This article provides examples of SSL termination (front-end SSL; ACE acting as a server), SSL initiation (back-end SSL; ACE acting as a client), and end-to-end SSL configurations. For details about configuring SSL on the ACE, see the *Cisco Application Control Engine Module SSL Configuration Guide*.

To return to the main article, click here.

Contents

- 1 Example of an SSL Termination Configuration
- 2 Example of an SSL Initiation Configuration
- 3 Examples of End-to-End SSL Configurations
  - 3.1 Example of an End-to-End SSL Example that Combines the Termination and Initiation Examples
  - 3.2 Simplified End-to-End SSL Configuration Example

Example of an SSL Termination Configuration

The following example illustrates a running configuration 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. The SSL termination-specific configuration elements appear in bold in the example.

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

probe https GEN-HTTPS
  port 80
  interval 50
  faildetect 5
  expect status 200 200

rserver SERVER1
  ip address 172.27.16.11
    inservice
rserver SERVER2
  ip address 172.27.16.12
    inservice
rserver SERVER3
  ip address 172.27.16.13
    inservice
rserver SERVER4
  ip address 172.27.16.14
    inservice

serverfarm host SFARM1
  description SERVER FARM 1 FOR SSL TERMINATION
  probe GEN-HTTPS
  rserver SERVER1 80
    inservice
  rserver SERVER2 80
    inservice

serverfarm host SFARM2
  description SERVER FARM 2 FOR SSL TERMINATION
  probe GEN-HTTPS
  rserver SERVER3 80
    inservice
```

```
  rserver SERVER4 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 illustrates a running configuration 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. The SSL initiation-specific configuration elements appear in bold in the example.

```
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 172.27.16.11
    inservice
rserver SERVER2
  ip address 172.27.16.12
    inservice
rserver SERVER3
  ip address 172.27.16.13
    inservice
rserver SERVER4
  ip address 172.27.16.14
    inservice

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

serverfarm host SFARM2
  description SERVER FARM 2 FOR SSL INITIATION
  probe GEN_HTTP
  rserver SERVER3 443
    inservice
  rserver SERVER4 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
```

Examples of End-to-End SSL Configurations

This section provides two SSl end-to-end configuration examples. The first example combines the previous SSL termination example and the SSL initiation example. The second example is a simplified approach to end-to-end SSL that you can modify to suit your own needs.

Example of an End-to-End SSL Example that Combines the Termination and Initiation Examples

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 ACL1 line 10 extended permit ip any any

probe https GEN-HTTPS
  port 80
  interval 50
  faildetect 5
  expect status 200 200

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

rserver SERVER1
  ip address 172.27.16.11
    inservice
rserver SERVER2
  ip address 172.27.16.12
    inservice
rserver SERVER3
  ip address 172.27.16.13
    inservice
rserver SERVER4
  ip address 172.27.16.14
    inservice

serverfarm host SFARM1
  description SERVER FARM 1 FOR SSL TERMINATION
  probe GEN-HTTPS
  rserver SERVER1 80
    inservice
  rserver SERVER2 80
    inservice
serverfarm host SFARM2
  description SERVER FARM 2 FOR SSL INITIATION
  probe GEN_HTTP
  rserver SERVER3 443
    inservice
  rserver SERVER4 443
    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

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

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

ssl-proxy service SSL_PSERVICE_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-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_CLASS1
    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_CLASS1
    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-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_CLASS2
    serverfarm SFARM2
    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_CLASS2
```

```
    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-TERM_CLASS
    loadbalance vip inserviceloadbalance policy L7_SSL-TERM_POLICY
    loadbalance vip icmp-reply
    ssl-proxy server SSL_PSERVICE_SERVER
    connection advanced-options TCP_PARAM
  class L4_SSL-INIT_CLASS
    loadbalance vip inserviceloadbalance policy L7_SSL-INIT_POLICY
    loadbalance vip icmp-reply active
    appl-parameter http advanced-options PARAMMAP_HTTP

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
```

Simplified End-to-End SSL Configuration 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
```