

Configure ACE Module for End to End SSL Termination

Document ID: 107401

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Procedure (Optional)

Related Information

Introduction

This document provides a sample configuration for the Application Control Module (ACE) for end to end Secure Socket Layer (SSL) termination. This configuration keeps traffic encrypted from client to server and provides the ability to use cookies for session persistence as well as make Layer 7 (L7) load balancing decisions.

This document does not cover how to create or import certificates and keys. Refer to Application Control Engine Module SSL Configuration Guide, Managing Certificates and Keys for more information.

This sample uses two contexts:

- The Admin context is used for remote management and Fault Tolerant (FT) configuration
- The context C1 is used for load balancing.

Prerequisites

Requirements

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

- Both ACE modules need to have certificates and keys.
- Load balanced servers need to be configured to accept SSL connections.

Components Used

This document is not restricted to specific software and hardware versions.

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 the Cisco Technical Tips Conventions for more information on document conventions.

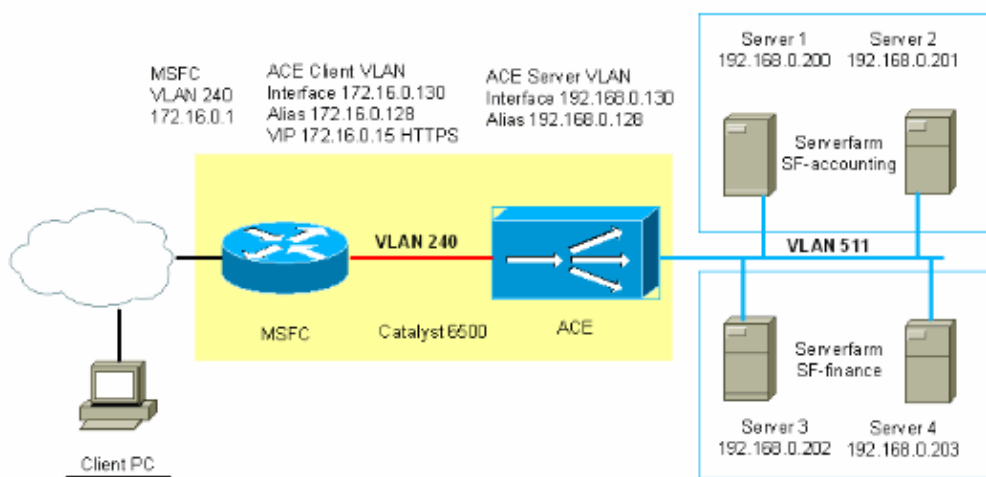
Configure

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



```

        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

```

Troubleshoot

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

The **show ft group status** command produces 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 certificates and keys are installed on both ACE modules.

Troubleshooting Procedure (Optional)

Complete the instructions in this section in order to troubleshoot your configuration. Refer to Configuring Redundant ACE Modules for more information on troubleshooting.

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

- **Show crypto files** Verify that both ACE modules have the same certificates and keys.
 - **Show ft group status** Display the status of each peer in the FT group.
1. Verify that both ACE modules have the same certificates and keys for each context.
 2. Import absent certificates and keys to the standby ACE
 3. Turn off auto-sync in the user context in configuration mode with the **no ft auto-sync running-config** command.
 4. Turn on auto-sync in the user context in configuration mode with the **ft auto-sync running-config** command.
 5. Verify FT state with the **show ft group status** command.
 6. Save the configurations with the **copy running-config startup-config** 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 14, 2008

Document ID: 107401
