为端到端 SSL 终端配置 ACE 模块

目录

简介

本文档为应用控制模块 (ACE) 的端到端安全套接字层 (SSL) 终端提供了一个配置范例。此配置将加密从客户端到服务器的流量并提供为会话持续性使用 Cookie 和进行第 7 层 (L7) 负载均衡决策的功能。

本文档并未包含有关如何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。
- 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：

- 这两个 ACE 模块需要具有证书和密钥。
- 负载均衡服务器需要配置为接受 SSL 连接。

使用的组件

本文档不限于特定的软件和硬件版本。

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 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.
```

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 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#
```

路由器配置

```
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#
```

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 crypto files** — 显示存储在上下文中的证书和密钥。此示例提供输出示例：：

```
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 verify 密钥 证书 — 验证**证书和密钥是否匹配。此示例提供输出示例：：

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

- **Show serverfarm 名称** — 显示有关服务器群和 rserver 的状态的信息。此示例提供输出示例：：

```
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
```

- **Show service-policy name detail** — 显示多匹配策略的详细统计信息，其中包括每个 L7 策略的信息。此示例提供输出示例：：

```
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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

show ft group status 命令可生成以下输出。

```
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 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 模块上是否安装了所有证书和密钥。

故障排除过程（可选）

请按照以下说明排除配置故障。有关故障排除的详细信息，请参阅配置冗余 ACE 模块。

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** 命令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** 命令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。
6. 使用 **copy running-config startup-config** 命令保存配置。

相关信息

- 技术支持和文档 - Cisco Systems