This article describes the process and CLI commands for troubleshooting SSL in the ACE.

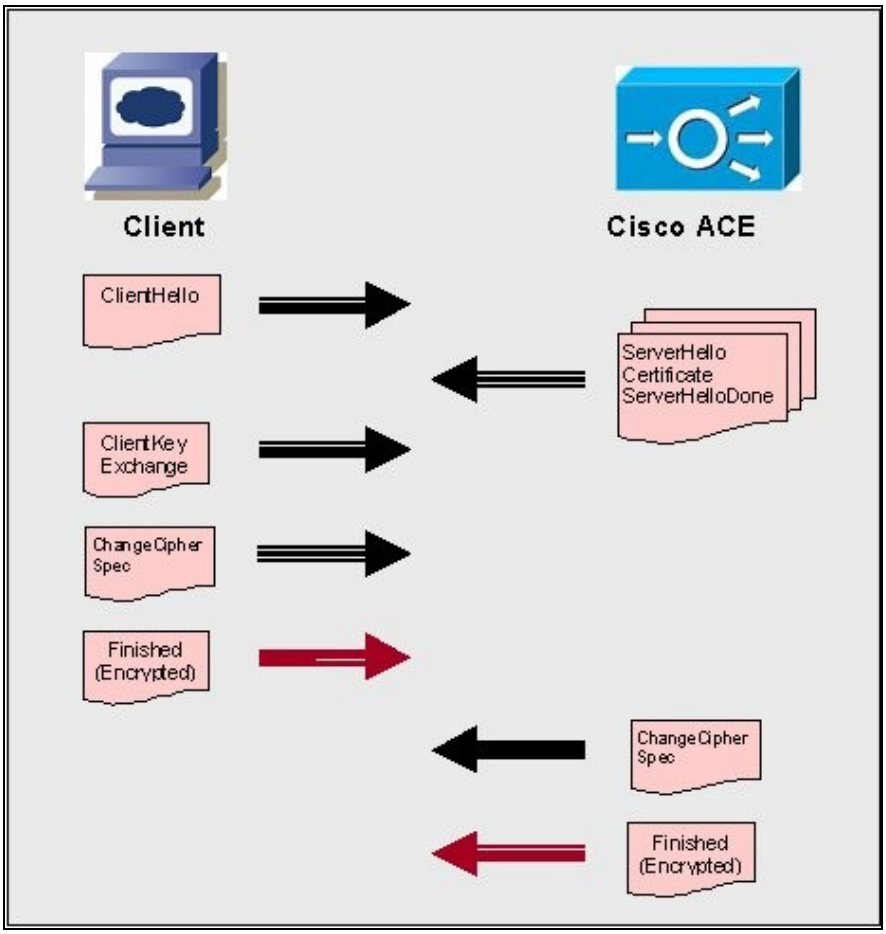
Guide Contents
Main Article
Overview of ACE Troubleshooting
Understanding the ACE Module Architecture and Traffic Flow
Preliminary ACE Troubleshooting
Troubleshooting ACE Boot Issues
Troubleshooting with ACE Logging
Troubleshooting Connectivity
Troubleshooting ACE Appliance Ethernet Ports
Troubleshooting Remote Access
Troubleshooting Access Control Lists
Troubleshooting Network Address Translation
Troubleshooting ACE Health Monitoring
Troubleshooting Layer 4 Load Balancing
Troubleshooting Layer 7 Load Balancing
Troubleshooting Redundancy
Troubleshooting SSL
Troubleshooting Compression
Troubleshooting Performance Issues
ACE Resource Limits
Managing ACE Resources
Show Counter Reference

Contents

Overview of ACE SSL Troubleshooting

Secure Sockets Layer (SSL) runs over TCP. After the TCP three-way handshake completes and the ACE has proxied the connection, the SSL handshake takes place. For information about proxied connections, see the Troubleshooting Connectivity article. See Figure 1 for an illustration of the SSL handshake.

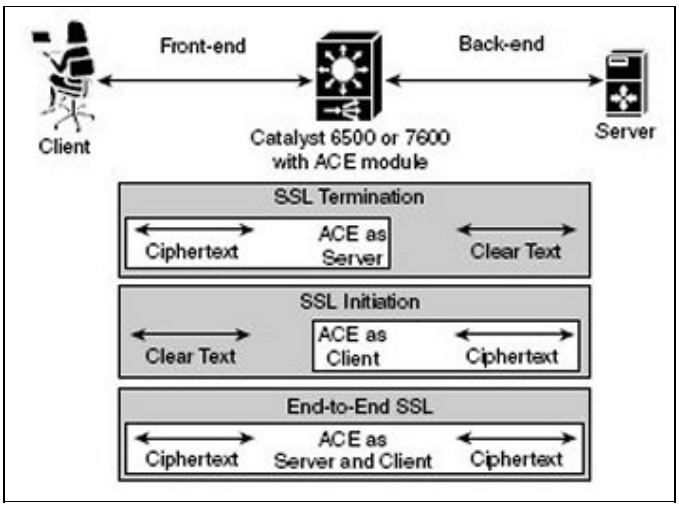
Figure 1. SSL Handshake



The ACE supports the following SSL configurations (see Figure 2):

- SSL termination (ACE acts as an SSL server)
- SSL initiation (ACE acts as a client)
- End-to-end SSL (SSL termination plus SSL initiation)

Figure 2. SSL Configurations



Before you begin to troubleshoot potential SSL issues, be sure that the following conditions exist:

- You have configured basic SLB and SSL on your ACE. For details about configuring SLB, see the *Cisco Application Control Engine Module Server Load-Balancing Configuration Guide* or the *Cisco ACE 4700 Series Appliance Server Load-Balancing Configuration Guide*. For details about configuring SSL, see the *Cisco Application Control Engine Module SSL Configuration Guide* or the *Cisco ACE 4700 Series Appliance SSL Configuration Guide*.

- If you are running multiple ACEs in a redundant configuration, be sure that you have copied the SSL certificates (certs) and keys to the standby ACE. Certs and keys are not replicated in a redundant configuration from the active ACE to the standby ACE. Also, ensure that the configurations on the active and the standby are identical, including the same licenses and software versions.

- Be sure that the certs and keys are no larger than 4096 bits and that they are of an RSA type supported by the ACE. For details about configuring SSL, see the *Cisco Application Control Engine Module SSL Configuration Guide* or the *Cisco ACE 4700 Series Appliance SSL Configuration Guide*. The ACE supports the following RSA key pair sizes:

    ◊ 512 (least security)

    ◊ 768 (normal security)

    ◊ 1024 (high security, level 1)

    ◊ 1536 (high security, level 2)

    ◊ 2048 (high security, level 3)

    ◊ 4096 (high security, level 4) - For software release A2(2.4) and later in the ACE module and software release A3(2.6) and later in the ACE appliance, you can use 4096-bit SSL certificates in chaingroups and authgroups. You can also import public certificates and keys that are 4096 bits in length.

- Server certs are valid, installed, and have not expired

Example of an SSL Termination Configuration

The following example shows a running-configuration file of the ACE acting as an SSL proxy server; terminating SSL or TLS connections from a client and then establishing a TCP connection to an HTTP server. When the ACE terminates the SSL or TLS connection, it decrypts the cipher text from the client and transmits the data as clear text to the HTTP server.

```
access-list ACL1 line 10 extended permit ip any any

probe http GEN-HTTP
  port 80
  interval 50
  faildetect 5
  expect status 200 200

rserver SERVER1
  ip address 10.1.0.11
  inservice
rserver SERVER2
  ip address 10.1.0.12
  inservice
rserver SERVER3
  ip address 10.1.0.13
  inservice
rserver SERVER4
  ip address 10.1.0.14
  inservice
rserver SERVER5
  ip address 10.1.0.15
  inservice
rserver SERVER6
  ip address 10.1.0.16
  inservice
rserver SERVER7
  ip address 10.1.0.17
  inservice
rserver SERVER8
  ip address 10.1.0.18
  inservice

serverfarm host SFARM1
  description SERVER FARM 1 FOR SSL TERMINATION
  probe GEN_HTTP
  rserver SERVER1 80
    inservice
  rserver SERVER2 80
    inservice
  rserver SERVER3 80
    inservice
  rserver SERVER4 80
    inservice

serverfarm host SFARM2
  description SERVER FARM 2 FOR SSL TERMINATION
  probe GEN_HTTP
  rserver SERVER5 80
    inservice
  rserver SERVER6 80
    inservice
  rserver SERVER7 80
    inservice
  rserver SERVER8 80
```

```
    inservice

parameter-map type ssl PARAMMAP_SSL_TERMINATION
  cipher RSA_WITH_3DES_EDE_CBC_SHA
  cipher RSA_WITH_AES_128_CBC_SHA priority 2
  cipher RSA_WITH_AES_256_CBC_SHA priority 3
  version all
parameter-map type connection TCP_PARAM
  syn-data drop
  exceed-mss allow

ssl-proxy service SSL_PSERVICE_SERVER
  ssl advanced-options PARAMMAP_SSL_TERMINATION
  key MYKEY.PEM
  cert MYCERT.PEM

class-map type http loadbalance match-all L7_SERVER_CLASS
  description Sticky for SSL Testing
  2 match http url .*.jpg
  3 match source-address 192.168.130.0 255.255.255.0
class-map type http loadbalance match-all L7_SLB-HTTP_CLASS
  2 match http url .*
  3 match source-address 192.168.130.0 255.255.255.0
class-map match-all L4_SSL-TERM_CLASS
  description SSL Termination VIP
  2 match virtual-address 192.168.130.11 tcp eq https

policy-map type loadbalance first-match L7_SSL-TERM_POLICY
  class L7_SERVER_CLASS
    serverfarm SFARM1
    insert-http I_AM header-value "SSL_TERM"
    insert-http SRC_Port header-value "%ps"
    insert-http DEST_IP header-value "%id"
    insert-http DEST_Port header-value "%pd"
    insert-http SRC_IP header-value "is"
  class L7_SLB-HTTP_CLASS
    serverfarm SFARM1
    insert-http I_AM header-value "SSL_TERM"
    insert-http SRC_Port header-value "%ps"
    insert-http DEST_IP header-value "%id"
    insert-http DEST_Port header-value "%pd"
    insert-http SRC_IP header-value "is"

policy-map multi-match L4_SSL-VIP_POLICY
  class L4_SSL-TERM_CLASS
    loadbalance vip inservice
    loadbalance policy L7_SSL-TERM_POLICY
    loadbalance vip icmp-reply
    ssl-proxy server SSL_PSERVICE_SERVER
    connection advanced-options TCP_PARAM

interface vlan 120
  description Upstream VLAN_120 - Clients and VIPs
  ip address 192.168.120.1 255.255.255.0
  fragment chain 20
  fragment min-mtu 68
  access-group input ACL1
  nat-pool 1 192.168.120.70 192.168.120.80 netmask 255.255.255.0 pat
  service-policy input L4_SSL-VIP_POLICY
  no shutdown

ip route 10.1.0.0 255.255.255.0 192.168.120.254
```

Example of an SSL Initiation Configuration

The following example shows a running-configuration file of the ACE acting as an SSL proxy client, initiating and maintaining an SSL connection between itself and an SSL server. The ACE receives clear text from an HTTP client, and then encrypts and transmits the 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.

```
access-list ACL1 line 10 extended permit ip any any

probe http GEN-HTTP
  port 80
  interval 50
  faildetect 5
  expect status 200 200

rserver SERVER1
  ip address 10.1.0.11
  inservice
rserver SERVER2
  ip address 10.1.0.12
  inservice
rserver SERVER3
  ip address 10.1.0.13
  inservice
rserver SERVER4
  ip address 10.1.0.14
  inservice
rserver SERVER5
  ip address 10.1.0.15
  inservice
rserver SERVER6
  ip address 10.1.0.16
  inservice
rserver SERVER7
  ip address 10.1.0.17
  inservice
rserver SERVER8
  ip address 10.1.0.18
  inservice

serverfarm host SFARM1
  description SERVER FARM 1 FOR SSL INITIATION
  probe GEN_HTTP
  rserver SERVER1 443
    inservice
  rserver SERVER2 443
    inservice
  rserver SERVER3 443
    inservice
  rserver SERVER4 443
    inservice

serverfarm host SFARM2
  description SERVER FARM 2 FOR SSL TERMINATION
  probe GEN_HTTP
  rserver SERVER5 443
    inservice
  rserver SERVER6 443
    inservice
  rserver SERVER7 443
    inservice
```

```
  rserver SERVER8 443
    inservice

parameter-map type http PARAMMAP_HTTP
  server-conn reuse
  case-insensitive
  persistence-rebalance
parameter-map type ssl PARAMMAP_SSL_INITIATION
  cipher RSA_WITH_RC4_128_MD5
  cipher RSA_WITH_RC4_128_SHA
  cipher RSA_WITH_DES_CBC_SHA
  cipher RSA_WITH_3DES_EDE_CBC_SHA
  cipher RSA_WITH_AES_128_CBC_SHA
  cipher RSA_WITH_AES_256_CBC_SHA
  cipher RSA_EXPORT_WITH_RC4_40_MD5
  cipher RSA_EXPORT1024_WITH_RC4_56_MD5
  cipher RSA_EXPORT_WITH_DES40_CBC_SHA
  cipher RSA_EXPORT1024_WITH_DES_CBC_SHA
  cipher RSA_EXPORT1024_WITH_RC4_56_SHA
  version all
parameter-map type connection TCP_PARAM
  syn-data drop
  exceed-mss allow

ssl-proxy service SSL_PSRVICE_CLIENT
  ssl advanced-options PARAMMAP_SSL_INITIATION

class-map type http loadbalance match-all L7_SERVER_CLASS
  description Sticky for SSL Testing
  2 match http url .*.jpg
  3 match source-address 192.168.130.0 255.255.255.0
class-map type http loadbalance match-all L7_SLB-HTTP_CLASS
  2 match http url .*
  3 match source-address 192.168.130.0 255.255.255.0
class-map match-all L4_SSL-INIT_CLASS
  description SSL Initiation VIP
  2 match virtual-address 192.168.130.12 tcp eq www

policy-map type loadbalance first-match L7_SSL-INIT_POLICY
  class L7_SERVER_CLASS
    serverfarm SFARM1
    insert-http SRC_IP header-value "%is"
    insert-http I_AM header-value "SSL_INIT"
    insert-http SRC_Port header-value "%ps"
    insert-http DEST_IP header-value "%id"
    insert-http DEST_Port header-value "%pd"
    ssl-proxy client SSL_PSERVICE_CLIENT
  class L7_SLB-HTTP_CLASS
    serverfarm SFARM2
    insert-http SRC_IP header-value "%is"
    insert-http I_AM header-value "SSL_INIT"
    insert-http DEST_Port header-value "%pd"
    insert-http DEST_IP header-value "%id"
    insert-http SRC_Port header-value "%ps"
    ssl-proxy client SSL_PSERVICE_CLIENT
policy-map multi-match L4_SSL-VIP_POLICY
  class L4_SSL-INIT_CLASS
    loadbalance vip inservice
    loadbalance policy L7_SSL-INIT_POLICY
    loadbalance vip icmp-reply active
    appl-parameter http advanced-options PARAMMAP_HTTP
    connection advanced-options TCP_PARAM

interface vlan 120
```

```
  description Upstream VLAN_120 - Clients and VIPs
  ip address 192.168.120.1 255.255.255.0
  fragment chain 20
  fragment min-mtu 68
  access-group input ACL1
  nat-pool 1 192.168.120.70 192.168.120.80 netmask 255.255.255.0 pat
  service-policy input L4_SSL-VIP_POLICY
  no shutdown

ip route 10.1.0.0 255.255.255.0 192.168.120.254
```

Troubleshooting ACE SSL

To troubleshoot SSL issues, follow these steps:

1. For the ACE module, check the health of the Nitrox-II (crypto module) and ensure that it has not become unresponsive. Stop all traffic, and then enter the following command:

ACE_module5/Admin# **show crypto hardware**

Figure 3. Example of the Show Crypto Hardware Command Output for an Unresponsive Crypto Module

```
=0x478860de, cpu_freq=0.6GHz, dwell=1, delta=600060015 (1s)
                  Total                        Delta
                  ------------------ --------------
obuf packets:      0x91821b6                         0       0.0 Packets/sec

Encrypt packets:   0x7313fc2                         0     nan Bytes/Packet
Decrypt packets:   0x137fda7                         0     nan Bytes/Packet
Enc/Dec packets:   0x8693d69                         0     nan Bytes/Packet
GP_OP packets:     0xaee44d                          0     nan Bytes/Packet
STX1 packets:      0x9181c30                         0     nan Bytes/Packet
IMX1 packets:      0x918232b                         0     nan Bytes/Packet
IMX1 errors :      0x0                               0     nan Bytes/Packet
IMX1 drops  :      0x0                               0     nan Bytes/Packet

Encrypt bytes:     0x1fa2c940d0                      0   0.000 Gbps
Decrypt bytes:     0x52cf12694                       0   0.000 Gbps
Enc/Dec bytes:     0x24cfba6764                      0   0.000 Gbps
GP_OP   bytes:     0x12b987203                       0   0.000 Gbps
STX1 bytes:        0x25aa3f2cbc                      0   0.000 Gbps
IMX1 bytes:        0x26440e1dfb                      0   0.000 Gbps

L3I Drop:          0x0                               0
L3I Fwd CP:        0x0                               0
L3I Fwd CP & DOS:  0x0                               0
L3I Decrypt Pass:  0x0                               0
L3I Total Pass:    0x0                               0

TX Backpressure:   0x0                               0 (STX1_BCKPRS_CNT)
RX Backpressure:   0x18                              0 (SPX1_BCKPRS_CNT)
TX Buffers used:   0x500                             0 (BMO_SP1_TPA)
TX Buffer:         0x500                (High Water Mark)
RX Buffers used:   0x206                             0 (BMI_SP1_TPA)
RX Buffer:         0x206                (High Water Mark)

enabled_cores:     0x3fffff
available_cores:   0x3ffffe  (Using:   0 )
pom_robq_empty:    0x7fffefff pom_inq_empty:      0x7fffefff
pom_tx0_outq_empty:0x0fffff pom_tx1_outq_empty: 0x01ffff
POM count:         762(0)   Interrupts:        0x0(0)
```

STX1 is a count of the number of packets transmitted by the Nitrox-II and IMX1 is the number of packets received by the Nitrox-II. On a normal system, these values should be the same once traffic has stopped. If the values are not the same, the Nitrox-II has become unresponsive.

The Nitrox-II uses 0x500 TX buffers to transmit packets and 0x200 RX buffers to receive packets. If the [TR]X Buffers used count ever exceeds the amount available, the Nitrox-II has become unresponsive.

The available cores field shows which of the 22 cores of the Nitrox-II are active. When no traffic is flowing, there should be no numbers following the Using: statement. If there are, as in the sample output above, then that core (0 in this case) is hung, and the Nitrox-II has become unresponsive.

For the POM count, there are two numbers, A(B). The "A" value is the number of outstanding packets to the Packet Order Manager, while the "B" value, counts the number of packets that have been processed in the last second. When no traffic is flowing, both of these values should be 0. If no traffic is flowing, and the value of "A" is nonzero as shown above, then there are outstanding requests to the POM that are not being processed, because the Nitrox-II has become unresponsive.

2. Ensure that appropriate ports are designated for PAT in an SSL termination configuration. By default, connections to the real server from the ACE will inherit the destination port from the client to VIP connection so that a connection to port 443 on the VIP will go to port 443 on the real server, unless otherwise specified in the server farm configuration. This will cause problems if you are using ACE to offload SSL between the client and the VIP and send clear-text traffic to the real servers. The following example demonstrates a port definition in a server farm configuration:

```
serverfarm host sf1
  probe HTTP_PROBE
  rserver rs1 80
    inservice
  rserver rs2 80
    inservice
```

3. Verify that the SSL certificate and key are correct by entering the following command:

```
ACE_module5/Admin# crypto verify key cert
```

4. Verify that a certificate revocation list (CRL) has been downloaded, enter the following command:

```
ACE_module5/Admin# show crypto crl test1

test1:
URL: http://192.168.12.23/test.crl
Last Downloaded: not downloaded yet
Total Number Of Download Attempts: 0
Failed Download Attempts: 0
```

5. Verify the contents of an authgroup by entering the following command:

```
ACE_module5/Admin# show crypto authgroup authgroup_name
```

6. Display client SSL statistics by entering the the following command:

```
ACE_module5/Admin# show stats crypto client

+-----------------------------------------------+
+---- Crypto client termination statistics ----+
+-----------------------------------------------+
SSLv3 negotiated protocol:                      0
TLSv1 negotiated protocol:                      0
SSLv3 full handshakes:                          0
SSLv3 resumed handshakes:                       0
SSLv3 rehandshakes:                             0
TLSv1 full handshakes:                          0
TLSv1 resumed handshakes:                       0
TLSv1 rehandshakes:                             0
SSLv3 handshake failures:                       0
SSLv3 failures during data phase:               0
TLSv1 handshake failures:                       0
TLSv1 failures during data phase:               0
Handshake Timeouts:                             0
total transactions:                             0
SSLv3 active connections:                       0
SSLv3 connections in handshake phase:           0
SSLv3 conns in renegotiation phase:             0
SSLv3 connections in data phase:                0
TLSv1 active connections:                       0
TLSv1 connections in handshake phase:           0
TLSv1 conns in renegotiation phase:             0
```

```
TLSv1 connections in data phase:                  0


+---------------------------------------------+
+------- Crypto client alert statistics -------+
+---------------------------------------------+
SSL alert CLOSE_NOTIFY rcvd:                      0
SSL alert UNEXPECTED_MSG rcvd:                    0
SSL alert BAD_RECORD_MAC rcvd:                    0
SSL alert DECRYPTION_FAILED rcvd:                 0
SSL alert RECORD_OVERFLOW rcvd:                   0
SSL alert DECOMPRESSION_FAILED rcvd:              0
SSL alert HANDSHAKE_FAILED rcvd:                  0
SSL alert NO_CERTIFICATE rcvd:                    0
SSL alert BAD_CERTIFICATE rcvd:                   0
SSL alert UNSUPPORTED_CERTIFICATE rcvd:           0
SSL alert CERTIFICATE_REVOKED rcvd:               0
SSL alert CERTIFICATE_EXPIRED rcvd:               0
SSL alert CERTIFICATE_UNKNOWN rcvd:               0
SSL alert ILLEGAL_PARAMETER rcvd:                 0
SSL alert UNKNOWN_CA rcvd:                        0
SSL alert ACCESS_DENIED rcvd:                     0
SSL alert DECODE_ERROR rcvd:                      0
SSL alert DECRYPT_ERROR rcvd:                     0
SSL alert EXPORT_RESTRICTION rcvd:                0
SSL alert PROTOCOL_VERSION rcvd:                  0
SSL alert INSUFFICIENT_SECURITY rcvd:             0
SSL alert INTERNAL_ERROR rcvd:                    0
SSL alert USER_CANCELED rcvd:                     0
SSL alert NO_RENEGOTIATION rcvd:                  0
SSL alert CLOSE_NOTIFY sent:                      0
SSL alert UNEXPECTED_MSG sent:                    0
SSL alert BAD_RECORD_MAC sent:                    0
SSL alert DECRYPTION_FAILED sent:                 0
SSL alert RECORD_OVERFLOW sent:                   0
SSL alert DECOMPRESSION_FAILED sent:              0
SSL alert HANDSHAKE_FAILED sent:                  0
SSL alert NO_CERTIFICATE sent:                    0
SSL alert BAD_CERTIFICATE sent:                   0
SSL alert UNSUPPORTED_CERTIFICATE sent:           0
SSL alert CERTIFICATE_REVOKED sent:               0
SSL alert CERTIFICATE_EXPIRED sent:               0
SSL alert CERTIFICATE_UNKNOWN sent:               0
SSL alert ILLEGAL_PARAMETER sent:                 0
SSL alert UNKNOWN_CA sent:                        0
SSL alert ACCESS_DENIED sent:                     0
SSL alert DECODE_ERROR sent:                      0
SSL alert DECRYPT_ERROR sent:                     0
SSL alert EXPORT_RESTRICTION sent:                0
SSL alert PROTOCOL_VERSION sent:                  0
SSL alert INSUFFICIENT_SECURITY sent:             0
SSL alert INTERNAL_ERROR sent:                    0
SSL alert USER_CANCELED sent:                     0
SSL alert NO_RENEGOTIATION sent:                  0


+---------------------------------------------+
+--- Crypto client authentication statistics ---+
+---------------------------------------------+
Total SSL client authentications:                 0
Failed SSL client authentications:                0
SSL client authentication cache hits:             0
SSL static CRL lookups:                           0
SSL best effort CRL lookups:                      0
```

```
SSL CRL lookup cache hits:                        0
SSL revoked certificates:                         0
Total SSL server authentications:                 0
Failed SSL server authentications:                0


+-----------------------------------------------+
+------- Crypto client cipher statistics -------+
+-----------------------------------------------+
Cipher sslv3_rsa_rc4_128_md5:                     0
Cipher sslv3_rsa_rc4_128_sha:                     0
Cipher sslv3_rsa_des_cbc_sha:                     0
Cipher sslv3_rsa_3des_ede_cbc_sha:                0
Cipher sslv3_rsa_exp_rc4_40_md5:                  0
Cipher sslv3_rsa_exp_des40_cbc_sha:               0
Cipher sslv3_rsa_exp1024_rc4_56_md5:              0
Cipher sslv3_rsa_exp1024_des_cbc_sha:             0
Cipher sslv3_rsa_exp1024_rc4_56_sha:              0
Cipher sslv3_rsa_aes_128_cbc_sha:                 0
Cipher sslv3_rsa_aes_256_cbc_sha:                 0
Cipher tlsv1_rsa_rc4_128_md5:                     0
Cipher tlsv1_rsa_rc4_128_sha:                     0
Cipher tlsv1_rsa_des_cbc_sha:                     0
Cipher tlsv1_rsa_3des_ede_cbc_sha:                0
Cipher tlsv1_rsa_exp_rc4_40_md5:                  0
Cipher tlsv1_rsa_exp_des40_cbc_sha:               0
Cipher tlsv1_rsa_exp1024_rc4_56_md5:              0
Cipher tlsv1_rsa_exp1024_des_cbc_sha:             0
Cipher tlsv1_rsa_exp1024_rc4_56_sha:              0
Cipher tlsv1_rsa_aes_128_cbc_sha:                 0
Cipher tlsv1_rsa_aes_256_cbc_sha:                 0
```

7. Display SSL server statistics by entering the following command:

```
ACE_module5/Admin# show stats crypto server

+-----------------------------------------------+
+---- Crypto server termination statistics ----+
+-----------------------------------------------+
SSLv3 negotiated protocol:                        0
TLSv1 negotiated protocol:                        0
SSLv3 full handshakes:                            0
SSLv3 resumed handshakes:                         0
SSLv3 rehandshakes:                               0
TLSv1 full handshakes:                            0
TLSv1 resumed handshakes:                         0
TLSv1 rehandshakes:                               0
SSLv3 handshake failures:                         0
SSLv3 failures during data phase:                 0
TLSv1 handshake failures:                         0
TLSv1 failures during data phase:                 0
Handshake Timeouts:                               0
total transactions:                               0
SSLv3 active connections:                         0
SSLv3 connections in handshake phase:             0
SSLv3 conns in renegotiation phase:               0
SSLv3 connections in data phase:                  0
TLSv1 active connections:                         0
TLSv1 connections in handshake phase:             0
TLSv1 conns in renegotiation phase:               0
TLSv1 connections in data phase:                  0
```

```
+---------------------------------------------+
+------- Crypto server alert statistics -------+
+---------------------------------------------+
SSL alert CLOSE_NOTIFY rcvd:                        0
SSL alert UNEXPECTED_MSG rcvd:                      0
SSL alert BAD_RECORD_MAC rcvd:                      0
SSL alert DECRYPTION_FAILED rcvd:                   0
SSL alert RECORD_OVERFLOW rcvd:                     0
SSL alert DECOMPRESSION_FAILED rcvd:                0
SSL alert HANDSHAKE_FAILED rcvd:                    0
SSL alert NO_CERTIFICATE rcvd:                      0
SSL alert BAD_CERTIFICATE rcvd:                     0
SSL alert UNSUPPORTED_CERTIFICATE rcvd:             0
SSL alert CERTIFICATE_REVOKED rcvd:                 0
SSL alert CERTIFICATE_EXPIRED rcvd:                 0
SSL alert CERTIFICATE_UNKNOWN rcvd:                 0
SSL alert ILLEGAL_PARAMETER rcvd:                   0
SSL alert UNKNOWN_CA rcvd:                          0
SSL alert ACCESS_DENIED rcvd:                       0
SSL alert DECODE_ERROR rcvd:                        0
SSL alert DECRYPT_ERROR rcvd:                       0
SSL alert EXPORT_RESTRICTION rcvd:                  0
SSL alert PROTOCOL_VERSION rcvd:                    0
SSL alert INSUFFICIENT_SECURITY rcvd:               0
SSL alert INTERNAL_ERROR rcvd:                      0
SSL alert USER_CANCELED rcvd:                       0
SSL alert NO_RENEGOTIATION rcvd:                    0
SSL alert CLOSE_NOTIFY sent:                        0
SSL alert UNEXPECTED_MSG sent:                      0
SSL alert BAD_RECORD_MAC sent:                      0
SSL alert DECRYPTION_FAILED sent:                   0
SSL alert RECORD_OVERFLOW sent:                     0
SSL alert DECOMPRESSION_FAILED sent:                0
SSL alert HANDSHAKE_FAILED sent:                    0
SSL alert NO_CERTIFICATE sent:                      0
SSL alert BAD_CERTIFICATE sent:                     0
SSL alert UNSUPPORTED_CERTIFICATE sent:             0
SSL alert CERTIFICATE_REVOKED sent:                 0
SSL alert CERTIFICATE_EXPIRED sent:                 0
SSL alert CERTIFICATE_UNKNOWN sent:                 0
SSL alert ILLEGAL_PARAMETER sent:                   0
SSL alert UNKNOWN_CA sent:                          0
SSL alert ACCESS_DENIED sent:                       0
SSL alert DECODE_ERROR sent:                        0
SSL alert DECRYPT_ERROR sent:                       0
SSL alert EXPORT_RESTRICTION sent:                  0
SSL alert PROTOCOL_VERSION sent:                    0
SSL alert INSUFFICIENT_SECURITY sent:               0
SSL alert INTERNAL_ERROR sent:                      0
SSL alert USER_CANCELED sent:                       0
SSL alert NO_RENEGOTIATION sent:                    0


+---------------------------------------------+
+--- Crypto server authentication statistics ---+
+---------------------------------------------+
Total SSL client authentications:                   0
Failed SSL client authentications:                  0
SSL client authentication cache hits:               0
SSL static CRL lookups:                             0
SSL best effort CRL lookups:                        0
SSL CRL lookup cache hits:                          0
SSL revoked certificates:                           0
Total SSL server authentications:                   0
```

```
Failed SSL server authentications:                0


+-----------------------------------------------+
+------- Crypto server cipher statistics -------+
+-----------------------------------------------+
Cipher sslv3_rsa_rc4_128_md5:                     0
Cipher sslv3_rsa_rc4_128_sha:                     0
Cipher sslv3_rsa_des_cbc_sha:                     0
Cipher sslv3_rsa_3des_ede_cbc_sha:                0
Cipher sslv3_rsa_exp_rc4_40_md5:                  0
Cipher sslv3_rsa_exp_des40_cbc_sha:               0
Cipher sslv3_rsa_exp1024_rc4_56_md5:              0
Cipher sslv3_rsa_exp1024_des_cbc_sha:             0
Cipher sslv3_rsa_exp1024_rc4_56_sha:              0
Cipher sslv3_rsa_aes_128_cbc_sha:                 0
Cipher sslv3_rsa_aes_256_cbc_sha:                 0
Cipher tlsv1_rsa_rc4_128_md5:                     0
Cipher tlsv1_rsa_rc4_128_sha:                     0
Cipher tlsv1_rsa_des_cbc_sha:                     0
Cipher tlsv1_rsa_3des_ede_cbc_sha:                0
Cipher tlsv1_rsa_exp_rc4_40_md5:                  0
Cipher tlsv1_rsa_exp_des40_cbc_sha:               0
Cipher tlsv1_rsa_exp1024_rc4_56_md5:              0
Cipher tlsv1_rsa_exp1024_des_cbc_sha:             0
Cipher tlsv1_rsa_exp1024_rc4_56_sha:              0
Cipher tlsv1_rsa_aes_128_cbc_sha:                 0
Cipher tlsv1_rsa_aes_256_cbc_sha:                 0
```

8. Display the number of SSL data messages sent and SSL FIN/RST messages sent by entering the following command:

```
ACE_module5/Admin# show stats http

+-----------------------------------------+
+-------------- HTTP statistics ----------+
+-----------------------------------------+
 LB parse result msgs sent : 0          , TCP data msgs sent       : 0
 Inspect parse result msgs : 0          , SSL data msgs sent       : 0 <-------
                       sent
 TCP fin/rst msgs sent     : 0          , Bounced fin/rst msgs sent: 0
 SSL fin/rst msgs sent     : 0          , Unproxy msgs sent        : 0 <-------
 Drain msgs sent           : 0          , Particles read           : 0
 Reuse msgs sent           : 0          , HTTP requests            : 0
 Reproxied requests        : 0          , Headers removed          : 0
 Headers inserted          : 0          , HTTP redirects           : 0
 HTTP chunks               : 0          , Pipelined requests       : 0
 HTTP unproxy conns        : 0          , Pipeline flushes         : 0
 Whitespace appends        : 0          , Second pass parsing      : 0
 Response entries recycled : 0          , Analysis errors          : 0
 Header insert errors      : 0          , Max parselen errors      : 0
 Static parse errors       : 0          , Resource errors          : 0
 Invalid path errors       : 0          , Bad HTTP version errors  : 0
 Headers rewritten         : 0          , Header rewrite errors    : 0
```

9. Display session cache statistics for the current context by entering the following command:

```
switch/Admin# show crypto session
SSL Session Cache Stats for Context
-----------------
Number of Client Sessions:                        0
Number of Server Sessions:                        0
```