This section describes how to configure SSL on the Cisco 4700 Series Application Control Engine (ACE) appliance.

Contents

Overview

After reading this section, you should have a basic understanding of how the ACE appliance provides SSL security for your network and how to configure SSL termination, in which the ACE operates as an SSL server.

SSL configuration in an ACE establishes and maintains a SSL session between the ACE and another device. It provides for secure data transactions between a client and a server. SSL provides authentication, encryption, and data integrity in a Public Key Infrastructure (PKI), a set of policies and procedures that establishes a secure information exchange between devices.

In SSL, data is encrypted using one or more symmetric keys that are known only by the two endpoints in the transaction. In a key exchange, one device generates the symmetric key and then encrypts it using an asymmetric encryption scheme before transmitting the key to the other device.

Asymmetric encryption requires each device to have a unique key pair consisting of a public key and a private key. A private key is an encryption/decryption key known only to the parties exchanging the messages. A public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digital signatures. The two keys are mathematically related; data that is encrypted using the public key can only be decrypted using the corresponding private key, and vice versa.

SSL facilitates client and server authentication through the use of digital certificates. Digital certificates are a form of digital identification to prove the identity of the server to the client, or optionally, the client to the server. A certificate ensures that the identification information is correct and the public key embedded in it actually belongs to the client or server.

A Certificate Authority (CA) issues digital certificates in the context of a PKI. CAs are trusted authorities that sign certificates to verify their authenticity. As the certificate issuer, the CA uses its private key to sign the certificate. Upon receiving a certificate, a client uses the issuer?s public key to decrypt and verify the certificate signature to ensure that the certificate was actually issued and signed by an authorized entity.

If you do not have a certificate and the corresponding key pair, you can use the ACE to generate a key pair and a certificate signing request (CSR) to apply for a certificate from a CA. The CA signs the CSR and returns the authorized digital certificate to you. The ACE supports import, export, and other management functions to manage the various certificates and key pair files within each context.

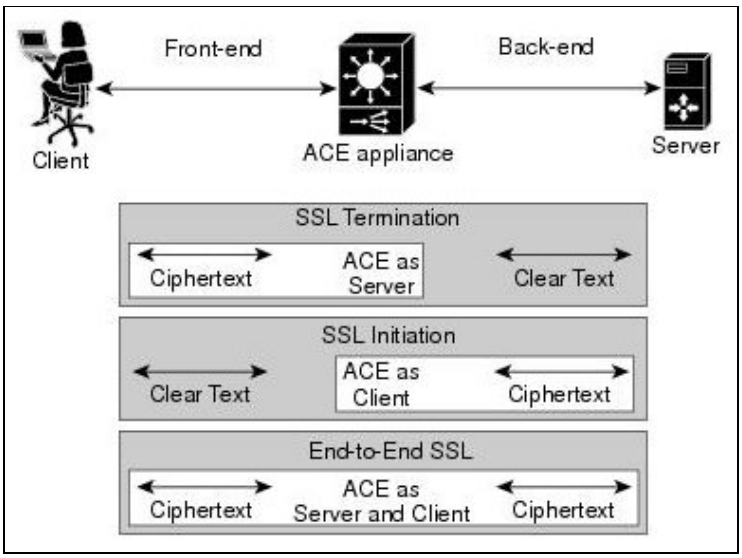
The client and server use the SSL handshake protocol to establish an SSL session between the two devices. During the handshake, the client and server negotiate the SSL parameters that they will use during the secure session. During the SSL handshake, the ACE uses an SSL proxy service, which includes the configuration of SSL session parameters, an RSA key pair, and a matching certificate.

The ACE applies SSL session parameters to an SSL proxy service. Creating an SSL parameter map allows you to apply the same SSL session parameters to different proxy services. The SSL session parameters include timeouts, close protocol behavior, and SSL version?SSL 3 and/or Transport Layer Security (TLS) 1. For more information on these parameters, see the Cisco ACE 4700 Series Appliance SSL Configuration Guide.

You can configure the ACE to act as a client or a server during an SSL session by defining operational attributes such as SSL session parameters, SSL key pairs and certificates, and traffic characteristics. When the traffic characteristics match the settings specified in the operational attributes, the ACE executes the actions associated with the SSL proxy service.

Figure 1 shows the three basic SSL configurations in which the ACE is used to encrypt and decrypt data between the client and the server: SSL termination, SSL initiation, and end-to-end SSL.

Figure 1 ACE SSL Configurations



In SSL termination, an ACE context is configured for a front-end application in which the ACE operates as an SSL server that communicates with a client. When you define the flow between an ACE and a client, the ACE operates as a virtual SSL server by adding security services between a web browser (the client) and the HTTP connection (the server).

All inbound SSL flows that come from a client terminate at the ACE. After the connection is terminated, the ACE decrypts the ciphertext (encrypted content) from the client and sends the data as clear text (unencrypted content) to an HTTP server. For information about configuring the ACE for SSL termination, see the Configuring SSL Termination section.

In SSL initiation, an ACE context is configured for a back-end application in which the ACE operates as a client that communicates with an SSL server. When you define the flow between an ACE and an SSL server, the ACE operates as a client and initiates the SSL session. SSL initiation enables the ACE to receive clear text from a client and then establish an SSL session with an SSL server, joining the client and SSL server connections.

The ACE encrypts the clear text that it receives from the client and sends the data as ciphertext to an SSL server. The SSL server can either be an ACE configured for SSL termination (a virtual SSL server) or a real SSL server (web server). On the outbound flow from the SSL server, the ACE decrypts the ciphertext from the server and sends clear text back to the client. For more information on configuring the ACE for SSL initiation, see the Cisco ACE 4700 Series Appliance SSL Configuration Guide.

In end-to-end SSL, an ACE context is configured for both SSL termination and SSL initiation. You configure the ACE for end-to-end SSL when you have an application that requires secure SSL channels between the client and the ACE, and between the ACE and the SSL server.

For example, a transaction between banks requires end-to-end SSL to protect all financial information exchanged. End-to-end SSL also allows the ACE to insert load-balancing and security information into the data. The ACE decrypts the ciphertext that it receives and inserts load-balancing and firewall information into the clear text. The ACE then re-encrypts the data and passes the ciphertext to its intended destination. For more information on configuring the ACE for end-to-end SSL initiation, see the Cisco ACE 4700 Series Appliance SSL Configuration Guide.

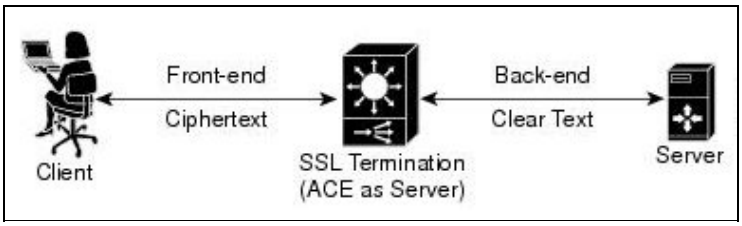
Configuring SSL Termination

SSL termination occurs when the ACE, acting as an SSL proxy server, terminates an SSL connection from a client and then establishes a TCP connection to an HTTP server. When the ACE terminates the SSL connection, it decrypts the ciphertext from the client and transmits the data as clear text to the HTTP server.

Figure 2 shows the following network connections in which the ACE terminates the SSL connection with the client:

- Client to ACE?An SSL connection exists between the client and the ACE acting as an SSL proxy server.
- ACE to Server?A TCP connection exists between the ACE and the HTTP server.

Figure 2 SSL Termination



Before configuring the ACE for an SSL operation, you must first configure it for server load balancing. To configure your ACE for server load balancing, see the Configuring Server Load Balancing section.

SSL termination is a Layer 3 and Layer 4 application because it is based on the destination IP address of the inbound traffic flow from the client. When configuring a policy map for SSL termination, you associate the following elements:

- The SSL proxy service, including SSL session parameters, certificate, and key pair.
- The virtual SSL server IP address that the destination IP address of the inbound traffic must match (a class map). When a match occurs, the ACE negotiates with the client to establish an SSL connection.

You can configure the ACE for SSL termination by following these steps:

1. Import a key file with a key pair.

2. Import a certificate that matches the imported key pair.

3. Configure a parameter map.

4. Configure an SSL proxy service using the key pair, certificate, and parameter map.

5. Create a virtual server for SSL termination using the SSL proxy service.

6. Deploy the configuration.

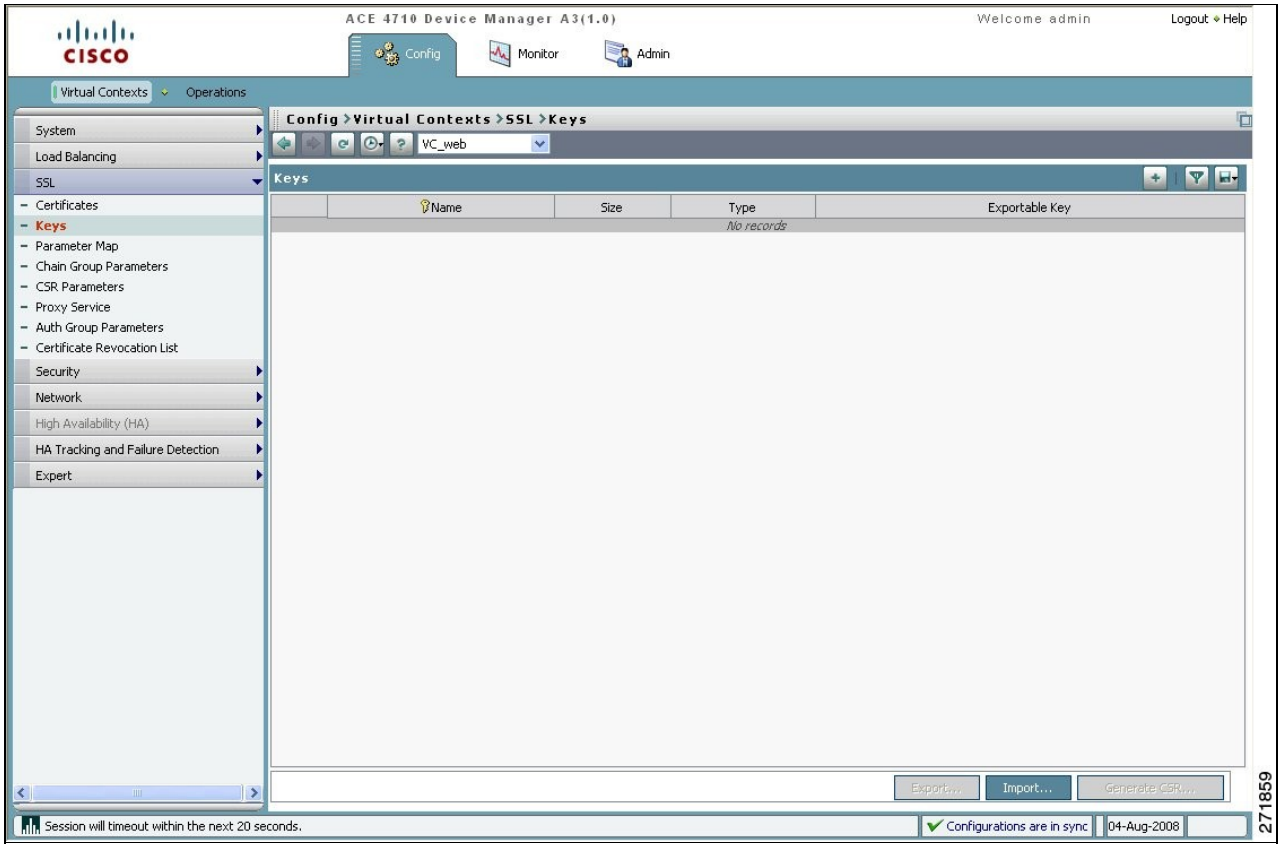
This section describes how to configure the ACE for SSL termination using either the Device Manager GUI or the CLI.

Configuring the ACE for SSL Termination Using the Device Manager GUI

You can configure the ACE for SSL termination using the Device Manager GUI by following these steps:

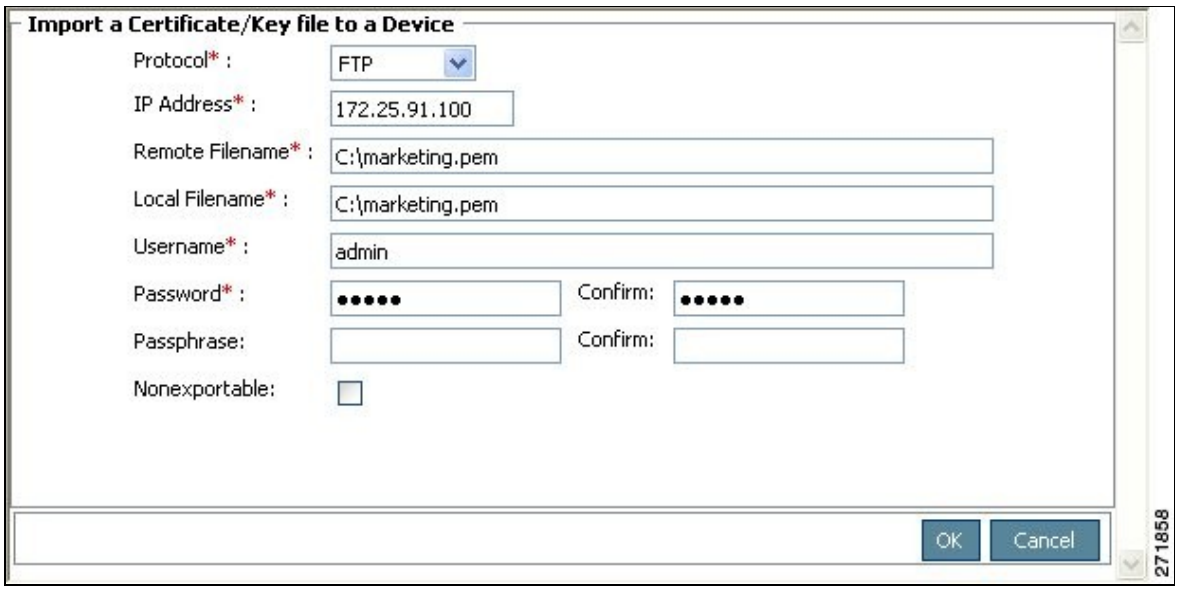
1. Choose the user context **VC_web**, and then choose **SSL > Keys**. The Keys pane appears (Figure 3).

Figure 3 Keys Pane



2. Click **Import** to import a key file. The Import a Certificate/Key File to a Device window appears (Figure 4).

Figure 4 Import a Certificate/Key File to a Device Window

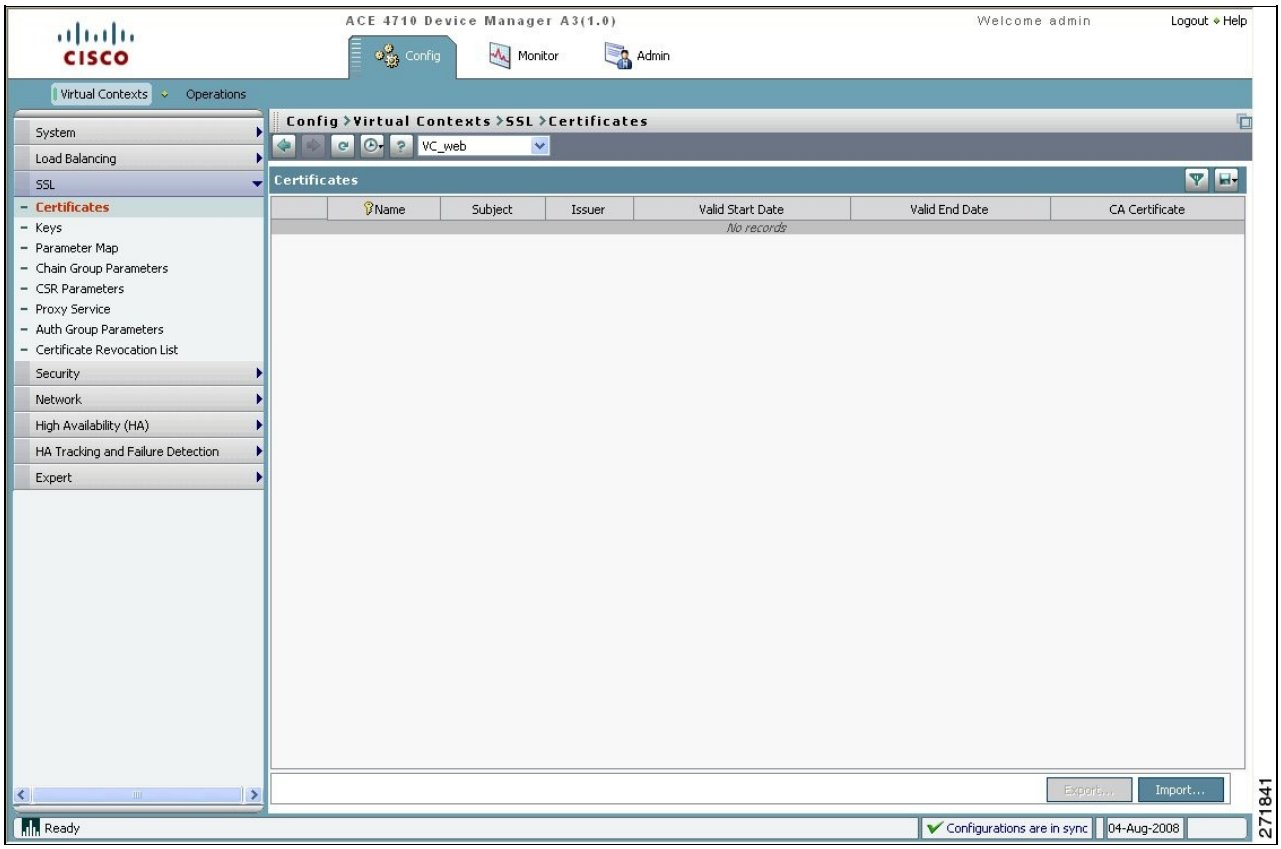


Enter the following parameters. Leave the remaining parameters blank or with their default values.

- ◊ Protocol: FTP
- ◊ IP Address: 172.25.91.100 (in order for this to work, you should use an IP address where you can access the remote key file)
- ◊ Remote Filename: C:\marketing.pem
- ◊ Local Filename: C:\marketing.pem
- ◊ Username: Admin
- ◊ Password: (password for your FTP server)
- ◊ Confirm: (retype the password for your FTP server)

3. Click **OK** to import the key file.
4. Choose **SSL > Certificates**. The Certificates pane appears (Figure 5).

Figure 5 Certificates Pane



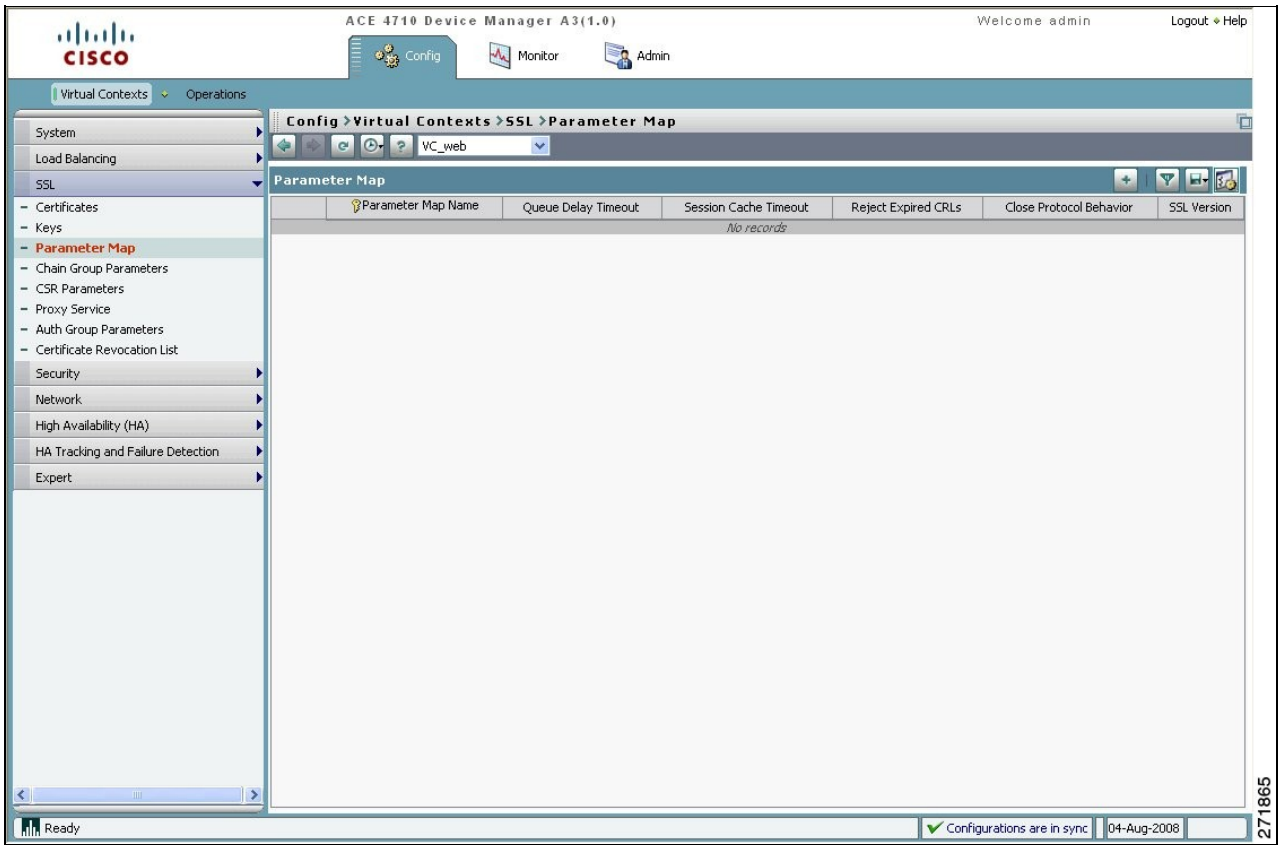
5. Click **Import** to import a certificate file. The Import a Certificate/Key File to a Device window reappears. Enter the following parameters. Leave the remaining parameters blank or with their default values.

- ◊ Protocol: FTP
- ◊ IP Address: 172.25.91.100 (in order for this to work, you should use an IP address where you can access the certificate file)
- ◊ Remote Filename: C:\marketing_cert.pem
- ◊ Local Filename: C:\marketing_cert.pem
- ◊ Username: Admin
- ◊ Password: (password for your FTP server)
- ◊ Confirm: (retype the password for your FTP server)

6. Click **OK** to import the certificate file.

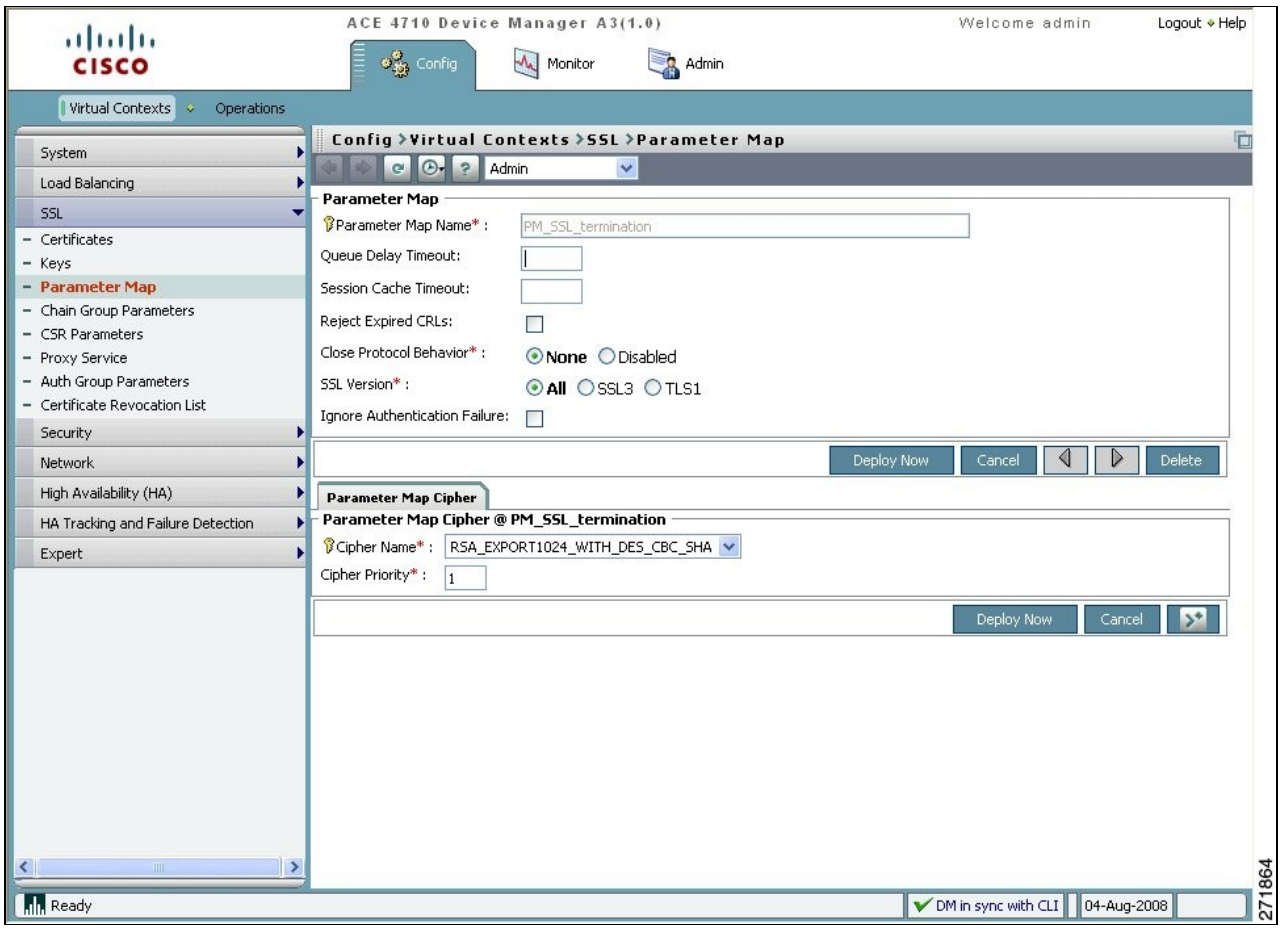
7. Choose **SSL > Parameter Map**. The Parameter Map pane appears (Figure 6).

Figure 6 Parameter Map Pane



8. Click **Add** to create a parameter map. The Parameter Map window appears (Figure 7).

Figure 7 Parameter Map Window



9. Enter the following parameter. Leave the remaining parameters blank or with their default values.

    ◊ Parameter Map Name: PM_SSL_termination

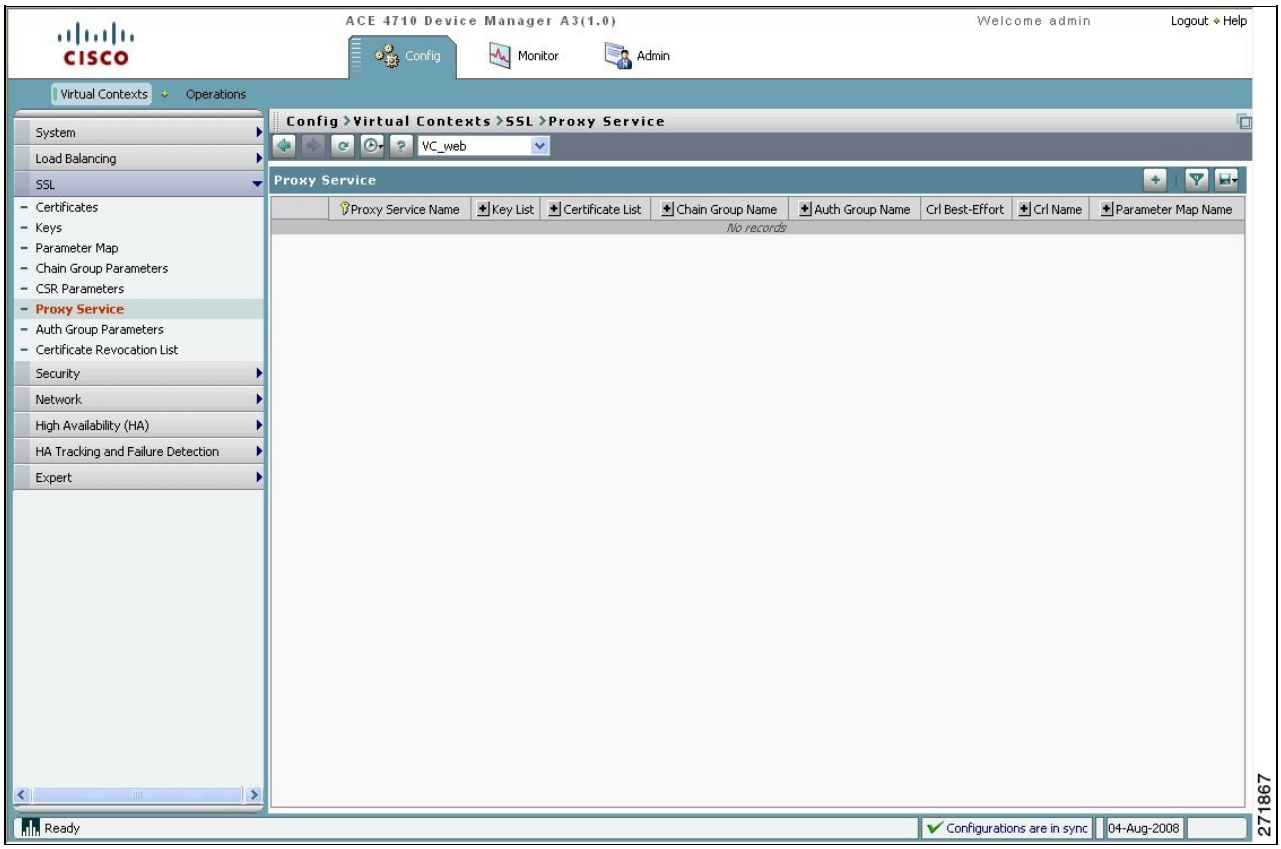
10. Click **Deploy Now** to deploy the parameter map on the ACE appliance. The Parameter Map Cipher pane appears.

11. Select **Add** in the Parameter Map Cipher pane (see Figure 7).

12. Accept the defaults and click **Deploy Now** in the Parameter Map Cipher pane to add a cipher to the parameter map.

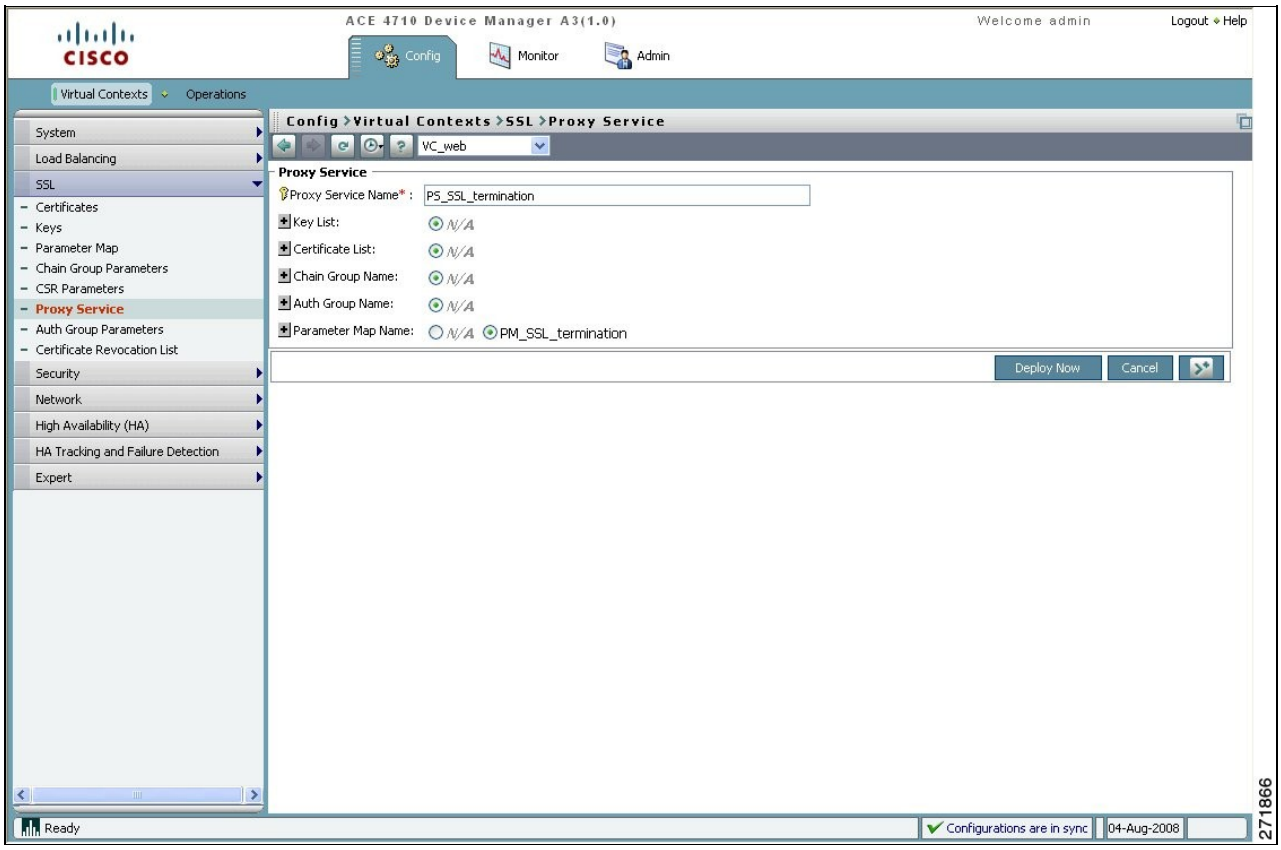
13. Create an SSL proxy service by choosing **SSL > Proxy Service**. The Proxy Service pane appears (Figure 8).

Figure 8 Proxy Service Pane



14. Click **Add** to create a proxy service. The Proxy Service window appears (Figure 9).

Figure 9 Proxy Service Window



15. Enter the following parameters. Leave the remaining parameters blank or with their default values.

    ◊ Proxy Service Name: PS_SSL_termination

    ◊ Key List: (choose the key file that you imported earlier)

    ◊ Certificate List: (choose the certificate that you imported earlier)

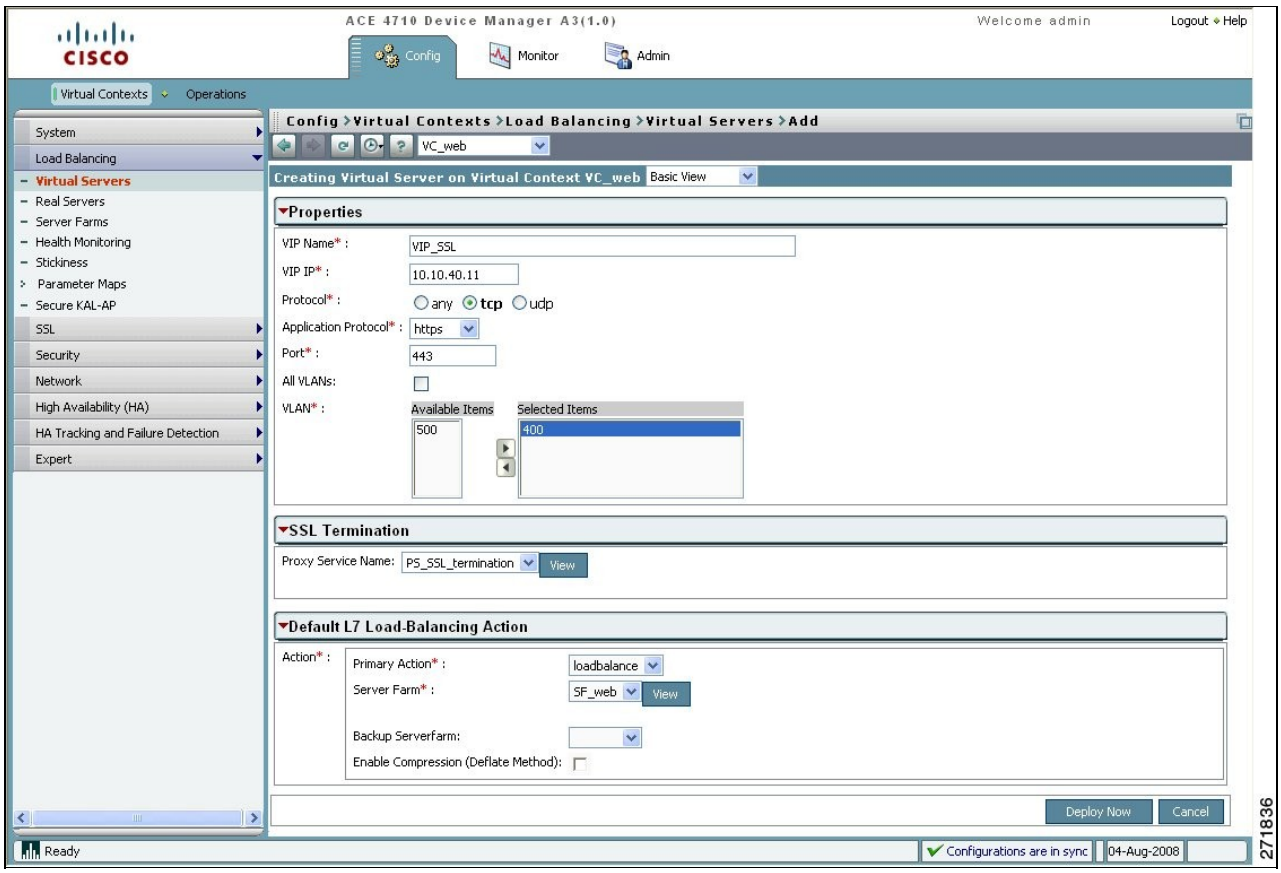
    ◊ Parameter Map Name: PM_SSL_termination

16. Click **Deploy Now** to deploy the proxy service on the ACE appliance.

17. Configure a virtual server for SSL termination by choosing **Load Balancing > Virtual Servers**. The Virtual Servers pane appears.

18. Click **Add** to create a virtual server. The Add virtual server window appears (Figure 10).

Figure 10 Add Virtual Server on Virtual Context Window



19. Enter the following parameters. Leave the remaining parameters blank or with their default values.

    ◊ VIP Name: VIP_SSL

    ◊ VIP IP: 10.10.40.11

    ◊ Protocol: tcp

    ◊ Application Protocol: https

    ◊ Port: 443

    ◊ VLAN: 400

    ◊ Proxy Service Name: PS_SSL_termination

    ◊ Primary Action: loadbalance

    ◊ Server Farm: SF_web

20. Click **Deploy Now** to deploy the virtual SSL server on the ACE appliance.

Configuring the ACE for SSL Termination Using the CLI

You can configure the ACE for SSL termination using the CLI by following these steps:

1. Verify that you are operating in the desired context, by checking the CLI prompt. If necessary, change to the correct context.

```
host1/Admin# changeto VC_web

host1/VC_web#
```

2. Import the key file marketing.pem from an FTP server.

```
host1/VC_web# crypto import ftp 172.25.91.100 Admin /marketing.pem marketing.pem

Password: ****

Passive mode on.

Hash mark printing on (1024 bytes/hash mark).

#

Successfully imported file from remote server.

host1/VC_web#
```

3. Copy the certificate information from the certificate you received from the CA, and paste it into a certificate file called marketing_cert.pem.

```
host1/VC_web# crypto import terminal marketing_cert.pem

Enter PEM formatted data ending with a blank line or ?quit? on a line by itself.

----------BEGIN CERTIFICATE----------

MIIC1DCCAj2gAwIBAgIDCCQAMA0GCSqGSIb3DQEBAgUAMIHEMQswCQYDVQQGEwJa

QTEVMBMGA1UECBMMV2VzdGVybiBDYXBlMRIwEAYDVQQHEwlDYXBlIFRvd24xHTAb

BgNVBAoTFFRoYXd0ZSBDb25zdWx0aW5nIGNjMSgwJgYDVQQLEx9DZXJ0aWZpY2F0

aW9uIFNlcnZpY2VzIERpdmlzaW9uMRkwFwYDVQQDExBUaGF3dGUgU2VydmVyIENB

MSYwJAYJKoZIhvcNAQkBFhdzZXJ2ZXItY2VydHNAdGhhd3RlLmNvbTAeFw0wMTA3

----------END CERTIFICATE----------
```

4. Enter quit to close the file.

```
quit

host1/VC_web#
```

5. Verify that the certificate matches the key pair.

```
host1/VC_web# crypto verify marketing.pem marketing_cert.pem

keypair in marketing.pem matches certificate in marketing_cert.pem
```

6. Start configuring SSL termination by entering configuration mode.

```
host1/VC_web# config
host1/VC_web(config)#
```

7. Create an SSL proxy service.

```
host1/VC_web(config)# ssl-proxy service PS_SSL_termination
host1/VC_web(config-ssl-proxy)#
```

8. Configure the SSL proxy service by defining the key pair and corresponding certificate.

```
host1/VC_web(config-ssl-proxy)# key marketing
host1/VC_web(config-ssl-proxy)# cert marketing_cert
host1/VC_web(config-ssl-proxy)# exit
host1/VC_web(config)#
```

9. Create a Layer 3 and Layer 4 class map and configure it with the input traffic match criteria.

```
host1/VC_web(config)# class-map CM_SSL
host1/VC_web(config-cmap)# match virtual-address 10.10.40.11 tcp any
host1/VC_web(config-cmap)# exit
host1/VC_web(config)#
```

10. Create a policy map and associate with it the class map CM_SSL.

```
host1/VC_web(config)# policy-map multi-match PM_SSL
host1/VC_web(config-pmap)# class CM_SSL
host1/VC_web(config-pmap-c)#
```

11. Associate the SSL proxy service PS_SSL_termination with the policy map.

```
host1/VC_web(config-pmap-c)# ssl-proxy server PS_SSL_termination
host1/VC_web(config-pmap-c)# exit
host1/VC_web(config-pmap)# exit
host1/VC_web(config)#
```

12. Apply the policy map to the input traffic of the VLAN 400 interface.

```
host1/VC_web(config)# interface vlan 400
host1/VC_web(config-if)# service-policy input PM_SSL
```

13. Display the running configuration to verify that the information that you just added is configured properly.

```
host1/VC_web(config-if)# do show running-config
```

In this section, you have configured a virtual server for SSL termination. In the next section, you will configure server health monitoring.