



Firewall Load Balancing

This chapter describes the Firewall Load Balancing (FWLB) feature. It includes the following sections:

- FWLB Overview, page 6-1
- Configurable FWLB Features, page 6-2
- Required FWLB Configuration Tasks, page 6-4
- FWLB Configuration Restrictions, page 6-4
- Monitoring and Maintaining FWLB, page 6-9
- Example of Firewall Load Balancing, page 6-9
- Example of Multiple Firewall Farms, page 6-11



Note

For detailed information about the commands described in this chapter, refer to *Appendix A*, “Command Reference.”

FWLB Overview

The FWLB feature allows you to configure load balancing on Catalyst 4840G SLB switches on both sides of a firewall farm. On a group of servers (a server farm), traffic is balanced by being allowed to travel over any available path; however, when traffic goes through a group of firewalls (a firewall farm), the reverse path must include the same firewall as the original path. Each of the FWLB switches can actively choose the same firewall for the reverse traffic that the other load-balancing switch chose for the original traffic.

Layer 3 firewalls, which have IP-addressable interfaces, are supported by IOS SLB firewall load balancing if they are subnet-adjacent to the firewall load-balancing device and they have unique MAC addresses. To send a user packet to the chosen firewall, the load balancer does not modify the IP address in the packet; instead it determines which interface to use and changes the appropriate Layer 2 headers accordingly. This is the standard dispatch routing method used by FWLB.

Layer 2 firewalls do not have IP addresses and are not visible to the load-balancing function. A Layer 2 firewall is supported by placing it between two IP-addressable interfaces.

Many Layer 3 firewalls can reside off a single Layer 3 interface on the load balancer (for example, a single LAN), but only one Layer 2 firewall can reside off each interface.

When you configure the load balancer, the Layer 3 firewall is defined by its IP address. The Layer 2 firewall is defined by the IP address of the interface of the device on the other side of the firewall.

**Note**

IOS SLB firewall load balancing *must* examine incoming packets and perform route lookup. On Catalyst 4840G SLB switches, some additional packets might need to be examined. FWLB will impact internal (secure) side routing performance and must be considered in the complete design.

Firewall farm load balancing provides the following capabilities:

- Connections initiated from both sides of a firewall farm are load balanced.
- Traffic load is distributed among a group of firewalls (the firewall farm).
- All packets for a connection travel through the same firewall. Subsequent connections can be “sticky,” ensuring that they are assigned to the same firewall.
- Probes are used to detect and recover firewall failures.
- Firewall load balancer redundancy is provided.
- Proxy firewalls are supported.

The “Example of Firewall Load Balancing” section on page 6-9 shows how load balancing works in FWLB.

Configurable FWLB Features

This section describes the features you can configure in FWLB:

- Delayed Removal of TCP Connection Context, page 6-2
- FWLB Algorithm, page 6-2
- Maximum Connections, page 6-3
- Probes, page 6-3
- Sticky Connections, page 6-3

Delayed Removal of TCP Connection Context

Because of anomalies in ordering of IP packets, FWLB might encounter the termination of a TCP connection (a finish [FIN] or reset [RST]) followed by other packets for the connection. This problem usually occurs when TCP connection packets can follow multiple paths. To correctly redirect the packets that arrive after the connection is terminated, FWLB retains the TCP connection information, or context, for a length of time you specify using a delay timer.

FWLB Algorithm

For each firewall interface used in FWLB, you configure the firewall interface IP address on the Catalyst 4840G SLB switch. FWLB uses a Layer 3 hash algorithm for balancing traffic across the firewalls in a firewall farm. The hash algorithm uses the source and destination IP addresses of incoming traffic to select the firewall that will handle the connection request.

FWLB can also be configured to hash both IP addresses and Layer 4 port number.

Maximum Connections

You can configure the maximum number of TCP and UDP connections that will be directed to each firewall farm. When the number of such connections reaches the maximum value specified for the entire farm, the FWLB feature drops any new connections.

Probes

FWLB supports both HTTP probes and ping probes. Probes are used to verify the connectivity through each firewall. All firewalls defined in the firewall farm must be probed.

You can configure more than one probe for each firewall in a firewall farm. If a firewall fails for one probe, it is considered failed. After the firewall recovers, all probes must acknowledge its recovery before it is restored to service.

Firewall Load Balancing

Probes detect firewall failures. All firewalls associated with the firewall farm are probed.

HTTP Probes

To eliminate password problems, make sure you configure the HTTP probe to expect status code 401. See the **expect** command in Appendix A for details.

Use the **ip http server** command to configure an HTTP server on the switch. For more information see the description of the **ip http server** command in the *Cisco IOS Configuration Fundamentals Command Reference*.

Ping Probes

Ping probes verify connectivity for devices being server load-balanced and for firewalls being firewall load-balanced

Sticky Connections

The sticky connections feature allows new connections from a client IP address to be assigned to the same firewall as previous connections from the same client address. “Sticky objects” are created to track client assignments. These objects remain in the FWLB database for a configurable period of time after the last sticky connection is deleted. If the timer is configured on a firewall farm, new connections from a client are sent to the same firewall that handled the previous client connection, provided one of the following is true:

- A connection for the same client already exists.
- The amount of time between the end of a previous connection from the client and the start of a new connection is within the timer duration.

For FWLB, sticky connections handle subnets as well as IP addresses.

FWLB Configuration Restrictions

The following restrictions apply to firewall load-balancing devices:

- Ethernet is required between each firewall load-balancing device and each firewall.
- There can be no more than one active firewall load-balancing device on each side of the firewall farm. Each firewall must have its own unique MAC address and must be Layer 2-adjacent to each device. The firewalls can be connected to individual interfaces on the device, or they can all share a VLAN and connect using a single interface.
- Each Layer 2 firewall must be connected to a single Layer 3 (IP) interface.
- Traffic with a destination IP address on the same subnet as the configured firewall IP addresses is not load balanced. (Such traffic could be a firewall console session or other traffic on the firewall LAN.)
- Redundancy on the firewall farm is optional.
- Real servers and firewalls must be configured on Fast Ethernet interfaces.
- Clients must be configured on Gigabit Ethernet interfaces, except when you use the **ip slb fast-ethernet client** command, in which case the clients can be configured on Fast Ethernet ports 37 to 40.

Required FWLB Configuration Tasks

This section describes the tasks required to configure a set of firewall load balancers on your Catalyst 4840G SLB switch. The following sections describe how to configure firewall load-balancing:

- Configuring FWLB, page 6-4
- Verifying the Firewall Farm, page 6-6
- Verifying Firewall Connectivity, page 6-6
- Configuring a Ping Probe, page 6-7
- Configuring an HTTP Probe, page 6-8

Configuring FWLB

To configure FWLB, perform these commands, beginning in global configuration mode:

	Command	Purpose
Step 1	FWLB-Switch (config)# ip slb firewallfarm <i>firewallfarm_name</i> FWLB-Switch (config-slb-firewallfarm)#	Adds a firewall to the FWLB configuration and initiates firewall farm configuration mode.
Step 2	FWLB-Switch(config-slb-fw)# access [source <i>source-ip-address network-mask</i>] [destination <i>destination-ip-address</i> <i>network-mask</i>]	Routes specific flows to a firewall farm. See the access command for details.
Step 3	FWLB-Switch (config-slb-fw)# real <i>ip-address</i>	Identifies a firewall as a member of a firewall farm and initiates real server configuration mode. See the real (firewall farm) command for details.

	Command	Purpose
Step 4	FWLB-Switch(config-slb-fw-real) # probe <i>name</i>	Associates a probe with the firewall. See the real (firewall farm) command for details.
Step 5	FWLB-Switch(config-slb-fw-real) # weight <i>weighting-value</i>	(Optional) Specifies the firewall's workload capacity relative to other firewalls in the firewall farm. See the weight (firewall farm real firewall) command for details.
Step 6	FWLB-Switch(config-slb-fw-real) # inservice	Enables the firewall for use by the firewall farm and by SLB. See the inservice (firewall farm real server) command for details.
Step 7	FWLB-Switch(config-slb-fw) # predictor hash address [<i>port</i>]	(Optional) Specifies whether the source and destination port numbers and IP addresses are to be used in the hash algorithm, which determines how a firewall is selected. See the predictor hash address (firewall farm) command for details.
Step 8	FWLB-Switch(config-slb-fw) # replicate casa <i>listening-ip remote-ip port-number</i> [<i>interval</i>] [password [0 7] <i>password</i> [<i>timeout</i>]]	(Optional) Configures a stateful backup of FWLB decision tables to a backup switch. See the replicate casa (firewall farm) command for details.
Step 9	FWLB-Switch(config-slb-fw) # tcp	(Optional) Initiates TCP protocol configuration mode. See the tcp command for details.
Step 10	FWLB-Switch(config-slb-fw-tcp) # delay <i>duration</i>	(Optional) Specifies the amount of time FWLB maintains TCP connection context after a connection has been terminated. See the delay (virtual server) command for details.
Step 11	FWLB-Switch(config-slb-fw-tcp) # idle <i>duration</i>	(Optional) Specifies the minimum amount of time FWLB maintains connection context in the absence of packet activity. See the idle (firewall farm TCP protocol) command for details.
Step 12	FWLB-Switch(config-slb-fw-tcp) # maxconns <i>number-conns</i>	(Optional) Specifies the maximum number of active connections allowed on the firewall farm at one time. See the maxconns (firewall farm TCP protocol) command for details.
Step 13	FWLB-Switch(config-slb-fw-tcp) # sticky <i>duration</i> [<i>netmask netmask</i>]	(Optional) Specifies that connections from the same IP address use the same firewall if either of the following conditions is met: <ul style="list-style-type: none"> Any connection from that IP address exists. For a period of time, defined by <i>duration</i>, after the last connection is destroyed. See the sticky (firewall farm TCP protocol) command for details.
Step 14	FWLB-Switch(config-slb-fw) # udp	(Optional) Initiates UDP protocol configuration mode. See the udp command for details.
Step 15	FWLB-Switch(config-slb-fw-udp) # idle <i>duration</i>	(Optional) Specifies the minimum amount of time FWLB maintains connection context in the absence of packet activity. See the idle (firewall farm UDP protocol) command for details.

	Command	Purpose
Step 16	FWLB-Switch(config-slb-fw-udp) # maxconns <i>number-conns</i>	(Optional) Specifies the maximum number of active connections allowed on the firewall farm at one time. See the maxconns (firewall farm UDP protocol) command for details.
Step 17	FWLB-Switch(config-slb-fw-udp) # sticky <i>duration [netmask netmask]</i>	(Optional) Specifies that connections from the same IP address use the same firewall if either of the following conditions is met: <ul style="list-style-type: none"> Any connection from that IP address exists. For a period of time, defined by <i>duration</i>, after the last connection is destroyed. See the sticky (firewall farm UDP protocol) command for details.
Step 18	FWLB-Switch(config-slb-fw) # inservice	Enables the firewall farm for use by SLB. See the inservice (firewall farm) command for details.
Step 19	FWLB-Switch (config-slb-fw-real) # exit	Returns to firewall farm configuration mode.
Step 20	FWLB-Switch (config) # end FWLB-Switch#	Returns to global configuration mode.

Verifying the Firewall Farm

The following example shows how to display the status of the real firewalls associated with the firewall farm FIRE1:

```
Router# show ip slb reals
```

```
real          farm name      weight  state          conns
-----
10.1.1.2      FIRE1           8       OPERATIONAL    0
10.1.2.2      FIRE1           8       OPERATIONAL    0
```

The following example shows how to display the configuration and status of the firewall farm FIRE1:

```
Router# show ip slb firewallfarm
```

```
firewall farm  hash      state      reals
-----
FIRE1          IPADDR   OPERATIONAL  2
```

Verifying Firewall Connectivity

To verify that firewall load-balancing has been configured and is operating correctly, follow these steps:

- Step 1** From the firewall load-balancing switch, ping the external real servers (the ones outside the firewall).
- Step 2** From the clients, ping the internal real servers (the ones inside the firewall).

Step 3 Enter the **show ip slb stats** command to display detailed firewall load balancing packet information:

```
FWLB-Switch# show ip slb stats
Pkts via normal switching: 0
Pkts via special switching: 0
Connections Created: 1911871
Connections Established: 1967754
Connections Destroyed: 1313251
Connections Reassigned: 0
Zombie Count: 0
Connections Reused: 59752
Connection Flowcache Purges:1776582
Failed Connection Allocs: 17945
Failed Real Assignments: 0
FWLB-Switch#
```

Step 4 Enter the **show ip slb real detail** command to display detailed firewall connection statistics:

```
SLB-Switch# show ip slb real detail
10.1.1.3, FIRE1, state = OPERATIONAL, type = firewall
  conns = 299310, dummy_conns = 0, maxconns = 4294967295
  weight = 10, weight(admin) = 10, metric = 104, remainder = 2
  total conns established = 1074779, hash count = 4646
  server failures = 0
  interface FastEthernet1/0, MAC 0010.f68f.7020
```

Step 5 Enter the **show ip slb conns** command to display detailed information about the active firewall load-balancing connections:

```
FWLB-Switch# show ip slb conns

vserver          prot client          real          state          nat
-----
FirewallTCP      TCP  80.80.50.187:40000  10.1.1.4      ESTAB          none
FirewallTCP      TCP  80.80.50.187:40000  10.1.1.4      ESTAB          none
FirewallTCP      TCP  80.80.50.187:40000  10.1.1.4      ESTAB          none
FirewallTCP      TCP  80.80.50.187:40000  10.1.1.4      ESTAB          none
FirewallTCP      TCP  80.80.50.187:40000  10.1.1.4      ESTAB          none
FWLB-Switch#
```

Configuring a Ping Probe

Ping probes verify connectivity for devices being server load balanced and for firewalls being firewall load balanced.

To configure a ping probe, follow these steps, beginning in global configuration mode:

	Command	Purpose
Step 1	FWLB-Switch(config)# ip slb probe name ping	Configures the FWLB probe name and changes to ping configuration submenu.
Step 2	FWLB-Switch(config-slb-probe)# address [ip-address]	Configures the ping probe to receive responses from an IP address.
Step 3	FWLB-Switch(config-slb-probe)# faildetect number-of-pings	(Optional) Specifies the number of consecutive unanswered pings that constitutes failure of the firewall.

	Command	Purpose
Step 4	FWLB-Switch(config-slb-probe)# interval <i>seconds</i>	(Optional) Configures the ping probe transmit timers.
Step 5	FWLB-Switch(config-slb-probe)# exit	Returns to firewall farm configuration mode.
Step 6	FWLB-Switch(config)# ip slb firewallfarm <i>firewallfarm-name</i>	Specifies a firewall farm.
Step 7	FWLB-Switch(config)# probe <i>probe-name</i>	Specifies an HTTP probe on the real server.
Step 8	FWLB-Switch(config)# end	Returns to global configuration mode.

This example shows how to configure a ping probe named TREADER:

```
FWLB-Switch(config)# ip slb probe TREADER ping
FWLB-Switch(config-slb-probe)# address 13.13.13.13
FWLB-Switch(config-slb-probe)# faildetect 16
FWLB-Switch(config-slb-probe)# interval 11
FWLB-Switch(config-slb-probe)# exit
FWLB-Switch(config)# ip slb firewallfarm FIRE1
FWLB-Switch(config-slb-fw)# probe TREADER
FWLB-Switch(config-slb-fw)# end
```

To verify that the ping probe is configured correctly, use the following **show ip slb probe** command:

```
FWLB-Switch# show ip slb probe

Server:Port          State          Outages  Current  Cumulative
-----
13.13.13.13:80      OPERATIONAL    0 never   00:00:00
```

Configuring an HTTP Probe

HTTP probes verify connectivity for devices being server load balanced, and for firewalls being firewall load balanced.

To configure an HTTP probe, follow these steps, beginning in global configuration mode:

	Command	Purpose
Step 1	FWLB-Switch(config)# ip slb probe <i>name</i> http	Configures the HTTP probe name and changes to HTTP configuration submenu.
Step 2	FWLB-Switch(config-slb-probe)# request method { get post head name <i>name</i> [<i>url path</i>]}	(Optional) Configures the method used to perform the request to the server. See the request method , request url command for details.
Step 3	Router(config-slb-probe)# address [<i>ip-address</i>]	(Optional) Configures the HTTP probe to receive responses from an IP address. See the address (http probe) command for details.
Step 4	Router(config-slb-probe)# expect [status number] [regex <i>regular-expression</i>]	(Optional) Configures the expected HTTP status code or regular expression. See the expect command for details.
Step 5	FWLB-Switch(config-slb-probe)# interval <i>seconds</i>	Configures the HTTP probe transmit timers. See the interval (http probe) command for details.

	Command	Purpose
Step 6	FWLB-Switch(config-slb-probe)# header { <i>field-name</i> }	(Optional) Configures authentication values for the HTTP probe. See the header command for details.
Step 7	FWLB-Switch(config-slb-probe)# credentials { <i>username</i> [<i>password</i>]}	(Optional) Configures authentication values for the HTTP probe. See the credentials command for details.
Step 8	FWLB-Switch(config-slb-probe)# exit	Returns to firewall farm configuration mode.

This example shows how to configure an HTTP probe named DOGULA:

```
FWLB-Switch(config)# ip slb probe DOGULA http
FWLB-Switch(config-slb-probe)# request method post url /probe.cgi?all
FWLB-Switch(config-slb-probe)# header Cookie
FWLB-Switch(config-slb-probe)# credentials Semisweet chips
FWLB-Switch(config-slb-probe)# exit
```

To verify that the HTTP probe is configured correctly, use the following **show ip slb probe** commands:

```
FWLB-Switch# show ip slb probe
DOGULA (http) 3 reals
FWLB-Switch# show ip slb probe detail
```

Server:Port	State	Outages	Current	Cumulative
10.1.1.1:80	OPERATIONAL	0	never	00:00:00
10.1.1.2:80	OPERATIONAL	0	never	00:00:00
10.1.1.3:80	OPERATIONAL	0	never	00:00:00

Monitoring and Maintaining FWLB

You can display runtime information about FWLB using these commands in EXEC mode:

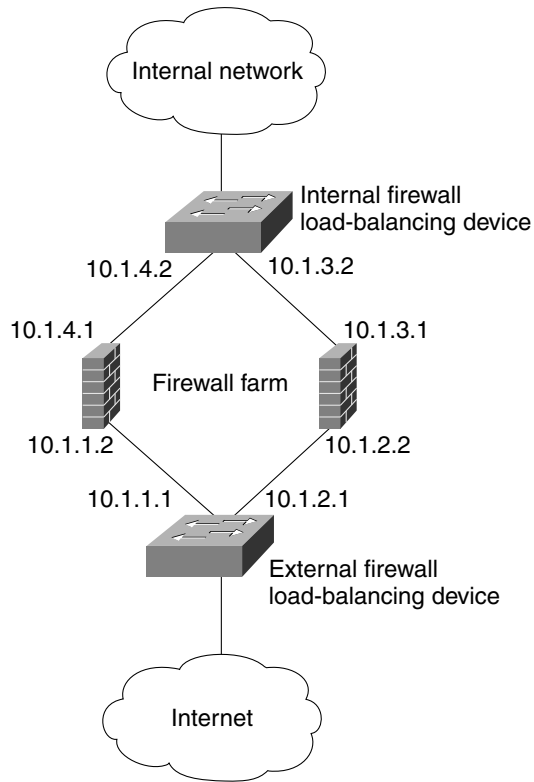
Command	Purpose
show ip slb conns [<i>client ip_address</i>] [<i>detail</i>]	Displays the connections handled by FWLB.
show ip slb probe [<i>name probe_name</i>] [<i>detail</i>]	Displays information about FWLB HTTP probes configured on real firewalls.
show ip slb reals [<i>detail</i>]	Displays information about the real firewalls.
show ip slb firewallfarm [<i>name firewallfarm_name</i>] [<i>detail</i>]	Displays information about the firewall farm.
show ip slb stats	Displays statistics that include the firewall farm.

Example of Firewall Load Balancing

Figure 6-1 shows a sample SLB firewall load-balancing network with the following components:

- Two firewalls with IP addresses as shown
- An internal firewall load-balancing device on the secure side of the firewalls
- An external firewall load-balancing device on the Internet side of the firewalls
- One firewall farm named FIRE1, containing both firewalls

Figure 6-1 SLB with Layer 3 Firewalls in Different Subnets



45194

When you configure SLB firewall load balancing, the load-balancing devices use route lookup to recognize flows destined for the firewalls. To enable route lookup, you must configure each device with the IP address of each firewall that will route flows to that device.

In the farm configuration examples in the following sections:

- The internal (secure side) firewall load-balancing device is configured with firewall IP addresses 10.1.4.1 and 10.1.3.1.
- The external (Internet side) firewall load-balancing device is configured with firewall IP addresses 10.1.1.2 and 10.1.2.2.

Internal Firewall Load-Balancing Device

The following commands configure ping probe PROBE1, HTTP probe PROBE2, and firewall farm FIRE1, and associate the two real servers for the load-balancing device on the internal (secure) side of the firewall:

```
FWLB-Switch(config)# ip slb probe PROBE1 ping
FWLB-Switch(config-slb-probe)# address 10.1.1.1
FWLB-Switch(config-slb-probe)# faildetect 4
FWLB-Switch(config-slb-probe)# ip slb probe PROBE2 http
FWLB-Switch(config-slb-probe)# address 10.1.2.1
FWLB-Switch(config-slb-probe)# expect status 401
FWLB-Switch(config-slb-probe)# ip slb firewallfarm FIRE1
FWLB-Switch(config-slb-fw)# real 10.1.4.1
FWLB-Switch(config-slb-fw-real)# probe PROBE1
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# real 10.1.3.1
FWLB-Switch(config-slb-fw-real)# probe PROBE2
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# exit
FWLB-Switch(config-slb-fw)# inservice
```

External Firewall Load-Balancing Device

The following commands configure ping probe PROBE1, HTTP probe PROBE2, and firewall farm FIRE1, and associate the two real servers for the load-balancing device on the external (Internet) side of the firewall:

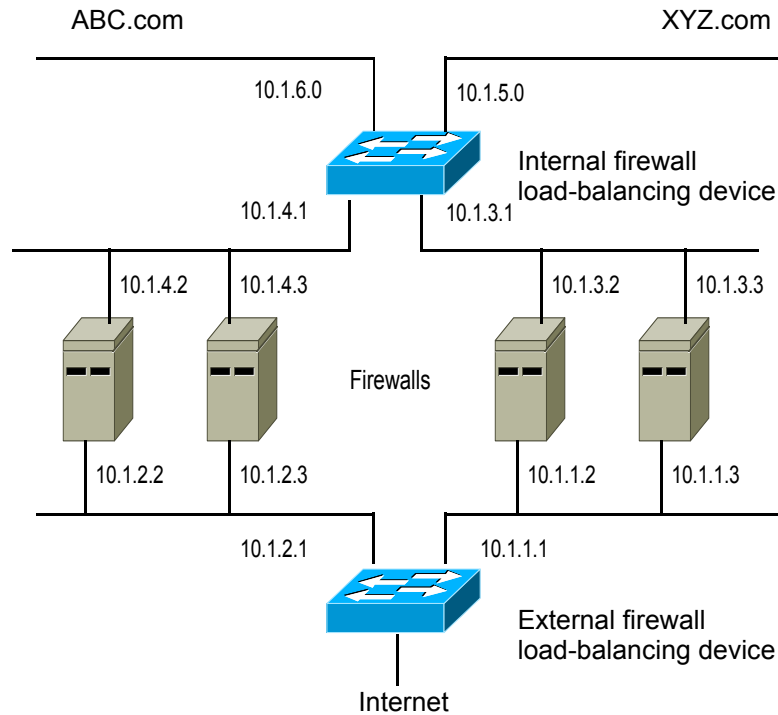
```
FWLB-Switch(config)# ip slb probe PROBE1 ping
FWLB-Switch(config-slb-probe)# address 10.1.4.2
FWLB-Switch(config-slb-probe)# faildetect 4
FWLB-Switch(config-slb-probe)# ip slb probe PROBE2 http
FWLB-Switch(config-slb-probe)# address 10.1.3.2
FWLB-Switch(config-slb-probe)# expect status 401
FWLB-Switch(config-slb-probe)# ip slb firewallfarm FIRE1
FWLB-Switch(config-slb-fw)# real 10.1.1.2
FWLB-Switch(config-slb-fw-real)# probe PROBE1
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# real 10.1.2.2
FWLB-Switch(config-slb-fw-real)# probe PROBE2
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# exit
FWLB-Switch(config-slb-fw)# inservice
```

Example of Multiple Firewall Farms

Figure 6-2 shows a sample IOS SLB network with multiple firewall farms and the following components:

- Four firewalls with IP addresses as shown
- An internal firewall load-balancing device on the secure side of the firewalls
- An external firewall load-balancing device on the Internet side of the firewalls
- One firewall farm named ABC.com, containing two firewalls (on the left)
- One firewall farm named XYZ.com, containing two firewalls (on the right)

Figure 6-2 IOS SLB with Multiple Firewall Farms



In the following firewall farm configuration samples:

- The internal (secure side) firewall load-balancing device is configured with firewall IP addresses 10.1.3.1 and 10.1.4.1.
- The external (Internet side) firewall load-balancing device is configured with firewall IP addresses 10.1.1.2 and 10.1.2.2.

Internal Firewall Load-Balancing Device

The following commands configure ping probes ABCPROBE and XYZPROBE and firewall farms ABCFARM and XYZFARM for the load-balancing device on the internal (secure) side of the firewalls:

```
FWLB-Switch(config)# ip slb probe ABCPROBE ping
FWLB-Switch(config-slb-probe)# address 10.1.2.1
FWLB-Switch(config-slb-probe)# ip slb probe XYZPROBE ping
FWLB-Switch(config-slb-probe)# address 10.1.1.1
FWLB-Switch(config-slb-probe)# ip slb firewallfarm ABCFARM
FWLB-Switch(config-slb-fw)# access source 10.1.6.0 255.255.255.0
FWLB-Switch(config-slb-fw)# inservice
FWLB-Switch(config-slb-fw)# real 10.1.4.2
FWLB-Switch(config-slb-fw-real)# probe ABCPROBE
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# real 10.1.4.3
FWLB-Switch(config-slb-fw-real)# probe ABCPROBE
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# ip slb firewallfarm XYZFARM
FWLB-Switch(config-slb-fw)# access source 10.1.5.0 255.255.255.0
FWLB-Switch(config-slb-fw)# inservice
FWLB-Switch(config-slb-fw)# real 10.1.3.2
FWLB-Switch(config-slb-fw-real)# probe XYZPROBE
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# real 10.1.3.3
FWLB-Switch(config-slb-fw-real)# probe XYZPROBE
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# exit
FWLB-Switch(config-slb-fw)# inservice
```

External Firewall Load-Balancing Device

The following commands configure ping probes ABCPROBE and XYZPROBE and firewall farms ABCFARM and XYZFARM for the load-balancing device on the external (Internet) side of the firewalls:

```
FWLB-Switch(config)# ip slb probe ABCPROBE ping
FWLB-Switch(config-slb-probe)# address 10.1.4.1
FWLB-Switch(config-slb-probe)# ip slb probe XYZPROBE ping
FWLB-Switch(config-slb-probe)# address 10.1.3.1
FWLB-Switch(config-slb-probe)# ip slb firewallfarm ABCFARM
FWLB-Switch(config-slb-fw)# access destination 10.1.6.0 255.255.255.0
FWLB-Switch(config-slb-fw)# inservice
FWLB-Switch(config-slb-fw)# real 10.1.2.2
FWLB-Switch(config-slb-fw-real)# probe ABCPROBE
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# real 10.1.2.3
FWLB-Switch(config-slb-fw-real)# probe ABCPROBE
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# ip slb firewallfarm XYZFARM
FWLB-Switch(config-slb-fw)# access destination 10.1.5.0 255.255.255.0
FWLB-Switch(config-slb-fw)# inservice
FWLB-Switch(config-slb-fw)# real 10.1.1.2
FWLB-Switch(config-slb-fw-real)# probe XYZPROBE
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# real 10.1.1.3
FWLB-Switch(config-slb-fw-real)# probe XYZPROBE
FWLB-Switch(config-slb-fw-real)# inservice
FWLB-Switch(config-slb-fw-real)# exit
FWLB-Switch(config-slb-fw)# inservice
```

■ Example of Multiple Firewall Farms