使用 SSL 终端和 URL 重写配置 ACE

目录

简介

本文档为配置应用控制模块 (ACE) 的安全套接字层 (SSL) 终端和 URL 重写提供了一个配置范例。ACE 将使用 Cookie 插入来维护会话的持续性。以明文抵达 VIP 的客户端会收到一个发送自 ACE 的 HTTPS 重定向。

本文档并未包含创建或导入证书和密钥的内容。有关详细信息，请参阅应用控制引擎模块 SSL 配置指南，管理证书和密钥。

此范例使用两上下文：

- 管理上下文用于远程管理和容错 (FT) 配置
- 第二个上下文 C1 用于负载均衡

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 版本c6ace-t1k9-mz.A2_1.bin或以上支持URL重写
- 这两个 ACE 模块需要具有证书和密钥。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 带有运行 12.2(18)SXF7 的 WS-SUP720-3B 的 Catalyst 6500
- 应用程序控制模块image:c6ace-t1k9-mz.A2_1_0a.bin

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- Catalyst 6500 — ACE 插槽 2 C1 上下文
- Catalyst 6500 — ACE 插槽 2 管理上下文
- Catalyst 6500 — MSFC 配置

ACE C1 上下文

```
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#
```

ACE 管理上下文

```
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#
```

路由器配置

```
!--- 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#
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show serverfarm name** — 显示有关服务器群和每个 rserver 的状态的信息。以下示例提供了一个输出范例：`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#`
- **show service-policy name** — 显示服务器策略的状态，并显示已经到达 VIP 的次数。以下示例提供了一个输出范例：`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#`
- **show stats http** — 显示 http 统计信息，其中包括解析长度错误、插入的报头和重写的报头。以下示例提供了一个输出范例：`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.
```

- **show crypto files** — 显示 ACE 上存储的证书和密钥。以下示例提供了一个输出范例

```
：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 verify 密钥证书** — 确认证书和密钥匹配。以下示例提供了一个输出范例

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

故障排除

本部分提供的信息可用于对配置进行故障排除。

发出 **show ft group status** 命令后，将获得以下输出：

```
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 不会将活动上下文中的 SSL 证书和密钥与 FT 组的备用上下文进行同步。如果 ACE 执行配置同步但未在备用上下文中找到所需的证书和密钥，则配置同步将失败，同时备用上下文将进入 STANDBY_COLD 状态。为更正此问题，请验证两个 ACE 模块上是否都安装了所有证书和密钥。

故障排除步骤

请按照以下说明排除配置故障。有关故障排除的详细信息，请参阅同步冗余配置。

如果备用模块的状态为 FSM_FT_STATE_STANDBY_COLD，请完成以下步骤：

- **show crypto files** — 验证两个 ACE 模块是否具有相同的证书和密钥。
- **show ft group status** — 显示 FT 组中每个对等体的状态。

1. 验证每个上下文中两个 ACE 模块是否具有相同的证书和密钥。
2. 将缺失的证书和密钥导入备用 ACE。
3. 在配置模式下使用 **no ft auto-sync running-config** 关闭用户上下文中的自动同步。
4. 在配置模式下使用 **ft auto-sync running-config** 打开用户上下文中的自动同步。
5. 使用 **show ft group status** 命令验证 FT 状态。

相关信息

- 技术支持和文档 - Cisco Systems