Configurar o módulo ACE para a terminação SSL do End to End

Índice

Introdução

Este documento fornece uma configuração de exemplo do Application Control Module (ACE) para a terminação fim-a-fim do Secure Socket Layer (SSL). Esta configuração mantém o tráfego cifrado do cliente ao server e fornece a capacidade para usar Cookie para a Persistência de sessão assim como para fazer decisões do Balanceamento de carga da camada 7 (L7).

Este documento não cobre como criar ou certificados de importação e chaves. Refira o guia de configuração de SSL do módulo de Engine do controle de aplicativo, controlando Certificados e chaves para mais informação.

Esta amostra usa dois contextos:

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

Pré-requisitos

Requisitos

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

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

- Os server equilibrados carga precisam de ser configurados para aceitar conexões SSL.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Note: 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 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 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#
```

Configuração do roteador

```
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#
```

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 arquivos criptos** — Certificados e chaves dos indicadores armazenados sob um contexto.Este exemplo fornece o exemplo de saída:

```
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
```

- **Cripto verifique o certificado *chave*** — Verifica que o fósforo do certificado e o chave.Este exemplo fornece o exemplo de saída:

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

- **Mostre o *nome do* serverfarm** — Informação dos indicadores sobre o serverfarm e o estado dos rservers.Este exemplo fornece o exemplo de saída:

```
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
```

- **Mostre o detalhe do nome da serviço-política** — Indica estatísticas detalhadas na política do multi-fósforo, que inclui a informação para cada política L7.Este exemplo fornece o exemplo de saída:

```
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

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

O comando status do grupo ft da mostra produz esta saída.

```
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
```

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 Certificados e chaves são instalados em ambos os módulos ACE.

Procedimento de Troubleshooting (opcional)

Termine as instruções nesta seção a fim pesquisar defeitos sua configuração. Refira configurar os módulos redundantes ACE 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** — Verifique que ambos os módulos ACE têm os mesmos Certificados e chaves.
- **Mostre a exibição de status do grupo ft o** estado de cada par no grupo FT.

1. Verifique que ambos os módulos ACE têm os mesmos Certificados e chaves para cada contexto.
2. Importe Certificados ausentes e chaves ao ACE à espera
3. Desligue a auto-sincronização no contexto do usuário no modo de configuração com **nenhum comando running-config auto-sincronização ft**.
4. Gire sobre a auto-sincronização no contexto do usuário no modo de configuração com o **comando running-config auto-sincronização ft**.
5. Verifique o estado FT com o **comando status do grupo ft da mostra**.
6. Salvar as configurações com o **comando copy running-config startup-config**.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems