



Configuring Firewall Load Balancing

This chapter describes how to configure firewall load balancing on your Cisco Application Control Engine (ACE) module. Firewall load balancing allows you to scale firewall protection by distributing traffic across multiple firewalls on a per-connection basis. All packets belonging to a particular connection must go through the same firewall. The firewall then allows or denies transmission of individual packets across its interfaces.

This chapter contains the following major sections:

- [Understanding How Firewalls Work](#)
- [Configuring Standard Firewall Load Balancing](#)
- [Configuring Stealth Firewall Load Balancing](#)
- [Firewall Load-balancing Configurational Examples](#)

Understanding How Firewalls Work

A firewall forms a physical barrier between two parts of a network, for example, the Internet and an intranet. When a firewall accepts a packet from one side (the Internet), it sends the packet through to the other side (the intranet). A firewall can modify a packet before passing it through or send it through unaltered. When a firewall rejects a packet, it typically discards the packet and logs the discarded packet as an event.

After a session is established and a flow of packets begins, a firewall can monitor each packet in the flow or allow the flow to continue unmonitored, depending on the policies that you configure on that firewall.

This section contains the following subsections:

- [Firewall Types](#)
- [How the ACE Distributes Traffic to Firewalls](#)
- [Supported Firewall Configurations](#)

Firewall Types

The two basic types of firewalls are:

- Standard firewalls
- Stealth firewalls

Standard firewalls have a presence on the network. You assign IP addresses to the firewalls, which allows other devices on the network to see and address them as devices. Each firewall has an IP address on the VLANs configured on both sides of the firewall.

Stealth firewalls have no presence on the network. You do not assign IP addresses to the firewalls, which prevents other devices on the network from seeing or addressing them. Instead, you configure IP addresses on the ACE VLAN interfaces on both sides of the firewall. To the network, a stealth firewall is part of the wire.

Both firewall types:

- Examine traffic moving in both directions (between the protected and the unprotected sides of the network)
- Accept or reject packets based on user-defined policies

How the ACE Distributes Traffic to Firewalls

The ACE load-balances traffic to devices configured in server farms. These devices can be firewalls, caches, servers, or any IP-addressable object. For more information about server farms, see the “[Configuring a Server Farm](#)” section in [Chapter 1, Configuring Real Servers and Server Farms](#). When the ACE load-balances traffic to firewalls, it performs the same function that it performs when it load-balances Layer 3 traffic to real servers in a server farm.

The ACE uses load-balancing algorithms or predictors to determine how to balance the traffic among the devices configured in the server farms, independent of the device type. For FWLB, we recommend that you use only the hash address source and the hash address destination predictors. Using any other predictor with FWLB may fail and block traffic, especially for applications that have separate control and data channels, for example, FTP.

For more information about load-balancing predictor methods, see the “[Configuring the Server Farm Predictor Method](#)” section in [Chapter 1, Configuring Real Servers and Server Farms](#).

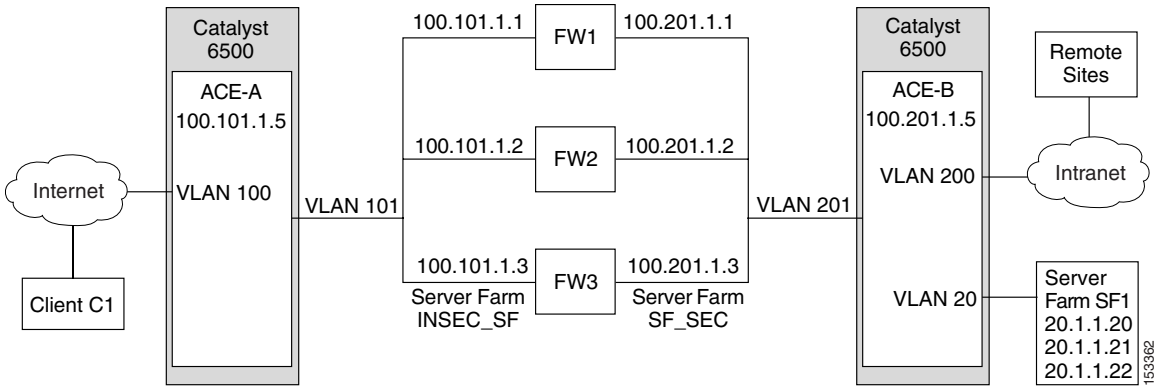
Supported Firewall Configurations

The ACE can load-balance traffic to both standard and stealth firewalls.

For standard firewalls, a single ACE or a pair of ACEs in two different Catalyst 6500 switches load-balances traffic among firewalls that contain unique IP addresses in a manner similar to how the ACE load-balances traffic among servers in a server farm (see [Figure 6-1](#)).

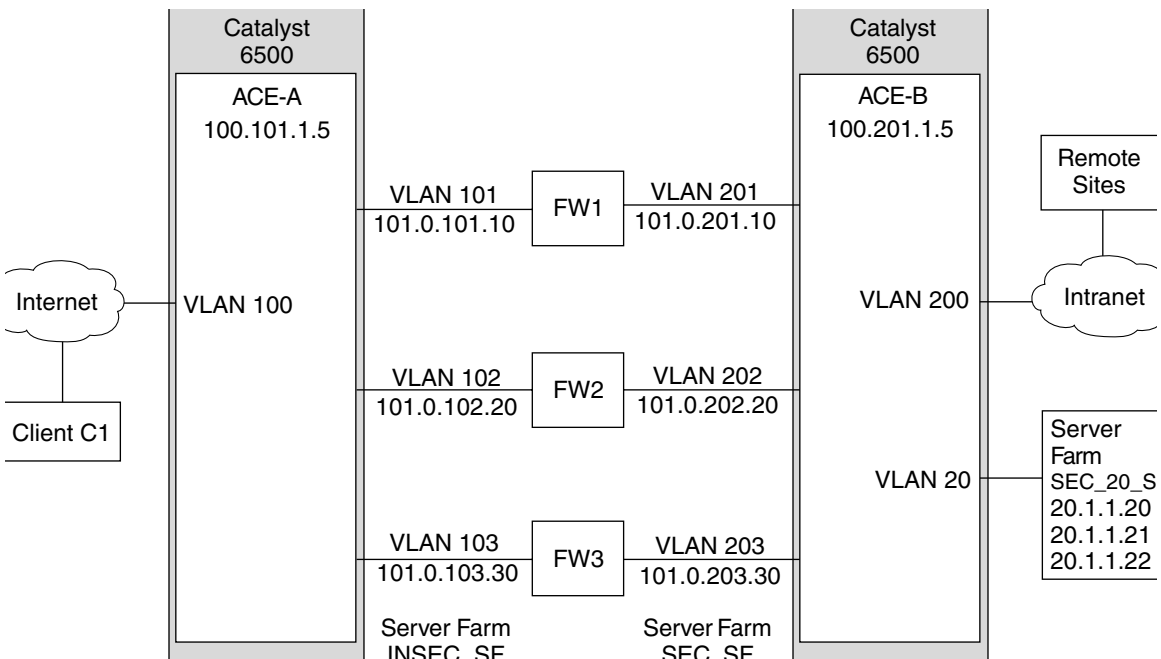
In [Figure 6-1](#), traffic moves through the firewalls and the firewalls filter the traffic in both directions. For traffic originating on the Internet, ACE A load-balances the traffic to the firewalls in the SF_INSEC server farm. For traffic originating on the intranet, ACE B load-balances the traffic to the firewalls in server farm SF_SEC. You configure the firewalls so that the return traffic flows through the same firewall as the original traffic.

Figure 6-1 Standard Firewall Configuration



For stealth firewalls, an ACE load-balances traffic among interfaces with unique IP addresses in different ACEs that provides paths through the firewalls (Figure 6-2). You configure a stealth firewall so that all traffic moving in both directions across a particular VLAN moves through the same firewall.

Figure 6-2 Stealth Firewall Configuration (Dual ACEs Only)



In [Figure 6-2](#), traffic flows through the firewalls and the firewalls filter the traffic in both directions. On the path to the intranet, ACE A balances traffic across VLANs 101, 102, and 103 through the firewalls to ACE B. On the path to the Internet, ACE B balances traffic across VLANs 201, 202, and 203 through the firewalls to ACE A.

Configuring Standard Firewall Load Balancing

This section describes how to configure firewall load balancing for standard firewalls. It contains the following subsections:

- [Standard FWLB Configuration Overview](#)
- [Standard FWLB Configuration Quick Starts](#)



Note

For information about configuring the firewall devices in your network, refer to the documentation included with your firewall product.

Standard FWLB Configuration Overview

In this standard FWLB configuration example (see [Figure 6-1](#)), you configure three firewalls (FW1, FW2, and FW3) between two ACEs (ACE A and ACE B). (You can also configure standard FWLB using a single ACE.) Traffic enters and exits the firewalls through shared VLANs on either side of the firewalls (VLAN 101 on the insecure side and VLAN 201 on the secure side). You assign unique IP addresses to each firewall configured as a real server in a server farm on each shared VLAN.

Other VLANs provide connectivity to:

- Internet (VLAN 100)
- Internal network (VLAN 200)
- Internal server farm (VLAN 20)

Standard FWLB Configuration Quick Starts

This section provides quick start tables that include step-by-step instructions for configuring standard FWLB on two ACE modules in separate Catalyst 6500 switches. Note that you can also configure standard FWLB on a single ACE. This section includes the following subsections:

- [Standard FWLB Configuration Quick Start for ACE A](#)
- [Standard FWLB Configuration Quick Start for ACE B](#)

Standard FWLB Configuration Quick Start for ACE A

[Table 6-1](#) provides a quick overview of the steps required to configure standard FWLB on ACE A (see [Figure 6-1](#)). Each step includes the CLI command required to complete the task.

Table 6-1 Standard FWLB Configuration Quick Start for ACE A

Task and Command Example

1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, change to, or directly log in to, the correct context.

```
host1/Admin# changeto C1
host1/C1#
```

The rest of the examples in this table use the Admin context for illustration purposes, unless otherwise specified. For details on creating contexts, refer to the *Cisco Application Control Engine Module Administration Guide*.

2. Enter configuration mode.

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)#
```

Table 6-1 Standard FWLB Configuration Quick Start for ACE A (continued)

Task and Command Example

3. Configure an access control list (ACL) to allow traffic. You can modify the ACL to suit your application needs. For more information about configuring ACLs, refer to the *Cisco Application Control Engine Module Security Configuration Guide*.

```
host1/Admin(config)# access-list ACL1 line 10 extended permit ip  
any any  
host1/Admin(config-acl)# exit
```

4. Configure three real servers to represent the insecure side of the firewalls on VLAN 101. For more information about configuring real servers, see [Chapter 1, Configuring Real Servers and Server Farms](#).

```
host1/Admin(config)# rserver FW_INSEC_1  
host1/Admin(config-rserver-host)# ip address 100.101.1.1  
host1/Admin(config-rserver-host)# inservice  
host1/Admin(config-rserver-host)# exit
```

```
host1/Admin(config)# rserver FW_INSEC_2  
host1/Admin(config-rserver-host)# ip address 100.101.1.2  
host1/Admin(config-rserver-host)# inservice  
host1/Admin(config-rserver-host)# exit
```

```
host1/Admin(config)# rserver FW_INSEC_3  
host1/Admin(config-rserver-host)# ip address 100.101.1.3  
host1/Admin(config-rserver-host)# inservice  
host1/Admin(config-rserver-host)# exit
```

Table 6-1 Standard FWLB Configuration Quick Start for ACE A (continued)**Task and Command Example**

5. Configure a server farm to handle connections originating from the insecure side of the firewalls (Internet). The ACE selects a firewall based on source IP address using the hash address source predictor. For more information about configuring server farms, see [Chapter 1, Configuring Real Servers and Server Farms](#).

```

host1/Admin(config)# serverfarm SF_INSEC
host1/Admin(config-sfarm-host)# transparent
host1/Admin(config-sfarm-host)# predictor hash address source
255.255.255.255
host1/Admin(config-sfarm-host)# rserver FW_INSEC_1
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# rserver FW_INSEC_2
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# rserver FW_INSEC_3
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# exit

```

6. Configure a Layer 7 load-balancing policy map to balance requests to server farm SF-INSEC. Associate the default class map and the SF-INSEC server farm with the policy map. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```

host1/Admin(config)# policy-map type loadbalance first-match
LB_FW_INSEC
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)# serverfarm SF_INSEC
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# exit

```

7. Configure a Layer 3 class map to classify traffic from the Internet that matches VIP address 200.1.1.1 on VLAN 100 on the insecure side of the firewalls. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```

host1/Admin(config)# class-map match-any FW_VIP
host1/Admin(config-cmap)# match virtual-address 200.1.1.1
255.255.0.0 any
host1/Admin(config-cmap)# exit

```

Table 6-1 Standard FWLB Configuration Quick Start for ACE A (continued)**Task and Command Example**

8. Configure a Layer 3 policy map and associate the Layer 3 class map and the Layer 7 policy map with it to complete the traffic policy configuration. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# policy-map multi-match POL_INSEC
host1/Admin(config-pmap)# class FW_VIP
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# loadbalance policy LB_FW_INSEC
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
```

9. Configure an interface that the ACE uses to receive traffic from the Internet and to send traffic originating from the intranet to the Internet. Apply the ACL (ACL1) and the Layer 3 policy (POL_INSEC) to the interface. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ip address 100.100.1.100 255.255.0.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# service-policy input POL_INSEC
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
```

10. Configure an interface on the insecure side of the firewalls. The ACE uses this interface to load-balance traffic to the firewalls and to receive traffic originating from the intranet. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 101
host1/Admin(config-if)# ip address 100.101.1.101 255.255.0.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# mac-sticky enable
host1/Admin(config-if)# service-policy input POL_INSEC
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# Ctrl-z
```

Table 6-1 Standard FWLB Configuration Quick Start for ACE A (continued)**Task and Command Example**

11. Use the following **show** commands to verify your FWLB configuration:

```

host1/Admin# show running-config access-list
host1/Admin# show running-config class-map
host1/Admin# show running-config interface
host1/Admin# show running-config policy-map
host1/Admin# show running-config rserver
host1/Admin# show running-config serverfarm

```

12. (Optional) If necessary, save your configuration changes to Flash memory.

```

host1/Admin# copy running-config startup-config

```

Standard FWLB Configuration Quick Start for ACE B

Table 6-2 provides a quick overview of the steps required to configure standard FWLB on ACE B (see Figure 6-1). Each step includes the CLI command and a reference to the procedure required to complete the task.

Table 6-2 Standard FWLB Configuration Quick Start for ACE B**Task and Command Example**

1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, change to, or directly log in to, the correct context.

```

host1/Admin# changeto C1
host1/C1#

```

The rest of the examples in this table use the Admin context for illustration purposes, unless otherwise specified. For details on creating contexts, refer to the *Cisco Application Control Engine Module Administration Guide*.

2. Enter configuration mode.

```

host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)#

```

Table 6-2 Standard FWLB Configuration Quick Start for ACE B (continued)

Task and Command Example

3. Configure an ACL to allow traffic. You can modify the ACL to suit your application needs. For more information about configuring ACLs, refer to the *Cisco Application Control Engine Module Security Configuration Guide*.

```
host1/Admin(config)# access-list ACL1 line 10 extended permit ip  
any any  
host1/Admin(config-acl)# exit
```

4. Configure three real servers to represent the secure side of the firewalls on VLAN 201. For more information about configuring real servers, see [Chapter 2, Configuring Real Servers and Server Farms](#).

```
host1/Admin(config)# rserver FW_SEC_1  
host1/Admin(config-rserver-host)# ip address 100.201.1.1  
host1/Admin(config-rserver-host)# inservice  
host1/Admin(config-rserver-host)# exit
```

```
host1/Admin(config)# rserver FW_SEC_2  
host1/Admin(config-rserver-host)# ip address 100.201.1.2  
host1/Admin(config-rserver-host)# inservice  
host1/Admin(config-rserver-host)# exit
```

```
host1/Admin(config)# rserver FW_SEC_3  
host1/Admin(config-rserver-host)# ip address 100.201.1.3  
host1/Admin(config-rserver-host)# inservice  
host1/Admin(config-rserver-host)# exit
```

Table 6-2 Standard FWLB Configuration Quick Start for ACE B (continued)**Task and Command Example**

5. Configure a server farm to handle connections originating from the secure side of the firewall (intranet). In this case, the ACE selects a firewall based on the destination IP address using the hash address destination predictor. This predictor allows the ACE to select the same firewall for return flows and buddy connections. For example, you want both the FTP control and data channels to pass through the same firewall. For more information about configuring server farms, see [Chapter 2, Configuring Real Servers and Server Farms](#).

```

host1/Admin(config)# serverfarm SF_SEC
host1/Admin(config-sfarm-host)# transparent
host1/Admin(config-sfarm-host)# predictor hash address
destination 255.255.255.255
host1/Admin(config-sfarm-host)# rserver FW_SEC_1
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# rserver FW_SEC_2
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# rserver FW_SEC_3
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit

```

6. Configure two real servers to load-balance content on VLAN 20 on the secure side of the firewall. For more information about configuring server farms, see [Chapter 2, Configuring Real Servers and Server Farms](#).

```

host1/Admin(config)# rserver REAL1
host1/Admin(config-rserver-host)# ip address 20.1.1.1
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit

host1/Admin(config)# rserver REAL2
host1/Admin(config-rserver-host)# ip address 20.1.1.2
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit

host1/Admin(config)# rserver REAL3
host1/Admin(config-rserver-host)# ip address 20.1.1.3
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit

```

Table 6-2 Standard FWLB Configuration Quick Start for ACE B (continued)

Task and Command Example

7. Configure a standard server farm of HTTP servers. For more information about configuring server farms, see [Chapter 2, Configuring Real Servers and Server Farms](#).

```
host1/Admin(config)# serverfarm SEC_20_SF
host1/Admin(config-sfarm-host)# rserver REAL1
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# rserver REAL2
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# rserver REAL3
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# exit
```

8. Configure a Layer 7 policy map that load-balances traffic to the HTTP server farm on VLAN 20 using the default class map. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# policy-map type loadbalance first-match
SEC_20_LB
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)# serverfarm SEC_20_SF
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# exit
```

9. Configure a Layer 3 class map to classify traffic destined to the virtual IP address 200.1.1.1 configured on VLAN 201. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# class-map match-any SEC_20_VS
host1/Admin(config-cmap)# match virtual-address 200.1.1.1
255.255.0.0 any
host1/Admin(config-cmap)# exit
```

Table 6-2 Standard FWLB Configuration Quick Start for ACE B (continued)**Task and Command Example**

10. Configure a Layer 3 policy map and associate the Layer 3 class map (SEC_20_VS) and the Layer 7 policy map (SEC_20_LB) with it. This step completes the policy that load-balances traffic to the HTTP servers on VLAN 20. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# policy-map multi-match POL_SEC_20
host1/Admin(config-pmap)# class SEC_20_VS
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# loadbalance policy SEC_20_LB
```

11. Configure a Layer 7 policy map to load-balance traffic that originates from either VLAN 200 or VLAN 20 and is destined for the Internet to the secure side of the firewalls on VLAN 201. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# policy-map type loadbalance first-match
LB_FW_SEC
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)# serverfarm SF_SEC
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# exit
```

12. Configure a Layer 3 class map to classify all traffic originating on the secure side of the firewalls and destined for the Internet. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# class-map match-any FW_SEC_VIP
host1/Admin(config-cmap)# match virtual-address 0.0.0.0 0.0.0.0
any
host1/Admin(config-cmap)# exit
```

Table 6-2 Standard FWLB Configuration Quick Start for ACE B (continued)

Task and Command Example

13. Configure a Layer 3 policy map and associate the Layer 7 policy map (LB_FW_SEC) and the Layer 3 class map (FW_SEC_VIP) with it. Enable the VIP for load balancing. This step completes the policy that load-balances any request originating on the secure side of the firewalls and destined for the Internet. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# policy-map multi-match POL_SEC
host1/Admin(config-pmap)# class FW_SEC_VIP
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# loadbalance LB_FW_SEC
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
```

14. Configure an interface on the secure side of the firewalls for traffic originating from the Internet and passing through the firewalls. The ACE uses this interface to catch traffic from the firewalls and load-balance it to the HTTP server farm and route traffic to the remote host. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 201
host1/Admin(config-if)# ip address 100.201.1.201 255.255.0.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# mac-sticky enable
host1/Admin(config-if)# service-policy input POL_SEC_20
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
```

15. Configure an interface on the secure side of the firewalls for traffic that originates from the HTTP server farm on VLAN 20. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 20
host1/Admin(config-if)# ip address 20.1.1.20 255.255.255.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# service-policy input POL_SEC
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
```

Table 6-2 Standard FWLB Configuration Quick Start for ACE B (continued)**Task and Command Example**

16. Configure an interface on the secure side of the firewalls for traffic that originates from the remote host on VLAN 200. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```

host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# ip address 200.1.1.200 255.255.255.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# service-policy input POL_SEC
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# Ctrl-z

```

17. Use the following **show** commands to verify your FWLB configuration:

```

host1/Admin# show running-config access-list
host1/Admin# show running-config class-map
host1/Admin# show running-config interface
host1/Admin# show running-config policy-map
host1/Admin# show running-config rserver
host1/Admin# show running-config serverfarm

```

18. (Optional) If necessary, save your configuration changes to Flash memory.

```

host1/Admin# copy running-config startup-config

```

Configuring Stealth Firewall Load Balancing

This section describes how to configure stealth FWLB. It contains the following subsections:

- [Stealth Firewall Load-Balancing Configuration Overview](#)
- [Stealth Firewall Load-Balancing Configuration Quick Starts](#)

**Note**

For information about configuring the firewall devices in your network, refer to the documentation included with your firewall product.

Stealth Firewall Load-Balancing Configuration Overview

**Note**

In a stealth FWLB configuration, you must configure two ACEs, each in a separate Catalyst 6500 switch.

In this stealth FWLB configuration example (see [Figure 6-2](#)), ACE A and ACE B load-balance traffic through three firewalls. Each firewall configured as a real server in a server farm connects to two different VLANs, one on the insecure side and one on the secure side of the firewall.

On the path from the Internet to the intranet, traffic enters the insecure side of the firewalls through separate VLANs (VLAN 101, VLAN 102, and VLAN 103) and exits the secure side of the firewalls through separate VLANs (VLAN 201, VLAN 202, and VLAN 203). On the path from the intranet to the Internet, the flow is reversed. Other VLANs provide connectivity to the:

- Internet (VLAN 100)
- Remote host (VLAN 200)
- Intranet server farm (VLAN 20)

Stealth Firewall Load-Balancing Configuration Quick Starts

This section provides quick start tables that include step-by-step instructions about how to configure stealth FWLB on two separate ACE modules. This section includes the following subsections:

- [Stealth FWLB Configuration Quick Start for ACE A](#)
- [Stealth FWLB Configuration Quick Start for ACE B](#)

Stealth FWLB Configuration Quick Start for ACE A

[Table 6-3](#) provides a quick overview of the steps required to configure stealth FWLB on ACE A (insecure side). Each step includes the CLI command required to complete the task.

Table 6-3 *Stealth FWLB Configuration Quick Start for ACE A*

Task and Command Example

1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, change to, or directly log in to, the correct context.

```
host1/Admin# changeto C1
host1/C1#
```

The rest of the examples in this table use the Admin context for illustration purposes, unless otherwise specified. For details on creating contexts, refer to the *Cisco Application Control Engine Module Administration Guide*.

2. Enter configuration mode.

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)#
```

3. Configure an ACL to allow traffic to the ACE. You can modify the ACL to suit your application needs. For more information about configuring ACLs, refer to the *Cisco Application Control Engine Module Security Configuration Guide*

```
host1/Admin(config)# access-list ACL1 line 10 extended permit ip
any any
host1/Admin(config-acl)# exit
```

Table 6-3 *Stealth FWLB Configuration Quick Start for ACE A (continued)*

Task and Command Example

4. Configure three real servers to represent the insecure side of the firewalls on VLANs 101, 102, and 103. For more information about configuring real servers, see [Chapter 2, Configuring Real Servers and Server Farms](#).

```
host1/Admin(config)# rserver FW_INSEC_1
host1/Admin(config-rserver-host)# ip address 101.0.201.100
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit
```

```
host1/Admin(config)# rserver FW_INSEC_2
host1/Admin(config-rserver-host)# ip address 101.0.202.100
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit
```

```
host1/Admin(config)# rserver FW_INSEC_3
host1/Admin(config-rserver-host)# ip address 101.0.203.100
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit
```

5. Configure a server farm to handle connections originating from the insecure side of the firewalls (Internet). The ACE selects a firewall based on source IP address using the hash address source predictor. For more information about configuring server farms, see [Chapter 2, Configuring Real Servers and Server Farms](#).

```
host1/Admin(config)# serverfarm SF_INSEC
host1/Admin(config-sfarm-host)# transparent
host1/Admin(config-sfarm-host)# predictor hash address source
255.255.255.255
host1/Admin(config-sfarm-host)# rserver FW_INSEC_1
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# rserver FW_INSEC_2
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# rserver FW_INSEC_3
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# exit
```

Table 6-3 Stealth FWLB Configuration Quick Start for ACE A (continued)**Task and Command Example**

6. Configure a Layer 7 load-balancing policy map to forward packets received from the firewall to the internet. Associate the default class map with the policy map. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# policy-map type loadbalance first-match
FORWARD_FW_INSEC
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)# forward
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# exit
```

7. Configure a Layer 3 class map to classify traffic from the firewalls that matches any VIP address, netmask, and protocol on VLANs 101, 102, and 103 on the insecure side of the firewalls.

```
host1/Admin(config)# class-map match-any FORWARD_VIP
host1/Admin(config-cmap)# match virtual-address 0.0.0.0 0.0.0.0
any
host1/Admin(config-cmap)# exit
```

8. Configure a Layer 3 policy map and associate the Layer 3 forwarding class map (FORWARD_VIP) and the Layer 7 forwarding policy map (FORWARD_FW_INSEC) with it to complete the forwarding policy configuration.

```
host1/Admin(config)# policy-map multi-match FORWARD_INSEC
host1/Admin(config-pmap)# class FORWARD_VIP
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# loadbalance policy FORWARD_FW_INSEC
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
```

9. Configure a Layer 7 load-balancing policy map to balance requests from the Internet to server farm SF-INSEC. Associate the default class map and the SF-INSEC server farm with the policy map.

```
host1/Admin(config)# policy-map type loadbalance first-match
LB-FW-INSEC
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)# serverfarm SF_INSEC
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# exit
```

Table 6-3 Stealth FWLB Configuration Quick Start for ACE A (continued)

Task and Command Example

10. Configure a Layer 3 class map to classify traffic from the Internet that matches VIP address 200.1.1.1, netmask 255.255.0.0, and any protocol on VLAN 100 on the insecure side of the firewalls.

```
host1/Admin(config)# class-map match-any FW_VIP
host1/Admin(config-cmap)# match virtual-address 200.1.1.1
255.255.0.0 any
host1/Admin(config-cmap)# exit
```

11. Configure a Layer 3 policy map and associate the Layer 3 class map (FW_VIP) and the Layer 7 policy map (LB_FW_INSEC) with it to complete the load-balancing policy configuration.

```
host1/Admin(config)# policy-map multi-match POL_INSEC
host1/Admin(config-pmap)# class FW_VIP
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# loadbalance policy LB_FW_INSEC
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
```

12. Configure an interface that the ACE uses to receive traffic from the Internet and load-balance the traffic to the insecure side of the firewall. Apply the ACL (ACL1) and the Layer 3 policy (POL_INSEC) to the interface. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 100
host1/Admin(config-if)# ip address 100.100.1.100 255.255.0.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# service-policy input POL_INSEC
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
```

Table 6-3 Stealth FWLB Configuration Quick Start for ACE A (continued)**Task and Command Example**

13. Configure an interface on the insecure side of the firewalls that ACE A uses to load-balance traffic to FW1 and to receive traffic originating from the intranet. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 101
host1/Admin(config-if)# ip address 101.0.101.10 255.255.0.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# mac-sticky enable
host1/Admin(config-if)# service-policy input FORWARD_INSEC
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
```

14. Configure an interface on the insecure side of the firewalls that ACE A uses to load-balance traffic to FW2 and to receive traffic originating from the intranet. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 102
host1/Admin(config-if)# ip address 101.0.102.20 255.255.0.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# mac-sticky enable
host1/Admin(config-if)# service-policy input FORWARD_INSEC
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
```

15. Configure an interface on the insecure side of the firewalls that ACE A uses to load-balance traffic to the FW3 and to receive traffic originating from the intranet. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 103
host1/Admin(config-if)# ip address 101.0.103.30 255.255.0.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# mac-sticky enable
host1/Admin(config-if)# service-policy input FORWARD_INSEC
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# Ctrl-z
```

Table 6-3 *Stealth FWLB Configuration Quick Start for ACE A (continued)*

Task and Command Example

16. Use the following **show** commands to verify your FWLB configuration:

```
host1/Admin# show running-config access-list
host1/Admin# show running-config class-map
host1/Admin# show running-config interface
host1/Admin# show running-config policy-map
host1/Admin# show running-config rserver
host1/Admin# show running-config serverfarm
```

17. (Optional) If necessary, save your configuration changes to Flash memory.

```
host1/Admin# copy running-config startup-config
```

Stealth FWLB Configuration Quick Start for ACE B

Table 6-4 provides a quick overview of the steps required to configure stealth FWLB on ACE B (secure side). Each step includes the CLI command required to complete the task.

Table 6-4 Stealth FWLB Configuration Quick Start for ACE B

Task and Command Example

1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, change to, or directly log in to, the correct context.

```
host1/Admin# changeto C1
host1/C1#
```

The rest of the examples in this table use the Admin context for illustration purposes, unless otherwise specified. For details on creating contexts, refer to the *Cisco Application Control Engine Module Administration Guide*.

2. Enter configuration mode.

```
host1/Admin# config
Enter configuration commands, one per line. End with CNTL/Z
host1/Admin(config)#
```

3. Configure an ACL to allow traffic to the ACE. You can modify the ACL to suit your application needs. For more information about configuring ACLs, refer to the *Cisco Application Control Engine Module Security Configuration Guide*

```
host1/Admin(config)# access-list ACL1 line 10 extended permit ip
any any
host1/Admin(config-acl)# exit
```

Table 6-4 *Stealth FWLB Configuration Quick Start for ACE B (continued)*

Task and Command Example

4. Configure three real servers to represent the secure side of the firewalls on VLANs 201, 202, and 203. For more information about configuring real servers, see [Chapter 2, Configuring Real Servers and Server Farms](#).

```
host1/Admin(config)# rserver FW_SEC_1
host1/Admin(config-rserver-host)# ip address 101.0.101.100
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit
```

```
host1/Admin(config)# rserver FW_SEC_2
host1/Admin(config-rserver-host)# ip address 101.0.102.100
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit
```

```
host1/Admin(config)# rserver FW_SEC_3
host1/Admin(config-rserver-host)# ip address 101.0.103.100
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit
```

5. Configure a server farm to handle connections originating from the secure side of the firewall (intranet). In this case, the ACE selects a firewall based on the destination IP address using the hash address destination predictor. This predictor allows the ACE to select the same firewall for return flows and buddy connections. For example, you want both the FTP control and data channels to pass through the same firewall. For more information about configuring server farms, see [Chapter 2, Configuring Real Servers and Server Farms](#).

```
host1/Admin(config)# serverfarm SF_SEC
host1/Admin(config-sfarm-host)# transparent
host1/Admin(config-sfarm-host)# predictor hash address
destination 255.255.255.255
host1/Admin(config-sfarm-host)# rserver FW_SEC_1
host1/Admin(config-sfarm-host)# inservice
host1/Admin(config-sfarm-host)# rserver FW_SEC_2
host1/Admin(config-sfarm-host)# inservice
host1/Admin(config-sfarm-host)# rserver FW_SEC_3
host1/Admin(config-sfarm-host)# inservice
host1/Admin(config-sfarm-host)# exit
```

Table 6-4 *Stealth FWLB Configuration Quick Start for ACE B (continued)***Task and Command Example**

6. Configure three real servers to load-balance content on VLAN 20 on the secure side of the firewall. For more information about configuring real servers, see [Chapter 2, Configuring Real Servers and Server Farms](#).

```
host1/Admin(config)# rserver REAL1
host1/Admin(config-rserver-host)# ip address 20.1.1.1
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit
```

```
host1/Admin(config)# rserver REAL2
host1/Admin(config-rserver-host)# ip address 20.1.1.2
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit
```

```
host1/Admin(config)# rserver REAL3
host1/Admin(config-rserver-host)# ip address 20.1.1.3
host1/Admin(config-rserver-host)# inservice
host1/Admin(config-rserver-host)# exit
```

7. Configure a standard server farm of HTTP servers to load-balance requests to the HTTP servers on VLAN 20. For more information about configuring server farms, see [Chapter 2, Configuring Real Servers and Server Farms](#).

```
host1/Admin(config)# serverfarm SEC_20_SF
host1/Admin(config-sfarm-host)# rserver REAL1
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# rserver REAL2
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# rserver REAL3
host1/Admin(config-sfarm-host-rs)# inservice
host1/Admin(config-sfarm-host-rs)# exit
host1/Admin(config-sfarm-host)# exit
```

Table 6-4 *Stealth FWLB Configuration Quick Start for ACE B (continued)*

Task and Command Example

8. Configure a Layer 7 policy map that load-balances traffic to the HTTP server farm on VLAN 20 using the default class map. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# policy-map type loadbalance first-match
SEC_20_LB
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)# serverfarm SEC_20_SF
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# exit
```

9. Configure a Layer 3 class map to classify traffic destined to the virtual IP address 200.1.1.1 on VLANs 201, 202, and 203. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# class-map match-any SEC_20_VS
host1/Admin(config-cmap)# match virtual-address 200.1.1.1
255.255.0.0 any
host1/Admin(config-cmap)# exit
```

10. Configure a Layer 3 policy map and associate the Layer 3 class map (SEC_20_VS) and the Layer 7 policy map (SEC_20_LB) with it. This step completes the policy that load-balances traffic to the HTTP servers on VLAN 20. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# policy-map multi-match POL_SEC_20
host1/Admin(config-pmap)# class SEC_20_VS
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# loadbalance policy SEC_20_LB
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
```

Table 6-4 Stealth FWLB Configuration Quick Start for ACE B (continued)**Task and Command Example**

11. Configure a Layer 7 policy map to load-balance requests originating from either VLAN 200 or VLAN 20 and destined for the Internet to the secure side of the firewalls on VLAN 201. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# policy-map type loadbalance first-match
LB_FW_SEC
host1/Admin(config-pmap-lb)# class class-default
host1/Admin(config-pmap-lb-c)# serverfarm SF_SEC
host1/Admin(config-pmap-lb-c)# exit
host1/Admin(config-pmap-lb)# exit
```

12. Configure a Layer 3 class map to classify all traffic with any IP address, netmask, and protocol originating on the secure side of the firewalls. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# class-map match-any FW_SEC_VIP
host1/Admin(config-cmap)# match virtual-address 0.0.0.0 0.0.0.0
any
host1/Admin(config-cmap)# exit
```

13. Configure a Layer 3 policy map and associate the Layer 7 policy map (LB_FW_SEC) and the Layer 3 class map (FW_SEC_VIP) with it. Enable the VIP for load balancing. This step completes the policy that load-balances any request originating on the secure side of the firewalls and destined for the Internet. For more information about configuring traffic policies for SLB, see [Chapter 1, Configuring Traffic Policies for Server Load Balancing](#).

```
host1/Admin(config)# policy-map multi-match POL_SEC
host1/Admin(config-pmap)# class FW_SEC_VIP
host1/Admin(config-pmap-c)# loadbalance vip inservice
host1/Admin(config-pmap-c)# loadbalance policy LB_FW_SEC
host1/Admin(config-pmap-c)# exit
host1/Admin(config-pmap)# exit
```

Table 6-4 *Stealth FWLB Configuration Quick Start for ACE B (continued)*

Task and Command Example

14. Configure an interface on the secure side of the firewalls that the ACE uses to send traffic to FW1 from the intranet and to receive traffic originating from the Internet and passing through the firewall. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 201
host1/Admin(config-if)# ip address 101.0.201.10 255.255.0.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# mac-sticky enable
host1/Admin(config-if)# service-policy input POL_SEC_20
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
```

15. Configure an interface on the secure side of the firewalls that the ACE uses to send traffic to FW2 from the intranet and to receive traffic originating from the Internet and passing through the firewall. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 202
host1/Admin(config-if)# ip address 101.0.202.20 255.255.0.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# mac-sticky enable
host1/Admin(config-if)# service-policy input POL_SEC_20
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
```

16. Configure an interface on the insecure side of the firewall that the ACE uses to send traffic to FW3 from the intranet and to receive traffic originating from the Internet passing through the firewall. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 203
host1/Admin(config-if)# ip address 101.0.203.30 255.255.0.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# mac-sticky enable
host1/Admin(config-if)# service-policy input POL_SEC_20
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
```

Table 6-4 Stealth FWLB Configuration Quick Start for ACE B (continued)**Task and Command Example**

17. Configure an interface that the ACE uses to receive traffic that originates from the remote host on VLAN 200 and destined to the Internet. Apply the ACL (ACL1) and the Layer 3 policy-map (POL_SEC) to the interface. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 200
host1/Admin(config-if)# ip address 200.1.1.200 255.255.255.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# service-policy input POL_SEC
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# exit
```

18. Configure an interface that ACE uses to receive traffic that originates from the HTTP server farm on VLAN 20 and destined to the Internet. Apply the ACL (ACL1) and the Layer 3 policy (POL_SEC) to the interface. For more information about configuring interfaces, refer to the *Cisco Application Control Engine Module Routing and Bridging Configuration Guide*.

```
host1/Admin(config)# interface vlan 20
host1/Admin(config-if)# ip address 20.100.1.100 255.255.0.0
host1/Admin(config-if)# access-group input ACL1
host1/Admin(config-if)# service-policy input POL_SEC
host1/Admin(config-if)# no shutdown
host1/Admin(config-if)# Ctrl-z
```

19. Use the following **show** commands to verify your FWLB configuration:

```
host1/Admin# show running-config access-list
host1/Admin# show running-config class-map
host1/Admin# show running-config interface
host1/Admin# show running-config policy-map
host1/Admin# show running-config rserver
host1/Admin# show running-config serverfarm
```

20. (Optional) If necessary, save your configuration changes to Flash memory.

```
host1/Admin# copy running-config startup-config
```

Displaying FWLB Configurations

To display your entire running configuration, use the **show running-config** command in Exec mode. The syntax of this command is:

```
show running-config
```

To display sections of the running-config that pertain to FWLB, use the following commands in Exec mode:

- **show running-config access-list**
- **show running-config class-map**
- **show running-config interface**
- **show running-config policy-map**
- **show running-config rserver**
- **show running-config serverfarm**
- **show running-config service-policy**

Firewall Load-balancing Configurational Examples

This section provides examples of standard and stealth FWLB configurations. It contains the following subsections:

- [Example of a Standard Firewall Load-Balancing Configuration](#)
- [Example of a Stealth Firewall Configuration](#)

Example of a Standard Firewall Load-Balancing Configuration

The following configuration example shows those portions of the running configuration that pertain to standard FWLB. The configuration is based on two ACE modules each in a separate Catalyst 6500 switch with the firewalls situated between them (see [Figure 6-1](#)). You can also configure standard FWLB using a single ACE.

ACE A Configuration—Standard Firewall Load Balancing

```

access-list ACL1 line 10 extended permit ip any any

rserver host FW_INSEC_1
  ip address 100.101.1.1
  inservice
rserver host FW_INSEC_2
  ip address 100.101.1.2
  inservice
rserver host FW_INSEC_3
  ip address 100.101.1.3
  inservice

serverfarm INSEC_SF
  transparent
  predictor hash address source 255.255.255.255
  rserver FW_INSEC_1
    inservice
  rserver FW_INSEC_2
    inservice
  rserver FW_INSEC_3
    inservice

class-map match-any FW_VIP
  10 match virtual-address 200.1.1.1 255.255.0.0 any
policy-map type loadbalance first-match LB_FW_INSEC
  class class-default
    serverfarm INSEC_SF
policy-map multi-match POL_INSEC
  class FW_VIP
    loadbalance vip inservice
    loadbalance policy LB_FW_INSEC

interface vlan 100
  ip addr 100.100.1.100 255.255.0.0
  access-group input ACL1
  service-policy input POL_INSEC
  no shutdown
interface vlan 101
  ip addr 100.101.1.101 255.255.0.0
  access-group input ACL1
  mac-sticky enable
  service-policy input POL_INSEC
  no shutdown

```

ACE B Configuration—Standard Firewall Load Balancing

```
access-list ACL1 line 10 extended permit ip any any

rserver FW_SEC_1
  ip address 100.201.1.1
  inservice
rserver FW_SEC_2
  ip address 100.201.1.2
  inservice
rserver FW_SEC_3
  ip address 100.201.1.3
  inservice

rserver REAL1
  ip address 20.1.1.1
  inservice
rserver REAL2
  ip address 20.1.1.2
  inservice
rserver REAL3
  ip address 20.1.1.3
  inservice

serverfarm SEC_SF
  predictor hash address destination 255.255.255.255
  transparent
  rserver FW_SEC_1
    inservice
  rserver FW_SEC_2
    inservice
  rserver FW_SEC_3
    inservice

serverfarm SEC_20_SF
  rserver REAL1
    inservice
  rserver REAL2
    inservice
  rserver REAL3
    inservice

class-map match-any SEC_20_VS
  10 match virtual-address 200.1.1.1 255.255.0.0 any
class-map match any FW_SEC_VIP
  10 match virtual-address 0.0.0.0 0.0.0.0 any
```

```
policy-map type loadbalance first-match SEC_20_LB
  class class-default
    serverfarm SEC_20_SF
policy-map multi-match POL_SEC_20
  class SEC_20_VS
    loadbalance vip inservice
    loadbalance policy SEC_20_LB

policy-map type loadbalance first-match LB_FW_SEC
  class class-default
    serverfarm SEC_SF
policy-map multi-match POL_SEC
  class FW_SEC_VIP
    loadbalance vip inservice
    loadbalance policy LB_FW_SEC

interface vlan 201
  ip address 100.201.1.201 255.255.255.0
  access-group input ACL1
  mac-sticky enable
  service-policy input POL_SEC_20
  no shutdown
interface vlan 20
  ip address 20.1.1.20 255.255.255.0
  access-group input ACL1
  service-policy input POL_SEC
  no shutdown
interface vlan 200
  ip address 200.1.1.200 255.255.255.0
  access-group input ACL1
  service-policy input POL_SEC
  no shutdown
```

Example of a Stealth Firewall Configuration

The following configuration example shows those portions of the running configuration that pertain to stealth FWLB. This configuration requires two ACE modules each residing in a different Catalyst 6500 switch.

ACE A Configuration—Stealth Firewall Load Balancing

```
access-list ACL1 line 10 extended permit ip any any

rserver FW_INSEC_1
  ip address 101.0.201.100
  inservice
rserver FW_INSEC_2
  ip address 101.0.202.100
  inservice
rserver FW_INSEC_3
  ip address 101.0.203.100
  inservice

serverfarm INSEC_SF
  transparent
  predictor hash address source 255.255.255.255
  rserver FW_INSEC_1
    inservice
  rserver FW_INSEC_2
    inservice
  rserver FW_INSEC_3
    inservice

class-map match-any FORWARD_VIP
  10 match virtual-address 0.0.0.0 0.0.0.0 any
class-map match-any FW_VIP
  10 match virtual-address 200.1.1.1 255.255.0.0 any
policy-map type loadbalance first-match FORWARD_FW_INSEC
  class class-default
    forward
policy-map type loadbalance first-match LB_FW_INSEC
  class class-default
    serverfarm INSEC_SF
policy-map multi-match FORWARD_INSEC
  class FORWARD_VIP
    loadbalance vip inservice
  class class-default
    loadbalance policy FORWARD_FW_INSEC
```

```
policy-map multi-match POL_INSEC
  class FW_VIP
    loadbalance vip inservice
    loadbalance policy LB_FW_INSEC

interface vlan 100
  ip address 100.100.1.10 255.255.0.0
  access-group input ACL1
  service-policy input POL_INSEC
  no shutdown
interface vlan 101
  ip address 101.0.101.10 255.255.0.0
  access-group input ACL1
  service-policy input FORWARD_INSEC
  no shutdown
interface vlan 102
  ip address 101.0.102.20 255.255.0.0
  access-group input ACL1
  service-policy input FORWARD_INSEC
  no shutdown
interface vlan 103
  ip address 101.0.103.30 255.255.0.0
  access-group input ACL1
  service-policy input FORWARD_INSEC
  no shutdown
```

ACE B Configuration—Stealth Firewall Load Balancing.

```
access-list ACL1 line 10 extended permit ip any any

rserver host REAL1
  ip address 20.1.1.1
  inservice
rserver host REAL2
  ip address 20.1.1.2
  inservice
rserver host REAL3
  ip address 20.1.1.3
  inservice

rserver host FW_SEC_1
  ip address 101.0.101.100
  inservice
rserver host FW_SEC_2
  ip address 101.0.102.100
  inservice
rserver host FW_SEC_3
  ip address 101.0.103.100
  inservice

serverfarm SEC_20_SF
  rserver REAL1
    inservice
  rserver REAL2
    inservice
  rserver REAL3
    inservice
serverfarm SEC_SF
  transparent
  predictor hash address destination 255.255.255.255
  rserver FW_SEC_1
    inservice
  rserver FW_SEC_2
    inservice
  rserver FW_SEC_3
    inservice

class-map match-any SEC_20_VS
  10 match virtual-address 200.1.1.1 255.255.0.0 any
class-map match-any FW_SEC_VIP
  10 match virtual-address 0.0.0.0 0.0.0.0 any
```

```
policy-map type loadbalance first-match SEC_20_LB
  class class-default
    serverfarm SEC_20_SF
policy-map type loadbalance first-match LB_FW_SEC
  class class-default
    serverfarm SEC_SF
policy-map multi-match POL_SEC_20
  class SEC_20_VS
    loadbalance vip inservice
    loadbalance policy SEC_20_LB
policy-map multi-match POL_SEC
  class FW_SEC_VIP
    loadbalance vip inservice
    loadbalance policy LB_FW_SEC

interface vlan 201
  ip address 101.0.201.10 255.255.0.0
  access-group input ACL1
  mac-sticky enable
  service-policy input POL_SEC_20
  no shutdown
interface vlan 202
  ip address 101.0.202.20 255.255.0.0
  access-group input ACL1
  mac-sticky enable
  service-policy input POL_SEC_20
  no shutdown
interface vlan 203
  ip address 101.0.203.30 255.255.0.0
  access-group input ACL1
  mac-sticky enable
  service-policy input POL_SEC_20
  no shutdown
interface vlan 20
  ip address 20.100.1.100 255.255.0.0
  access-group input ACL1
  service-policy input POL_SEC
  no shutdown
interface vlan 200
  ip address 200.1.1.200 255.255.255.0
  access-group input ACL1
  service-policy input POL_SEC
  no shutdown
```