SSL ターミネーションおよび URL リライトを含めた ACE の設定

目次

概要
前提条件
要件
使用するコンポーネント
表記法
設定
ネットワーク図
設定
確認
トラブルシューティング
トラブルシューティング手順
関連情報

概要

このドキュメントでは、Secure Socket Layer（SSL）ターミネーションおよび URL リライト用に Application Control Module（ACE）を設定する設定例を示します。 ACE では、cookie insert を使用してセッションの持続性を維持します。 クリア テキストで VIP にアクセスするクライアントは、ACE から送信された HTTPS リダイレクトを受信します。

このドキュメントでは、証明書および鍵の作成およびインポートを扱いません。 詳細については、『Application Control Engine モジュール SSL コンフィギュレーション ガイド』の「証明書および鍵の管理」を参照してください。

この例では、次の 2 つのコンテキストを使用します。

- 管理コンテキストは、リモート管理およびフォールト トレラント（FT）設定に使用されます。
- もう 1 つのコンテキスト C1 は、ロード バランシングに使用されます。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- URL リライトは、バージョン c6ace-t1k9-mz.A2_1.bin 以降でサポートされています。

- 両方の ACE モジュールで証明書と鍵が必要になります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- 12.2(18)SXF7 を実行する WS-SUP720-3B を搭載した Catalyst 6500
- Application Control Module イメージ：c6ace-t1k9-mz.A2_1_0a.bin

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

設定

このドキュメントでは、次の設定を使用します。

- Catalyst 6500：ACE スロット 2 C1 コンテキスト
- Catalyst 6500：ACE スロット 2 管理コンテキスト
- Catalyst 6500：MSFC 構成

ACE C1 コンテキスト

```
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 管理コンテキスト

```
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#
```

ルータの設定

```
!--- 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#
```

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show serverfarm name**：serverfarm および各 rserver の状態に関する情報が表示されます。次の例に、出力例を示します。`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**：サービス ポリシーの状態および VIP へのアクセス回数が表示さ

れます。次の例に、出力例を示します。`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**：解析長エラー、挿入ヘッダー数、書き換えヘッダー数を含む HTTP 統計が表示されます。次の例に、出力例を示します。`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**：ACE 上に格納されている証明書および鍵を表示します。次の例に、出力例を示します。`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 key certificate**：証明書および鍵が一致していることを確認します。次の例に、出力例を示します。`switch/C1#crypto verify rsakey.pem slot2-1tier.pem Keypair in rsakey.pem matches certificate in slot2-1tier.pem. switch/C1#`

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

show ft group status コマンドを発行すると、次の出力が得られます。

```
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 で、アクティブ コンテキスト内に存在する SSL 証明書および鍵ペアと、FT グループのスタンバイ コンテキストが同期されることはありません。 ACE で設定同期が実行され、スタンバイ コンテキストで必要な証明書と鍵が見つからなかった場合は、config sync が失敗して、スタンバイ コンテキストが STANDBY_COLD ステートに移行します。 この問題を修正するためには、すべての証明書および鍵が両方の ACE モジュールにインストールされていることを確認します。

トラブルシューティング手順

設定をトラブルシューティングするには、次の手順を実行します。 トラブルシューティングの詳細については、「冗長構成の同期」を参照してください。

スタンバイ側のモジュールが FSM_FT_STATE_STANDBY_COLD 状態の場合は、次の手順を実行します。

- **show crypto files**：両方の ACE モジュールに同じ証明書および鍵が格納されていることを確認します。

- **show ft group status**：ft グループ内の各ピアのステータスを表示します。

1. 各コンテキストについて、両方の ACE モジュールに同じ証明書および鍵が格納されていることを確認します。
2. 欠落している証明書および鍵をスタンバイ側の ACE にインポートします。
3. コンフィギュレーション モードでユーザ コンテキスト内の自動同期をオフにします（**no ft auto-sync running-config**）。
4. コンフィギュレーション モードでユーザ コンテキスト内の自動同期をオンにします（**ft auto-sync running-config**）。
5. **show ft group status** コマンドを使用して、FT 状態を確認します。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems