CHAPTER 5

Configuring End-to-End SSL

This chapter describes how to configure a Cisco 4700 Series Application Control Engine (ACE) appliance to provide end-to-end SSL connectivity. This process involves combining SSL termination (front end) with SSL initiation (back end) to provide a secure link between the client, the ACE, and the server. All data is encrypted and sent as ciphertext among the three devices.

This chapter contains the following major sections:

- End-to-End SSL Overview
- ACE End-to-End SSL Configuration Prerequisites
- Configuring End-to-End SSL
- Example of an End-to-End SSL Configuration

End-to-End SSL Overview

End-to-end SSL refers to the ACE's establishing and maintaining SSL connections between the client at one end of the connection and the server at the other end of the connection. When you configure the ACE for end-to-end SSL, the ACE performs the following functions:

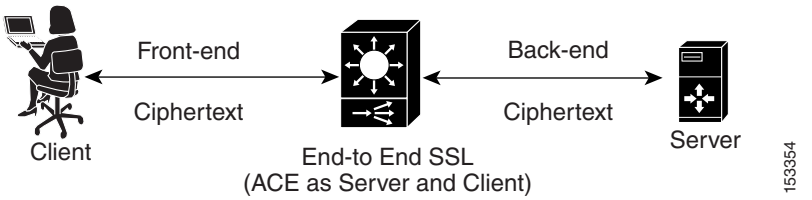
- Terminates an SSL session with the client (front-end connection)
- Initiates an SSL session with the server (back-end connection)
- Load balances the back-end content

End-to-end SSL combines the configurations that you use to configure the ACE for SSL termination and SSL initiation. For end-to-end SSL, you must create the following policy map types:

- Layer 7 policy map—Directs the back-end flow of traffic between the ACE and the server.
- Layer 3 and Layer 4 policy map—Performs the following functions:
  - Directs the front-end flow of traffic between the client and the ACE.
  - Applies the associated Layer 7 policy map to the traffic that meets the criteria of the Layer 3 and Layer 4 policy map.

Figure 5-1 shows an end-to-end SSL application in which the ACE terminates an SSL connection with an SSL client and initiates an SSL connection with an SSL server.

Figure 5-1 End-to-End SSL

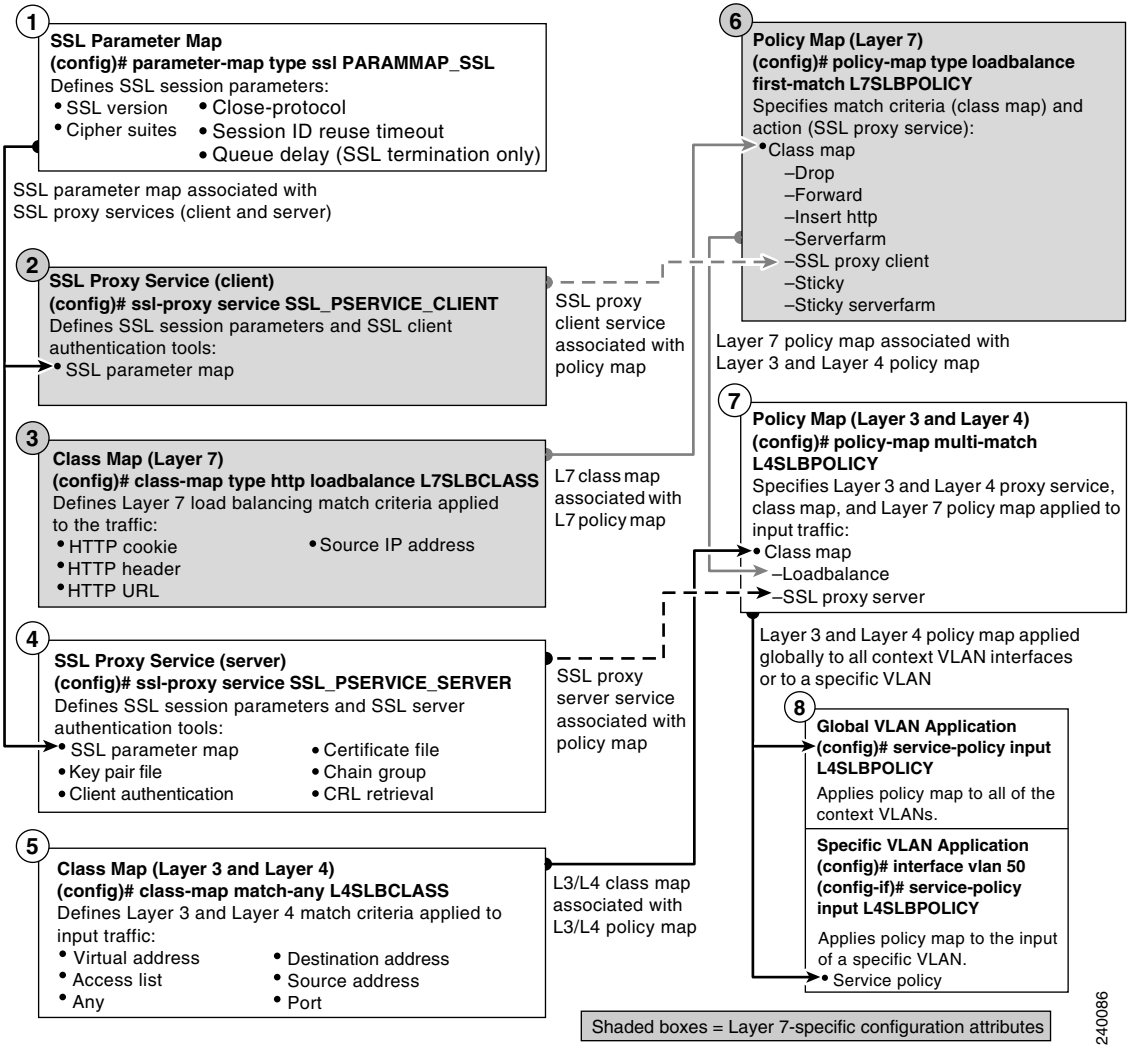


The ACE uses a combination of parameter maps, SSL proxy services, and class maps to build the policy maps that determine the flow of information between the client, the ACE, and the SSL server.

Figure 5-2 provides a basic overview of the process required to build the Layer 7 load-balancing policy map and associate it with the Layer 3 and Layer 4 policy map to create an end-to-end SSL configuration. To allow you to easily discern between the Layer 7 and Layer 3 and Layer 4 configuration attributes, the Layer 7 attributes are shaded gray.

In the final step of the process, you apply the Layer 3 and Layer 4 policy map to the input traffic of the context. The figure also shows how the various components of the policy map configurations are associated with each other.

Figure 5-2 Basic End-to-End SSL Configuration Flow Diagram



ACE End-to-End SSL Configuration Prerequisites

Before configuring your ACE for SSL operation, you must first configure it for server load balancing (SLB). During the SLB configuration process, you create the following configuration objects:

- Layer 7 class map
- Layer 3 and Layer 4 class map
- Layer 7 policy map
- Layer 3 and Layer 4 policy map

After configuring SLB, modify the existing SLB class maps and policy maps with the SSL configuration requirements described in this guide for end-to end SSL.

To configure your ACE for SLB, see the *Cisco 4700 Series Application Control Engine Appliance Server Load-Balancing Configuration Guide*.

Configuring End-to-End SSL

Table 5-1 provides an overview of the process required to configure the ACE for end-to-end SSL. Because end-to-end SSL combines the configuration processes of SSL termination and SSL initiation, the procedure provides links to the sections of this guide where the specified process is described in detail.

Table 5-1 End-to-End SSL Configuration Quick Start

Task
1. Configure the ACE for SSL initiation as described in Chapter 4, Configuring SSL Initiation. The SSL initiation configuration configures all of the back-end operation and a portion of the front-end operation. Do not apply the configuration to the VLANs at this time.
2. Create a parameter map for the ACE to use in the front-end operation as described in the "Creating and Defining an SSL Parameter Map" section of Chapter 3, Configuring SSL Termination. Skip this step if the ACE is to use the same parameter map that you created in Step 1 for the back-end operation.

Table 5-1 End-to-End SSL Configuration Quick Start (continued)

Task
3. Create an SSL proxy server service as described in the "Creating and Defining an SSL Proxy Service" section of Chapter 3, Configuring SSL Termination.
4. Associate the SSL proxy server service with the Layer 3 and Layer 4 policy map created in Step 1. For information on making this association, see the "Associating an SSL Proxy Server Service with the Policy Map" section of Chapter 3, Configuring SSL Termination.
5. Apply the Layer 3 and Layer 4 policy map to the VLANs as described in the "Applying the Policy Map to the VLANs" section of Chapter 3, Configuring SSL Termination.
6. (Optional) Save the configuration changes to flash memory by copying the running configuration to the startup configuration. `host1/Admin(config-if)# do copy running-config startup-config`

Example of an End-to-End SSL Configuration

The following example illustrates an end-to-end SSL configuration, which combines front-end SSL and back-end SSL. The ACE receives encrypted text from an HTTP client, and also transmits the encrypted data as cipher text to the SSL server. On the reverse side, the ACE decrypts the cipher text that it receives from the SSL server and sends the data to the client as clear text. The SSL-specific configuration elements appear in bold in the example.

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

rserver host TEST4
  ip address 20.20.2.11
  inservice

serverfarm host TEST
  rserver TEST4
    inservice

parameter-map type ssl PM1
  session-cache timeout 300
  queue-delay timeout 1
```

```
ssl-proxy service SSL_CLIENT
  ssl advanced-options PM1

ssl-proxy service SSL_SERVER
  key KEY12.PEM
  cert CERT12.PEM
  ssl advanced-options PM1

class-map type http loadbalance match-any SSL
  2 match http url .*
class-map match-any SSL_C1
  2 match virtual-address 10.10.2.101 tcp eq https
  3 match virtual-address 10.10.2.101 tcp any

policy-map type loadbalance first-match SSL_BACK
  class SSL
    serverfarm TEST
    ssl-proxy client SSL_CLIENT

policy-map multi-match L7_1
  class SSL_C1
    loadbalance vip inservice
    loadbalance policy SSL_BACK
    loadbalance vip icmp-reply
    ssl-proxy server SSL_SERVER

interface vlan 210
  ip address 10.10.2.1 255.255.255.0
  service-policy input L7_1
  access-group input ACL
  no shutdown
interface vlan 220
  ip address 20.20.2.1 255.255.255.0
  no shutdown
interface vlan 226
  ip address 10.90.15.27 255.255.255.0
  no shutdown

ip route 0.0.0.0 0.0.0.0 10.90.15.1
```