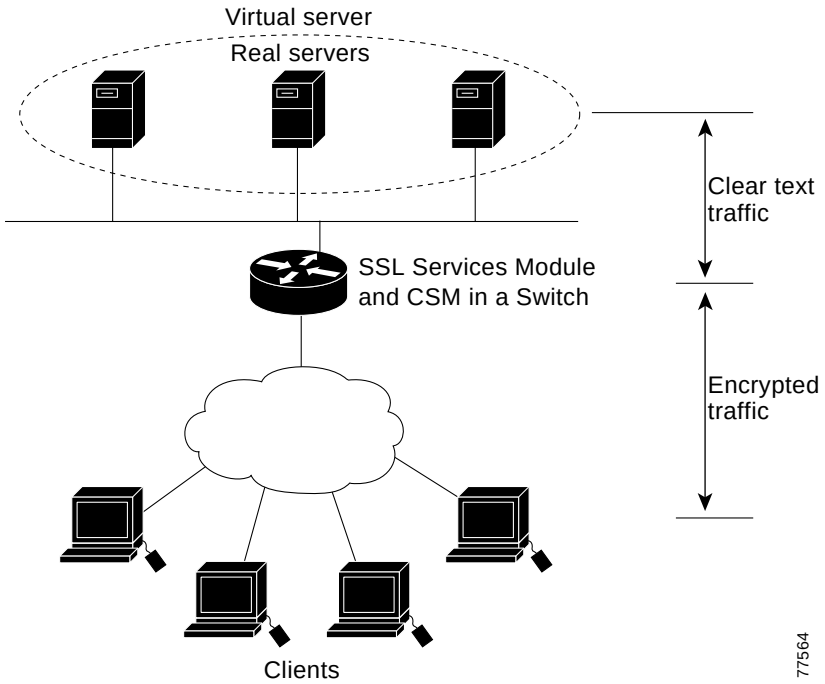
Configuring Different Modes of Operation

The SSL Services Module operates either in a standalone configuration or with a Content Switching Module (CSM). In a standalone configuration, secure traffic is directed to the SSL Services Module using policy-based routing. When used with a CSM, only encrypted client traffic is forwarded to the SSL Services Module, while clear text traffic is forwarded to real servers.

The following sections describe how to configure the SSL Services Module in a standalone configuration or with a CSM:

Figure 5-1 shows a sample network topology with an SSL Services Module and a CSM in a single Catalyst 6500 series switch.

Figure 5-1 Sample Network Layout—SSL Services Module with CSM



Configuring Policy-Based Routing

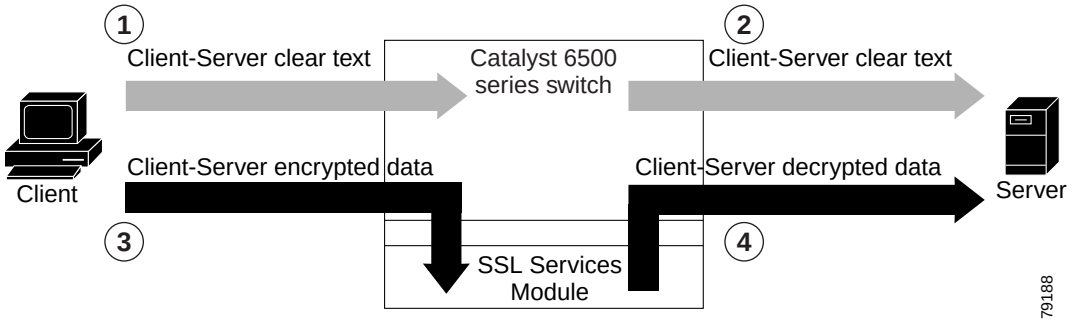
In a standalone configuration, encrypted SSL traffic is directed to the SSL Services Module using policy-based routing.

When you configure policy-based routing on the SSL Services Module, use the following guidelines:

- Configure clients and servers on separate subnets.
- Configure two VLANs (one for each subnet) on the switch.
- Configure IP interfaces on each VLAN.
- Configure an IP interface on the server-side VLAN of the SSL Services Module.

Two flows exist for each direction of traffic. In the client-to-server direction, traffic flow originates from the client as either clear text or as encrypted data. (See Figure 5-2.) In the server-to-client direction, all traffic originates from the server as clear text. However, depending on the source port, the traffic in the server-to-client direction may or may not be encrypted by the SSL Services Module before being forwarded to the client.

Figure 5-2 Client-to-Server Traffic Flow—Standalone Configuration



In Figure 5-2, the client sends clear text traffic to the server (as shown in flow 1). The switch then forwards clear text traffic to the server (flow 2).

The client sends encrypted traffic to the server (port 443); policy-based routing intercepts the traffic and forwards it to the SSL Services Module (flow 3). The SSL Services Module decrypts the traffic and forwards the stream to a well-known port (a port that has been configured on the server to expect decrypted traffic) (flow 4).

To enable policy-based routing, perform this task:

	Command	Purpose
Step 1	`Router(config)# ip access-list extended` *name*	Defines an IP extended access list.
Step 2	`Router(config-ext-nacl)# permit tcp` *source source-wildcard operator port destination destination-wildcard operator port*	Specifies conditions for the named access list. **Note** Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* or *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255.
Step 3	`Router(config-ext-nacl)# route-map` *map-tag* [**permit** | **deny**] [*sequence-number*]	Defines a route map to control where packets are output. **Note** This command puts the switch into route map configuration mode.

	Command	Purpose
Step 4	`Router(config-route-map)# match ip address` *name*	Specifies the match criteria. Matches the source and destination IP address that is permitted by one or more standard or extended access lists.
Step 5	`Router(config-route-map)# set ip next-hop` *ip-address*	Sets the next hop to which to route the packet. (The next hop must be adjacent.)
Step 6	`Router(config-route-map)# interface` *interface-type interface-number*	Specifies the interface. **Note** This command puts the switch into interface configuration mode.
Step 7	`Router(config-if)# ip policy route-map` *map-tag*	Identifies the route map to use for policy-based routing. **Note** One interface can only have one **route-map** tag, but you can have multiple route map entries with different sequence numbers. These entries are evaluated in sequence number order until the first match. If there is no match, packets will be routed as usual.

Configuring the Content Switching Module

Note For detailed information on configuring the CSM, refer to the *Catalyst 6500 Series Switch Content Switching Module Installation and Configuration Note*, Release 3.1, at this URL:

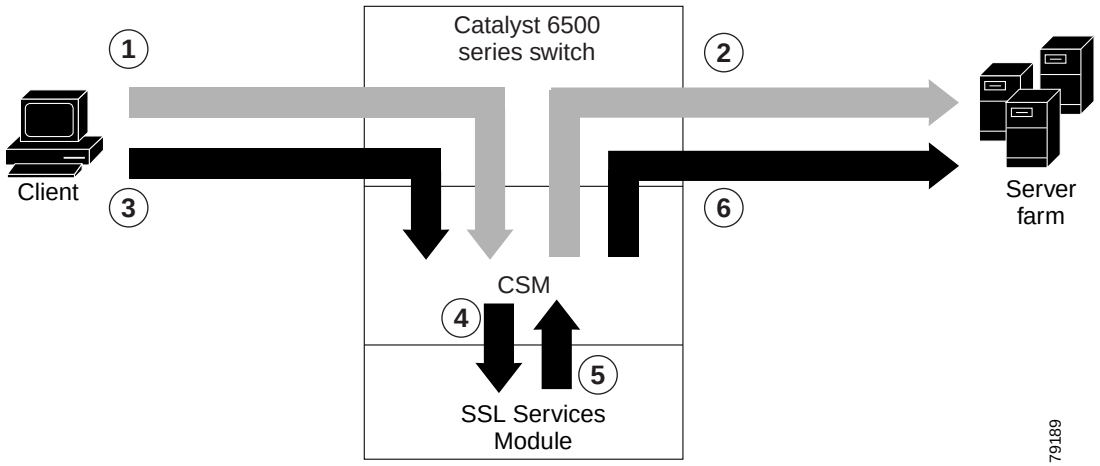
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/cfgnotes/csm_3_1/index.htm

The Content Switching Module (CSM) provides high-performance server load balancing (SLB) between network devices and server farms based on Layer 4 through Layer 7 packet information.

When you use the SSL Services Module with the CSM, only encrypted client traffic is forwarded to the SSL Services Module, while clear text traffic is forwarded to real servers.

The CSM parses for traffic destined to the server farm virtual IP address, port 443. The CSM forwards this traffic to the SSL Services Module without modifying the destination IP address. If there are multiple SSL Services Modules in the configuration, the CSM load balances the traffic across the SSL Services Modules. The SSL Services Module decrypts the traffic and forwards the new stream back to the CSM. The SSL Services Module does not change the destination IP address (the original server farm virtual IP address), but it does perform a port translation. With this new virtual IP address and port combination, the CSM balances the data across the servers in the server farm. (See Figure 5-3.)

Figure 5-3 Client-to-Server Traffic Flow—SSL Services Module and CSM



In Figure 5-3, clear text traffic is sent from the client to a virtual IP address, non-SSL port (for example, 80) (shown in flow 1). The CSM balances the clear text traffic across the servers in the server farm (flow 2).

Encrypted traffic is sent from the client to a virtual IP address, SSL port (443) (flow 3). The CSM forwards the encrypted traffic to the SSL Services Module (flow 4); if there is more than one SSL Services Module, the CSM balances the encrypted traffic across SSL Services Modules.

The SSL Services Module decrypts the traffic and forwards it to a virtual IP address and port on the CSM (flow 5).

The CSM balances the decrypted traffic across the servers in the server farm (flow 6).

On the return path, the CSM must monitor the port from which the server transmits data. If it is the standard clear text port (for example, 80), the data is forwarded back to the client unaltered, with the exception of the source address. If server NAT is configured on the clear text flow, the virtual IP address replaces the source IP address.

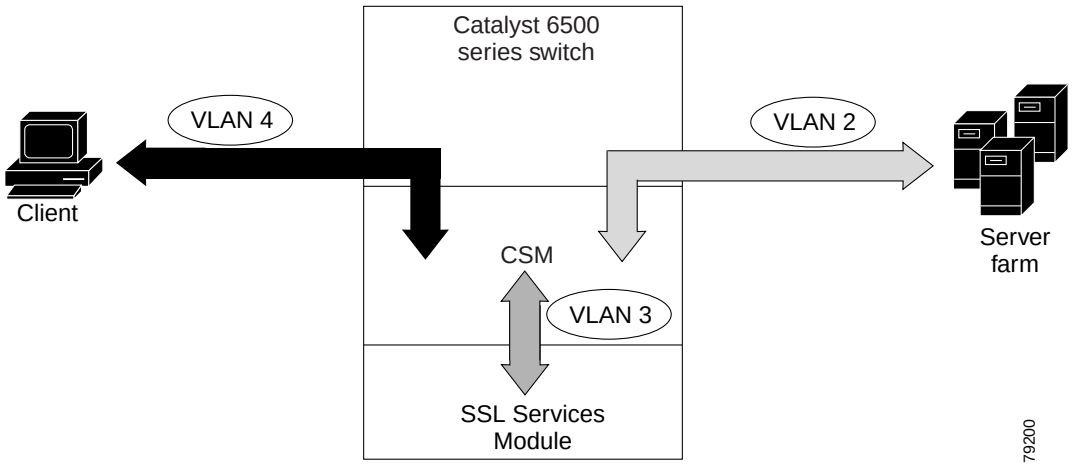
If traffic is destined to the virtual IP address and port 443, the CSM forwards this flow to the SSL Services Module. The SSL Services Module encrypts the traffic and performs port translation on the packet header. The SSL Services Module directs the traffic to the CSM with source port 443 (the SSL port to which the client originally directed encrypted traffic) so that the CSM can handle the reverse path traffic.

VLANs

As with normal CSM operation, you must configure separate client and server VLANs. If the CSM client and server VLANs are not on the same subnet, the CSM acts as a switch between the client and server VLANs.

To allow traffic to pass between the CSM and the SSL Services Module, you must configure a single VLAN between them. (See Figure 5-4.) All flows between the CSM and the SSL Services Module are on that VLAN.

Figure 5-4 SSL Services Module with CSM—3-VLAN Configuration



In Figure 5-4, VLAN 4 involves clear text and encrypted traffic between the client and the CSM virtual IP address.

VLAN 2 involves the following types of traffic between the server and the client:

- Clear text traffic between the client and the server
- Traffic sent by the client that was decrypted by the SSL Services Module
- Traffic sent by the server that needs to be encrypted by the SSL Services Module

VLAN 3 involves the following types of traffic between the CSM and the SSL Services Module:

- Encrypted client traffic that needs to be decrypted
- Decrypted client traffic that needs to be forwarded to the server farm
- Unencrypted server traffic that needs to be encrypted
- Encrypted server traffic that needs to be forwarded back to the client

To configure VLANs on the CSM, perform this task:

	Command	Purpose
Step 1	`Router(config)# mod csm slot`	Specifies the slot of the CSM.
Step 2	`Router(config-module-csm)# vlan vlan {client|server}`	Configures the VLAN as either a client or a server on the CSM.
Step 3	`Router(config-slb-vlan-client)# ip address ip_addr netmask`	Configures the IP address and netmask of the interface on the VLAN.
Step 4	`Router(config-slb-vlan-client)# gateway ip_addr`	Configures the gateway IP address.

Server Farms

When you use the SSL Services Module with a CSM, the CSM sees two types of server farms. The first server farm is the traditional farm that consists of a group of real servers and is mapped to one or more virtual server IP addresses. You may or may not choose to allow server or client NAT to act on traffic that goes to these servers.

The second type of server farm consists of the SSL Services Modules that are present in the chassis. The CSM views these SSL Services Modules as real servers and balances SSL traffic across the modules.

To configure a server farm on the CSM, perform this task:

	Command	Purpose
Step 1	`Router(config)# mod csm slot`	Specifies the slot of the CSM.
Step 2	`Router(config-module-csm)# serverfarm server_farm`	Configures the name of the server farm.
Step 3	`Router(config-slb-sfarm)# no nat server`	(Optional) Disables server NAT.
Step 4	`Router(config-slb-sfarm)# nat client natpool_name`	(Optional) Enables client NAT.
Step 5	`Router(config-slb-sfarm)# real ip_addr`	Configures the real IP address of the server.
Step 6	`Router(config-slb-real)# inservice`	Puts the server farm in service.

Virtual Servers

Three types of virtual servers are required for every real server farm supported in a CSM and SSL Services Module configuration. The main distinction between the three types of virtual servers is the port number. The clear text virtual server and the SSL virtual server have the same virtual IP address. The decryption virtual server may or may not have the same virtual IP address. The three types of virtual servers are as follows:

- Clear text virtual server—The clear text virtual server is the destination for any clear text traffic sent by the client. Typically, this traffic is destined to port 80. The CSM balances traffic sent to this virtual server directly to a real server in the server farm. The SSL Services Module is uninvolved.
- SSL virtual server—The SSL virtual server should be the destination for any SSL-encrypted traffic from the client to the server. This traffic is destined to port 443. The CSM forwards this type of traffic to the SSL Services Module for decryption.
- Decryption virtual server—After the SSL Services Module decrypts SSL traffic from the client, it forwards it back to the CSM, destined for the decryption virtual server. The CSM balances the traffic to a real server in the server farm, similar to the action it took for traffic destined to the clear text virtual server. The port associated with this decryption virtual server should match the port from which the real server has been configured to expect traffic decrypted by the SSL Services Module.

To configure a virtual server on the CSM, perform this task:

	Command	Purpose
Step 1	`Router(config)# mod csm slot`	Specifies the slot of the CSM.
Step 2	`Router(config-module-csm)# vserver vserver`	Configures the name of the virtual server.
Step 3	`Router(config-slb-vserver)# virtual ip_address tcp port`	Configures the IP address, protocol, and port of the virtual server.
Step 4	`Router(config-slb-vserver)# serverfarm server_farm`	Configures the destination server farm.

	Command	Purpose
Step 5	`Router(config-slb-vserver)#` **`vlan`** *`vlan`*	Specifies the VLAN from which the CSM accepts traffic for a specified virtual server. **Note** For security reasons, this command is required for the decryption virtual server.
Step 6	`Router(config-slb-vserver)#` **`inservice`**	Puts the virtual server in service.

Sticky Connections

Note Configuring the SSL sticky feature requires CSM software release 3.1(1a) or later releases on the CSM.

If a CSM and SSL Services Module configuration consists of multiple SSL Services Modules connected to a single CSM, configure the SSL sticky feature on the CSM to ensure that the CSM always forwards traffic from a particular client to the same SSL Services Module.

A 32-byte SSL session ID is created for each connection between a client and an SSL Services Module. With the SSL sticky feature configured, the CSM looks at a specific portion of the SSL session ID (the MAC address of the SSL Services Module) and load balances SSL traffic among the SSL Services Modules.

Note The MAC address of the SSL Services Module is always located at bytes 21 though 26 of the SSL session ID, even when the session ID is renegotiated.

To configure a sticky connection on the CSM, perform this task:

	Command	Purpose
Step 1	`Router(config)#` **`mod csm`** *`mod`*	Specifies the slot of the CSM.
Step 2	`Router(config-module-csm)#` **`sticky`** *`group`* **`ssl`**	Configures the sticky group ID.
Step 3	`Router(config-module-csm)#` **`vserver`** *`vserver`*	Associates the group ID with the virtual server.
Step 4	`Router(config-slb-vserver)#` **`sticky`** *`group`* **`timeout`** *`time`*	Specifies the amount of time, in minutes, that the connection remains sticky.
Step 5	`Router(config-slb-vserver)#` **`ssl-sticky offset 20 length 6`**	Specifies the location of the SSL Services Module MAC address in the SSL ID.