

Configuración ACE con la terminación SSL y la reescritura URL

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Procedimiento de Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una configuración de ejemplo para configurar el módulo de control de la aplicación (ACE) para la terminación SSL (Secure Socket Layer) y la reescritura de URL. ACE utilizará la inserción de cookies para mantener la persistencia de sesión. Los clientes que golpean el VIP en el texto claro recibirán un HTTPS reorientan enviado de ACE.

Este documento no cubre crear o las importaciones de certificado y las claves. Para más información, 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](#).

Esta muestra utiliza dos contextos:

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

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- la URL-reescritura se soporta en la versión c6ace-t1k9-mz.A2_1.bin o más adelante

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- El Catalyst 6500 con WS-SUP720-3B éste ejecuta 12.2(18)SXF7
- Módulo de control de la aplicación image:c6ace-t1k9-mz.A2_1_0a.bin

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 Cisco](#) para obtener más información sobre las convenciones del documento.

Configurar

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

Nota: 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
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 for generating 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 from 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 is used to detect the health of the
load balanced servers. action-list type modify http
urlrewrite ssl url rewrite location "www\.cisco\.com" !-
-- Servers are accepting traffic on port 80. When the
server sends a redirect !--- it is not always sent back
to the client as https://. ACE will rewrite the !---
location field when it sees http://www.cisco.com and
will change it to !--- https://www.cisco.com before
encrypting it back to the client. 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 slot2-1tier.pem !--- Add
the certificates and key needed for SSL termination.
serverfarm host SF-1 probe WEB_SERVERS rserver S1 80
inservice rserver S2 80 inservice rserver S3 80
inservice rserver S4 80 inservice sticky http-cookie
ACE-COOKIE COOKIE-STICKY cookie insert browser-expire
serverfarm SF-1 !--- Sticky group used to maintain
client session persistency. !--- ACE will insert a
cookie on the server response. class-map match-all L4-
CLASS-HTTPS 2 match virtual-address 172.16.0.15 tcp eq
https !--- Layer 4 class-map defining the ip and port
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
defining what proto cols 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 class-default
sticky-serverfarm COOKIE-STICKY action urlrewrite !---
Apply the sticky group serverfarm, and url rewrite under
the layer 7 policy-map. policy-map multi-match VIPs
class L4-CLASS-HTTPS loadbalance vip inservice
loadbalance policy HTTPS-POLICY loadbalance vip icmp-
reply loadbalance vip advertise active ssl-proxy server
CISCO-SSL-PROXY !--- Multi-match policy ties the class-
maps and policy-maps together. 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
will 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. switch/C1#

```

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 defining
heartbeat parameters and to associate 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 will use. 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 domain default-domain username www password 5
$1$UZIiwUk7$QMvYN1JASaycabrHkhGcS/ role Admin domain
default-domain switch/Admin#

```

Config del router

```

!--- Only portions of the config relevant to the ACE are
displayed. sf-cat1-7606#show run Building
configuration... !--- Output Omitted. svclc multiple-
vlan-interfaces svclc module 2 vlan-group 2 svclc vlan-
group 2 220,240,250,510,511,520,540,550 !--- Before the
ACE can receive traffic from the supervisor engine in
the Catalyst 6500 !--- or Cisco 6600 series router, you
must create VLAN groups on the supervisor engine, !---
and then assign the groups to the ACE. !--- Add vlans to
the vlan-group that are needed for ALL contexts on the
ACE. interface Vlan240 description public-vip-172.16.0.x
ip address 172.16.0.2 255.255.255.0 standby ip
172.16.0.1 standby priority 20 standby name ACE_slot2 !-
-- SVI (Switch Virtual Interface). The standby address
is the default gateway for the ACE. !--- Output Omitted.
sf-cat1-7606#

```

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 el nombre del serverfarm** — Información de las visualizaciones sobre el serverfarm y el estado de cada rserver. Este ejemplo proporciona una salida de muestra: `switch/C1#show serverfarm SF-1`

```

serverfarm SF-1 serverfarm : SF-1, type: HOST total rservers : 4 -----
----- connections----- real weight state current total failures ---+-----
-----+-----+-----+-----+-----+-----+----- rserver: S1

```

```
192.168.0.200:80 8 OPERATIONAL 0 249 0 rserver: S2 192.168.0.201:80 8 OPERATIONAL 0 0 0
rserver: S3 192.168.0.202:80 8 OPERATIONAL 0 0 0 rserver: S4 192.168.0.203:80 8 OPERATIONAL
0 0 0 switch/C1#
```

- **muestre el nombre de la servicio-directiva** — Visualiza el estado de la servicio-directiva, y mostrará que se ha golpeado la cantidad de veces el VIP. Este ejemplo proporciona una salida de muestra:


```
switch/C1#show service-policy VIPs Status : ACTIVE -----
----- Interface: vlan 240 service-policy: VIPs class: L4-CLASS-HTTPS ssl-proxy
server: CISCO-SSL-PROXY 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 : 260 dropped conns : 0 client pkt count : 2396 , client byte
count: 276190 server pkt count : 1384 , server byte count: 1231598 conn-rate-limit : 0 ,
drop-count : 0 bandwidth-rate-limit : 0 , drop-count : 0 switch/C1#
```
- **muestre el HTTP stats** — Visualiza las estadísticas HTTP que incluye analiza los errores de extensión, las encabezados insertadas, y las encabezados reescritas. Este ejemplo proporciona una salida de muestra:


```
switch/C1#show stats http +-----
-----+ +----- HTTP statistics -----+ +-----
-----+ LB parse result msgs sent : 198 , TCP data msgs sent : 241 Inspect parse result
msgs : 0 , SSL data msgs sent : 878 sent TCP fin/rst msgs sent : 198 , Bounced fin/rst msgs
sent: 4 SSL fin/rst msgs sent : 44 , Unproxy msgs sent : 0 Drain msgs sent : 0 , Particles
read : 607 Reuse msgs sent : 0 , HTTP requests : 202 Reproxied requests : 0 , Headers
removed : 0 Headers inserted : 192 , 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 : 5 , Header rewrite errors : 0 switch/C1#
!--- Headers rewritten: will increment when the url rewrite is used. !--- Headers inserted:
Will increment when the cookie is inserted.
```
- **muestre los archivos crypto** — Visualiza los Certificados y las claves salvados en ACE. Este ejemplo proporciona una salida de muestra:


```
switch/C1#show crypto files Filename File File
Expor Key/ Size Type table Cert -----
----- rsakey.pem 891 PEM Yes KEY slot2-1tier.pem 1923 PEM Yes CERT switch/C1#
```
- **crypto verifique el certificado dominante** — Confirma que el certificado y la clave hacen juego. Este ejemplo proporciona una salida de muestra:


```
switch/C1#crypto verify rsakey.pem
slot2-1tier.pem Keypair in rsakey.pem matches certificate in slot2-1tier.pem. switch/C1#
```

[Troubleshooting](#)

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

Cuando está publicado, el **comando status del grupo pie de la demostración** da esta salida:

```
switch/C1#show ft group status FT Group : 2 Configured Status : in-service Maintenance mode :
MAINT_MODE_OFF My State : FSM_FT_STATE_STANDBY_COLD Peer State : FSM_FT_STATE_ACTIVE Peer Id : 1
No. of Contexts : 1 switch/C1#
```

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 certs y claves están instalados en ambos módulos de ACE.

[Procedimiento de Troubleshooting](#)

Sigue estas instrucciones de resolver problemas su configuración. Refiera a [sincronizar las configuraciones redundantes](#) 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** — Verifica que ambos módulos de ACE tengan los mismos Certificados y claves.
 - **muestre a se muestra el estados del grupo pie el estatus de cada par en el grupo pie.**
1. Verifique que ambos módulos de ACE tengan los mismos certs y claves para cada contexto.
 2. Importe los certs y las claves que falta a ACE espera.
 3. Dé vuelta apagado auto-sincronizan en el contexto del usuario en el modo de configuración que **ningunos pies auto-sincronizan los ejecutar-config.**
 4. Dé vuelta encendido auto-sincronizan en el contexto del usuario en el modo de configuración que los **pies auto-sincronizan los ejecutar-config.**
 5. Verifique el estado pie con el **comando status del grupo pie de la demostración.**

[Información Relacionada](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)