Configurer un module ACE pour la terminaison SSL de bout en bout

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour la module de commande d'application (ACE) pour de bout en bout l'arrêt de Protocole SSL (Secure Socket Layer). Cette configuration maintient le trafic chiffré du client au serveur et fournit la capacité d'utiliser des Témoins pour la Persistance de session aussi bien que de prendre à couche 7 décisions de l'Équilibrage de charge (L7).

Ce document ne couvre pas comment créer ou Certificats et clés d'importation. Référez-vous au guide de configuration SSL de module d'engine de contrôle d'application, en gérant des Certificats et introduisez le pour en savoir plus.

Cet échantillon utilise deux contextes :

- Le contexte d'admin est utilisé pour la gestion à distance et la configuration (pi) insensible aux défaillances.
- Le contexte C1 est utilisé pour l'Équilibrage de charge.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Les deux modules d'ACE doivent avoir des Certificats et des clés.
- Des serveurs équilibrés par chargement doivent être configurés pour recevoir des connexions SSL.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Note: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise les configurations suivantes :

- Catalyst 6500 — ACE rainent le contexte 2 C1
- Catalyst 6500 — ACE rainent le contexte de l'admin 2
- Catalyst 6500 — Config MSFC

Contexte d'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.
```

Contexte d'admin d'ACE

```
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#
```

Configuration du routeur

```
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#
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **Affichez les cryptos fichiers** — Certificats et clés d'affichages enregistrés sous un contexte.Voici un exemple de résultat :

```
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 vérifiez le certificat *principal*** — Vérifie que la correspondance de certificat et principale.Voici un exemple de résultat :

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

- **Affichez le *nom de* serverfarm** — Affiche des informations au sujet du serverfarm et l'état des rservers.Voici un exemple de résultat :

```
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
```

- **Détail de nom de show service-policy** — Affiche des statistiques détaillées sur la stratégie de multi-correspondance, qui inclut les informations pour chaque stratégie L7.Voici un exemple de résultat :

```
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
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

La commande d'**état de show ft group** produit cette sortie.

```
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 ne synchronise pas les Certificats et les paires de clés SSL qui sont présents dans le contexte actif avec le contexte de réserve d'un ft group. Si ACE exécute la synchronisation de configuration et ne trouve pas les Certificats et les clés nécessaires dans le contexte de réserve, le sync de config échoue et le contexte de réserve entre dans l'état STANDBY_COLD.

Afin de corriger ce problème, vérifiez si tous les Certificats et clés sont installés sur les deux modules d'ACE.

Procédure de dépannage (facultative)

Terminez-vous les instructions dans cette section afin de dépanner votre configuration. Référez-vous à configurer les modules redondants d'ACE pour plus d'informations sur le dépannage.

Si le module de réserve est dans l'état FSM_FT_STATE_STANDBY_COLD, terminez-vous ces étapes :

- **Affichez les cryptos fichiers** — Vérifiez que les deux modules d'ACE ont les mêmes Certificats et clés.
- **État de show ft group** — Affichez l'état de chaque pair dans le ft group.

1. Vérifiez que les deux modules d'ACE ont les mêmes Certificats et clés pour chaque contexte.
2. Importez les Certificats absents et les clés à ACE de réserve
3. Arrêtez l'auto-sync dans le contexte d'utilisateur dans le mode de configuration avec l'**aucune** commande de **running-config de ft auto-sync**.
4. Activez l'auto-sync dans le contexte d'utilisateur dans le mode de configuration avec la commande de **running-config de ft auto-sync**.
5. Vérifiez l'état pi avec la commande d'**état de show ft group**.
6. Sauvegardez les configurations avec la commande de **copy running-config startup-config**.

Informations connexes

- Support et documentation techniques - Cisco Systems