192.168.28.3
```

2. Use the **ip route** command to define the static route for firewall 1. For example:

```
(config)# ip route 0.0.0.0/0 firewall 1
```

3. Use the **ip firewall** command to define firewall 2. For example:

```
(config)# ip firewall 2 192.168.27.2 192.168.28.2 192.168.28.3
```

4. Use the **ip route** command to define the static route for firewall 2. For example:

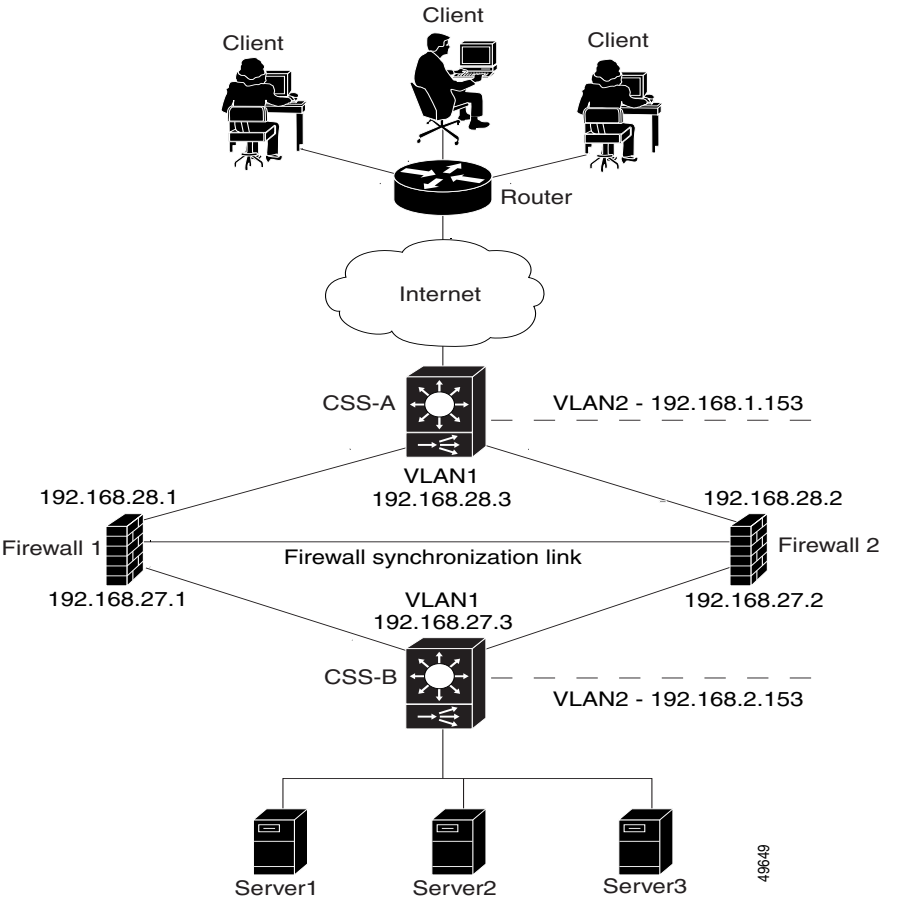
```
(config)# ip route 0.0.0.0/0 firewall 2
```

Firewall configurations are displayed in the IP portion of the running-config. For example:

```
(config)# show running-config
```

Figure 5-1 illustrates the configuration defined in the firewall commands.

Figure 5-1 Example of FWLB



Configuring FWLB with VIP and Virtual Interface Redundancy

Configure FWLB with VIP and virtual interface redundancy to provide the following benefits:

- Very fast failover (typically 1 to 3 seconds)
- No single point of failure
- All CSSs forward traffic (active-backup configuration)

Note For details on configuring VIP and virtual interface Redundancy, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

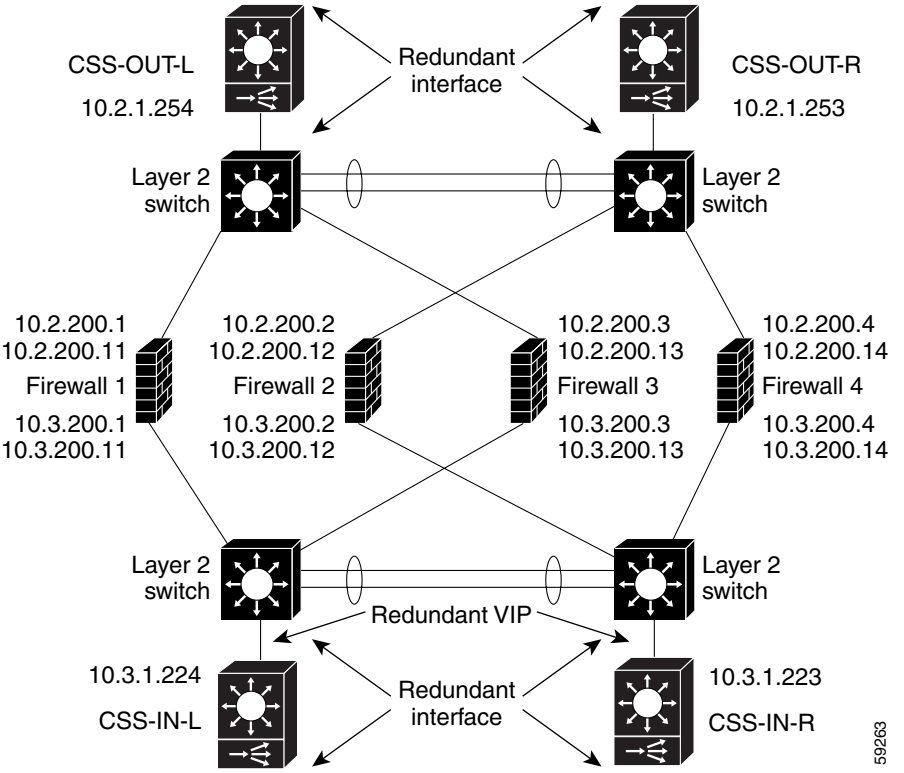
This configuration consists of two redundant CSSs and two Layer 2 devices on either side of the firewall. If a CSS fails, the redundant CSS on the same side of the firewall assumes the additional load.

Note When you configure FWLB with VIP and virtual interface redundancy, do not configure shared VIPs. Shared VIPs are not supported by the FWLB topology. For more information about shared VIPs, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

You must configure the VIPs on the CSS that has the services directly connected to it or connected through a Layer 2 device. Do not configure content rules with VIPs on a CSS when the services are located on the other side of the firewall and connected to another CSS participating in FWLB. This type of configuration will result in asymmetric paths and could cause firewalls performing stateful inspection to tear down connections.

In Figure 5-2, odd-numbered firewalls are connected to the Layer 2 switches servicing the CSS-OUT-L and CSS-IN-L CSSs. Even-numbered firewalls are connected to the Layer 2 switches servicing the CSS-OUT-R and CSS-IN-R CSSs.

Figure 5-2 FWLB with VIP/Interface Redundancy Configuration



Each firewall must have two addresses on either side of it. The first address is used for the next hop on the lower-cost static (primary) path. The second address is used for the next hop on the higher-cost floating-static (secondary) path.

Set the floating-static paths with a higher cost (typically a cost of 10) than those associated with the static paths (typically a cost of 1). If a CSS fails (for example, CSS-OUT-L), CSS-OUT-R will use the higher cost path to send traffic to CSS-IN-L.

If the firewall supports it, you can use multinetting by configuring multiple addresses on the firewall. If the firewall does not support multiple addresses per physical interface, use the ap-kal-fwlb-multinet script to simulate multiple addresses for the firewall. The script takes arguments of "realAddress secondaryAddress". The script creates a static ARP entry for each firewall interface.

Note You can also enter the static ARP entries manually. However, the benefit of the script is that it will change the ARP entries if you replace the firewall and the MAC address changes.

Failover time is very fast at 1 to 3 seconds, because:

- Floating-static path is already up
- Firewall path information has been exchanged
- Circuits are up

If a Layer 2 switch fails, traffic will rehash over every other firewall. If there are an even number of firewalls, 50 percent of the traffic will rehash to the same firewalls.

Note If you configure redundant interfaces on both sides of a CSS, use critical services to ensure that if one interface fails over to backup, the other interface does the same. If you are implementing multiple interfaces, use firewall interfaces as critical services on external CSSs, and firewall interfaces (configured as service type redundancy-up) and backend servers on internal CSSs. For details on configuring critical services and configuring redundant uplink services, refer to the *Cisco Content Services Switch Redundancy Configuration Guide*.

Example of Firewall and Route Configurations

The following **ip firewall** and **ip route** example configurations are valid for Figure 5-2 with four active firewalls.

CSS-OUT-L Configuration

```
ip firewall 1 10.2.200.1 10.3.200.1 10.3.1.224
ip firewall 2 10.2.200.2 10.3.200.2 10.3.1.224
ip firewall 3 10.2.200.3 10.3.200.3 10.3.1.224
ip firewall 4 10.2.200.4 10.3.200.4 10.3.1.224
ip firewall 11 10.2.200.11 10.3.200.11 10.3.1.223
ip firewall 12 10.2.200.12 10.3.200.12 10.3.1.223
ip firewall 13 10.2.200.13 10.3.200.13 10.3.1.223
ip firewall 14 10.2.200.14 10.3.200.14 10.3.1.223
ip route 10.3.0.0 255.255.0.0 firewall 1 1
ip route 10.3.0.0 255.255.0.0 firewall 2 1
ip route 10.3.0.0 255.255.0.0 firewall 3 1
ip route 10.3.0.0 255.255.0.0 firewall 4 1
ip route 10.3.0.0 255.255.0.0 firewall 11 10
ip route 10.3.0.0 255.255.0.0 firewall 12 10
ip route 10.3.0.0 255.255.0.0 firewall 13 10
ip route 10.3.0.0 255.255.0.0 firewall 14 10
```

CSS-OUT-R Configuration

```
ip firewall 11 10.2.200.11 10.3.200.11 10.3.1.223
ip firewall 12 10.2.200.12 10.3.200.12 10.3.1.223
ip firewall 13 10.2.200.13 10.3.200.13 10.3.1.223
ip firewall 14 10.2.200.14 10.3.200.14 10.3.1.223
ip firewall 1 10.2.200.1 10.3.200.1 10.3.1.224
ip firewall 2 10.2.200.2 10.3.200.2 10.3.1.224
ip firewall 3 10.2.200.3 10.3.200.3 10.3.1.224
ip firewall 4 10.2.200.4 10.3.200.4 10.3.1.224
ip route 10.3.0.0 255.255.0.0 firewall 11 1
ip route 10.3.0.0 255.255.0.0 firewall 12 1
ip route 10.3.0.0 255.255.0.0 firewall 13 1
ip route 10.3.0.0 255.255.0.0 firewall 14 1
ip route 10.3.0.0 255.255.0.0 firewall 1 10
ip route 10.3.0.0 255.255.0.0 firewall 2 10
ip route 10.3.0.0 255.255.0.0 firewall 3 10
ip route 10.3.0.0 255.255.0.0 firewall 4 10
```

CSS-IN-L Configuration

```
ip firewall 1 10.3.200.1 10.2.200.1 10.2.1.254
ip firewall 2 10.3.200.2 10.2.200.2 10.2.1.254
ip firewall 3 10.3.200.3 10.2.200.3 10.2.1.254
ip firewall 4 10.3.200.4 10.2.200.4 10.2.1.254
ip firewall 11 10.3.200.11 10.2.200.11 10.2.1.253
ip firewall 12 10.3.200.12 10.2.200.12 10.2.1.253
ip firewall 13 10.3.200.13 10.2.200.13 10.2.1.253
ip firewall 14 10.3.200.14 10.2.200.14 10.2.1.253
ip route 0.0.0.0 0.0.0.0 firewall 1 1
ip route 0.0.0.0 0.0.0.0 firewall 2 1
ip route 0.0.0.0 0.0.0.0 firewall 3 1
ip route 0.0.0.0 0.0.0.0 firewall 4 1
ip route 0.0.0.0 0.0.0.0 firewall 11 10
ip route 0.0.0.0 0.0.0.0 firewall 12 10
ip route 0.0.0.0 0.0.0.0 firewall 13 10
ip route 0.0.0.0 0.0.0.0 firewall 14 10
```

CSS-IN-R Configuration

```
ip firewall 11 10.3.200.11 10.2.200.11 10.2.1.253
ip firewall 12 10.3.200.12 10.2.200.12 10.2.1.253
ip firewall 13 10.3.200.13 10.2.200.13 10.2.1.253
ip firewall 14 10.3.200.14 10.2.200.14 10.2.1.253
ip firewall 1 10.3.200.1 10.2.200.1 10.2.1.254
ip firewall 2 10.3.200.2 10.2.200.2 10.2.1.254
ip firewall 3 10.3.200.3 10.2.200.3 10.2.1.254
ip firewall 4 10.3.200.4 10.2.200.4 10.2.1.254
ip route 0.0.0.0 0.0.0.0 firewall 11 1
ip route 0.0.0.0 0.0.0.0 firewall 12 1
ip route 0.0.0.0 0.0.0.0 firewall 13 1
ip route 0.0.0.0 0.0.0.0 firewall 14 1
ip route 0.0.0.0 0.0.0.0 firewall 1 10
ip route 0.0.0.0 0.0.0.0 firewall 2 10
ip route 0.0.0.0 0.0.0.0 firewall 3 10
ip route 0.0.0.0 0.0.0.0 firewall 4 10
```

Displaying Firewall Flow Summaries

Use the **show flows** command to display the flow summary for a source IP address, or for a specific source address and its destination IP address on a Switch Processor (SP) in a CSS. You can display up to 4096 flows per SP.

This information allows you to:

- Identify which firewall is used for a particular flow
- View flows to ensure the proper operation of FWLB

The syntax is:

show flows *source_address destination_address*

The variables are:

- *source_address* - The source IP address for the flows. Enter the address in dotted-decimal format (for example, 192.168.11.1).
- *destination_address* - The destination IP address. Enter the address in dotted-decimal format (for example, 192.168.11.1).

For example:

```
(config)# show flows 192.165.22.1 192.163.2.3
```

To display the flows for a specific source IP address, enter:

```
(config)# show flows 192.165.22.1
```

To display the flows for specific source and destination IP addresses, enter:

```
(config)# show flows 192.165.22.1 192.163.2.3
```

Table 5-1 describes the fields in the **show flows** output.

Table 5-1 Field Descriptions for the show flow Command

Field	Description
Src Address	The source address for the flow
SPort	The source port for the flow
Dst Address	The destination address for the flow
DPort	The destination port for the flow
NAT Dst Address	The NAT destination address
Prot	The protocol of the flow (TCP or UDP)
InPort	The interface port for the in flow
OutPort	The interface port for the out flow

Displaying Firewall IP Routes

Use the **show ip routes firewall** command to display all static firewall routes. For example:

```
(config)# show ip routes firewall
```

Table 5-2 describes the fields in the **show ip routes firewall** output.

Table 5-2 Field Descriptions for the show ip routes firewall Command

Field	Description
Prefix/length	The IP address and prefix length for the route.
Next hop	The IP address for the next hop.
If	The ifIndex value that identifies the local interface through which the next hop of this route should be reached.
Type	The type of the route entry. The type is remote.
Proto	The protocol for the route, firewall.
Age	The maximum age for the route.
Metric	The metric cost for the route.

Displaying Firewall IP Information

Use the **show ip firewall** command to display the configured values of the IP firewall keepalive timeout and the state of each firewall path configured on the CSS. For example:

```
(config)# show ip firewall
```

Table 5-3 describes the fields in the **show ip routes** output.

Table 5-3 Field Descriptions for the show ip routes firewall Command

Field	Description
IP Firewall KAL Timeout	The number of seconds the CSS will wait to receive a keepalive message from the remote CSS before declaring the firewall unreachable.
Firewall Index	The index number to identify the firewall.
State	The current state of the connection to the remote switch (Init, Reachable, or Unreachable).
Next Hop	The IP address used for the next hop.
Remote Firewall	The IP address of the firewall on the remote subnet that connects to the remote CSS.
Remote Switch	The IP address of the remote CSS.
Time Since Last KAL Tx	The length of time since the last keepalive message was transmitted.
Time Since Last KAL Rx	The length of time since the last keepalive message was received.