Configurar o ACE com terminação SSL e reescrita URL

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenções](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configurações](#)
[Verificar](#)
[Troubleshooting](#)
[Procedimento de Troubleshooting](#)
[Informações Relacionadas](#)

Introdução

Este documento fornece uma configuração de exemplo do Application Control Module (ACE) para terminação Secure Socket Layer (SSL) e reescrita de URL. O ACE usará a inserção do cookie para manter a persistência da sessão. Os clientes que batem o VIP no texto claro receberão um HTTPS reorientam enviado do ACE.

Este documento não cobre a criação ou os certificados de importação e as chaves. Para mais informação, refira o guia de configuração de SSL do módulo de Engine do controle de aplicativo, controlando Certificados e chaves.

Esta amostra usa dois contextos:

- o contexto Admin é usado para o Gerenciamento remoto e a configuração tolerante da falha (FT)
- o segundo contexto, C1, é usado para o Balanceamento de carga

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- a URL-reescrita é apoiada a versão em c6ace-t1k9-mz.A2_1.bin ou em mais tarde

- Ambos os módulos ACE precisarão de ter Certificados e chaves.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalyst 6500 com WS-SUP720-3B que executa 12.2(18)SXF7
- Módulo de controle de aplicativo image:c6ace-t1k9-mz.A2_1_0a.bin

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

Este documento utiliza as seguintes configurações:

- Catalyst 6500 — Contexto C1 do entalhe 2 ACE
- Catalyst 6500 — Contexto Admin do entalhe 2 ACE
- Catalyst 6500 — Configuração MSFC

Contexto ACE C1

```
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 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 domai n default-domain username www password 5
$1$UZIiwUk7$QMVYN1JASaycabrHkhGcS/ role Admin domain
default-domain switch/Admin#
```

Configuração do roteador

```
!--- 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#
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre o nome do serverfarm** — Informação dos indicadores sobre o serverfarm e o estado de cada rserver.Este exemplo fornece um exemplo de saída:`switch/C1#show 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#
```

- **mostre o nome da serviço-política** — Indica o estado da serviço-política, e mostrá-lo-á que o número de vezes o VIP esteve batido.Este exemplo fornece um exemplo de saída:`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#`
- **mostre o HTTP stats** — Indica estatísticas HTTP que inclui analisa gramaticalmente erros de comprimento, encabeçamentos introduzidos, e encabeçamentos reescritos.Este exemplo fornece um exemplo de saída:`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.`
- **mostre arquivos criptos** — Indica os Certificados e as chaves armazenados no ACE.Este exemplo fornece um exemplo de saída:`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#`
- **cripto verifique o** *certificado chave* — Confirma que o fósforo do certificado e o chave.Este exemplo fornece um exemplo de saída:`switch/C1#crypto verify rsakey.pem slot2-1tier.pem Keypair in rsakey.pem matches certificate in slot2-1tier.pem. switch/C1#`

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Quando emitido, o **comando status do grupo ft da mostra** dá esta saída:

```
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#
```

O ACE não sincroniza os Certificados e os pares de chaves SSL que estam presente no contexto ativo com o contexto à espera de um grupo FT. Se o ACE executa a sincronização de configuração e não encontra os Certificados e as chaves necessários no contexto à espera, a sincronização da configuração falha e o contexto à espera incorpora o estado STANDBY_COLD. A fim corrigir este problema, verifique se todos os certs e chaves são instalados em ambos os módulos ACE.

Procedimento de Troubleshooting

Siga estas instruções para resolver problemas da sua configuração. Refira a sincronização de configurações redundantes para obter mais informações sobre do Troubleshooting.

Se o módulo em standby está no estado FSM_FT_STATE_STANDBY_COLD, termine estas etapas:

- **mostre arquivos criptos** — Verifica que ambos os módulos ACE têm os mesmos Certificados e chaves.
- **mostre a exibições de status do grupo ft o** estado de cada par no grupo ft.

1. Verifique que ambos os módulos ACE têm os mesmos certs e chaves para cada contexto.
2. Importe certs e chaves faltantes ao ACE à espera.
3. Desligue a auto-sincronização no contexto do usuário no modo de configuração **nenhuma executar-configuração auto-sincronização ft**.
4. Gire sobre a auto-sincronização no contexto do usuário na executar-**configuração auto-sincronização ft do** modo de configuração.
5. Verifique o estado FT com o **comando status do grupo ft da mostra**.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems