



## Configuring Firewall Load Balancing

---

This chapter describes how to configure firewall load balancing and contains these sections:

- [Understanding How Firewalls Work, page 13-1](#)
- [Configuring Stealth Firewall Load Balancing, page 13-7](#)
- [Configuring Regular Firewall Load Balancing, page 13-16](#)
- [Configuring Reverse-Sticky for Firewalls, page 13-24](#)
- [Configuring Stateful Firewall Connection Remapping, page 13-26](#)

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.

### 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 sending it through unaltered. When a firewall rejects a packet, it usually drops the packet and logs the dropped 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 are configured on that firewall.

This section contains the following:

- [Firewall Types, page 13-2](#)
- [How the CSM-S Distributes Traffic to Firewalls, page 13-2](#)
- [Supported Firewalls, page 13-2](#)
- [Layer 3 Load Balancing to Firewalls, page 13-2](#)
- [Types of Firewall Configurations, page 13-3](#)
- [IP Reverse-Sticky for Firewalls, page 13-3](#)
- [CSM-S Firewall Configurations, page 13-3](#)
- [Fault-Tolerant CSM-S Firewall Configurations, page 13-6](#)

## Firewall Types

The two basic types of firewalls are as follows:

- Regular firewalls
- Stealth firewalls

Regular firewalls have a presence on the network; they are assigned an IP address that allows them to be addressed as a device and seen by other devices on the network.

Stealth firewalls have no presence on the network; they are not assigned an IP address and cannot be addressed or seen by other devices on the network. 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 side of the network) and accept or reject packets based on user-defined sets of policies.

## How the CSM-S Distributes Traffic to Firewalls

The CSM-S load balances traffic to devices configured in server farms. These devices can be servers, firewalls, or any IP-addressable object including an alias IP address. The CSM-S uses load-balancing algorithms to determine how the traffic is balanced among the devices configured in server farms, independent of device type.



### Note

---

We recommend that you configure Layer 3 load balancing on server farms that contain firewalls because of the interactions between higher-layer load-balancing algorithms and server applications.

---

## Supported Firewalls

The CSM-S can load balance traffic to regular or stealth firewalls.

For regular firewalls, a single CSM-S or a pair of CSMs balances traffic among firewalls that contain unique IP addresses, similar to how the CSM-S balances traffic to servers.

For stealth firewalls, a CSM-S balances traffic among unique VLAN alias IP address interfaces on another CSM-S that provides paths through stealth firewalls. A stealth firewall is configured so that all traffic moving in both directions across that VLAN moves through the firewall.

## Layer 3 Load Balancing to Firewalls

When the CSM-S load balances traffic to firewalls, the CSM-S performs the same function that it performs when it load balances traffic to servers. To configure Layer 3 load balancing to firewalls, follow these steps:

- 
- Step 1** Create a server farm for each side of the firewall.
  - Step 2** In serverfarm submode, enter the predictor **hash address** command.
  - Step 3** Assign that server farm to the virtual server that accepts traffic destined for the firewalls.
-

**Note**

When you configure Layer 3 load balancing to firewalls, use source NAT in the forward direction and destination NAT in the reverse direction.

## Types of Firewall Configurations

The CSM-S supports these two firewall configuration types:

- Dual-CSM-S configuration—Firewalls are located between two CSM modules. The firewalls accept traffic from one CSM-S and send it to a second CSM-S for load balancing to servers or return to the requesting device.
- Single-CSM-S configuration—Firewalls accept traffic from a CSM-S and send it back to the same CSM-S for load balancing to servers, or they can return traffic to the requesting device.

## IP Reverse-Sticky for Firewalls

The CSM-S currently supports sticky connections. Sticky connections ensure that two distinct data flows originating from the same client are load balanced to the same destination.

Load-balanced destinations are often real servers. They may be firewalls, caches, or other networking devices. Sticky connections are necessary for the proper functioning of load-balanced applications. These applications utilize multiple connections from the same client to a server. The information transferred on one connection may affect the processing of information transferred on another connection.

The IP reverse-sticky feature is configured for balancing new connections from the same client to the same server, as described in the [“Configuring Reverse-Sticky for Firewalls” section on page 13-24](#). This feature is especially important in the case of buddy connections, such as an FTP data channel or a streaming UDP data channel.

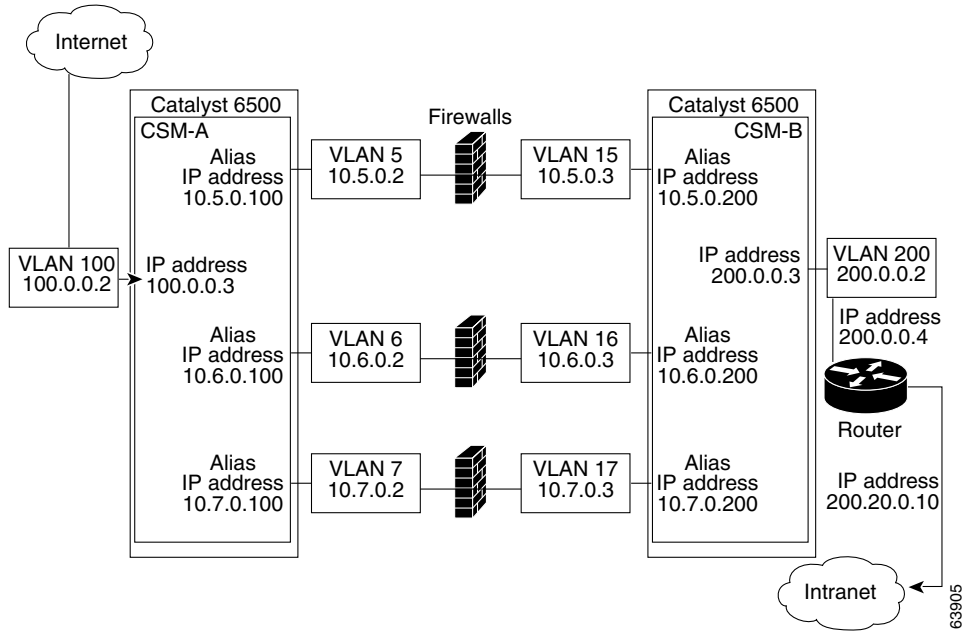
## CSM-S Firewall Configurations

The CSM-S can support these firewall configurations:

- Stealth firewalls for dual CSM-S configurations ([Figure 13-1](#))
- Regular firewalls for dual CSM-S configurations ([Figure 13-2](#))
- Regular firewalls for single CSM-S configurations ([Figure 13-3](#))
- Mixed firewalls (stealth and regular) for dual CSM-S configurations ([Figure 13-4](#))

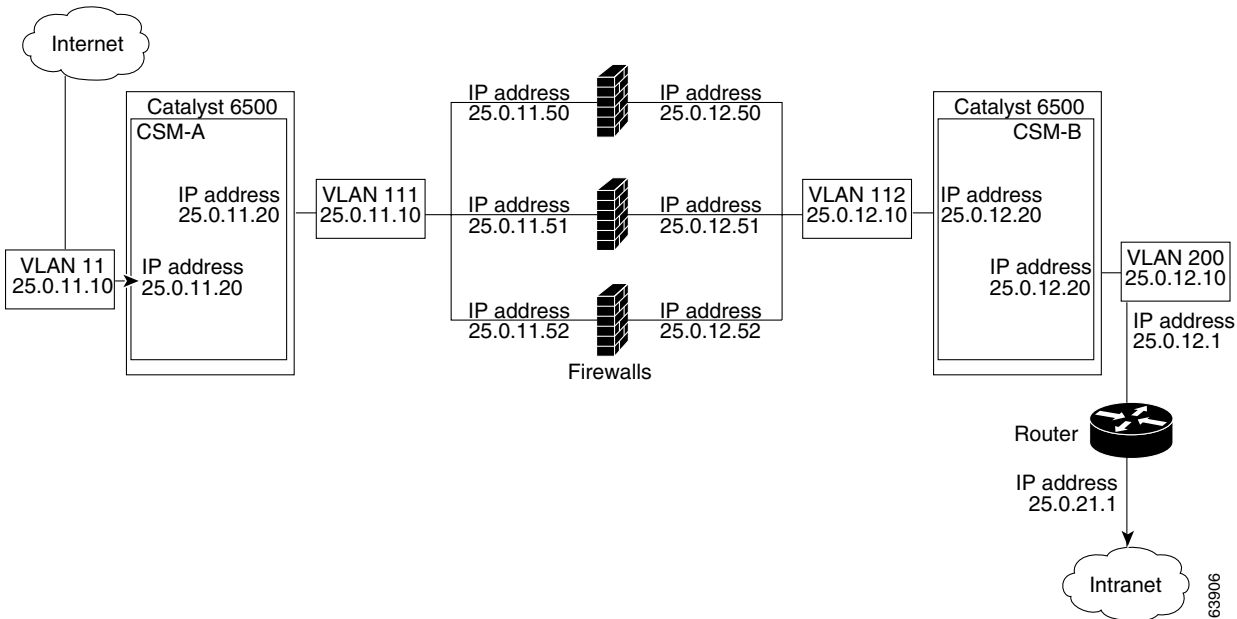
In [Figure 13-1](#), traffic moves through the firewalls and is filtered in both directions. The figure shows the flow from the Internet to the intranet. On the path to the intranet, CSM-S A balances traffic across VLANs 5, 6, and 7 through firewalls to CSM-S B. On the path to the Internet, CSM-S B balances traffic across VLANs 15, 16, and 17 through firewalls to CSM-S A. CSM-S A uses the VLAN aliases of CSM-S B in its server farm, and CSM-S B uses the VLAN aliases of CSM-S A in its server farm.

Figure 13-1 Stealth Firewall Configuration (Dual CSM-S modules Only)



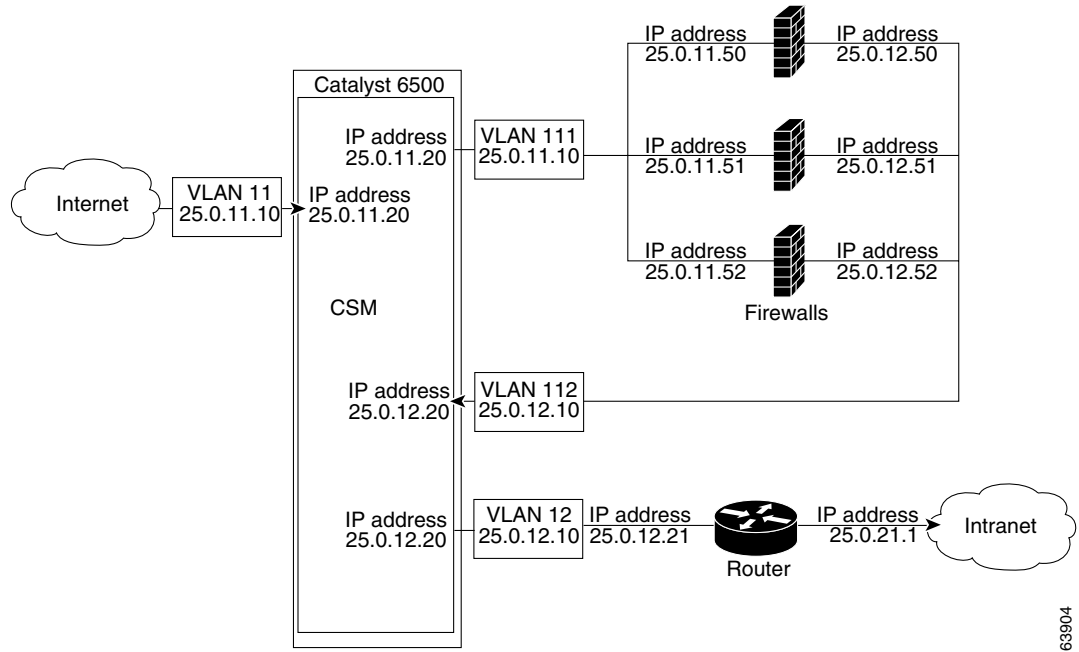
In Figure 13-2, traffic moves through the firewalls and is filtered in both directions. The figure shows the flow from the Internet to the intranet. VLANs 11 and 111 are on the same subnet, and VLANs 12 and 112 are on the same subnet.

Figure 13-2 Regular Firewall Configuration (Dual CSM-S modules)



In Figure 13-3, traffic moves through the firewalls and is filtered in both directions. The figure shows only the flow from the Internet to the intranet, and VLANs 11 and 111 are on the same subnet. VLANs 12 and 112 are on the same subnet.

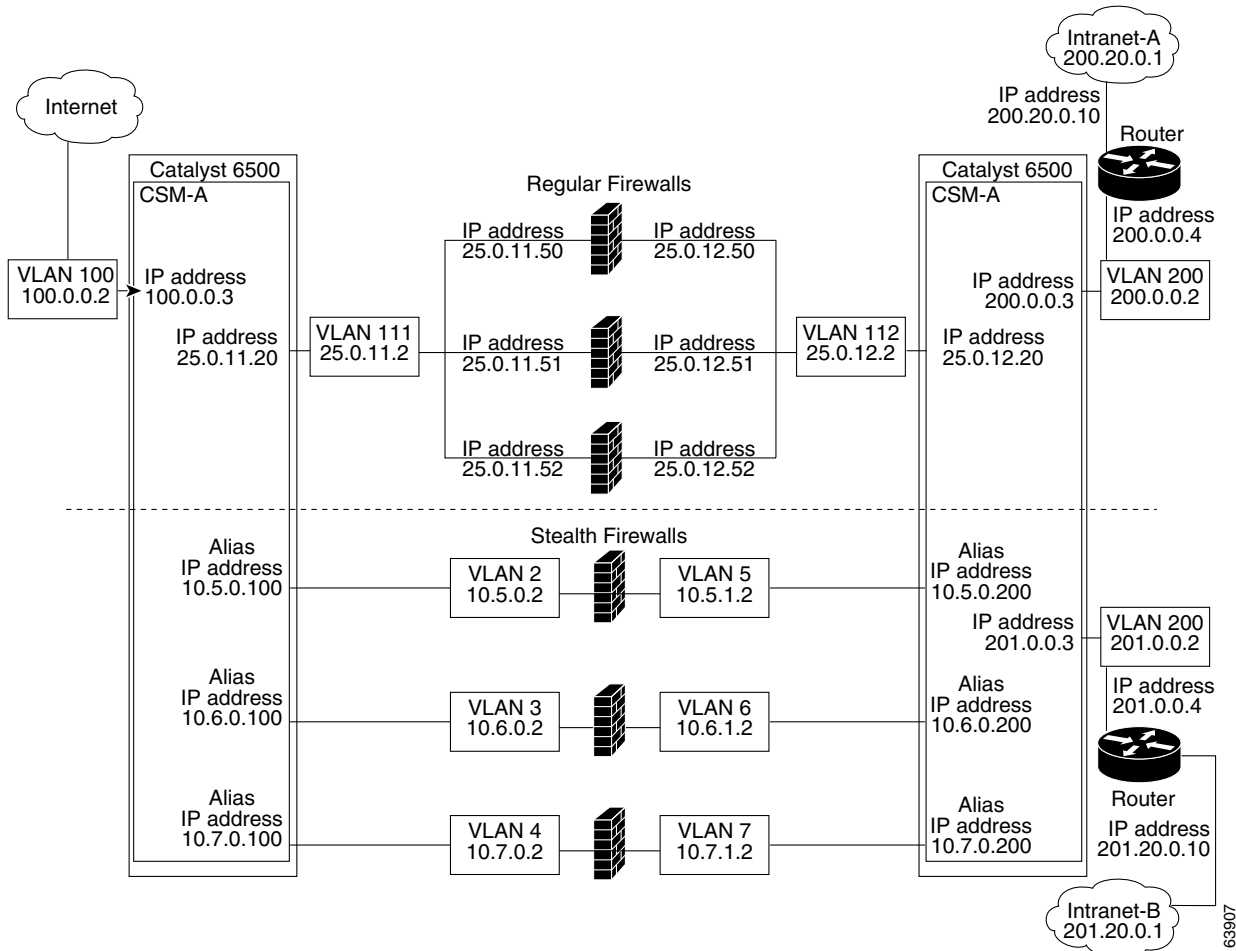
Figure 13-3 Regular Firewall Configuration (Single CSM-S)



In Figure 13-4, traffic moves through both the regular and stealth firewalls and is filtered in both directions. The figure shows the flow from the Internet to the intranet. VLANs 5, 6, and 7 are shared between CSM-S A and CSM-S B. On the path to the intranet, CSM-S A balances traffic across VLANs 5, 6, and 7 through firewalls to CSM-S B. On the path to the intranet, CSM-S B balances traffic across VLANs 5, 6, and 7 through firewalls to CSM-S A.

63904

Figure 13-4 Mixed Firewall Configuration for Stealth and Regular Firewalls (Dual CSM-S Only)



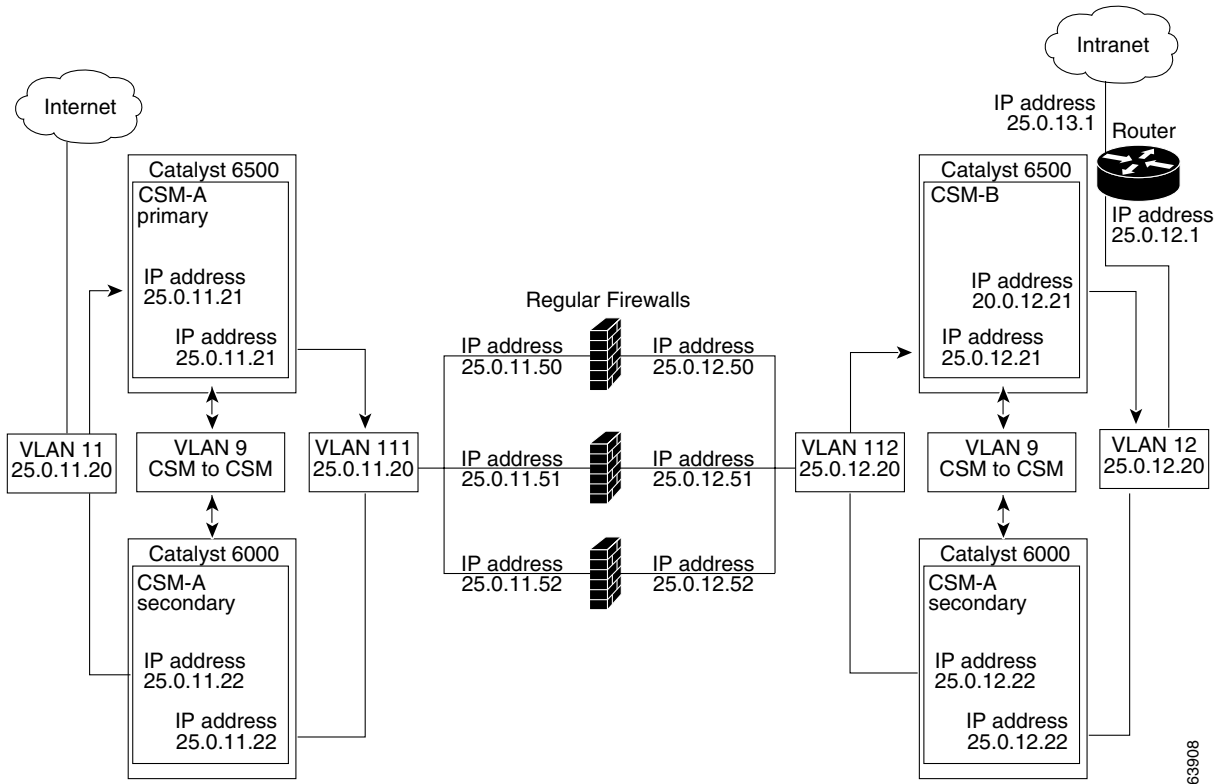
## Fault-Tolerant CSM-S Firewall Configurations

The CSM-S supports fault tolerance for these configurations:

- Stealth firewalls in a fault-tolerant dual CSM-S configuration
- Regular firewalls in a fault-tolerant dual CSM-S configuration
- Regular firewalls in a fault-tolerant single CSM-S configuration
- Mixed firewalls (stealth and regular) in a fault-tolerant dual CSM-S configuration

In [Figure 13-5](#), the traffic moves through the firewalls and is filtered in both directions. The figure only shows the flow from the Internet to the intranet through the primary CSMs, and VLANs 11 and 111 are on the same subnet. VLANs 12 and 112 are on the same subnet.

Figure 13-5 Fault-Tolerant, Regular Firewall Configuration—(Dual CSMs)



## Configuring Stealth Firewall Load Balancing

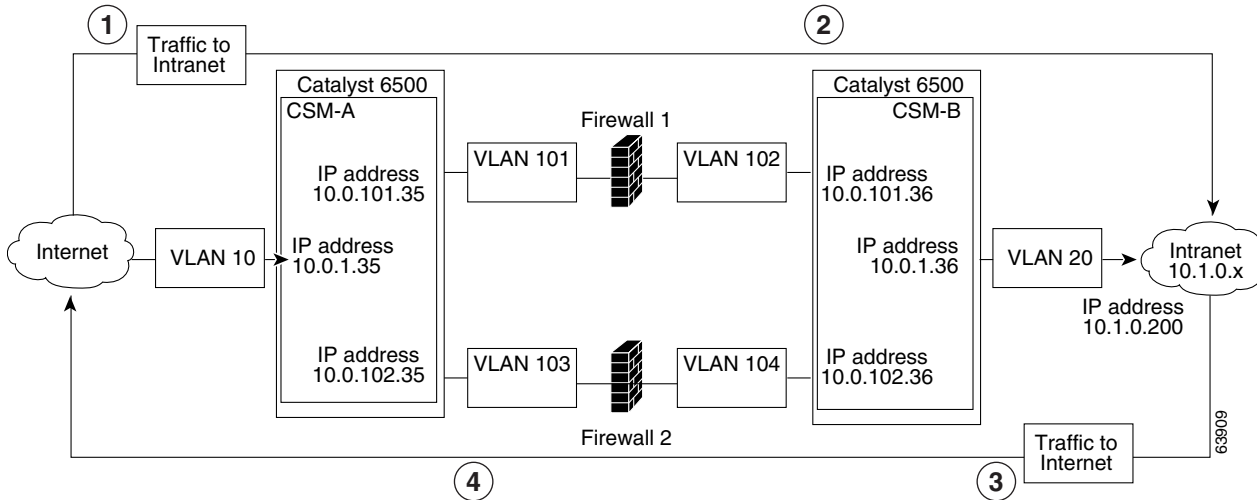
This section describes how to configure firewall load balancing for stealth firewalls and covers the following information:

- [Stealth Firewall Configuration, page 13-7](#)
- [Stealth Firewall Configuration Example, page 13-8](#)

### Stealth Firewall Configuration

In a stealth firewall configuration, firewalls connect to two different VLANs and are configured with IP addresses on the VLANs to which they connect. (See [Figure 13-6](#).)

Figure 13-6 Stealth Firewall Configuration Example



Location	Traffic Direction	Arrives On	Exits On
1	To intranet	VLAN 10	VLANs 101 and 103
2	To intranet	VLANs 101 and 103	VLAN 20
3	To Internet	VLAN 20	VLANs 102 and 104
4	To Internet	VLANs 101 and 103	VLAN 10

Figure 13-6 shows two regular firewalls (Firewall 1 and Firewall 2) located between two CSM modules (CSM-S A and CSM-S B).

**Note**

Stealth firewalls do not have addresses on VLANs.

On the path from the Internet to the intranet, traffic enters the insecure side of the firewalls through separate VLANs, VLAN 101 and VLAN 103, and exits the secure side of the firewalls through separate VLANs, VLAN 102 and VLAN 104. On the path from the intranet to the Internet, the flow is reversed. VLANs also provide connectivity to the Internet (VLAN 10) and to the intranet (VLAN 20).

In a stealth configuration, CSM-S A and CSM-S B load balance traffic through the firewalls.

## Stealth Firewall Configuration Example

The stealth firewall configuration example contains two CSM-S modules (CSM-S A and CSM-S B) installed in separate Catalyst 6500 series switches.

**Note**

In a stealth firewall configuration, each CSM-S must be installed in a separate Catalyst 6500 series switch.

This section describes how to create the stealth firewall configuration for CSM-S A and CSM-S B.

## Configuring CSM-S A (Stealth Firewall Example)

To create the regular configuration example, perform these tasks for CSM-S A:

- [Creating VLANs on Switch A, page 13-9](#)
- [Configuring VLANs on CSM-S A, page 13-9](#)
- [Configuring Server Farms on CSM-S A, page 13-10](#)
- [Configuring Virtual Servers on CSM-S A, page 13-11](#)



### Note

Although the configuration tasks are the same for both the CSM-S A and CSM-S B, the steps, commands, and parameters that you enter are different.

### Creating VLANs on Switch A

To create two VLANs on Switch A, perform this task:

	Command	Purpose
Step 1	Switch-A(config)# <b>vlan</b>	Enters the VLAN mode <sup>1</sup> .
Step 2	Switch-A(vlan)# <b>vlan 10</b>	Creates VLAN 10 <sup>2</sup> .
Step 3	Switch-A(vlan)# <b>vlan 101</b>	Creates VLAN 101 <sup>3</sup> .
Step 4	Switch-A(vlan)# <b>vlan 103</b>	Creates VLAN 103 <sup>4</sup> .

1. Perform this step on the switch console of the switch that contains CSM-S A.
2. VLAN 10 connects CSM-S A to the Internet.
3. VLAN 101 provides a connection through Firewall 1 to CSM-S B.
4. VLAN 103 provides a connection through Firewall 2 to CSM-S B.

### Configuring VLANs on CSM-S A

To configure the three VLANs, perform this task:

	Command	Purpose
Step 1	Switch-A(config)# <b>module csm 5</b>	Enters multiple module configuration mode and specifies that CSM-S A is installed in slot 5.
Step 2	Switch-A(config-module-csm)# <b>vlan 10 client</b>	Specifies VLAN 10 as the VLAN that is being configured, identifies it as a client VLAN, and enters VLAN configuration mode.
Step 3	Switch-A(config-slb-vlan-client)# <b>ip address 10.0.1.35 255.255.255.0</b>	Specifies an IP address and netmask for VLAN 10.
Step 4	Switch-A(config-slb-vlan-client)# <b>alias 10.0.1.30 255.255.255.0</b>	Specifies an alias IP address and netmask for VLAN 10 <sup>1</sup> .
Step 5	Switch-A(config-slb-vlan-client)# <b>exit</b>	Returns to VLAN configuration mode.
Step 6	Switch-A(config-module-csm)# <b>vlan 101 server</b>	Specifies VLAN 101 as the VLAN that is being configured, identifies it as a server VLAN, and enters VLAN configuration mode.

	Command	Purpose
Step 7	Switch-A(config-slb-vlan-server)# <b>ip address 10.0.101.35 255.255.255.0</b>	Specifies an IP address and netmask for VLAN 101.
Step 8	Switch-A(config-slb-vlan-server)# <b>alias 10.0.101.100 255.255.255.0</b>	Specifies an alias IP address and netmask for VLAN 101 <sup>1</sup> .
Step 9	Switch-A(config-slb-vlan-server)# <b>exit</b>	Returns to VLAN configuration mode.
Step 10	Switch-A(config-module-csm)# <b>vlan 103 server</b>	Specifies VLAN 103 as the VLAN that is being configured, identifies it as a server VLAN, and enters VLAN configuration mode.
Step 11	Switch-A(config-slb-vlan)# <b>ip address 10.0.102.35 255.255.255.0</b>	Specifies an IP address and netmask for VLAN 103.
Step 12	Switch-A(config-slb-vlan)# <b>alias 10.0.102.100 255.255.255.0</b>	Specifies an alias IP address and netmask for VLAN 103 <sup>1</sup> .

1. This step provides a target for CSM-S B to use in making a load-balancing decision.

## Configuring Server Farms on CSM-S A



**Note** Because the IP addresses of CSM-S B are listed in the INSIDE-SF server farm as real servers, CSM-S A will load balance the two firewalls that exist in the path to CSM-S B.

To configure two server farms on CSM-S A, perform this task:

	Command	Purpose
Step 1	Switch-A(config)# <b>module csm 5</b>	Enters multiple module configuration mode and specifies that CSM-S A is installed in slot 5.
Step 2	Switch-A(config-module-csm)# <b>serverfarm FORWARD-SF</b>	Creates and names the FORWARD-SF <sup>1</sup> server farm (actually a forwarding policy) and enters serverfarm configuration mode.
Step 3	Switch-A(config-slb-sfarm)# <b>no nat server</b>	Disables the NAT of server IP addresses and port numbers <sup>2</sup> .
Step 4	Switch-A(config-slb-sfarm)# <b>predictor forward</b>	Forwards traffic in accordance with its internal routing tables rather than a load-balancing algorithm.
Step 5	Switch-A(config-slb-sfarm)# <b>exit</b>	Returns to multiple module configuration mode.
Step 6	Switch-A(config-module-csm)# <b>serverfarm TO-INSIDE-SF</b>	Creates and names the INSIDE-SF <sup>3</sup> server farm (that will contain alias IP addresses rather than real servers) and enters serverfarm configuration mode.
Step 7	Switch-A(config-slb-sfarm)# <b>no nat server</b>	Disables the NAT of the server IP address and port number <sup>4</sup> .
Step 8	Switch-A(config-slb-sfarm)# <b>predictor hash address source 255.255.255.255</b>	Selects a server using a hash value based on the source IP address <sup>5</sup> .
Step 9	Switch-A(config-slb-sfarm)# <b>real 10.0.101.200</b>	Identifies the alias IP address of CSM-S B that lies on the path to Firewall 1 as a real server and enters real server configuration submenu.

	Command	Purpose
Step 10	Switch-A(config-slb-real)# <b>inservice</b>	Enables the firewall.
Step 11	Switch-A(config-slb-real)# <b>exit</b>	Returns to serverfarm configuration mode.
Step 12	Switch-A(config-slb-sfarm)# <b>real</b> <b>10.0.102.200</b>	Identifies the alias IP address of CSM-S B that lies on the path to Firewall 2 as a real server and enters real server configuration submode.
Step 13	Switch-A(config-slb-real)# <b>inservice</b>	Enables the firewall.

- FORWARD-SF is actually a route forwarding policy, not an actual server farm, that allows traffic to reach the Internet (through VLAN 10). It does not contain any real servers.
- This step is required when configuring a server farm that contains a forwarding policy rather than real servers.
- INSIDE-SF contains the two alias IP addresses of CSM-S B listed as real servers that allow traffic from the intranet to reach CSM-S B.
- This step is required when configuring a server farm that contains firewalls.
- We recommend that you perform this step when configuring insecure-side firewall interfaces in a server farm.

### Configuring Virtual Servers on CSM-S A

To configure three virtual servers on CSM-S A, perform this task:

	Command	Purpose
Step 1	Switch-A(config)# <b>module csm 5</b>	Enters multiple module configuration mode and specifies that the CSM-S A is installed in slot 5.
Step 2	Switch-A(config-module-csm)# <b>vserver</b> <b>FORWARD-V101</b>	Specifies FORWARD-V101 <sup>1</sup> as the virtual server that is being configured and enters virtual server configuration mode.
Step 3	Switch-A(config-slb-vserver)# <b>virtual</b> <b>0.0.0.0 0.0.0.0 any</b>	Specifies a match for any IP address and any protocol <sup>2</sup> .
Step 4	Switch-A(config-slb-vserver)# <b>vlan 101</b>	Specifies that the virtual server will only accept traffic arriving on VLAN 101, which is traffic arriving from the insecure side of the firewalls.
Step 5	Switch-A(config-slb-vserver)# <b>serverfarm</b> <b>FORWARD-SF</b>	Specifies the server farm for this virtual server <sup>3</sup> .
Step 6	Switch-A(config-slb-vserver)# <b>inservice</b>	Enables the virtual server.
Step 7	Switch-A(config-slb-vserver)# <b>exit</b>	Returns to multiple module configuration mode.
Step 8	Switch-A(config-module-csm)# <b>vserver</b> <b>FORWARD-V103</b>	Specifies FORWARD-V103 <sup>4</sup> as the virtual server that is being configured and enters virtual server configuration mode.
Step 9	Switch-A(config-slb-vserver)# <b>virtual</b> <b>0.0.0.0 0.0.0.0 any</b>	Specifies a match for any IP address and any protocol <sup>5</sup> .
Step 10	Switch-A(config-slb-vserver)# <b>vlan 103</b>	Specifies that the virtual server will only accept traffic arriving on VLAN 103, which is traffic arriving from the insecure side of the firewalls.
Step 11	Switch-A(config-slb-vserver)# <b>serverfarm</b> <b>FORWARD-SF</b>	Specifies the server farm for this virtual server <sup>3</sup> .
Step 12	Switch-A(config-slb-vserver)# <b>inservice</b>	Enables the virtual server.
Step 13	Switch-A(config-slb-vserver)# <b>exit</b>	Returns to multiple module configuration mode.

	Command	Purpose
Step 14	Switch-A(config-module-csm) # <b>vserver</b> <b>OUTSIDE-VS</b>	Specifies OUTSIDE-VS <sup>6</sup> as the virtual server that is being configured and enters virtual server configuration mode.
Step 15	Switch-A(config-slb-vserver) # <b>virtual</b> <b>10.1.0.0 255.255.255.0 any</b>	Specifies the IP address, netmask, and protocol (any) for this virtual server. Clients reach the server farm represented by this virtual server through this address.
Step 16	Switch-A(config-slb-vserver) # <b>vlan 10</b>	Specifies that the virtual server will only accept traffic arriving on VLAN 10, which is traffic arriving from the Internet.
Step 17	Switch-A(config-slb-vserver) # <b>serverfarm</b> <b>TO-INSIDE-SF</b>	Specifies the server farm for this virtual server <sup>7</sup> .
Step 18	Switch-A(config-slb-vserver) # <b>inservice</b>	Enables the virtual server.

1. FORWARD-V101 allows Internet traffic to reach the insecure side of the firewalls (through VLAN 101).
2. Client matching is only limited by VLAN restrictions. (See Step 4.)
3. This server farm is actually a forwarding predictor rather than an actual server farm containing real servers.
4. FORWARD-V103 allows Internet traffic to reach the insecure side of the firewalls (through VLAN 103).
5. Clients will always match (see Step 9)—only being limited by VLAN restrictions. (See Step 10.)
6. OUTSIDE-VS allows traffic from the Internet to reach CSM-S A (through VLAN 10).
7. The server farm contains the alias IP addresses of CSM-S B that lie along the path of Firewall 1 and Firewall 2.

## Configuring CSM-S B (Stealth Firewall Example)

To create the regular configuration example, perform the following configuration tasks for CSM-S B:

- [Creating VLANs on Switch B, page 13-12](#)
- [Configuring VLANs on CSM-S B, page 13-13](#)
- [Configuring Server Farms on CSM-S B, page 13-13](#)
- [Configuring Virtual Servers on CSM-S B, page 13-15](#)



### Note

Although the configuration tasks are the same for both CSM-S A and CSM-S B, the steps, commands, and parameters that you enter are different.

## Creating VLANs on Switch B

To create three VLANs on Switch B, perform this task:



### Note

This example assumes that the CSM-S modules are in separate Catalyst 6500 series switches. If they are in the same chassis, you can create all of the VLANs on the same Catalyst 6500 series switch console.

	Command	Purpose
Step 1	Switch-B(config) # <b>vlan</b>	Enters the VLAN mode <sup>1</sup> .
Step 2	Switch-B(vlan) # <b>vlan 102</b>	Creates VLAN 102 <sup>2</sup> .

	Command	Purpose
Step 3	Switch-B(vlan)# <b>vlan 104</b>	Creates VLAN 104 <sup>3</sup> .
Step 4	Switch-B(vlan)# <b>vlan 200</b>	Creates VLAN 200 <sup>4</sup> .

1. Do this step on the switch console of the switch that contains CSM-S B.
2. VLAN 102 provides a connection through Firewall 1 to CSM-S A.
3. VLAN 104 provides a connection through Firewall 2 to CSM-S A.
4. VLAN 200 provides the connection to the internal network.

### Configuring VLANs on CSM-S B

To configure the three VLANs, perform this task:

	Command	Purpose
Step 1	Switch-B(config)# <b>module csm 6</b>	Enters multiple module configuration mode and specifies that CSM-S B is installed in slot 6.
Step 2	Switch-B(config-module-csm)# <b>vlan 102 server</b>	Specifies VLAN 102 as the VLAN that is being configured, identifies it as a server VLAN, and enters VLAN configuration mode.
Step 3	Switch-B(config-slb-vlan-server)# <b>ip address 10.0.101.36 255.255.255.0</b>	Specifies an IP address and netmask for VLAN 102.
Step 4	Switch-B(config-slb-vlan-server)# <b>alias 10.0.101.200 255.255.255.0</b>	Specifies an alias IP address and netmask for VLAN 102 <sup>1</sup> .
Step 5	Switch-B(config-slb-vlan-server)# <b>exit</b>	Returns to multiple module configuration mode.
Step 6	Switch-B(config-module-csm)# <b>vlan 104 server</b>	Specifies VLAN 104 as the VLAN that is being configured, identifies it as a server VLAN, and enters VLAN configuration mode.
Step 7	Switch-B(config-slb-vlan-server)# <b>ip address 10.0.102.36 255.255.255.0</b>	Specifies an IP address and netmask for VLAN 104.
Step 8	Switch-B(config-slb-vlan)# <b>alias 10.0.102.200 255.255.255.0</b>	Specifies an alias IP address and netmask for VLAN 104 <sup>1</sup> .
Step 9	Switch-B(config-slb-vlan-server)# <b>exit</b>	Returns to multiple module configuration mode.
Step 10	Switch-B(config-module-csm)# <b>vlan 20 server</b>	Specifies VLAN 20 as the VLAN that is being configured, identifies it as a server VLAN, and enters VLAN configuration mode.
Step 11	Switch-B(config-slb-vlan-server)# <b>ip address 10.1.0.36 255.255.255.0</b>	Specifies an IP address and netmask for VLAN 20.

1. This step provides a target for CSM-S A to use in making a load-balancing decision.

### Configuring Server Farms on CSM-S B

To configure three server farms on CSM-S B, perform this task:



**Note** SERVERS-SF specifies that client NAT will be performed using a pool of client NAT addresses that are created earlier in the example using the **natpool** command. You must create the NAT pool before referencing the command.

	<b>Command</b>	<b>Purpose</b>
<b>Step 1</b>	Switch-B(config)# <b>module csm 6</b>	Enters multiple module configuration mode and specifies that CSM-S B is installed in slot 6.
<b>Step 2</b>	Switch-B(config-module-csm)# <b>serverfarm FORWARD-SF</b>	Creates and names the FORWARD-SF <sup>1</sup> server farm (actually a forwarding policy) and enters serverfarm configuration mode.
<b>Step 3</b>	Switch-B(config-slb-sfarm)# <b>no nat server</b>	Disables the NAT of server IP addresses and port numbers <sup>2</sup> .
<b>Step 4</b>	Switch-B(config-slb-sfarm)# <b>predictor forward</b>	Forwards traffic in accordance with its internal routing tables rather than a load-balancing algorithm.
<b>Step 5</b>	Switch-B(config-slb-sfarm)# <b>exit</b>	Returns to multiple module configuration mode.
<b>Step 6</b>	Switch-B(config-module-csm)# <b>serverfarm TO-OUTSIDE-SF</b>	Creates and names the GENERIC-SF server farm and enters serverfarm configuration mode <sup>3</sup> .
<b>Step 7</b>	Switch-B(config-slb-sfarm)# <b>no nat server</b>	Disables NAT of server IP addresses and port numbers <sup>4</sup> .
<b>Step 8</b>	Switch-B(config-slb-sfarm)# <b>real 10.0.101.100</b>	Identifies the alias IP address of CSM-S A that is locked on the path to Firewall 1 as a real server and enters real server configuration submode.
<b>Step 9</b>	Switch-B(config-slb-real)# <b>inservice</b>	Enables the real server (actually an alias IP address).
<b>Step 10</b>	Switch-B(config-slb-real)# <b>exit</b>	Returns to the serverfarm configuration mode.
<b>Step 11</b>	Switch-B(config-slb-sfarm)# <b>real 10.0.102.100</b>	Identifies the alias IP address of CSM-S B that is located on the path to Firewall 2 as a real server and enters real server configuration submode.
<b>Step 12</b>	Switch-B(config-slb-real)# <b>inservice</b>	Enables the real server (actually an alias IP address).
<b>Step 13</b>	Switch-B(config-slb-real)# <b>exit</b>	Returns to serverfarm configuration mode.
<b>Step 14</b>	Switch-B(config-module-csm)# <b>serverfarm SERVERS-SF</b>	Creates and names the SERVERS-SF <sup>5</sup> server farm and enters serverfarm configuration mode.
<b>Step 15</b>	Switch-B(config-slb-sfarm)# <b>real 10.1.0.101</b>	Identifies a server in the intranet as a real server, assigns it an IP address, and enters real server configuration submode.
<b>Step 16</b>	Switch-B(config-slb-real)# <b>inservice</b>	Enables the real server.
<b>Step 17</b>	Switch-B(config-slb-real)# <b>exit</b>	Returns to serverfarm configuration mode.
<b>Step 18</b>	Switch-B(config-slb-sfarm)# <b>real 10.1.0.102</b>	Identifies a server in the intranet as a real server, assigns it an IP address, and enters real server configuration submode.
<b>Step 19</b>	Switch-B(config-slb-real)# <b>inservice</b>	Enables the real server.
<b>Step 20</b>	Switch-B(config-slb-sfarm)# <b>real 10.1.0.103</b>	Identifies a server in the intranet as a real server, assigns it an IP address, and enters real server configuration submode.
<b>Step 21</b>	Switch-B(config-slb-real)# <b>inservice</b>	Enables the real server.

1. FORWARD-SF is actually a route forwarding policy, not an actual server farm, that allows traffic to reach the intranet (through VLAN 20). It does not contain any real servers.

2. This step is required when configuring a server farm that contains a forwarding policy rather than real servers.
3. OUTSIDE-SF contains the two alias IP addresses of CSM-S A as the real servers allowing traffic from the intranet to reach CSM-S A.
4. This step is required when configuring a server farm that contains a forwarding policy rather than real servers.
5. SERVERS-SF contains the IP addresses of the real servers located within the intranet.

## Configuring Virtual Servers on CSM-S B

To configure three virtual servers on CSM-S, perform this task:

	Command	Purpose
Step 1	Switch-B(config)# <b>module csm 6</b>	Enters multiple module configuration mode and specifies that CSM-S B is installed in slot 6.
Step 2	Switch-B(config-module-csm)# <b>vserver FORWARD-VS-102</b>	Specifies FORWARD-VS as the virtual server that is being configured and enters virtual server configuration mode.
Step 3	Switch-B(config-slb-vserver)# <b>virtual 0.0.0.0 0.0.0.0 any</b>	Specifies a match for any IP address and any protocol <sup>1</sup> .
Step 4	Switch-B(config-slb-vserver)# <b>vlan 102</b>	Specifies that the virtual server will only accept traffic arriving on VLAN 102, which is traffic arriving from the secure side of the Firewall 1.
Step 5	Switch-B(config-slb-vserver)# <b>serverfarm FORWARD-SF</b>	Specifies the server farm for this virtual server <sup>2</sup> .
Step 6	Switch-B(config-slb-vserver)# <b>inservice</b>	Enables the virtual server.
Step 7	Switch-B(config-slb-vserver)# <b>exit</b>	Returns to multiple module configuration mode.
Step 8	Switch-B(config-module-csm)# <b>vserver FORWARD-VS-104</b>	Specifies FORWARD-VS <sup>3</sup> as the virtual server that is being configured and enters virtual server configuration mode.
Step 9	Switch-B(config-slb-vserver)# <b>virtual 0.0.0.0 0.0.0.0 any</b>	Specifies a match for any IP address and any protocol <sup>1</sup> .
Step 10	Switch-B(config-slb-vserver)# <b>vlan 104</b>	Specifies that the virtual server will only accept traffic arriving on VLAN 104, which is traffic arriving from the secure side of the Firewall 2.
Step 11	Switch-B(config-slb-vserver)# <b>serverfarm FORWARD-SF</b>	Specifies the server farm for this virtual server <sup>2</sup> .
Step 12	Switch-B(config-slb-vserver)# <b>inservice</b>	Enables the virtual server.
Step 13	Switch-B(config-slb-vserver)# <b>exit</b>	Returns to multiple module configuration mode.
Step 14	Switch-B(config-module-csm)# <b>vserver INSIDE-VS</b>	Specifies INSIDE-VS <sup>4</sup> as the virtual server that is being configured and enters virtual server configuration mode.
Step 15	Switch-B(config-slb-vserver)# <b>virtual 0.0.0.0 0.0.0.0 any</b>	Specifies a match for any IP address and any protocol <sup>1</sup> .
Step 16	Switch-B(config-slb-vserver)# <b>vlan 20</b>	Specifies that the virtual server will only accept traffic arriving on VLAN 20, which is traffic arriving from the intranet.

	Command	Purpose
Step 17	Switch-B(config-slb-vserver) # <b>serverfarm TO-OUTSIDE-SF</b>	Specifies the server farm for this virtual server (containing the alias IP addresses of CSM-S A as real servers and allowing traffic to flow through Firewalls 1 and 2) and enters real server configuration submode.
Step 18	Switch-B(config-slb-vserver) # <b>inservice</b>	Enables the virtual server.
Step 19	Switch-B(config-slb-vserver) # <b>exit</b>	Returns to multiple module configuration mode.
Step 20	Switch-B(config-module-csm) # <b>vserver TELNET-VS</b>	Specifies TELNET-VS <sup>5</sup> as the virtual server that is being configured and enters virtual server configuration mode.  <b>Note</b> TELNET-VS does not use a VLAN limit; any source traffic (from firewalls or internal network) will be load balanced through this address.
Step 21	Switch-B(config-slb-vserver) # <b>virtual 10.1.0.200 255.255.255.0 tcp telnet</b>	Specifies the IP address, netmask, protocol (TCP), and port (Telnet) for this virtual server <sup>6</sup> .
Step 22	Switch-B(config-slb-vserver) # <b>serverfarm SERVERS-SF</b>	Specifies the server farm containing real servers for this virtual server.
Step 23	Switch-B(config-slb-vserver) # <b>inservice</b>	Enables the virtual server.

1. Client matching is only limited by VLAN restrictions.
2. This server farm is actually a forwarding predictor rather than an actual server farm containing real servers.
3. FORWARD-VS allows traffic from the Internet to reach the intranet through VLAN 20.
4. INSIDE-VS allows traffic from the intranet to reach CSM-S A through Firewall 1 (through VLANs 102 and 101) or Firewall 2 (through VLANs 104 and 103).
5. TELNET-VS allows traffic from the Internet to reach Telnet servers in the internal network.
6. Clients reach the server farm represented by this virtual server through this address.

## Configuring Regular Firewall Load Balancing

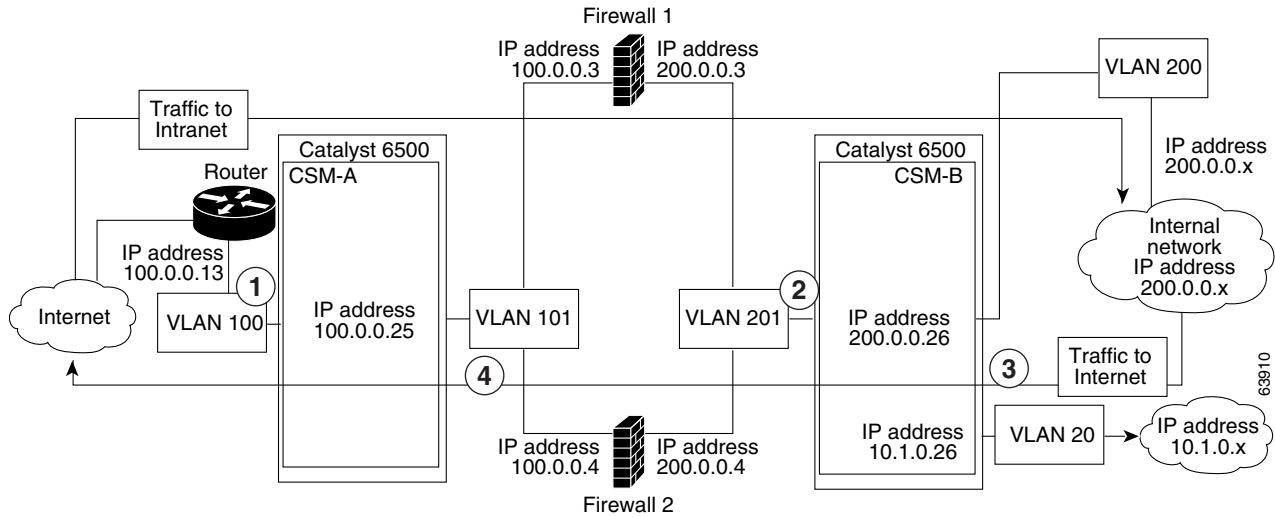
This section describes how to configure firewall load balancing for regular firewalls and provides the following information:

- [Packet Flow in a Regular Firewall Configuration, page 13-16](#)
- [Regular Firewall Configuration Example, page 13-17](#)

## Packet Flow in a Regular Firewall Configuration

In a regular firewall configuration, firewalls connect to two different VLANs and are configured with IP addresses on the VLANs to which they connect. (See [Figure 13-7](#).)

Figure 13-7 Regular Firewall Configuration Example



Item	Traffic Direction	Arrives On	Exits On
1	To intranet	VLAN 100	VLANs 101
2	To intranet	VLANs 201	VLAN 200 and 20
3	To Internet	VLAN 200 and 20	VLANs 201
4	To Internet	VLANs 101	VLAN 100

Figure 13-7 shows two regular firewalls (Firewall 1 and Firewall 2) located between two CSM-S modules (CSM-S A and CSM-S B). Traffic enters and exits the firewalls through shared VLANs (VLAN 101 and VLAN 201). Both regular firewalls have unique addresses on each shared VLAN.

VLANs provide connectivity to the Internet (VLAN 100), the internal network (VLAN 200), and to internal server farms (VLAN 20).

The CSM-S balances traffic among regular firewalls as if they were real servers. Regular firewalls are configured in server farms with IP addresses like real servers. The server farms to which regular firewalls belong are assigned a load-balancing predictor and are associated with virtual servers.

## Regular Firewall Configuration Example

The regular firewall configuration example contains two CSM-S modules (CSM-S A and CSM-S B) installed in separate Catalyst 6500 series switches.



**Note**

You can use this example when configuring two CSM-S modules in the same Catalyst 6500 series switch chassis. You can also use this example when configuring a single CSM-S in a single switch chassis, assuming that you specify the slot number of that CSM-S when configuring both CSM-S A and CSM-S B.

## Configuring CSM-S A (Regular Firewall Example)

To create the regular configuration example, perform the following configuration tasks for CSM-S A:

- [Creating VLANs on Switch A, page 13-18](#)
- [Configuring VLANs on CSM-S A, page 13-18](#)
- [Configuring Server Farms on CSM-S A, page 13-19](#)
- [Configuring Virtual Servers on CSM-S A, page 13-20](#)



### Note

Although the configuration tasks are the same for both CSM-S A and CSM-S B, the steps, commands, and parameters that you enter are different.

## Creating VLANs on Switch A

The example, shown in [Figure 13-7](#), requires that you create two VLANs on Switch A.



### Note

This example assumes that the CSM-S modules are in separate Catalyst 6500 series switch chassis. If they are in the same chassis, all of the VLANs can be created on the same Catalyst 6500 series switch console.

To configure VLANs on Switch A, perform this task:

	Command	Purpose
Step 1	Switch-A(config)# <b>vlan</b>	Enters the VLAN mode <sup>1</sup> .
Step 2	Switch-A(vlan)# <b>vlan 100</b>	Creates VLAN 100 <sup>2</sup> .
Step 3	Switch-A(vlan)# <b>vlan 101</b>	Creates VLAN 101 <sup>3</sup> .

1. Do this step on the switch console of the switch that contains CSM-S A.
2. VLAN 100 connects CSM-S A to the Internet.
3. VLAN 101 connects CSM-S A to the insecure side of the firewalls.

## Configuring VLANs on CSM-S A

To configure the two VLANs, perform this task:

	Command	Purpose
Step 1	Switch-A(config)# <b>module csm 5</b>	Enters multiple module configuration mode and specifies that CSM-S A is installed in slot 5.
Step 2	Switch-A(config-module-csm)# <b>vlan 100 client</b>	Specifies VLAN 100 as the VLAN that is being configured, identifies it as a client VLAN, and enters VLAN configuration mode.
Step 3	Switch-A(config-slb-vlan-client)# <b>ip address 100.0.0.25 255.255.255.0</b>	Specifies an IP address and netmask for VLAN 100.
Step 4	Switch-A(config-slb-vlan-client)# <b>gateway 100.0.0.13</b>	Configures a gateway IP address for the router on the Internet side of CSM-S A.
Step 5	Switch-A(config-slb-vlan-client)# <b>exit</b>	Returns to multiple module configuration mode.

	Command	Purpose
Step 6	Switch-A(config-module-csm)# <b>vlan 101 server</b>	Specifies VLAN 101 as the VLAN that is being configured, identifies it as a server VLAN, and enters VLAN configuration mode.
Step 7	Switch-A(config-slb-vlan-server)# <b>ip address 100.0.0.25 255.255.255.0</b>	Specifies an IP address and netmask for VLAN 101.
Step 8	Switch-A(config-slb-vlan-server)# <b>alias 100.0.0.20 255.255.255.0</b>	Specifies an alias IP address and netmask for VLAN 101 <sup>1</sup> .

1. This step provides a target for CSM-S B to use in making a load-balancing decision.

## Configuring Server Farms on CSM-S A



**Note** Firewall 1 and Firewall 2 secure-side IP addresses are configured as real servers in the SEC-SF server farm associated with CSM-S B.

To configure two server farms on CSM-S A, perform this task:

	Command	Purpose
Step 1	Switch-A(config)# <b>module csm 5</b>	Enters multiple module configuration mode and specifies that CSM-S A is installed in slot 5.
Step 2	Switch-A(config-module-csm)# <b>serverfarm FORWARD-SF</b>	Creates and names the FORWARD-SF <sup>1</sup> server farm (actually a forwarding policy) and enters serverfarm configuration mode.
Step 3	Switch-A(config-slb-sfarm)# <b>no nat server</b>	Disables the NAT of server IP addresses and port numbers <sup>2</sup> .
Step 4	Switch-A(config-slb-sfarm)# <b>predictor forward</b>	Forwards traffic by adhering to its internal routing tables rather than a load-balancing algorithm.
Step 5	Switch-A(config-slb-sfarm)# <b>exit</b>	Returns to multiple module configuration mode.
Step 6	Switch-A(config-module-csm)# <b>serverfarm INSEC-SF</b>	Creates and names the INSEC-SF <sup>3</sup> server farm (which will contain firewalls as real servers) and enters serverfarm configuration mode.
Step 7	Switch-A(config-slb-sfarm)# <b>no nat server</b>	Disables the NAT of the server IP address and port number <sup>4</sup> .
Step 8	Switch-A(config-slb-sfarm)# <b>predictor hash address source 255.255.255.255</b>	Selects a server using a hash value based on the source IP address <sup>5</sup> .
Step 9	Switch-A(config-slb-sfarm)# <b>real 100.0.0.3</b>	Identifies Firewall 1 as a real server, assigns an IP address to its insecure side, and enters real server configuration submode.
Step 10	Switch-A(config-slb-real)# <b>inservice</b>	Enables the firewall.
Step 11	Switch-A(config-slb-real)# <b>exit</b>	Returns to serverfarm configuration mode.
Step 12	Switch-A(config-slb-sfarm)# <b>real 100.0.0.4</b>	Identifies Firewall 2 as a real server, assigns an IP address to its insecure side, and enters real server configuration submode.
Step 13	Switch-A(config-slb-real)# <b>inservice</b>	Enables the firewall.

1. FORWARD-SF is actually a route forwarding policy, not an actual server farm, that allows traffic to reach the Internet (through VLAN 100); it does not contain any real servers.
2. This is a required step when configuring a server farm that contains a forwarding policy rather than real servers.
3. INSEC-SF contains (Firewall 1 and Firewall 2); their insecure-side IP addresses are configured as real servers in this server farm.
4. This is a required step when configuring a server farm that contains firewalls.
5. We recommend this step when configuring insecure-side firewall interfaces in a server farm.

## Configuring Virtual Servers on CSM-S A

To configure two virtual servers on CSM-S A, perform this task:

	Command	Purpose
Step 1	Switch-A(config)# <b>module csm 5</b>	Enters multiple module configuration mode and specifies that the CSM-S A is installed in slot 5.
Step 2	Switch-A(config-module-csm)# <b>vserver FORWARD-VS</b>	Specifies FORWARD-VS <sup>1</sup> as the virtual server that is being configured and enters virtual server configuration mode.
Step 3	Switch-A(config-slb-vserver)# <b>virtual 0.0.0.0 0.0.0.0 any</b>	Specifies a match for any IP address and any protocol <sup>2</sup> .
Step 4	Switch-A(config-slb-vserver)# <b>vlan 101</b>	Specifies that the virtual server will only accept traffic arriving on VLAN 101, which is traffic arriving from the insecure side of the firewalls.
Step 5	Switch-A(config-slb-vserver)# <b>serverfarm FORWARD-SF</b>	Specifies the server farm for this virtual server <sup>3</sup> .
Step 6	Switch-A(config-slb-vserver)# <b>inservice</b>	Enables the virtual server.
Step 7	Switch-A(config-slb-vserver)# <b>exit</b>	Returns to multiple module configuration mode.
Step 8	Switch-A(config-module-csm)# <b>vserver INSEC-VS</b>	Specifies INSEC-VS <sup>4</sup> as the virtual server that is being configured and enters virtual server configuration mode.
Step 9	Switch-A(config-slb-vserver)# <b>virtual 200.0.0.0 255.255.255.0 any</b>	Specifies the IP address, netmask, and protocol (any) for this virtual server <sup>5</sup> .
Step 10	Switch-A(config-slb-vserver)# <b>vlan 100</b>	Specifies that the virtual server will only accept traffic arriving on VLAN 100, which is traffic arriving from the Internet.
Step 11	Switch-A(config-slb-vserver)# <b>serverfarm INSEC-SF</b>	Specifies the server farm for this virtual server <sup>6</sup> .
Step 12	Switch-A(config-slb-vserver)# <b>inservice</b>	Enables the virtual server.

1. FORWARD-VS allows Internet traffic to reach the insecure side of the firewalls (through VLAN 101).
2. Client matching is only limited by VLAN restrictions. (See Step 4.)
3. This server farm is actually a forwarding predictor rather than an actual server farm containing real servers.
4. INSEC-VS allows traffic from the Internet to reach CSM-S A (through VLAN 101).
5. Clients reach the server farm represented by this virtual server through this address.
6. The server farm contains firewalls rather than real servers.

## Configuring CSM-S B (Regular Firewall Example)

To create the regular configuration example, perform the following configuration tasks for CSM-S B:

- [Creating VLANs on Switch B, page 13-21](#)
- [Configuring VLANs on CSM-S B, page 13-21](#)
- [Configuring Server Farms on CSM-S B, page 13-22](#)
- [Configuring Virtual Servers on CSM-S B, page 13-23](#)



### Note

Although the configuration tasks are the same for both CSM-S A and CSM-S B, the steps, commands, and parameters that you enter are different.

## Creating VLANs on Switch B



### Note

This example assumes that the CSM-S modules are in separate Catalyst 6500 series switch chassis. If they are in the same chassis, all of the VLANs can be created on the same Catalyst 6500 series switch console.

To create three VLANs on Switch B, perform this task:

	Command	Purpose
Step 1	Switch-B(config)# <b>vlan</b>	Enters the VLAN mode <sup>1</sup> .
Step 2	Switch-B(vlan)# <b>vlan 201</b>	Creates VLAN 201 <sup>2</sup> .
Step 3	Switch-B(vlan)# <b>vlan 200</b>	Creates VLAN 200 <sup>3</sup> .
Step 4	Switch-B(vlan)# <b>vlan 20</b>	Creates VLAN 20 <sup>4</sup> .

1. Do this step on the switch console of the switch that contains CSM-S B.
2. VLAN 201 provides the connection to the secure side of the firewalls.
3. VLAN 20 provides the connection to the internal server farms.
4. VLAN 200 provides the connection to the internal network.

## Configuring VLANs on CSM-S B

To configure the three VLANs on CSM-S B, perform this task:

	Command	Purpose
Step 1	Switch-B(config)# <b>module csm 6</b>	Enters multiple module configuration mode and specifies that CSM-S B is installed in slot 6.
Step 2	Switch-B(config-module-csm)# <b>vlan 201 server</b>	Specifies VLAN 201 as the VLAN that is being configured, identifies it as a server VLAN, and enters VLAN configuration mode.
Step 3	Switch-B(config-slb-vlan-server)# <b>ip address 200.0.0.26 255.255.255.0</b>	Specifies an IP address and netmask for VLAN 201.
Step 4	Switch-B(config-slb-vlan-server)# <b>alias 200.0.0.20 255.255.255.0</b>	Specifies an alias IP address and netmask for VLAN 201 <sup>1</sup> .

	Command	Purpose
Step 5	Switch-B(config-slb-vlan-server)# <b>exit</b>	Returns to VLAN configuration mode.
Step 6	Switch-B(config-module-csm)# <b>vlan 20 server</b>	Specifies VLAN 20 as the VLAN that is being configured, identifies it as a server VLAN, and enters VLAN configuration mode.
Step 7	Switch-B(config-slb-vlan-server)# <b>ip address 10.1.0.26 255.255.255.0</b>	Specifies an IP address and netmask for VLAN 20.
Step 8	Switch-B(config-slb-vlan-server)# <b>exit</b>	Returns to VLAN configuration mode.
Step 9	Switch-B(config-module-csm)# <b>vlan 200 client</b>	Specifies VLAN 200 as the VLAN that is being configured, identifies it as a client VLAN, and enters VLAN configuration mode.
Step 10	Switch-B(config-slb-vlan)# <b>ip address 200.0.0.26 255.255.255.0</b>	Specifies an IP address and netmask for VLAN 200.

1. This step provides a target for CSM-S A to use in making a load-balancing decision.

## Configuring Server Farms on CSM-S B



**Note** Firewall 1 and Firewall 2 secure-side IP addresses are configured as real servers in the INSEC-SF server farm associated with CSM-S A.

To configure two server farms on CSM-S B, perform this task:

	Command	Purpose
Step 1	Switch-B(config)# <b>module csm 6</b>	Enters multiple module configuration mode and specifies that CSM-S B is installed in slot 6.
Step 2	Switch-B(config-module-csm)# <b>serverfarm GENERIC-SF</b>	Creates and names the GENERIC-SF <sup>1</sup> server farm and enters serverfarm configuration mode.
Step 3	Switch-B(config-slb-sfarm)# <b>real 10.1.0.101</b>	Identifies a server in the internal server farm as a real server, assigns it an IP address, and enters real server configuration submenu.
Step 4	Switch-B(config-slb-real)# <b>inservice</b>	Enables the real server.
Step 5	Switch-B(config-slb-real)# <b>exit</b>	Returns to serverfarm configuration mode.
Step 6	Switch-B(config-slb-sfarm)# <b>real 10.1.0.102</b>	Identifies a server in the internal server farm as a real server, assigns it an IP address, and enters real server configuration submenu.
Step 7	Switch-B(config-slb-real)# <b>inservice</b>	Enables the real server.
Step 8	Switch-B(config-slb-real)# <b>exit</b>	Returns to serverfarm configuration mode.
Step 9	Switch-B(config-slb-sfarm)# <b>exit</b>	Returns to multiple module configuration mode.
Step 10	Switch-B(config-module-csm)# <b>serverfarm SEC-SF</b>	Creates and names the SEC-SF <sup>2</sup> server farm and enters serverfarm configuration mode.
Step 11	Switch-B(config-slb-sfarm)# <b>no nat server</b>	Disables the NAT of server IP address and port number <sup>3</sup> .

	Command	Purpose
Step 12	Switch-B(config-slb-sfarm)# <b>predictor hash address destination 255.255.255.255</b>	Selects a server using a hash value based on the destination IP address <sup>4</sup> .
Step 13	Switch-B(config-slb-sfarm)# <b>real 200.0.0.3</b>	Identifies Firewall 1 as a real server, assigns an IP address to its insecure side, and enters real server configuration submode.
Step 14	Switch-B(config-slb-real)# <b>inservice</b>	Enables the firewall.
Step 15	Switch-B(config-slb-real)# <b>exit</b>	Returns to serverfarm configuration mode.
Step 16	Switch-B(config-slb-sfarm)# <b>real 200.0.0.4</b>	Identifies Firewall 2 as a real server, assigns an IP address to its insecure side, and enters real server configuration submode.
Step 17	Switch-B(config-slb-real)# <b>inservice</b>	Enables the firewall.

1. GENERIC-SF contains the real servers in the internal server farm.
2. SEC-SF contains (Firewall 1 and Firewall 2); their secure-side IP addresses are configured as real servers in this server farm.
3. This is a required step when configuring a server farm that contains firewalls.
4. We recommend this step when configuring secure-side firewall interfaces in a server farm.

### Configuring Virtual Servers on CSM-S B

To configure three virtual servers on CSM-S B, perform this task:

	Command	Purpose
Step 1	Switch-B(config)# <b>module csm 6</b>	Enters multiple module configuration mode and specifies that CSM-S B is installed in slot 6.
Step 2	Switch-B(config-module-csm)# <b>vserver GENERIC-VS</b>	Specifies GENERIC-VS <sup>1</sup> as the virtual server that is being configured and enters virtual server configuration mode.
Step 3	Switch-B(config-slb-vserver)# <b>virtual 200.0.0.127 tcp 0</b>	Specifies the IP address, protocol (TCP), and port (0=any) for this virtual server <sup>2</sup> .
Step 4	Switch-B(config-slb-vserver)# <b>vlan 201</b>	Specifies that the virtual server will only accept traffic arriving on VLAN 201, which is traffic arriving from the secure side of the firewalls.
Step 5	Switch-B(config-slb-vserver)# <b>serverfarm GENERIC-SF</b>	Specifies the server farm for this virtual server <sup>3</sup> .
Step 6	Switch-B(config-slb-vserver)# <b>inservice</b>	Enables the virtual server.
Step 7	Switch-B(config-slb-vserver)# <b>exit</b>	Returns to multiple module configuration mode.
Step 8	Switch-B(config-module-csm)# <b>vserver SEC-20-VS</b>	Specifies SEC-20-VS <sup>4</sup> as the virtual server that is being configured and enters virtual server configuration mode.
Step 9	Switch-B(config-slb-vserver)# <b>virtual 200.0.0.0 255.255.255.0 any</b>	Specifies the IP address, netmask, and protocol (any) for this virtual server <sup>2</sup> .
Step 10	Switch-B(config-slb-vserver)# <b>vlan 20</b>	Specifies that the virtual server will only accept traffic arriving on VLAN 20, which is traffic arriving from the internal server farms.

	Command	Purpose
Step 11	Switch-B(config-slb-vserver) # <b>serverfarm SEC-SF</b>	Specifies the server farm for this virtual server <sup>5</sup> .
Step 12	Switch-B(config-slb-vserver) # <b>inservice</b>	Enables the virtual server.
Step 13	Switch-B(config-slb-vserver) # <b>exit</b>	Returns to multiple module configuration mode.
Step 14	Switch-B(config-module-csm) # <b>vserver SEC-200-VS</b>	Specifies SEC-20-VS <sup>6</sup> as the virtual server that is being configured and enters virtual server configuration mode.
Step 15	Switch-B(config-slb-vserver) # <b>virtual 200.0.0.0 255.255.255.0 any</b>	Specifies the IP address, netmask, and protocol (any) for this virtual server <sup>2</sup> .
Step 16	Switch-B(config-slb-vserver) # <b>vlan 200</b>	Specifies that the virtual server will only accept traffic arriving on VLAN 200, which is traffic arriving from the internal network.
Step 17	Switch-B(config-slb-vserver) # <b>serverfarm SEC-SF</b>	Specifies the server farm for this virtual server <sup>5</sup> .
Step 18	Switch-B(config-slb-vserver) # <b>inservice</b>	Enables the virtual server.

1. GENERIC-VS allows traffic from the internal server farms and the internal network that is destined for the Internet to reach the secure side of the firewalls (through VLAN 101).
2. Clients reach the server farm represented by this virtual server through this address.
3. The server farm exists in the internal server farms network.
4. SEC-20-VS allows traffic from the Internet to reach the internal server farms (through VLAN 20).
5. The server farm contains firewalls rather than real servers.
6. SEC-200-VS allows traffic from the Internet to reach the internal network (through VLAN 20).

## Configuring Reverse-Sticky for Firewalls

The reverse-sticky feature creates a database of load-balancing decisions based on the client's IP address. This feature overrides the load-balancing decision when a reverse-sticky entry is available in the database. If there is no reverse-sticky entry in the database, a load-balancing decision takes place, and the result is stored for future matching.

## Understanding Reverse-Sticky for Firewalls

Reverse-sticky provides a way of inserting entries into a sticky database as if the connection came from the other direction. A virtual server with reverse-sticky places an entry into the specified database containing the inbound real server.



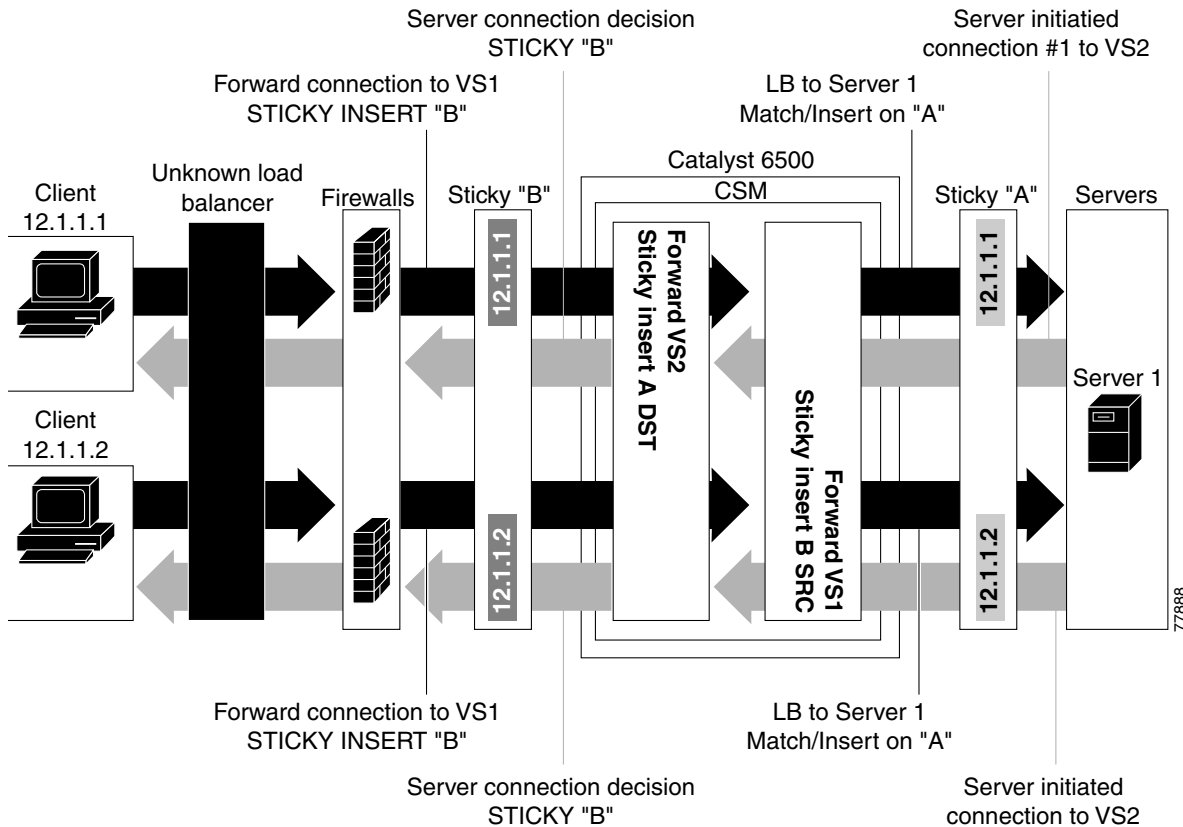
### Note

The inbound real server must be a real server within a server farm.

This entry is matched by a sticky command on a different virtual server. The other virtual server sends traffic to the client, based on this pregenerated entry.

The CSM-S stores reverse-sticky information as links from a source IP key to a real server. When the load balancer gets a new session on a virtual server with an assigned sticky database, it first checks the database for an existing entry. If a matching entry is found, the session is connected to the specified real server. Otherwise, a new entry is created linking the sticky key with the appropriate real server. [Figure 13-8](#) shows how the reverse-sticky feature is used for firewalls.

**Figure 13-8 Reverse-Sticky for Firewalls**



As shown in [Figure 13-8](#), the reverse-sticky process is as follows:

- A client connects to the CSM-S virtual server, VS1, through a load-balanced firewall. This load-balancing decision is made without interaction with the CSM-S.
- Server 1 creates a connection back to the original client. This connection matches virtual server VS2. VS2 uses the sticky information inserted by the original VS1 reverse-sticky. The connection now is forced to the same Firewall 1.
- A second client, coming in through a different firewall, connects to the same VS1. Reverse-sticky creates a new entry into database B for the second client, pointing to Firewall 2. VS1 also performs a normal sticky to Server 1.
- Server 1 creates a connection back to Client 2. The connection matches the connection in VS2. VS2 uses the sticky information inserted by the original VS1 reverse-sticky. This connection is used for the connection to Firewall 2.
- If the server had originated the first connection, the link back to the server would have been inserted by VS2, and a normal load-balancing decision would have generated a connection to one of the firewalls.

**Note**

This configuration supports forward direction connections (client to server) using any balancing metric. However, the balancing metric to the firewalls from VS2 must match that of the unknown load balancer, or the unknown load balancer must stick new buddy connections in a similar manner if client responses to server-initiated traffic are to be sent to the correct firewall.

## Configuring Reverse-Sticky for Firewalls

To configure IP reverse-sticky for firewall load balancing, perform this task:

	Command	Purpose
Step 1	SLB-Switch(config)# <b>module csm slot</b>	Associates load-balancing commands to a specific CSM-S module and enters the CSM-S module configuration submode for the specified slot.
Step 2	SLB-Switch(config-module-csm)# <b>vserver virtserver-name</b>	Identifies a virtual server and enters the virtual server configuration submode.
Step 3	SLB-Switch(config-slb-vserver)# <b>sticky duration [group group-id] [netmask ip-netmask] [source   destination   both]</b>	Defines the portion of the IP information (source, destination, or both) that is used for the sticky entry key.
Step 4	SLB-Switch(config-slb-vserver)# <b>reverse-sticky group-id</b>	Ensures that the CSM-S maintains connections in the opposite direction back to the original source.
Step 5	SLB-Switch# <b>show module csm slot sticky</b>	Displays the sticky database.

## Configuring Stateful Firewall Connection Remapping

To configure the firewall reassignment feature, you must have an MSFC image from Cisco IOS Release 12.1(19)E.

To configure firewall reassignment, perform these steps:

**Step 1** In the serverfarm submode for firewalls, configure the action:

```
Cat6k-2(config)# serverfarm FW-FARM
failaction reassign
```

**Step 2** Assign a backup real server for each firewall if it failed (probe or ARP):

```
Cat6k-2(config-slb-sfarm)# serverfarm FW-FARM
Cat6k-2(config-slb-sfarm)# real 1.1.1.1
Cat6k(config-slb-module-real)# backup real 2.2.2.2
Cat6k(config-slb-module-real)# inservice
Cat6k-2(config-slb-sfarm)# real 2.2.2.2
Cat6k(config-slb-module-real)# backup real 3.3.3.3
Cat6k(config-slb-module-real)# inservice
Cat6k-2(config-slb-sfarm)# real 3.3.3.3
Cat6k(config-slb-module-real)# backup real 1.1.1.1
Cat6k(config-slb-module-real)# inservice
```

**Step 3** Configure the ICMP probe (through the firewall) for this server farm.

**Step 4** Configure the ICMP probes for the CSM-S modules outside and inside the firewall.

Make sure that the backup real server is configured in the same order in both CSM-S modules.

The `inservice standby` option assigned to a real server specifies that this server only receives connections if they are destined or load-balanced to the failed primary server. If you configure the real server designated as `real 2.2.2.2` with `inservice standby`, then all connections would go to either of the real servers designated as `real 1.1.1.1` or `real 3.3.3.3`. When real server `real 1.1.1.1` failed, the real server designated as `real 2.2.2.2` will be active in place of real server `real 1.1.1.1`.

