エンドツーエンドの SSL 終了の ACE モジュールの設定

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（オプション）](#)
[関連情報](#)

概要

このドキュメントでは、エンドツーエンドの Secure Socket Layer（SSL）ターミネーション用の Application Control Module（ACE）の設定例を紹介します。 この設定では、クライアントからサーバへの暗号化されたトラフィックを保持し、セッション永続化のために Cookie を使用する機能はもちろん、レイヤ 7（L7）ロード バランシングの判断を行うための機能を提供します。

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方法については説明していません。 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）設定で使用されます。
- 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。

- 両方の ACE モジュールには証明書と鍵が必要です。

- ロード バランシングされたサーバは、SSL 接続を受け入れるように設定する必要があります。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

本書の情報は、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、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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 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 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#
```

ルータの設定

```
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#
```

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 crypto files**：コンテキストの下に格納されている証明書および鍵を表示します。出力例を以下に示します。

```
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 key certificate**：証明書および鍵が一致していることを確認します。出力例を以下に示します。

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

- **Show serverfarm name**：serverfarm および rserver の状態に関する情報が表示されます。出力例を以下に示します。

```
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**：各 L7 ポリシーの情報を含む、マルチマッチ ポリシーに関する詳細な統計情報を表示します。出力例を以下に示します。

```
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
```

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 コマンドでは、次の出力が生成されます。

```
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 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（オプション）

設定に関するトラブルシューティングを実行するには、ここに記載されている手順を完了してください。 トラブルシューティングの詳細については、『冗長 ACE モジュールの設定』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** コマンドを使用）。
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** コマンドを使用）。
5. **show ft group status** コマンドを使用して、FT 状態を確認します。
6. **copy running-config startup-config** コマンドを使用して設定を保存します。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems