Displaying SSL Configuration Information and Statistics

This chapter describes the **show** commands available for displaying CSS SSL configuration information and statistics and an explanation of the fields displayed in the **show** command output. It contains the following major sections:

Showing Certificate and Key Pair Information

A number of **show** commands in the CSS enable you to display information about SSL certificates and key pairs stored on the CSS. Enter the following **show** commands from any mode:

- **show ssl associate cert** - Displays certificate associations
- **show ssl associate rsakey** - Displays RSA key pair associations
- **show ssl associate dsakey** - Displays DSA key pair associations

- **show ssl associate dhparam** - Displays information about Diffie-Hellman parameter associations
- **show ssl associate** - Displays all file associations for the CSS
- **show ssl files** - Displays all certificate, key pair, and Diffie-Hellman parameter files loaded on the CSS

Showing SSL Certificates

Use the **show ssl associate cert** *certname* command to display summary data for certificate associations in the CSS. You can optionally specify a certificate name to view detailed information about the certificate, corresponding to the certificate association. If you do not specify a certificate name, all certificate associations appear in the **show ssl associate cert** output.

To display information about all certificate associations, enter:

```
show ssl associate cert
```

Table 7-1 describes the fields in the **show ssl associate cert** output.

Table 7-1 Field Descriptions for the show ssl associate cert Command

Field	Description
Certificate Name	The name of the certificate association
File Name	The name of the file containing the certificate
Used By List	Indicates if the certificate association is used by the SSL proxy list containing the VIP address of the virtual server

To display information about a specific certificate association, enter:

```
show ssl associate cert myrsacert1
```

Table 7-2 describes the fields in the **show ssl associate cert** *certname* output.

Table 7-2 Field Descriptions for the show ssl associate cert certname Command

Field	Description
Certificate	The name of the Certificate Association (CA) that issued the certificate.
Version	The version of the certificate.
Serial Number	The serial number associated with the certificate.
Signature Algorithm	The digital signature algorithm (such as RSA) used for the encryption of information with a public/private key pair.
Issuer	The organization that generated the certificate and will vouch for it. An issuer is also the Certificate Authority (CA).
Validity	
Not Before	The starting time period, before which the certificate is not considered valid.
Not After	The ending time period, after which the certificate is not considered valid.
Subject	The certified party that possesses the private key.
Subject Public Key Info	
Public Key Algorithm	The name of the key exchange algorithm used to generate the public key (for example, RSA).
RSA Public Key	The number of bits in the key to define the size of the RSA key pair used to secure Web transactions.
Modulus	The actual public key on which the certificate was built.
Exponent	One of the base numbers used to generate the key.
X509v3 Extensions	An array of X509v3 extensions added to the certificate.

Table 7-2 Field Descriptions for the show ssl associate cert certname Command (continued)

Field	Description
X509v3 Basic Constraints	Indicates if the subject may act as a CA, with the certified public key being used to verify certificate signatures. If so, a certification path length constraint may also be specified.
Netscape Comment	A comment that may be displayed when the certificate is viewed.
X509v3 Subject Key Identifier	Identifies the public key being certified. It enables distinct keys used by the same subject to be differentiated (for example, as key updating occurs).
X509v3 Authority Key Identifier	Identifies the public key to be used to verify the signature on this certificate or CRL. It enables distinct keys used by the same CA to be distinguished (for example, as key updating occurs).
Signature Algorithm	The name of the algorithm used for digital signatures (but not for key exchanges).
Hex Numbers	The actual signature of the certificate. The client can regenerate this signature using the specified algorithm to make sure that the certificate data has not been changed.

Showing SSL RSA Private Keys

Use the **show ssl associate rsakey** *keyname* command to obtain information about RSA private key associations in the CSS. You can optionally specify an RSA key name to view information about a specific RSA key association (key size and type). If you do not specify an RSA keyname, you see a list of all RSA key associations.

Note When you view the contents of a specific key only, specifics on the key size and key type appears. This restriction occurs because the key contents are secure and should not be viewed.

To display information about all RSA private key associations:

```
(config) # show ssl associate rsakey
```

Table 7-3 describes the fields in the **show ssl associate rsakey** output.

Table 7-3 Field Descriptions for the show ssl associate rsakey Command

Field	Description
Key Name	The name of the RSA key association
File Name	The name of the file containing the RSA key pair
Used By List	Indicates if the RSA key association is used by the SSL proxy list containing the VIP address of the virtual server

To display information about a specific RSA key pair association, enter:

```
(config) # show ssl associate rsakey myrsakey1
1024-bit RSA keypair
```

Showing SSL DSA Private Keys

Use the **show ssl associate dsakey** *keyname* command to obtain information about DSA private key associations in the CSS. You can optionally specify a DSA key name to view information about a specific DSA key association (key size and type). If you do not specify a DSA keyname, you see a list of all DSA key associations.

Note When you view the contents of a specific key only, specifics on the key size and key type appears. This restriction occurs because the key contents are secure and should not be viewed.

To display information about all DSA key associations, enter:

```
(config) # show ssl associate dsakey
```

Table 7-4 describes the fields in the **show ssl associate dsakey** output.

Table 7-4 Field Descriptions for the show ssl associate dsakey Command

Field	Description
Key Name	The name of the DSA key association
File Name	The name of the file containing the DSA key pair
Used By List	Indicates if the DSA key association is used by the SSL proxy list containing the VIP address of the virtual server

To display information about a specific DSA key pair association, enter:

```
(config) # show ssl associate dsakey mydsakey1
1024-bit DSA keypair
```

Showing SSL Diffie-Hellman Parameters

Use the **show ssl associate dhparam** *paramname* to obtain information about Diffie-Hellman parameters. You can optionally specify a parameter filename to view information about a specific Diffie-Hellman parameter file association. If you do not specify a Diffie-Hellman parameter filename, you see a list of all Diffie-Hellman parameter file associations.

To display information about all Diffie-Hellman associations:

```
(config) # show ssl associate dhparam
```

Table 7-5 describes the fields in the **show ssl associate dhparam** output.

Table 7-5 Field Descriptions for the show ssl associate dhparam Command

Field	Description
Parameter Name	The name of the Diffie-Hellman parameter association
File Name	The name of the file containing the Diffie-Hellman parameters

Table 7-5 Field Descriptions for the show ssl associate dhparam Command (continued)

Field	Description
Used By List	Indicates if the Diffie-Hellman file association is used by the SSL proxy list containing the VIP address of the virtual server

To display information about a specific Diffie-Hellman parameter file association, enter:

```
(config) # show ssl associate dhparam mydhparam1
 512-bit DH parameters
```

Showing SSL Associations

Use the **show ssl associate** to display a summary of all certificate and key associations stored on the CSS.

To display a summary of SSL associations for the CSS, enter:

```
CSS11506(config)# show ssl associate

 Certificate Name        File Name           Used by List
 ----------------        ---------           ------------
 rsacert                 rsacert.pem         yes

 RSA Key Name            File Name           Used by List
 ------------            ---------           ------------
 rsakey                  rsakey.pem          yes

 DH Param Name           File Name           Used by List
 -------------           ---------           ------------
 dhparams                dhparams.pem        no

 DSA Key Name            File Name           Used by List
 ------------            ---------           ------------
 dsakey                  dsakey.pem          no
```

Showing SSL Certificates, Key Pairs, and Diffie-Hellman Parameter Files

Use the **show ssl files** to display a list of certificates, key pairs, and Diffie-Hellman parameter files loaded on the CSS.

For example, enter:

```
(config) # show ssl files
```

Table 7-6 describes the fields in the **show ssl files** output.

Table 7-6 Field Descriptions for the show ssl files Command

Field	Description
File Name	The name of the imported or manually-generated certificate, RSA key pair, DSA key pair, or Diffie-Hellman parameter file.
File Type	The format of the imported or manually-generated certificate, RSA key pair, DSA key pair, or Diffie-Hellman parameter file. File types can include DES-encoded, PEM-encoded, or PKCS#12-encoded.
File Size	The total size (in Kbytes) of the certificate, RSA key pair, DSA key pair, or Diffie-Hellman parameter file.

Showing SSL Proxy Configuration Information

Use the **show ssl-proxy-list** command to display information about SSL proxy lists. You can display general information about all SSL proxy lists or detailed information about a specific SSL proxy list.

Enter the **show ssl-proxy-list** commands from the specified command modes to display configuration information for an SSL proxy list:

- **show ssl-proxy-list**:
  - In ssl-proxy-list mode, this command displays detailed configuration information for the specified SSL proxy list.
  - In global, content, owner, service, SuperUser, and User modes, this command displays general configuration information for all existing SSL proxy lists.
- **show ssl-proxy-list** [**ssl-server**|**backend-server**] {*number*} - Displays detailed configuration information for the SSL proxy list and the virtual SSL servers or back-end servers in the list. Optionally, you can specify an SSL or back-end server number to display its configuration information. This command is available in ssl-proxy-list mode.
- **show ssl-proxy-list** *list_name* - Displays detailed configuration information for the specified SSL proxy list and all virtual SSL servers associated with the list. This command is available in global, content, owner, service, SuperUser, and User modes.
- **show ssl-proxy-list** *list_name* [**ssl-server**|**backend-server**] {*number*} - Displays detailed configuration information for the SSL proxy list and all virtual SSL servers or back-end servers in the list. Optionally, you can specify an SSL or back-end server number to display its configuration information. This command is available in global, content, owner, service, SuperUser, and User modes.

To view general information about all configured SSL proxy lists, enter:

```
# show ssl-proxy-list
```

Table 7-7 describes the fields in the **show ssl-proxy-list** output.

Table 7-7 Field Descriptions for the show ssl-proxy-list Command

Field	Description
Name	The name of the SSL proxy list
Description	The description for the SSL proxy list
State	The state of the SSL proxy list (active or suspended)
Services Associated	The number of services associated with the SSL proxy list
Rules Associated	The number of content rules associated with the SSL proxy list

For example, to display detailed configuration information about *ssl_list1* from the ssl-proxy-list mode, enter:

```
(config-ssl-proxy-list[ssl_list1])# show ssl-proxy-list
```

To display detailed configuration information about *ssl_list1* from global configuration mode, enter:

```
(config)# show ssl-proxy-list ssl_list1
```

Table 7-8 describes the fields in the **show ssl-proxy-list** *list_name* output.

Table 7-8 Field Descriptions for the show ssl-proxy-list Command

Field	Description
Description	The description for the SSL proxy list.
SSL-Server	
Number of SSL-Servers	The total number of virtual SSL servers specified for the SSL proxy list.
SSL-Server	A unique number for the virtual SSL server.
Number of Backend-Servers	The total number of back-end servers specified for the SSL proxy list.
Backend-server	A unique number for the back-end server.

Table 7-8 Field Descriptions for the show ssl-proxy-list Command (continued)

Field	Description
VIP Address	The VIP address for the virtual SSL or back-end server (corresponding to an SSL proxy list).
VIP Port	The virtual TCP port for the virtual SSL or back-end server (corresponding to an SSL proxy list).
Server Address	The circuit IP address of the back-end SSL server.
Server Port	The back-end SSL server port used for the SSL initiation connection.
Type	The type of SSL.
RSA Certificate	The name of the RSA certificate.
RSA Keypair	The name of the RSA key.
DSA Certificate	The name of the DSA certificate.
DSA Keypair	The name of the DSA key pair.
DH Param	The name of the Diffie-Hellman parameter association.
Client Authentication	State of client authentication on the virtual SSL server: enabled or disabled.
Client Authentication Failure	Configured method by which the CSS responds to a client certificate failure; ignore, redirect, or reject (default).
Authentication Redirect URL	URL used by the CSS to redirect a client connection when the client authentication failure method is configured to redirect.
CA Certificate	Name of the CA certificate imported on the CSS for client authentication.
CRL	CRL record name.
Session Cache Timeout	The period of time an SSL session ID remains valid before the CSS requires the full SSL handshake to establish a new SSL connection.
SSL Version	The specified SSL (version 3.0), TLS (version 1.0), or SSL and TLS protocol in use.

Table 7-8 Field Descriptions for the show ssl-proxy-list Command (continued)

Field	Description
Re-handshake Timeout	The period of time the CSS waits before initiating an SSL rehandshake message.
Re-handshake Data	The maximum amount of data to be exchanged between the CSS and the client, after which the CSS transmits the SSL handshake message and reestablishes the SSL session.
Virtual TCP Inactivity Timeout	The time period that the CSS waits before terminating a TCP connection with a client when there is little or no activity occurring on the connection.
Virtual TCP Syn Timeout	The time period that the CSS waits before terminating a TCP connection with a client that has not successfully completed the TCP three-way handshake with the CSS prior to transferring data.
Server TCP Inactivity Timeout	The time period that the CSS waits before terminating a TCP connection with a server when there is little or no activity occurring on the connection.
Server TCP Syn Timeout	The time period that the CSS waits before terminating a TCP connection with a server that has not successfully completed the TCP three-way handshake with the CSS prior to transferring data.
Cipher Suite(s)	The name of the cipher suite(s) assigned to the SSL content rule (see Table 4-1 for a list of all supported cipher suites and values for the specific SSL server).
Weight	The priority assigned to the cipher suite.
Port	The TCP port of the back-end content rule through which the back-end HTTP connections are sent.
Server	The VIP address of the back-end content rule through which the back-end HTTP connections are sent.
URL Rewrite Rule(s)	

Table 7-8 Field Descriptions for the show ssl-proxy-list Command (continued)

Field	Description
Number	The number of the URL rewrite rule in the SSL server.
Rule	The domain name of the URL to be redirected.
SSL Port	The port used for rewriting the HTTP Header Location field to contain an HTTPS location when the URL rewrite rule matches.
Clear Port	The port used for performing the URL rewrite rule match.
Server	The IP address assigned to the back-end content rule used with the cipher suite.
HTTP Header Insert Prefix	Configured prefix text string inserted in front of each client certificate, server certificate, and session field.
HTTP Header Insert	Type of field information inserted in the HTTP request header; Client Cert for client certificate, Server Cert for server certificate, and Session Data for SSL connection information. For information on the fields inserted in the header, see Chapter 4, Configuring SSL Termination.
HTTP Header Insert Static	Configured static text string inserted in the HTTP request header.

Showing CRL Record Configuration

Use the **show ssl crl-record** command to display the configuration for all Certificate Revocation List (CRL) records. Use the **show ssl crl-record** *name* command to display the configuration for a specific CRL record.

Note To verify that a CRL downloaded successfully, view the output of the **show ssl statistics ssl** command and the CSS syslog messages. For information on the **show ssl statistics** command, see the "Showing SSL Module Statistics" section.

For example, to display the configuration for all CRL records, enter:

```
(config) # show ssl crl-record
```

Table 7-9 describes the fields in the **show ssl crl-record** output.

Table 7-9 Field Descriptions for the show ssl crl-record Command

Field	Description
CRL Record	Configured name of the CRL record.
Signer Cert	Name of the CA certificate imported on the CSS. This certificate verifies that the CRL is from the CA.
Update Delay	How long the CSS waits before updating the CRL on the CSS.
CRL URL	URL where the CSS downloads the latest CRL.

Showing SSL URL Rewrite Statistics

Use the **show ssl urlrewrite** command to view the URL rewrite rule statistics for one or more SSL modules. This command displays statistics related to the number of flows received and evaluated by the SSL module, and the number of HTTP 300-series redirects found and then rewritten.

The syntax for this command is:

show ssl urlrewrite {**slot** *number*}

The **slot** *number* option displays URL rewrite statistics for a specific SSL module in the CSS 11503 or CSS 11506 chassis (assuming more than one module is installed). The valid slot entries are 2 and 3 (CSS 11503) or 2 to 6 (CSS 11506). If no slot number is specified, the **show ssl urlrewrite** command displays URL rewrite statistics for all SSL modules in the chassis.

For example, to view URL rewrite statistics for all SSL modules, enter:

```
# show ssl urlrewrite
```

For example, to view URL rewrite statistics for the SSL module in slot 5 of the CSS 11506, enter:

```
# show ssl urlrewrite slot 5
```

Table 7-10 describes the fields in the **show ssl urlrewrite** output.

Table 7-10 Field Descriptions for the show ssl urlrewrite Command

Field	Description
Virtual	The VIP address for the virtual SSL server.
Port	The virtual TCP port for the virtual SSL server.
Searches	The total number of flows received from the back-end server and evaluated by the SSL module to search for the presence of HTTP 300-series redirects.

Table 7-10 Field Descriptions for the show ssl urlrewrite Command (continued)

Field	Description
Redirects Found	The total number of flows examined by the SSL module for which an HTTP 300-series redirect was detected.
Redirects Rewritten	The total number of flows examined by the SSL module for which an HTTP 300-series redirect was found matching one of the configured URL rewrite rules. This number represents the total number of redirects that have been rewritten for this VIP address.

Showing SSL Module Statistics

Use the **show ssl statistics** command to view the statistics for the cryptography components and client authentication on one or more SSL modules. If you do not specify any options for this command, SSL statistics appear for all SSL modules in the CSS chassis.

The syntax for this command is:

show ssl statistics {*component*} {**slot** *number*}

The options and variables are:

- *component* - Selects a specific component in the SSL module to display statistics. The components include:
  - **backend-session-cache** - Displays counter statistics for back-end SSL or SSL initiation, where the CSS is acting as a client.
  - **crypto** - Displays counter statistics for the cryptography chip
  - **session-cache** - Displays counter statistics for SSL termination, where the CSS is acting as an SSL server.
  - **ssl** - Displays counter statistics for the SSL server counter
  - **ssl-proxy-server** - Displays counter statistics for the SSL proxy list component that provides SSL termination in the SSL module

- **slot** *number* - Displays statistics for a component in a specific SSL module in the CSS chassis (assuming more than one module is installed). Specify **slot** *number* after each **show ssl statistics** command. The valid slot entries are 2 and 3 (CSS 11503) or 2 to 6 (CSS 11506). If no slot number is specified, the **show ssl statistics** command displays statistics for all installed SSL modules.

For example, to view all SSL statistics for the SSL module in slot 5 of the CSS chassis, enter:

```
# show ssl statistics slot 5
```

Table 7-11 describes the fields in the **show ssl statistics** output.

Table 7-11 Field Descriptions for the show ssl statistics Command

Field	Description
Component	Indicates the specific component in the SSL module for which statistics are displayed. The SSL statistic functions include: • **ssl-proxy-server** - Displays counter statistics for the SSL proxy list component that provides SSL termination in the SSL module • **crypto** - Displays counter statistics for the cryptography chip in the SSL module • **ssl** - Displays counter statistics for the SSL server counter
Slot	Indicates the slot number of the SSL module for which statistics are displayed. Valid slots are 2 (CSS 11501), 2 and 3 (CSS 11503), or 2 to 6 (CSS 11506).
SSL Proxy List Statistics	
Handshake started for incoming SSL connections	Number of times the handshake process was initiated for incoming SSL connections from a client to the SSL module.
Handshake completed for incoming SSL connections	Number of times the handshake process was completed for incoming SSL connections from a client to the SSL module.

Table 7-11 Field Descriptions for the show ssl statistics Command (continued)

Field	Description
Handshake started for outgoing SSL connections	Number of times the handshake process was initiated for outgoing SSL connections from the SSL module to a client.
Handshake completed for outgoing SSL connections	Number of times the handshake process was completed for outgoing SSL connections from a client to the SSL module.
HTTP header insert of session data	Number of times that the CSS inserted SSL connection data information in the HTTP request header to a back-end server.
HTTP header insert of client certificate data	Number of times that the CSS inserted client certificate information in the HTTP request header to a back-end server.
HTTP header insert of server certificate data	Number of times that the CSS inserted server certificate information in the HTTP request header to a back-end server.
HTTP header insert of user defined prefix	Number of times that the CSS inserted the prefix field in the HTTP request header to a back-end server.
HTTP header insert of static phrase	Number of times that the CSS inserted the configured static text in the HTTP request header to a back-end server.
Active SSL flows high water mark	Maximum number of active SSL flows on the CSS.
Crypto Statistics	
RSA Private	Number of RSA private key calculations requested.
RSA Public	Number of RSA public key calculations requested.
DH Shared	Number of Diffie-Hellman shared secret key calculations requested.
DH Public	Number of Diffie-Hellman public key calculations requested.
DSA Sign	Number of DSA signings requested.
DSA Verify	Number of DSA verifications requested.

Table 7-11 Field Descriptions for the show ssl statistics Command (continued)

Field	Description
SSL MAC	Number of SSL MAC calculations requested.
TLS HMAC	Number of TLS HMAC calculations requested.
3DES	Number of 3 DES calculations requested.
ARC4	Number of ARC4 calculations requested.
HASH	Number of pure hash calculations requested.
RSA Private Failed	Number of RSA private key calculations that failed.
RSA Public Failed	Number of RSA public key calculations that failed.
DH Shared Failed	Number of Diffie-Hellman shared secret key calculations that failed.
DH Public Failed	Number of Diffie-Hellman public key calculations that failed.
DSA Sign Failed	Number of DSA signings that failed.
DSA Verify Failed	Number of DSA verifications that failed.
SSL MAC Failed	Number of SSL MAC calculations that failed.
TLS HMAC Failed	Number of TLS HMAC calculations that failed.
3DES Failed	Number of 3 DES calculations that failed.
ARC4 Failed	Number of ARC4 calculations that failed.
HASH Failed	Number of pure hash calculations that failed.
Hardware Device Not Found	Number of times that a call was made to the cryptography hardware and no hardware acceleration device was available.
Hardware Device Timed Out	Number of times the cryptography hardware did not complete an acceleration request within the specified time. This function is not currently implemented. This counter should always be 0.

Table 7-11 Field Descriptions for the show ssl statistics Command (continued)

Field	Description
Invalid Crypto Parameter	Number of times a hardware acceleration function was requested with an invalid parameter from the CSS. Invalid parameters include an invalid bit length for the operation, a buffer that is not a multiple of 4 bytes in length, a buffer that does not begin on an even 4-byte boundary, requesting an operation on a buffer with too many fragments or too few fragments (such as with no input), or requesting an illegal (nonsense) function.
Hardware Device Failed	Number of times the hardware acceleration device failed. This counter only increments on a DMA error.
Hardware Device Busy	Number of times he hardware acceleration device was busy and could not accept an acceleration request.
Out Of Resources	Number of times no hardware buffers were available and the cryptography hardware could not accept an acceleration request.
Cancelled -- Device Reset	Number of cancelled status returns due to a CSS reboot.
SSL Statistics	
RSA Private Decrypt calls	Number of RSA private decryption calls.
RSA Public Decrypt calls	Number of RSA public encryption calls.
DH Compute key calls	Number of Diffie-Hellman Compute key calls.
DH Generate key calls	Number of Diffie-Hellman Generate key calls.
DSA Verify calls	Number of DSA Verifications calls.
DSA Sign calls	Number of DSA Signing calls.
MD5 raw hash calls	Number of MD5 pure hash calls.
SHA1 raw hash calls	Number of SHA1 pure hash calls.
3-DES calls	Number of 3-DES calls.

Table 7-11 Field Descriptions for the show ssl statistics Command (continued)

Field	Description
RC4 calls	Number of RC4 calls.
SSL MAC (MD5) calls	Number of SSL Message Authentication Code (MAC) computations using MD5 algorithm.
SSL MAC (SHA1) calls	Number of SSL MAC computations using SHA algorithm.
TLS MAC (MD5) calls	Number of TLS MAC computations using MD5 algorithm.
TLS MAC (SHA1) calls	Number of TLS MAC computations using SHA algorithm.
Level 1 Alerts Received	Number of Level 1 alerts received.
Level 2 Alerts Received	Number of Level 2 alerts received.
Level 1 Alerts Sent	Number of Level 1 alerts transmitted.
Level 2 Alerts Sent	Number of Level 2 alerts transmitted.
SSL received bytes from TCP	Number of bytes SSL received from TCP.
SSL transmitted bytes to TCP	Number of bytes SSL transmitted to TCP.
SSL received Application Data bytes	Number of Application Data bytes received by the SSL module.
SSL transmitted Application Data bytes	Number of Application Data bytes transmitted by the SSL module.
SSL received non-application data bytes	Number of non-application data (handshake, alert, and change cipher) bytes received by the SSL module.
SSL transmitted non-application data bytes	Number of non-application data (handshake, alert, and change cipher) bytes transmitted by the SSL module.
RSA Private Decrypt failures	Number of RSA Private Decrypt calls that failed.
MAC failures for packets received	Number of times the MAC could not be verified for the incoming SSL messages.

Table 7-11 Field Descriptions for the show ssl statistics Command (continued)

Field	Description
Rehandshake TimerAlloc failed	Number of times the SSL module was unable to allocate the Rehandshake Timer.
Successful client authentications	Number of times that the CSS successfully authenticated a client certificate.
Client authentication failures	Number of times that the CSS could not authenticate a client certificate.
Unknown issuer certificates	Number of times that the CSS could not identify the issuer of a client certificate.
Signature unable to decrypt	Number of times that the CSS could not decrypt the signature on a client certificate.
Invalid issuer keys	Number of times that the CSS identified an invalid key of a client certificate.
Not yet valid certificate	Number of times that the CSS received a certificate that had not been validated by a CA at that time.
Expired certificates	Number of times that the CSS received a certificate with an expired time stamp.
Revoked certificate	Number of times that the CSS received a client certificate revoked by the issuer.
CRLs not obtained from host	A timeout occurred when the CSS tried to obtain a CRL from a host.
CRLs obtained but failed to load	The CSS successfully obtained the CRL but the CRL failed to load.
CRLs with invalid signatures	Number of times that the CSS could not validate the signer of the CRL with the signer certificate on the CSS.
CRL out of memory error	Number of times that the SSL module was out of memory and could not store the CRL. When a CRL cannot be stored in memory, all incoming client authentications will fail.
Session Cache Statistics	
Handshakes Accepted from Client	Number of handshakes that the SSL module accepted from clients.

Table 7-11 Field Descriptions for the show ssl statistics Command (continued)

Field	Description
Handshakes Renegotiated	Number of handshakes that the SSL module had to renegotiate.
Handshakes Completed	Number of successful handshakes that the SSL module completed with clients.
Session ID Misses	Number of session IDs offered by peers and looked up in the cache, but not found.
Session ID Timeouts	Number of cached sessions that reached their timeout limit and expired.
Session Cache Full	Number of times the cache was full.
Session ID Hits	Number of session IDs offered by peers that the SSL module found in its cache.
Total Number of Items Cached	Total number of sessions in the cache.
Backend Session Cache Statistics	
Handshakes Sourced to Server	Number of handshakes that the SSL module offered to servers.
Handshakes Renegotiated	Number of handshakes that the SSL module had to renegotiate.
Handshakes Completed	Number of successful handshakes that the SSL module completed with servers.
Session ID Misses	Number of times that there was not an existing valid session ID to send to the server.
Session ID Timeouts	Number of cached sessions that reached their timeout limit and expired.
Session Cache Full	Number of times that the cache was full.
Session ID Hits	Number of times that there was a valid session ID to offer to the server.
Total Number of Items Cached	Total number of sessions in the cache.

Clearing SSL Statistics

Use the **clear ssl statistics** command to clear the SSL statistics counters for all SSL modules in the CSS chassis. The reset statistics appear as 0 in the **show ssl statistics** display.

To clear SSL statistics counters for a specific module, use the **clear ssl statistics** command and specify the **slot** *number* following the command. The valid slot entries are 2 and 3 (CSS 11503) or 2 to 6 (CSS 11506).

To clear the SSL statistics counter, enter:

```
# clear ssl statistics
```

Showing SSL Flows

Use the **show ssl flows** command to display information about the active flows for each VIP address, port, and SSL module. The output displays TCP proxy flows, active SSL flows (a subset of TCP proxy flows), and SSL flows occurring during the handshake phase of the protocol (a subset of active SSL flows).

The syntax for this command is:

show ssl flows {**slot** *number*}

The **slot** *number* option displays information about the active flows for a specific SSL module in the CSS chassis (assuming more than one module is installed). The valid slot entries are 2 and 3 (CSS 11503) or 2 to 6 (CSS 11506). If no slot number is specified, the **show ssl flows** command displays statistics for all installed SSL modules.

To view SSL flows for all SSL modules in the CSS, enter:

```
# show ssl flows
```

To view SSL flows for a specific SSL module in the CSS chassis (for example, installed in slot 5), enter:

```
# show ssl flows slot 5
```

Table 7-12 describes the fields in the **show ssl flows** output.

Table 7-12 Field Descriptions for the show ssl flows Command

Field	Description
SSL Acceleration Flows for Slot	The slot number of the SSL module for which flows are displayed. Valid slots are 2 (CSS 11501), 2 and 3 (CSS 11503), or 2 to 6 (CSS 11506).
Virtual	Virtual address of the ssl-server.
Port	Virtual TCP port of the ssl-server.
TCP Proxy Flows	Number of TCP connections that are currently being proxied through the SSL virtual IP address. These connections could either be in: • The TCP handshake or teardown phase and, therefore, not carrying any SSL traffic • The Established TCP phase and carrying SSL traffic
Active SSL Flows	Current number of TCP Proxy Flows that are carrying active SSL connections. These flows are the Established TCP connections in which an SSL Client Hello message has been received by the CSS. The SSL flows remain in this active state until the teardown process is initiated, either by sending or receiving an SSL Alert message. The Active SSL Flows number is a subset of the TCP Proxy Flows column.
SSL Flows in Handshake	The current number of Active SSL Flows that are in the handshake phase of the SSL protocol but are not yet sending data. This means that an SSL Client Hello message has been received by the CSS but the final finished message still has not been sent. The SSL Flows in Handshake number is a subset of the Active SSL Flows column.