Configurer ACE avec terminaison SSL et réécriture des URL

Contenu

Introduction

Ce document propose un exemple de configuration pour configurer le module de contrôle des applications (ACE) pour la terminaison et la réécriture de l'URL selon le protocole Secure Socket Layer (SSL). Le module ACE emploiera des témoins pour maintenir la persistance de session. Les clients qui frappent le VIP en texte clair recevront un HTTPS réorientent envoyé d'ACE.

Ce document ne couvre pas créer ou importer des Certificats et des clés. Le pour en savoir plus, se rapportent au guide de configuration SSL de module d'engine de contrôle d'application, gérant des Certificats et des clés.

Cet échantillon utilise deux contextes :

- le contexte d'admin est utilisé pour la gestion à distance et la configuration (pi) insensible aux défaillances
- le deuxième 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 :

- L'url rewrite est pris en charge sur la version c6ace-t1k9-mz.A2_1.bin ou plus tard

- Les deux modules d'ACE devront avoir des Certificats et des clés.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Catalyst 6500 avec WS-SUP720-3B qui exécute 12.2(18)SXF7
- Module de commande d'application image:c6ace-t1k9-mz.A2_1_0a.bin

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.

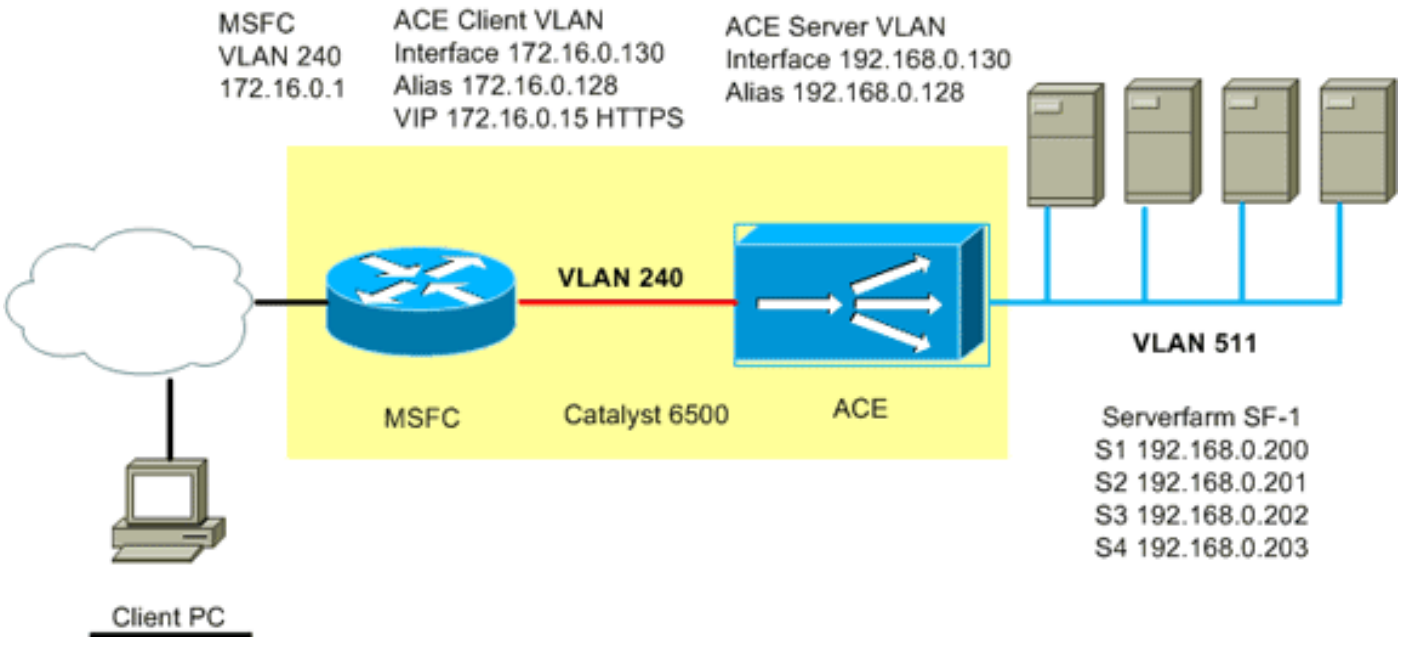
Configurez

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

Remarque: 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
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#
```

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 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#
```

Configuration du routeur

```
!--- 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#
```

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 le nom de serverfarm** — Affiche des informations au sujet du serverfarm et l'état de chaque rserver.Cet exemple fournit un résultat témoin :`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#`
- **nom de show service-policy** — Affiche l'état de la service-stratégie, et affichera que le nombre de fois où le VIP a été frappé.Cet exemple fournit un résultat témoin :`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#`
- **HTTP de show stats** — Affiche les statistiques de HTTP qui incluent analysent des erreurs, des en-têtes insérées, et des en-têtes de longueur réécrites.Cet exemple fournit un résultat témoin :`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.`*
- **affichez les cryptos fichiers** — Affiche les Certificats et les clés enregistrés sur ACE.Cet exemple fournit un résultat témoin :`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 vérifiez le** *certificat principal* — Confirme que la correspondance de certificat et principale.Cet exemple fournit un résultat témoin :`switch/C1#`**`crypto verify rsakey.pem slot2-1tier.pem`** `Keypair in rsakey.pem matches certificate in slot2-1tier.pem. switch/C1#`

Dépannez

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

Une fois émise, la commande d'**état de show ft group** donne cette sortie :

```
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 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 CERT et clés sont installés sur les deux modules d'ACE.

Procédure de dépannage

Suivez ces instructions pour dépanner votre configuration. Référez-vous à synchroniser des configurations redondantes 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** — Vérifie que les deux modules d'ACE ont les mêmes Certificats et clés.
- **état de show ft group** — Affiche l'état de chaque pair dans le ft group.

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

Informations connexes

- Support et documentation techniques - Cisco Systems