# Módulo de ACE de la configuración para la terminación SSL del End to End

## Contenido



## Introducción

Este documento provee una configuración de ejemplo del Application Control Module (ACE) para la terminación de la Secure Socket Layer (SSL) de extremo a extremo. Esta configuración mantiene el tráfico cifrado del cliente al servidor y proporciona la capacidad de utilizar los Cookie para la Persistencia de sesión así como de tomar capa 7 decisiones del Equilibrio de carga (L7).

Este documento no cubre cómo crear o los Certificados y las claves de importación. Refiera a la guía de configuración de SSL del módulo del motor del control de la aplicación, manejo de los Certificados y de las claves para más información.

Esta muestra utiliza dos contextos:

- El contexto Admin se utiliza para la administración remota y la configuración tolerante del incidente (pie).
- El c1 del contexto se utiliza para el Equilibrio de carga.

## prerrequisitos

### Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Ambos módulos de ACE necesitan tener los Certificados y claves.

- Los servidores equilibrados carga necesitan ser configurados para validar las conexiones SSL.

## Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

## Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

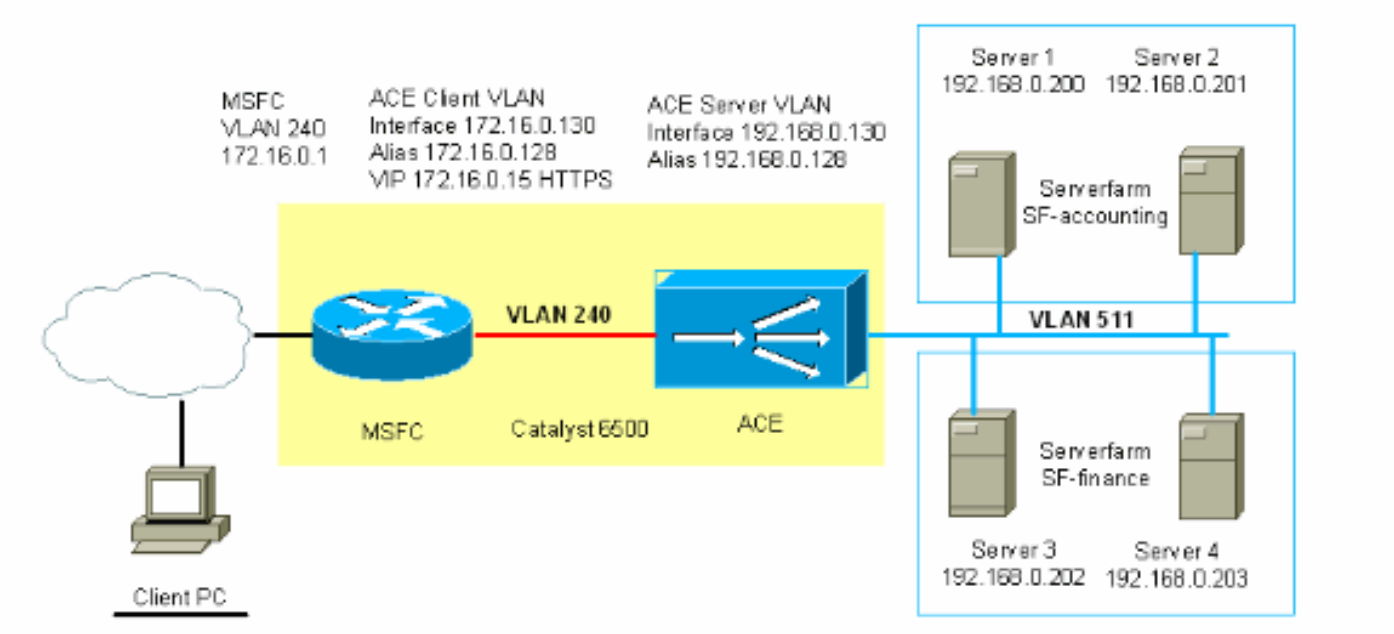
# Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Note**: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:




## Configuraciones

En este documento, se utilizan estas configuraciones:

- Catalyst 6500 — ACE ranura el contexto del c1 2
- Catalyst 6500 — ACE ranura el contexto 2 Admin
- Catalyst 6500 — Config MSFC

**Contexto del c1 de ACE**

```
switch/C1# show run
Generating configuration....



crypto chaingroup Chaingroup1
  cert inter.pem


!--- Add intermediate certificates to the chaingroup.
crypto csr-params CSR_1 country US state MA locality
Boxborough organization-name Cisco organization-unit LAB
common-name www.cisco.com serial-number 67893 email
admin@cisco.com !--- Certificate Signing Request (CSR)
used to generate !--- a request for a certificate from a
certificate Authority (CA). access-list any line 8
extended permit icmp any any access-list any line 16
extended permit ip any any !--- Access-list to permit or
deny traffic entering the ACE. probe http WEB_SERVERS
interval 5 passdetect interval 10 passdetect count 2
request method get url /index.html expect status 200 200
!--- Probe to test the availability of the load balanced
servers. parameter-map type http http_parameter_map
persistence-rebalance !--- Parameter-map used in order
to configure advanced http behavior. !--- Persistence-
rebalance inspects every get and matches to specific
content. !--- Without this command, only the first get
in a tcp session is inspected. rserver redirect HTTP-to-
HTTPS webhost-redirection https://%h%p 301 inservice !--
- Rserver to redirect HTTP client traffic to HTTPS. This
sends a HTTPS !--- redirect to the client and maintains
the domain and url that is requested. rserver host S1 ip
address 192.168.0.200 inservice rserver host S2 ip
address 192.168.0.201 inservice rserver host S3 ip
address 192.168.0.202 inservice rserver host S4 ip
address 192.168.0.203 inservice ssl-proxy service CISCO-
SSL-PROXY key rsakey.pem cert slot2-2tier.pem chaingroup
Chaingroup1 !--- ssl-proxy service used for SSL
termination. ssl-proxy service CLIENT-SSL-PROXY !---
ssl-proxy service used for SSL initiation to the load
balanced servers. !--- For basic SSL initiation, no
parameters are needed in the proxy-service. serverfarm
redirect REDIRECT-Serverfarm rserver HTTP-to-HTTPS
inservice !--- Serverfarm to redirect http connections
to https. serverfarm host SF-1 probe WEB_SERVERS rserver
S1 443 inservice rserver S2 443 inservice rserver S3 443
inservice rserver S4 443 inservice !--- Default
serverfarm used when content does not match !--- one of
the L7 class-maps. serverfarm host SF-accounting rserver
S1 443 inservice rserver S2 443 inservice !---
Serverfarm used when content matches /finance/*
serverfarm host SF-finance rserver S3 443 inservice
rserver S4 443 inservice !--- Serverfarm used when
```

```
content matches /accounting/* sticky http-cookie ACE-
COOKIE COOKIE-STICKY cookie insert browser-expire
serverfarm SF-1 sticky http-cookie ACE-FINANCE COOKIE-
FINANCE cookie insert browser-expire serverfarm SF-
finance sticky http-cookie ACE-ACCOUNTING COOKIE-
ACCOUNTING cookie insert browser-expire serverfarm SF-
accounting !--- Define the serverfarm and sticky method
used in the sticky group. class-map match-all L4-CLASS-
HTTPS 2 match virtual-address 172.16.0.15 tcp eq https
class-map match-all L4-CLASS-REDIRECT 2 match virtual-
address 172.16.0.15 tcp eq www !--- Layer 4 (L4) class-
map define virtual IP address and port. class-map type
http loadbalance match-all L7CLASS-accounting 2 match
http url /accounting/* class-map type http loadbalance
match-all L7CLASS-finance 2 match http url /finance/* !-
-- Layer 7 class-map that defines specific content on
which to parse. class-map type management match-any
REMOTE_ACCESS 2 match protocol ssh any 3 match protocol
telnet any 4 match protocol icmp any 5 match protocol
snmp any 6 match protocol http any !--- Remote
management class-map that defines what protocols can
manage the ACE. policy-map type management first-match
REMOTE_MGMT_ALLOW_POLICY class REMOTE_ACCESS permit
policy-map type loadbalance http first-match HTTPS-
POLICY class L7CLASS-accounting sticky-serverfarm
COOKIE-ACCOUNTING ssl-proxy client CLIENT-SSL-PROXY
class L7CLASS-finance sticky-serverfarm COOKIE-FINANCE
ssl-proxy client CLIENT-SSL-PROXY class class-default
sticky-serverfarm COOKIE-STICKY ssl-proxy client CLIENT-
SSL-PROXY policy-map type loadbalance http first-match
REDIRECT-POLICY class class-default serverfarm REDIRECT-
Serverfarm !--- Layer 7 policy-map that specifies
serverfarms for different layer 7 content. !--- class-
default is used if the traffic does not match any of the
layer 7 !--- class-maps. policy-map multi-match VIPs
class L4-CLASS-HTTPS loadbalance vip inservice
loadbalance policy HTTPS-POLICY loadbalance vip icmp-
reply loadbalance vip advertise active appl-parameter
http advanced-options http_parameter_map ssl-proxy
server CISCO-SSL-PROXY class L4-CLASS-REDIRECT
loadbalance vip inservice loadbalance policy REDIRECT-
POLICY loadbalance vip icmp-reply active !--- Multi-
match policy ties the class-maps and policy-maps
together. !--- Add the parameter-map with the command
appl-parameter. interface vlan 240 ip address
172.16.0.130 255.255.255.0 alias 172.16.0.128
255.255.255.0 peer ip address 172.16.0.131 255.255.255.0
access-group input any service-policy input
REMOTE_MGMT_ALLOW_POLICY service-policy input VIPs no
shutdown !--- Client side VLAN. This is the VLAN clients
enter the ACE. !--- Apply access-lists and policies that
are needed on this interface. interface vlan 511 ip
address 192.168.0.130 255.255.255.0 alias 192.168.0.128
255.255.255.0 peer ip address 192.168.0.131
255.255.255.0 no shutdown !--- Server side VLAN. !---
Alias is used for the servers default gateway. ip route
0.0.0.0 0.0.0.0 172.16.0.1 !--- Default gateway points
to the MSFC.
```

## Contexto de ACE Admin

```
switch/Admin#show running-config
Generating configuration....
```

```
boot system image:c6ace-t1k9-mz.A2_1_0a.bin

resource-class RC1
  limit-resource all minimum 50.00 maximum equal-to-min


!--- Resource-class used to limit the amount of
resources a !--- specific context can use. access-list
any line 8 extended permit icmp any any access-list any
line 16 extended permit ip any any rserver host test
class-map type management match-any REMOTE_ACCESS 2
match protocol ssh any 3 match protocol telnet any 4
match protocol icmp any 5 match protocol snmp any 6
match protocol http any policy-map type management
first-match REMOTE_MGMT_ALLOW_POLICY class REMOTE_ACCESS
permit interface vlan 240 ip address 172.16.0.4
255.255.255.0 alias 172.16.0.10 255.255.255.0 peer ip
address 172.16.0.5 255.255.255.0 access-group input any
service-policy input REMOTE_MGMT_ALLOW_POLICY no
shutdown interface vlan 511 ip address 192.168.0.4
255.255.255.0 alias 192.168.0.10 255.255.255.0 peer ip
address 192.168.0.5 255.255.255.0 access-group input any
no shutdown ft interface vlan 550 ip address 192.168.1.4
255.255.255.0 peer ip address 192.168.1.5 255.255.255.0
no shutdown !--- VLAN used for fault tolerant traffic.
ft peer 1 heartbeat interval 300 heartbeat count 10 ft-
interface vlan 550 !--- FT peer definition that defines
heartbeat parameters !--- and associates the ft VLAN. ft
group 1 peer 1 peer priority 90 associate-context Admin
inservice !--- FT group used for Admin context. ip route
0.0.0.0 0.0.0.0 172.16.0.1 context C1 allocate-interface
vlan 240 allocate-interface vlan 511 member RC1 !---
Allocate vlans the context C1 is used. ft group 2 peer 1
no preempt associate-context C1 inservice !--- FT group
used for the load balancing context C1. username admin
password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/ role Admin
domai n default-domain username www password 5
$1$UZIiwUk7$QMVYN1JASaycabrHkhGcS/ role Admin domain
default-domain switch/Admin#
```

## Configuración del router

```
switch/Admin#show running-config
Generating configuration....



boot system image:c6ace-t1k9-mz.A2_1_0a.bin

resource-class RC1
  limit-resource all minimum 50.00 maximum equal-to-min


!--- Resource-class used to limit the amount of
resources a !--- specific context can use. access-list
any line 8 extended permit icmp any any access-list any
line 16 extended permit ip any any rserver host test
class-map type management match-any REMOTE_ACCESS 2
match protocol ssh any 3 match protocol telnet any 4
match protocol icmp any 5 match protocol snmp any 6
```

```
match protocol http any policy-map type management
first-match REMOTE_MGMT_ALLOW_POLICY class REMOTE_ACCESS
permit interface vlan 240 ip address 172.16.0.4
255.255.255.0 alias 172.16.0.10 255.255.255.0 peer ip
address 172.16.0.5 255.255.255.0 access-group input any
service-policy input REMOTE_MGMT_ALLOW_POLICY no
shutdown interface vlan 511 ip address 192.168.0.4
255.255.255.0 alias 192.168.0.10 255.255.255.0 peer ip
address 192.168.0.5 255.255.255.0 access-group input any
no shutdown ft interface vlan 550 ip address 192.168.1.4
255.255.255.0 peer ip address 192.168.1.5 255.255.255.0
no shutdown !--- VLAN used for fault tolerant traffic.
ft peer 1 heartbeat interval 300 heartbeat count 10 ft-
interface vlan 550 !--- FT peer definition that defines
heartbeat parameters !--- and associates the ft VLAN. ft
group 1 peer 1 peer priority 90 associate-context Admin
inservice !--- FT group used for Admin context. ip route
0.0.0.0 0.0.0.0 172.16.0.1 context C1 allocate-interface
vlan 240 allocate-interface vlan 511 member RC1 !---
Allocate vlans the context C1 is used. ft group 2 peer 1
no preempt associate-context C1 inservice !--- FT group
used for the load balancing context C1. username admin
password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/ role Admin
domai n default-domain username www password 5
$1$UZIiwUk7$QMVYN1JASaycabrHkhGcS/ role Admin domain
default-domain switch/Admin#
```

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **Muestre los archivos crypto** — Certificados y claves de las visualizaciones salvados bajo contexto.Este ejemplo proporciona la salida de muestra:

```
switch/C1#show crypto files
Filename                                  File  File    Expor      Key/
                                          Size  Type    table      Cert
------------------------------------------------------------------------
inter.pem                                 1992  PEM     Yes        CERT
rsakey.pem                                891   PEM     Yes         KEY
slot2-1tier.pem                           1923  PEM     Yes        CERT
slot2-2tier.pem                           1762  PEM     Yes        CERT
```

- **Crypto verifique el certificado *dominante*** — Verifica que el certificado y la clave hagan juego.Este ejemplo proporciona la salida de muestra:

```
switch/C1#crypto verify rsakey.pem slot2-2tier.pem
Keypair in rsakey.pem matches certificate in slot2-2tier.pem.
```

- **Muestre el *nombre del* serverfarm** — Información de las visualizaciones sobre el serverfarm y el estado de los rservers.Este ejemplo proporciona la salida de muestra:

```
switch/C1#show serverfarm SF-accounting
 serverfarm     : SF-accounting, type: HOST
 total rservers : 2

 ---------------------------------
                                                ----------connections---------
--
       real                  weight state        current    total      failures
   ---+--------------------+------+-----------+----------+----------+-------
```

```
--
   rserver: S1
       192.168.0.200:443     8      OPERATIONAL  0          4          0
   rserver: S2
       192.168.0.201:443     8      OPERATIONAL  0          2          0
```

- **Muestre el detalle del nombre de la servicio-directiva** — Visualiza las estadísticas detalladas en la directiva de la multi-coincidencia, que incluye la información para cada directiva L7.Este ejemplo proporciona la salida de muestra:

```
switch/C1#show service-policy VIPs detail

Status     : ACTIVE
Description: -
----------------------------------------
Interface: vlan 240
  service-policy: VIPs
    class: L4-CLASS-HTTPS
      ssl-proxy server: CISCO-SSL-PROXY
     VIP Address:    Protocol:  Port:
     172.16.0.15     tcp        eq    443
      loadbalance:
        L7 loadbalance policy: HTTPS-POLICY
        VIP Route Metric     : 77
        VIP Route Advertise  : ENABLED-WHEN-ACTIVE
        VIP ICMP Reply       : ENABLED
        VIP State: INSERVICE
        curr conns       : 1         , hit count        : 360
        dropped conns    : 0
        client pkt count : 5078      , client byte count: 682725
        server pkt count : 6512      , server byte count: 5967833
        conn-rate-limit      : 0         , drop-count : 0
        bandwidth-rate-limit : 0         , drop-count : 0
        L7 Loadbalance policy : HTTPS-POLICY
          class/match : L7CLASS-accounting
            ssl-proxy client : CLIENT-SSL-PROXY
            LB action :
               sticky group: COOKIE-ACCOUNTING
                  primary serverfarm: SF-accounting
                    state: UP
                  backup serverfarm : -
            hit count        : 5
            dropped conns    : 0
          class/match : L7CLASS-finance
            ssl-proxy client : CLIENT-SSL-PROXY
            LB action :
               sticky group: COOKIE-FINANCE
                  primary serverfarm: SF-finance
                    state: UP
                  backup serverfarm : -
            hit count        : 7
            dropped conns    : 0
          class/match : class-default
            ssl-proxy client : CLIENT-SSL-PROXY
            LB action :
               sticky group: COOKIE-STICKY
                  primary serverfarm: SF-1
                    state: UP
                  backup serverfarm : -
            hit count        : 515
            dropped conns    : 1
        Parameter-map(s):
          http_parameter_map
    class: L4-CLASS-REDIRECT
     VIP Address:    Protocol:  Port:
```

```
        172.16.0.15     tcp        eq    80
         loadbalance:
           L7 loadbalance policy: REDIRECT-POLICY
           VIP Route Metric     : 77
           VIP Route Advertise  : DISABLED
           VIP ICMP Reply       : ENABLED-WHEN-ACTIVE
           VIP State: INSERVICE
           curr conns       : 0         , hit count        : 1
           dropped conns    : 0
           client pkt count : 5         , client byte count: 584
           server pkt count : 0         , server byte count: 0
           conn-rate-limit      : 0         , drop-count : 0
           bandwidth-rate-limit : 0         , drop-count : 0
           L7 Loadbalance policy : REDIRECT-POLICY
             class/match : class-default
               LB action :
                  primary serverfarm: REDIRECT-Serverfarm
                       state: UP
                   backup serverfarm : -
               hit count        : 1
               dropped conns    : 0
```

# Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

**El comando status del grupo pie de la demostración** produce esta salida.

```
switch/C1#show service-policy VIPs detail

Status     : ACTIVE
Description: -
---------------------------------------
Interface: vlan 240
  service-policy: VIPs
    class: L4-CLASS-HTTPS
      ssl-proxy server: CISCO-SSL-PROXY
     VIP Address:    Protocol:  Port:
     172.16.0.15     tcp        eq    443
      loadbalance:
        L7 loadbalance policy: HTTPS-POLICY
        VIP Route Metric     : 77
        VIP Route Advertise  : ENABLED-WHEN-ACTIVE
        VIP ICMP Reply       : ENABLED
        VIP State: INSERVICE
        curr conns       : 1         , hit count        : 360
        dropped conns    : 0
        client pkt count : 5078      , client byte count: 682725
        server pkt count : 6512      , server byte count: 5967833
        conn-rate-limit      : 0         , drop-count : 0
        bandwidth-rate-limit : 0         , drop-count : 0
        L7 Loadbalance policy : HTTPS-POLICY
          class/match : L7CLASS-accounting
            ssl-proxy client : CLIENT-SSL-PROXY
            LB action :
               sticky group: COOKIE-ACCOUNTING
                  primary serverfarm: SF-accounting
                    state: UP
                  backup serverfarm : -
```

```
          hit count        : 5
          dropped conns    : 0
        class/match : L7CLASS-finance
          ssl-proxy client : CLIENT-SSL-PROXY
          LB action :
             sticky group: COOKIE-FINANCE
                primary serverfarm: SF-finance
                  state: UP
                backup serverfarm : -
          hit count        : 7
          dropped conns    : 0
        class/match : class-default
          ssl-proxy client : CLIENT-SSL-PROXY
          LB action :
             sticky group: COOKIE-STICKY
                primary serverfarm: SF-1
                  state: UP
                backup serverfarm : -
          hit count        : 515
          dropped conns    : 1
      Parameter-map(s):
        http_parameter_map
  class: L4-CLASS-REDIRECT
   VIP Address:    Protocol:  Port:
   172.16.0.15     tcp        eq    80
    loadbalance:
      L7 loadbalance policy: REDIRECT-POLICY
      VIP Route Metric     : 77
      VIP Route Advertise  : DISABLED
      VIP ICMP Reply       : ENABLED-WHEN-ACTIVE
      VIP State: INSERVICE
      curr conns       : 0         , hit count        : 1
      dropped conns    : 0
      client pkt count : 5         , client byte count: 584
      server pkt count : 0         , server byte count: 0
      conn-rate-limit      : 0         , drop-count : 0
      bandwidth-rate-limit : 0         , drop-count : 0
      L7 Loadbalance policy : REDIRECT-POLICY
        class/match : class-default
          LB action :
             primary serverfarm: REDIRECT-Serverfarm
                  state: UP
              backup serverfarm : -
          hit count        : 1
          dropped conns    : 0
```

ACE no sincroniza los Certificados y los pares claves SSL que están presentes en el contexto activo con el contexto espera de un grupo pie. Si el ACE realiza la sincronización de la configuración y no encuentra los Certificados y las claves necesarios en el contexto espera, los config sincronizan fallan y el contexto espera ingresa el estado STANDBY_COLD.

Para corregir este problema, verifique si todos los Certificados y claves están instalados en ambos módulos de ACE.

## Procedimiento deTroubleshooting (opcional)

Complete las instrucciones en esta sección para resolver problemas su configuración. Refiera a configurar los módulos redundantes de ACE para más información sobre el troubleshooting.

Si el módulo en espera está en el estado FSM_FT_STATE_STANDBY_COLD, complete estos pasos:

- **Muestre los archivos crypto** — Verifique que ambos módulos de ACE tengan los mismos Certificados y claves.
- **Muestre a se muestra el estado del grupo pie el** estatus de cada par en el grupo pie.

1. Verifique que ambos módulos de ACE tengan los mismos Certificados y claves para cada contexto.
2. Importe los Certificados ausentes y las claves a ACE espera
3. Dé vuelta apagado auto-sincronizan en el usuario que el contexto en el modo de configuración con el **ningún pie auto-sincroniza el comando running-config**.
4. Dé vuelta encendido auto-sincronizan en el usuario que el contexto en el modo de configuración con el **pie auto-sincroniza el comando running-config**.
5. Verifique el estado pie con el **comando status del grupo pie de la demostración**.
6. Salve las configuraciones con el **comando copy running-config startup-config**.

## Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems