

Configure ACE with SSL Termination and URL Rewrite

Document ID: 107402

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Procedure

Related Information

Introduction

This document provides a sample configuration to configure the Application Control Module (ACE) for Secure Socket Layer (SSL) termination and URL-rewrite. The ACE will use cookie insert to maintain session persistence. Clients that hit the VIP in clear text will receive an HTTPS redirect sent from the ACE.

This document does not cover creating or importing certificates and keys. For more information, refer to Application Control Engine Module SSL Configuration Guide, Managing Certificates and Keys.

This sample uses two contexts:

- the Admin context is used for remote management and Fault Tolerant (FT) configuration
- the second context, C1, is used for load balancing

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- URL-rewrite is supported on version c6ace-t1k9-mz.A2_1.bin or later
- Both ACE modules will need to have certificates and keys.

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 6500 with WS-SUP720-3B that runs 12.2(18)SXF7
- Application Control Module image:c6ace-t1k9-mz.A2_1_0a.bin

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure

that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

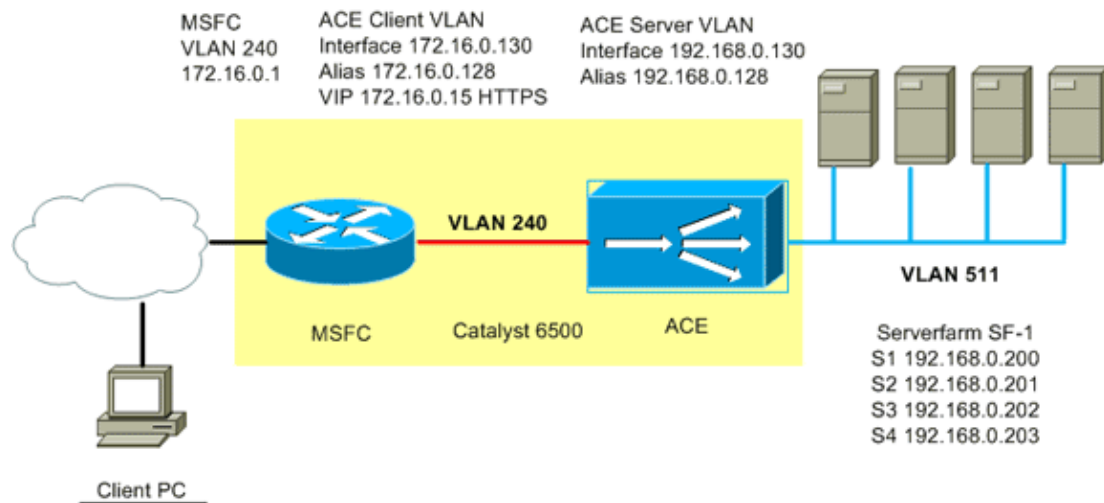
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- Catalyst 6500 ACE slot 2 C1 context
- Catalyst 6500 ACE slot 2 Admin context
- Catalyst 6500 MSFC config

ACE C1 context

```
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-ltier.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 Admin context

```

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 domain default-domain
username www password 5 $1$UZIiwUk7$QMvYN1JASaycabrHkhGcS/ role Admin domain default-domain

switch/Admin#

```

Router config

```

!--- 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#

```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show serverfarm name** Displays information about the serverfarm and the state of each rserver.

This example provides a sample output:

```
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** Displays the state of the service-policy, and will show the number of times the VIP has been hit.

This example provides a sample output:

```
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** Displays http statistics which includes parse length errors, headers inserted, and headers rewritten.

This example provides a sample output:

```
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** Displays the certificates and keys stored on the ACE.

This example provides a sample output:

```

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** Confirms that the certificate and key match.

This example provides a sample output:

```

switch/C1#crypto verify rsakey.pem slot2-1tier.pem
Keypair in rsakey.pem matches certificate in slot2-1tier.pem.
switch/C1#

```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

When issued, the **show ft group status** command gives this output:

```

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#

```

The ACE does not synchronize the SSL certificates and key pairs that are present in the active context with the standby context of an FT group. If the ACE performs configuration synchronization and does not find the necessary certificates and keys in the standby context, config sync fails and the standby context enters the STANDBY_COLD state. In order to correct this problem, verify if all certs and keys are installed on both ACE modules.

Troubleshooting Procedure

Follow these instructions to troubleshoot your configuration. Refer to Synchronizing Redundant Configurations for more information on troubleshooting.

If the standby module is in the state `FSM_FT_STATE_STANDBY_COLD`, complete these steps:

- **show crypto files** Verifies that both ACE modules have the same certificates and keys.
 - **show ft group status** Displays the status of each peer in the ft group.
1. Verify that both ACE modules have the same certs and keys for each context.
 2. Import missing certs and keys to the standby ACE.
 3. Turn off auto-sync in the user context in configuration mode **no ft auto-sync running-config**.
 4. Turn on auto-sync in the user context in configuration mode **ft auto-sync running-config**.
 5. Verify FT state with the **show ft group status** command.

Related Information

- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 09, 2008

Document ID: 107402
